Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Cobertura 5G para la integración de las radios tácticas SDR

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Luis Rojo Pinilla

DIRECTOR Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Cobertura 5G para la integración de las radios tácticas SDR

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de Telecomunicación

Universidade Vigo

RESUMEN

El trabajo es un proyecto a corto plazo, que propone la posibilidad integrar los futuros sistemas de telecomunicaciones tácticas en concreto a las Radio Definidas por Software (SDR), mediante la utilización la Tecnología 5G.

Esto proporcionaría a las unidades tácticas las ventajas del 5G (mayores anchos de banda, menores latencias, eficacia de los sistemas de mando y control, etc.), mediante las SDR,s, con capacidad de integración en la "Nube hibrida", todo esto siguiendo las leyes, Reglamento y Directivas marcadas por el Gobierno, el Ministerio de Defensa (MINISDEF).

Se presenta un estudio para la creación de una red de telecomunicaciones propia "Non-Public Network", la necesidad de implementar la Nube, diferenciándola de la "Nube de Combate", Integración en la Infraestructura Integral de la Informacion de la Defensa I3D, posibilidad para que sea acreditable hasta la clasificación de Difusión Limitada (LD), siguiendo las Guías STIC actualizadas del Centro Criptológico Nacional (CCN) y la Planificación y viabilidad del proyecto.

PALABRAS CLAVE

Tecnología 5G, Radios definidas por Software, Nube (Cloud), Nube de Combate, Seguridad.

AGRADECIMIENTOS

Agradezco y dedico este Trabajo Fin de Master a mi familia y en especial a mi mujer Rosa, por el apoyo, paciencia que ha tenido soportando toda las cargas familiares durante el desarrollo de este Master.

También quiero hacer mención para agradecer el apoyo que me han proporcionada mis mandos y compañeros durante estos meses.

Y sin olvidar a los profesores del CUD y compañeros del MASTER, por los conocimientos adquiridos con su ayuda.

CONTENIDO

Contenido 1

Índice de Figuras 3

Índice de Tablas 5

1 Introducción y objetivos 6

1.1 Introducción. 6

1.2 Objetivos 6

2 Estado del arte 8

2.1 DOCUMENTACION DE REFERENCIA DEL MINISDEF. PARA LA IMPLANTACION DE LA TECNOLOGÍA 5G 8

2.1.1 Resolución 307/08136/21, de 17 de mayo de 2021, del Secretario de Estado de Defensa, por la que se establece la Estrategia de Explotación de la Nube en el Ministerio. [1] 8

2.1.2 Resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa. Tipografía. [2] 9

2.1.3 Plan Nacional 5G. Secretaria de Estado para la Sociedad de la Información y la Agenda Digital. [3] 12

2.2 INTRODUCCIÓN A LAS RADIOS TÁCTICAS SDR. (SOFTWARE DEFINED RADIO). [4] 15

2.2.1 Definición y Objetivos de los SDR,s. 15

2.2.2 Evolución de los Sistemas en la Red táctica de Combate. 15

2.2.3 Estandarización y Arquitectura de Red 18

2.2.4 Forma de Onda ESSOR HDRWF. [5] 20

2.2.5 Soberanía en las Comunicaciones. 21

i. Forma de onda 21

ii. Plataforma 21

iii. Seguridad 21

iv. Portabilidad. 22

v. Estandarización. 22

2.3 CONSTITUCIÓN DE GRUPOS DE TRABAJO PERMANENTES PARA LA IMPLANTACIÓN Y EMPLEO DE LA TECNOLOGÍA 5G Y DE LAS COMUNICACIONES DE RADIOS TÁCTICAS SDR EN EL MINISTERIO DE DEFENSA. 22

2.3.1 Grupo de Trabajo Permanente para la Implantación y Empleo de la tecnología 5G. 22

2.3.2 Grupo de Trabajo de las comunicaciones de radios Tácticas. SDR. 23

2.3.1 Redimensionamiento y priorización del Sistema Conjunto de Radio Táctica (SCRT-SDR). 25

2.1 NECESIDAD DE INTEGRACIÓN EN SISTEMAS DE GESTIÓN DE COMUNICACIONES EN LAS PEQUEÑAS UNIDADES DEL EJÉRCITO DE TIERRA. 25

2.2 INTRODUCCIÓN A LA TECNOLOGÍA 5G. 27
2.2.1 Características de la arquitectura 5G. 27
2.2.1 La importancia en Defensa de adquirir un 5G Core (5GC) en propiedad. 29
2.2.2 Núcleo de acceso múltiple: Núcleo 5G de modo dual. 31
2.3 INICIATIVAS PARA IMPLEMENTAR LA TECNOLOGÍA 5G EN OTAN Y PROYECTOS 5G MINISDEF- EJÉRCITO DE TIERRA. 32
2.3.1 Iniciativas OTAN. [5] 32
2.3.1 Proyecto 5G del Ministerio de Defensa – Ejército de Tierra. [6]. 33
3 Proyecto de integración. 38
3.1 Descripción de la solución para sistemas de Mando y Control. [7] 39
3.2 Necesidad de diseño de una red definida por Software (SDN). [8] 45
3.3 Desarrollo de una arquitectura de seguridad para el acceso en la nube [9]. 49
3.3.1 Resposibilidad de seguridad “de” y “en”. 51
4 Desarrollo del TFM 62
4.1 Viabilidad del Proyecto. Gestión del Proceso de Negocio. Business Process Management . 62
4.1.1 Introducción BPM. 62
4.1.1 Planificación del Proyecto. 63
5 Conclusiones y líneas futuras 71
5.1 Descripción del apartado ..... **¡Error! Marcador no definido.**
5.1.1 Adquisición de las SDR,s. 71
5.1.2 Adquisición de equipos con tecnología 5G. 71
5.1.3 Implantación de Redes Definidas por Software. SDN. 72
5.1.4 Capacidad de acreditación de la red, hasta Difusión Limitada. 72
5.1.5 Viabilidad del proyecto. 72
6 Bibliografía 79
Anexo I: Proyecto para la integración de la cobertura 5G en las SDR,s 81
Anexo II: Planificacion del proyecto 82

ÍNDICE DE FIGURAS

Figura 1 Resolución 307/08135/21. Taxonomía de Servicios CIS/TIC del MDEF establecida en la AG CIS/TIC....10

Figura 2 Resolución 307/08135/21. Esquema de componentes de las Redes 5G, elementos habilitadores y funcionalidades. 12

Figura 3 Aspectos regulatorios Plan Nacional 5G. [3]....13

Figura 4 Ejes del Plan Nacional 5G. Plan Nacional 5G 2018-2020. [3] 14

Figura 5 Bandas de Frecuencias Identificadas por la Unión Europea. Plan Nacional 5G 2018-2020 [3]....15

Figura 6 Conceptos básicos del sistema de aeronaves no tripuladas (UAS) - Missile Defense Advocacy Alliance....17

Figura 7 Fuente: ESSOR Architecture – Motivation and Overview (WInnF Technical Conference – December 2010)....19

Figura 8 . Conferencia SDR en OTAN II CSUP CIS ET 2021.Coronel de Transmisiones EM Ignacio Javier Simón Andújar 20

Figura 9 Dimensionamiento de necesidades de Equipos para el programa SCRT. Dato JTEW-MCCE....25

Figura 10. Logotipo de GESCOMET. RF Española. (GESCOMET - RFE)....26

Figura 11. Fase para la implementación 5G....29

Figura 12. Arquitectura 3GPP 5G. Ejemplo CORE de ERICSSON....30

Figura 13. Logotipo de NCIA. Agencia del NCI | Hogar (nato.int)....33

Figura 14. NCIA. Potencial de la Tecnología 5G para Aplicaciones Militares. 33

Figura 15 JCISAT. Ensayo Tecnología LTE (4G). 2016 ..... **¡Error! Marcador no definido.**

Figura 16 JCISAT. Despliegue LTE entre PC, s....36

Figura 17. JCISAT. LTE. Pruebas de Servicios no simultáneas....37

Figura 18 Casos de uso 5G. El 5G transforma tu vida conectando el Internet de las cosas. - ARTÍCULO - YTTEK Technology Corp 42

Figura 19 Espectro 5G. La solución de diseño 5G se adapta al mercado real. - ARTÍCULO - YTTEK Technology Corp 43

Figura 20. Empleo 5G en PC,s desplegables (Nivel Mando Componente o Nivel Operacional)....44

Figura 21 Empleo del 5G en PC,s desplegables (Nivel Brigada y Grupo Táctico). 44

Figura 22 Producto Basado en Software. STIC 140 [8]. 47

Figura 23. Tipos de Servicios en la Nube. AaaS, PaaS y IaaS. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iaas/ [8] 50

Figura 24. Modelo de Responsabilidad compartida en IaaS....51

Figura 25. Medidas de Seguridad en la IaaS Sin Clasificar. STIC 499 [9]. 59

Figura 26.Diagrama IaaS para manejar Información Sin Clasificar. STIC 499 [9]....59

Figura 27 Medidas de Seguridad en nube para Difusión Limitada. STIC 499....60

Figura 28. Diagrama de IaaS para manejar información de Difusión Limitada. STIC 499 [9].....61
Figura 29. Etapas del Ciclo PDCA.https:// public-library.safetyculture.io. 63
Figura 30. Estimación temporal del proyecto. 66
Figura 31. Equipos radio SDR por prioridades del 1º ciclo de adquisición.....67
Figura 33. Costes generales.....68

ÍNDICE DE TABLAS

Tabla 2-1. Arquitectura 3GPP 5G. Red 5G Core (5GC): llegar al núcleo de 5G - Ericsson.....30
Tabla 3-1 Medidas de Seguridad para la Arquitectura Iaas.....58
Tabla 3-2. Modelo de Despliegue. STIC 499. [10].....61

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción.

Este trabajo tiene como fin plantear soluciones para poder utilizar la tecnología 5G, referida como una nueva tecnología móvil que aumentará la velocidad de conexión, reducirá el tiempo mínimo de latencia, para que pueda integrase con los sistemas de radio tácticos definidos por software.

Para esto se hace referencia, a la Arquitectura de Referencia definida por el Ministerio de Defensa, así como la Estrategia de la utilización de la nube y de la utilización de la tecnología 5G, definida por el mismo Ministerio en el entorno operativo.

Cabe destacar que en este trabajo no se va a presentar una solución única, debido a que hay que tener en cuenta los distintos entornos operativos que se pueden encontrar nuestras unidades, ya que no es lo mismo su utilización en los distintos medios como Mar, Tierra o Aire, y en las circunstancias donde se desarrollan las operaciones, por ejemplo, diferente manera de desplegar los medios CIS en una operación convencional, en un combate hibrido, en Zona de Operaciones, desembarcos paracaidistas, operaciones en ambientes confinados, etc.

Al haber un número muy elevado de formas que se puede presentar un conflicto, voy a hacer solo hincapié en las posibles soluciones para entornos que se desarrollen en Tierra.

La importancia de la seguridad en las comunicaciones y en los sistemas de información será uno de los principales objetivos, donde se presentarán soluciones para los entornos antes descritos.

Para desarrollar un proyecto fiable y siguiendo las especificación que marca en Defensa y la OTAN para la implantación de la Tecnología 5G en los Sistemas de Telecomunicaciones e Información de las Fuerzas Armadas así como un apunte de las normativas y restricciones que se marca su uso así como se desarrollara un Business Process Management (BPM) en español Gestión de Procesos de Negocio, para realizar un estudio de la viabilidad del proyecto que se quiere desarrollar en este Trabajo Fin de Master.

Es importante tener en cuenta que este proyecto un planeamiento personal que puede coincidir con los proyectos que se estén desarrollando por los distintos Grupos de Trabajo de Defensa tanto del 5G como de las Radios Definidas por Software para este fin.

1.2 Objetivos

El objetivo principal de este trabajo es dar una solución fiable para la utilización de la cobertura 5G y que sea interoperable con los medios CIS Tácticos que se van a dotar a las unidades tácticas del ET en un futuro próximo y en las diferentes formas de combate que se puede enfrentar.

Se presentará un proyecto utilizando equipos COTS , empleando aplicaciones y elementos de securización que existan en el mercado y acreditados por el Centro Criptológico Nacional (CCN) organismo dependiente del Centro Nacional de Inteligencia, responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material Criptológico y formar al personal de la Administración especialista en este campo.

Otro objetivo es de reducir de manera considerable el coste económico, que implicaría no contratar a empresas tengan en propiedad el diseño exclusivo e impida la competencia.

Y por último implementar los requisitos de seguridad necesarios para que las comunicaciones sean fiables y siempre siguiendo la Arquitectura Objeto y de la Documentación de Referencia que marca en Ministerio de Defensa.

2 ESTADO DEL ARTE

2.1 DOCUMENTACION DE REFERENCIA DEL MINISDEF. PARA LA IMPLANTACION DE LA TECNOLOGÍA 5G

2.1.1 Resolución 307/08136/21, de 17 de mayo de 2021, del Secretario de Estado de Defensa, por la que se establece la Estrategia de Explotación de la Nube en el Ministerio. [1]

Tras la Resolución 307/08136/21, del Ministerio de Defensa (MINISDEF), se estable la Estrategia de Explotación de la Nube, y se define la Arquitectura Global CIS/TIC, ante la incorporación de nuevas tecnologías y la actualización de las infraestructuras del MINISDEF, asegurando la interoperabilidad con los sistemas externos-internos y la armonización técnica y operativa.

Uno de los objetivos específicos de su eje estratégico 5 «Transformación digital del Sector Público», es la actualización de las infraestructuras tecnológicas de las Administraciones Públicas, avanzando hacia un modelo de consolidación de Centros de Procesamiento de Datos (CPD), con un enfoque hacia una arquitectura de información que soporte la visión de los datos «como servicio» («as-a-Service») y que garantice la hiperconectividad de los servicios y datos.

En su capítulo IV apartado Vigesimotercero, se desarrolla la manera de implantación de la Estrategia de Explotación de la Nube para el ámbito Operativo, considerando que en el campo operativo no ha alcanzo la misma madurez que en el estratégico, por lo que es necesario en consonancia con las líneas de acción estratégica, de impulsa la investigación sobre la tecnología, en el marco de desarrollo e investigación del MINISDEF y de alinear los proyectos identificados con la Estrategia Industrial de Defensa y fortalecer las capacidades industriales y áreas de conocimiento de la Base Industrial y Tecnología de Defensa nacional cuando afecten a los intereses de la Defensa y Seguridad Nacional. Estos proyectos deben ser realizados de manera conjunta entre los ámbitos operativos del Departamento (EMAD, Ejércitos, Armada y UME) y el CESTIC. Para aquellas líneas de actuación en materia de I+D+i, esta definición será coordinada por la Dirección General de Armamento y Material (DGAM).

También se deben concretar en un plazo no superior a seis meses desde la aprobación y entrada en vigor de esta Estrategia y serán validados por el grupo de trabajo permanente para la implantación y empleo de la tecnología de nube del MINISDEF.

Para cada proyecto se identificarán y en este caso en particular “Cobertura 5G para la integración de las radios tácticas SDR” los siguientes puntos:

Necesidad operativa / funcional a la que se asocia.

Objetivos esperados y plazos previstos de inicio y consecución.

Dominio/s de aplicación, escenario/s de referencia y opción de despliegue y uso más adecuada.

Actores implicados y matriz de responsabilidades (RASCI)[1].

[1] Las siglas, en inglés, de su nombre corresponden a Responsible, Accountable, Support, Consulted and Informed.

Interdependencia con proyectos de desarrollo del PECIS[2] (o integración en ellos).

Interdependencia con proyectos y experiencias sobre servicios de nube de la OTAN.

Recursos implicados (humanos, materiales, financieros y formativos).

La definición y desarrollo de estos proyectos se adaptará, en todo caso, a la evolución en el contexto tecnológico y normativo que afecte al empleo de la tecnología de nube.

Al margen de estos proyectos, el MINISDEF podrá impulsar los proyectos que considere oportuno para adoptar la tecnología de nube fuera del ámbito operativo.

2.1.2 Resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa. [2]

Esta Estrategia tiene por finalidad:

- Proporcionar una visión general de la tecnología de nube, de su situación actual y prospección de futura.
- Establecer los **principios** que deben regir la implantación de la tecnología 5G en el Ministerio de Defensa.
- Determinar los **objetivos generales** que se persiguen con la implantación de la tecnología 5G en el Ministerio de Defensa.
- Definir las **líneas de actuación** para la consecución de los objetivos de la Estrategia. Su desarrollo se coordinará con los Planes de Acción de desarrollo del Plan Estratégico CIS del Ministerio (PECIS).
- Identificar las áreas de aplicación de **esta tecnología para el Ministerio de Defensa** y su alineación con las Capacidades Militares y otras capacidades del Departamento.
- Analizar las posibles áreas de aplicación actual y futura de esta tecnología para los cometidos del MINISDEF, con especial relevancia para las misiones de las FAS y sus implicaciones para las capacidades militares.
- En esta estrategia se definen por primera vez tres modelos de nube:

a. Nube Pública.

b. Nube privada.

c. Y nube híbrida.

Responsible, “R”, (responsable de la ejecución): es quien ejecuta una tarea. Su función es “HACER”. Lo más habitual es que exista sólo un encargado R por cada tarea.

Accountable, “A”, (responsable del proceso en conjunto): es quien vela porque la tarea se cumpla, aún sin tener que ejecutarla en persona. Su función es “HACER QUE SE HAGA”.

Support, “S”, (apoyo): Alguien que apoya un rol ejecutivo en un proceso, contribuyendo a la implementación de una tarea en un proceso. Bien podría ser un substituto. (Backup)

Consulted, “C”, (consultado): Persona que debe ser consultada para la realización de una tarea.

Informed, “I”, (Informado): Persona que debe ser informada de la realización de una tarea.

[2] Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS) MINISTERIO DE DEFENSA.

Así como las diferentes tipologías de servicios y evolución constante que proporciona la nube. (SaaS, IaaS y PaaS).

En cuanto a la aplicación de las capacidades CIS/TIC para el MINISDEF, aparecen descritas en el apartado 6 de la Arquitectura Global CIS/TIC y se organizan en cuatro áreas de capacidades: usuario, de infraestructura tecnológica, de seguridad de la información y de gestión.

Esta Capacidades CIS/TIC deben de dar soporte a las Capacidades Operativas y cumplir los objetivos y requisitos operativos identificados.

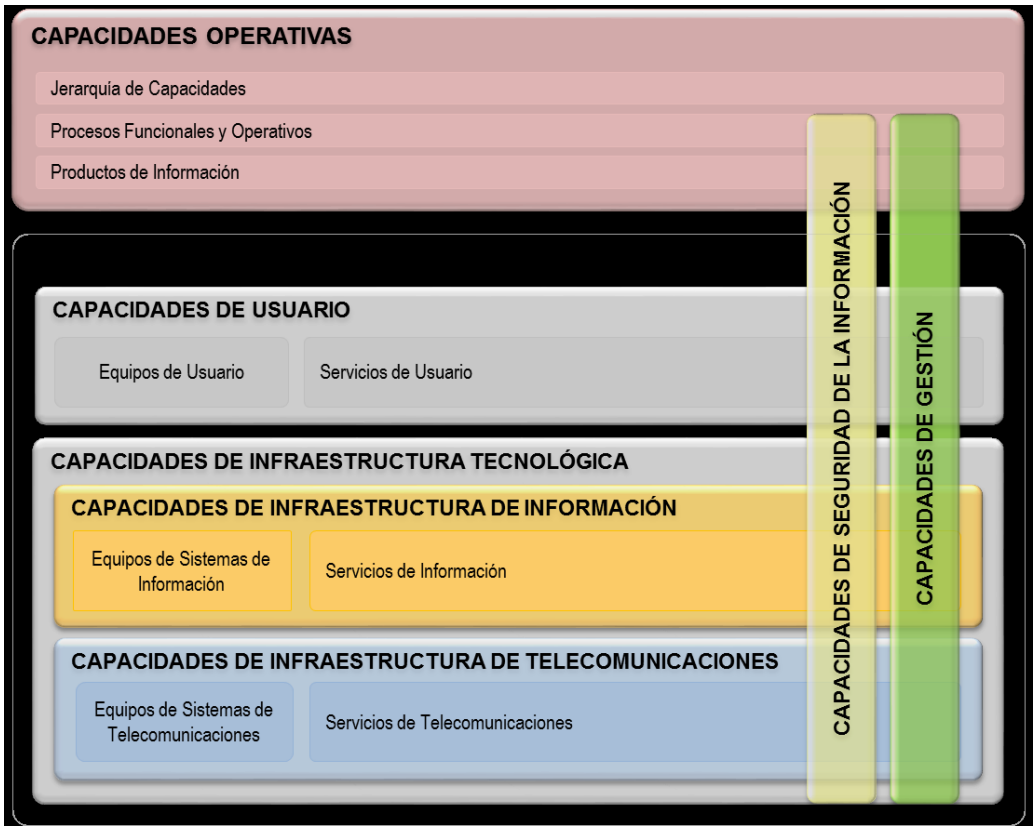


Figura 1 Resolución 307/08135/21. Taxonomía de Servicios CIS/TIC del MDEF establecida en la AG CIS/TIC. [2]

La aplicación de la tecnología 5G en el ámbito Operativo, es considerada por MINISDEF como un área de aplicación prioritaria. Al aumentar considerablemente la densidad de comunicaciones y ejercer como capacidad habilitadora y plataforma vertebradora e integradora de otras tecnologías emergentes y disruptivas, 5G proporciona capacidad analítica y predictiva avanzada y permite incrementar el conocimiento de la situación, agilizar, descentralizar y acortar los procesos de toma de decisiones y proporcionar superioridad de información, potenciando, en general todas las capacidades militares identificadas en el proceso de Planeamiento Militar y en particular, la C4ISTAR[15].

Las ventajas potenciales de la tecnología 5G para su uso en el ámbito militar son:

- La disponibilidad de capacidades de comunicaciones móviles, tanto para usuario en entorno permanentes como desplegables.

- El incremento de información disponible y de las capacidades de análisis en los entornos operativos. La integración del procesamiento distribuido de información proporcionada por sensores facilita la toma de decisiones descentralizadas y el desarrollo de sus misiones de un modo más eficiente y seguro.

- Un continuo y coordinado entendimiento del entorno operativo gracias a la recepción de información y la generación de inteligencia en tiempo real.

- El incremento de las capacidades de las fuerzas desplegadas gracias a la implementación de funcionalidades de movimiento y transporte autónomo, logística inteligente, formación inmersiva o telemedicina.
- Una reducción de los riesgos y vulnerabilidades del personal, frente a amenazas a través de la explotación y el procesamiento de un gran número de sensores y de la posibilidad de seguimiento de fuerzas propias (*FFT - Friendly Force Tracking*).
- La mejora de la interacción con Fuerzas y Cuerpos de Seguridad del Estado, Organizaciones y Fuerzas Aliadas y Organizaciones No Gubernamentales, durante operaciones.

Se definen las siguientes capacidades y funcionalidades de la tecnología 5G:

- **Comunicaciones móviles de banda ancha mejoradas** *(Enhanced mobile broadband–eMBB-)*, que permitirá velocidades iniciales de 1Gbps con descargas superiores a 200 Mbps.
- **Comunicaciones Ultrafiables y de baja latencia** *(Ultra-reliable and low latency communications –URLLC-)*, para el desarrollo de aplicaciones de misión crítica que requieren la obtención de datos en tiempo real necesarios para un conocimiento lo más detallado posible de todas las circunstancias que impactan sobre un escenario operativo (*situational awareness*) y para la rápida toma de decisiones.
- **Comunicaciones masivas entre dispositivos y máquinas** *(Massive machine type communications –mMTC-)*, que permitirá a dispositivos inteligentes, vehículos y equipamiento industrial estar permanentemente interconectados para satisfacer las necesidades del Internet de las Cosas.

La visión de dispositivos inteligentes, ciudades inteligentes o bases militares inteligentes, requiere que los objetos y dispositivos incorporen sensores e inteligencia para detectar y tomar decisiones sin intervención humana sobre tareas complejas hasta el nivel que se decida, de ejecución inmediata, basadas en flujos de trabajo complejos.

Las máquinas (dispositivos, objetos…) tendrán la capacidad de comunicarse en tiempo real con el resto de objetos que conforman el ecosistema tecnológico en proximidad, generando un entorno colaborativo para alcanzar los objetivos que se encomienden.

Para ello, la tecnología 5G se sustenta en cuatro elementos habilitadores: el espectro radioeléctrico, una nueva interfaz radio, una nueva red de acceso y la red de núcleo 5G.

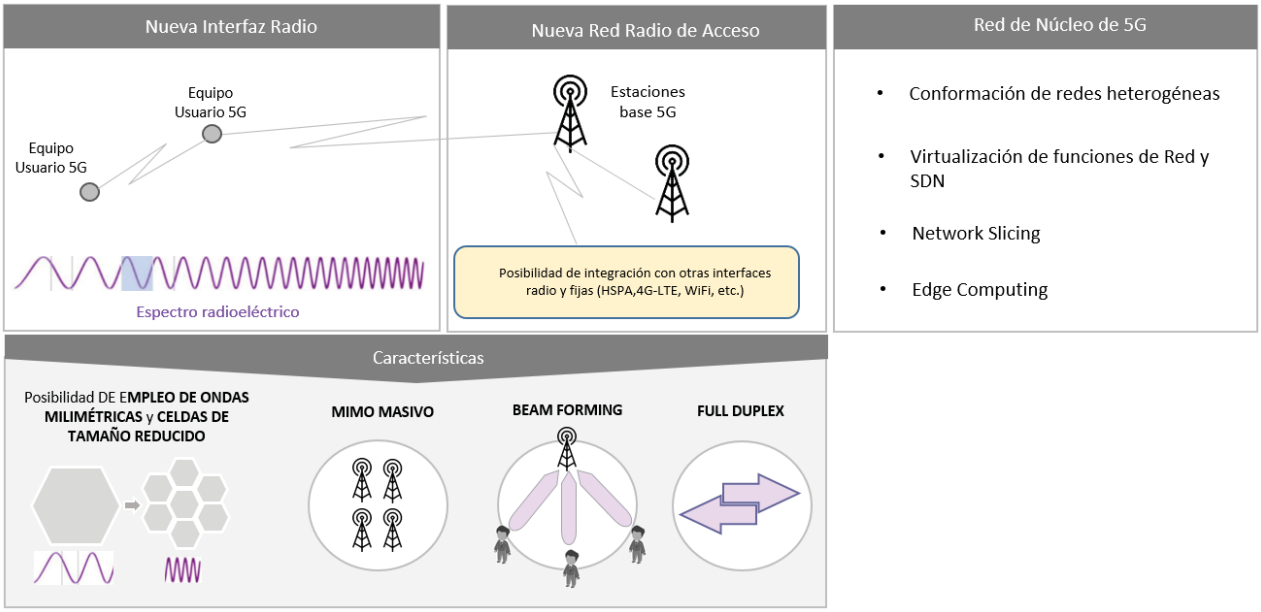


Figura 2 Resolución 307/08135/21. Esquema de componentes de las Redes 5G, elementos habilitadores y funcionalidades. [2]

2.1.3 Plan Nacional 5G. Secretaria de Estado para la Sociedad de la Información y la Agenda Digital. [3]

En este documento de referencia publicado por el MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL, se define las aplicaciones de la tecnología 5G y las expectativas de impacto de la introducción de las redes y servicios 5G se apoyan en las innovaciones tecnológicas que incorpora sobre las capacidades de las actuales infraestructuras de comunicaciones móviles.

En concreto, las redes 5G facilitarán:

- Banda ancha móvil de muy alta velocidad y capacidad, que facilitarán velocidades en movilidad superiores a 100 Mbit/s con picos de 1 Gbit/s, lo que permitirá por ejemplo ofrecer contenidos en ultra alta definición o experiencias de realidad virtual.

- Comunicaciones ultra fiables y de baja latencia, en torno a 1 milisegundo (ms) frente a 20-30 ms propios de las redes 4G. Esta condición podría hacerlas apropiadas para aplicaciones que tienen requerimientos específicos en este ámbito, como el vehículo conectado o el vehículo autónomo, servicios de telemedicina, sistemas de seguridad y control en tiempo real y otros como la fabricación inteligente.

- Comunicaciones masivas tipo máquina a máquina (M2M). Se incrementará la capacidad para gestionar gran cantidad de conexiones simultáneas, lo que permitirá entre otras cosas, el despliegue masivo de sensores, el Internet de las cosas (Internet of Things, IoT) y el crecimiento de los servicios de Big Data.

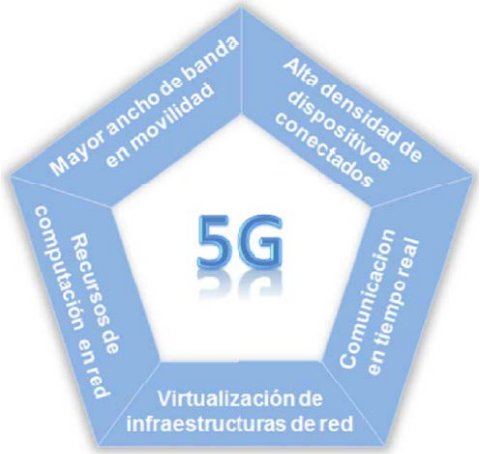


Figura 3 Aspectos regulatorios Plan Nacional 5G. [3]

Tras el análisis de las aportaciones recibidas en la Consulta y tomando en consideración los objetivos comunes de los Estados miembros de la Unión Europea, las medidas a desarrollar dentro del Plan Nacional se han estructurado en los siguientes ejes de actuación:

Gestión y planificación del espectro radioeléctrico. Acciones dedicadas a garantizar la disponibilidad en los plazos adecuados de las diferentes bandas de frecuencias necesarias para la prestación de los servicios de comunicaciones sobre redes 5G.

Impulso a la tecnología 5G: Pilotos de red y servicios y Actividades I+D+i. Experiencias piloto y casos de uso impulsados por la Administración destinados a facilitar a operadores, suministradores, fabricantes de equipos e industria en general experimentar con la nueva tecnología que permita desarrollar ecosistemas 5G y asegure una prestación futura adecuada de los servicios 5G e identificar nuevos modelos de negocio. También se incluyen acciones de promoción del emprendimiento, la investigación y el desarrollo servicios innovadores que faciliten la creación de un ecosistema español de provisión de servicios, contenidos aplicaciones y plataformas 5G.

Aspectos regulatorios. Identificación y desarrollo de instrumentos legales, adicionales a los relacionados con la gestión del espectro, que sean necesarios para proporcionar un marco jurídico adecuado y flexible que proporciones la seguridad jurídica imprescindible para incentivar y facilitar las inversiones necesarias para el despliegue de las infraestructuras y tecnologías 5G.

Coordinación del Plan y cooperación internacional. Desarrollo de infraestructuras de gobernanza y coordinación de las medidas incluidas en el plan y acciones de cooperación internacional y apoyo y seguimiento de los trabajos de estandarización de la 5G.

Figura 4 Ejes del Plan Nacional 5G. Plan Nacional 5G 2018-2020. [3]

Las atribuciones de bandas de espectro destinadas al uso para los servicios 5G se acuerdan en las Conferencias Mundiales de Radiocomunicaciones de la UIT[3]. Dentro de la Unión Europea, el Grupo de Política del Espectro Radioeléctrico (Radio Spectrum Policy Group, RSPG) aprobó en noviembre de 2016 la Opinión en la que identifica las bandas de frecuencias para ser utilizadas en el Unión Europea:

- La banda 3,4-3,8 GHz (3.400-3.800 MHz) se considera como lanzamiento del 5G en la banda principal para la introducción de servicios basados en 5G en Europa, incluso antes de 2020. Esta banda tiene la posibilidad de situar a Europa en el liderazgo del despliegue 5G.
- El 5G necesitará desplegarse en bandas que ya están armonizadas por debajo de 1 GHz, incluyendo en particular la banda de 700 MHz.
- Hay apoyo de la industria móvil a la banda de 26 GHz (24,25-27,5 GHz) como una banda pionera para una implementación temprana a 24 GHz.

[3] La **Unión Internacional de Telecomunicaciones** (**UIT**) es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. Su sede se encuentra en la ciudad de Ginebra (Suiza).

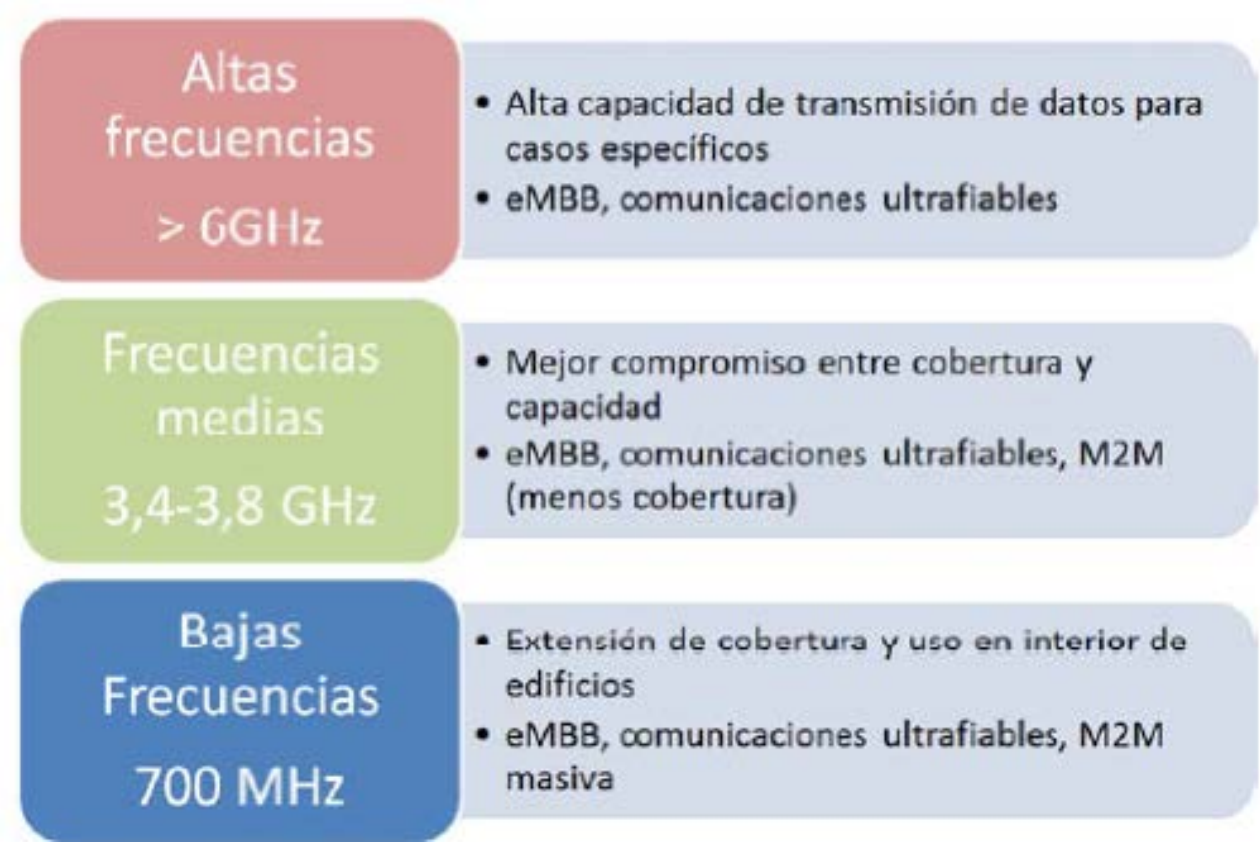


Figura 5 Bandas de Frecuencias Identificadas por la Unión Europea. Plan Nacional 5G 2018-2020 [3]

2.2 INTRODUCCIÓN A LAS RADIOS TÁCTICAS SDR. (SOFTWARE DEFINED RADIO). [4]

2.2.1 Definición y Objetivos de los SDR,s.

La Radio definida por Software SDR (siglas en ingles "Software Defined Radio), es un dispositivo radio en el cual la totalidad, o parte de las funcionalidades asociadas a la capa física de comunicaciones (transmisión a recepción radio) están definidas mediante software. De acuerdo con la definición conjunta del IEEE y el Wireless Innovation Forum.[4], el Objetivo principal de la utilización de esta tecnología en la Red Táctica de Combate, es disponer de un sistema de telecomunicaciones radio en el cual independientemente del marco de empleo tanto conjunto como combinado. Estos sistemas permitan la interoperabilidad e integración de las comunicaciones con los mismos sistemas propios de cada ejecito o país solo mediante la configuración de un software en cada equipo.

Otros objetivos que también son muy importantes como es la estandarización, la definición de la arquitectura de red y sobre todo la forma de onda a emplear, se trataran durante el desarrollo de este trabajo.

2.2.2 Evolución de los Sistemas en la Red táctica de Combate.

El sistema actual de las comunicaciones radio táctica en la OTAN, presenta los siguientes inconvenientes a la hora de interoperar entre los distintos países que componen la Alianza, los cuales se van a reseñar a continuación:

[4] Foro de Innovación Inalámbrica | CBRS, SDR y Estándares de Uso Compartido del Espectro (wirelessinnovation.org).

Problemas de interoperabilidad.

Cada país es propietario de su propios medios de comunicación a la hora de realizar un ejercicio combinado con otro país, estos deben de coordinarse mediante los denominados oficiales de enlace de transmisiones, siendo su función principal la coordinación de las comunicaciones, implicando que el país anfitrión del ejercicio apoyará con sus propios medios al país invitado. E esto es simple ya que solo están implicados en el ejercicio dos naciones, pero piensen que pasa cuando el ejercicio es de todos los países que componen la Alianza y tienen que enlazar entre sí, la implicación de personal y medios de la nación anfitriona sería desmesurada.

Complejidad Logística.

Todo esto implica una gran complejidad logística, debido a problemas de espacio en las plataformas y sobre todo en unidades ligeras que carecen de vehículos o están muy limitados por lo que en la mayoría de los casos deben ser portátiles.

Complejidad coexistencia con Inhibidores.

En plataformas donde coexisten Inhibidores contra los artefactos explosivos improvisados y guerra electrónica (CREW, Counter RC-IED EW), los sistemas de radio de dotación pierden gran parte de su eficacia y efectividad, por las interferencias que estos producen.

Diversidad de equipos.

Las plataformas Hardware desplegadas en estos momentos en las unidades táctica del Ejercito de Tierra, solo permiten la posibilidad de funcionar en una determinada banda de frecuencias ya sea HF, VHF o UHF, implica que para empleo táctico se deba utilizar un equipo, produciendo que sea necesario para un puesto de mando tipo Batallón disponer de los distintos medios para poder tener enlace tanto con sus unidades subordinadas como con su unidad superior.

Limitaciones del Ancho de Banda.

Tras las nuevas necesidades de transmisión de datos en tiempo real, como pueden ser el envio de imágenes de una Aeronave no Tripuladas (siglas en ingles UAS), Streaming de Videos, informes, etc., los sistemas radio disponibles no tienen el suficiente ancho de banda para soportarlo. Ver Figura 6 .

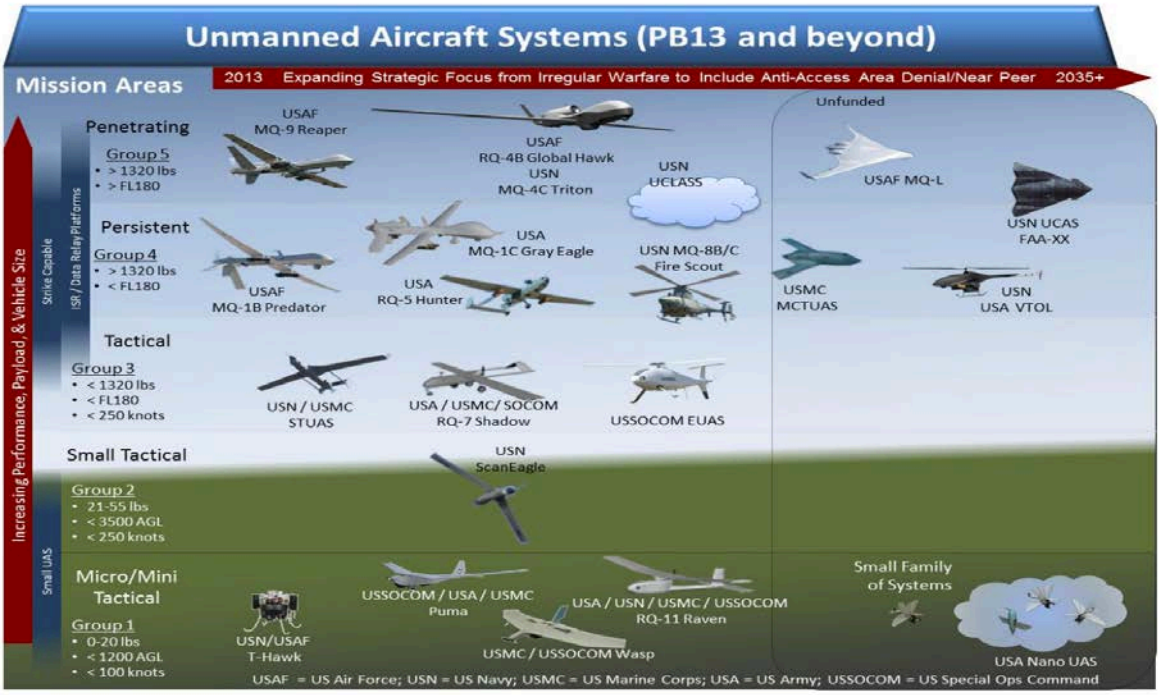


Figura 6 [Conceptos básicos del sistema de aeronaves no tripuladas (UAS) - Missile Defense Advocacy Alliance]

Continuando con la evolución de los sistemas tácticos de comunicaciones radio empleados a lo largo de su implementación en los ejércitos, se puede comprobar la necesidad de la utilización de SDR:

1. Primeras radios: Dispositivos ligados a un único fabricante, donde tanto la plataforma como la forma de onda se encuentran integrados mediante hardware y software propietarios.
2. Desde 1992 a 1995 se lanza el proyecto SpeakEasy Phase I con el objetivo de interoperar desde 2MHz a 2GHz.

SpeakEasy Phase II, se lanza teniendo en cuenta no solo reconfigurabilidad (mecanismos Open source) si no también conceptos SWaP (Intercambios financieros).

El proyecto SpeakEasy Phase I demostró la consecución de sus objetivos en el TF-XXI Advanced Warfighting Exercise. La fase II introduce las FPGA (Procesadores Digitales de Señales).

3. En 1999 se libera la primera versión de la **SCA**, estandarizando la arquitectura software para plataformas radio, y abriendo parte de la especificación.
4. La SCA es publicado por el Joint Tactical Networking Center (JTNC). Esta arquitectura fue desarrollada para ayudar en el desarrollo de sistemas de comunicación de radio definidos por software (SDR), capturando los beneficios de los recientes avances tecnológicos que se espera que mejoren en gran medida la interoperabilidad de los sistemas de comunicación y reduzcan los costos de desarrollo e implementación. La arquitectura también es aplicable a otras aplicaciones integradas de computación distribuida, como los terminales de comunicaciones o la guerra electrónica (EW).

La SCA se ha estructurado para:

a. Proporcionar la portabilidad del software de aplicaciones entre diferentes implementaciones de SCA.

b. Aprovechar los estándares comerciales para reducir los costos de desarrollo,

c. Reducir el tiempo de desarrollo de software a través de la capacidad de reutilizar los módulos de diseño.

d. Y se construya sobre marcos y arquitecturas comerciales en evolución.

La SCA está diseñada deliberadamente para cumplir con los requisitos de aplicación comercial, así como los de las aplicaciones militares. Dado que la SCA está destinada a convertirse en una norma autosostenible, se ha invitado a una amplia muestra representativa de la industria a participar en su desarrollo y validación. La SCA no es una especificación del sistema, sino un conjunto de reglas independientesdos anteriormente.

5. En 2009 se lanza una iniciativa europea formada por 6 naciones (ESP, FIN, FRA, ITA, POL, SUE) para una estandarización completa de arquitectura SDR (ESSOR) y la definición e implementación de una forma de onda táctica de banda ancha (HDRWF) de acuerdo con la arquitectura definida.

El objetivo principal de este proyecto es proporcionar una arquitectura de radio definida por software (SDR) para fines militares y una forma de onda de datos alta (HDR WF) militar que cumpla con dicha arquitectura, ofreciendo así el referencial normativo requerido para el desarrollo y la producción de radios de software en Europa. Además, el proyecto proporcionará directrices relacionadas con la validación y verificación de la portabilidad de la forma de onda y la reconfigurabilidad de la plataforma, estableciendo una base de seguridad común para aumentar la interoperabilidad entre las fuerzas europeas.

Los productos de ESSOR se basarán en la Arquitectura de Comunicación de Software (SCA) desarrollada originalmente en los Estados Unidos en la Oficina Ejecutiva del Programa Conjunto para el programa Joint Tactical Radio System (JPEO JTRS).

6. Las ventajas de la implementación de la SDR son simplificar el ciclo de vida de los equipos radio, mejorar la interoperabilidad de las comunicaciones (distintas radios, misma waveform), reaprovechar el mismo software de forma de onda para distintos tipos de radio (portabilidad) y agilizar el desarrollo de nuevos tipos de comunicaciones al separar plataforma y forma de onda

2.2.3 Estandarización y Arquitectura de Red

2.2.3.1 Estandarización.

Definición de un marco común para el desarrollo de aplicaciones de comunicaciones (formas de onda) mediante la utilización de la tecnología Radio Definida por Software (SDR), facilita la portabilidad de la misma forma de onda entre diferentes plataformas operativas (e.j. Manpack, Vehicular, Aerotransportada, …), facilita la interoperabilidad entre diferentes implementaciones de un mismo protocolo de comunicaciones a partir de un modelo común, facilita la soberanía de las comunicaciones si se controlan las aplicaciones de comunicaciones (forma de onda), Servicios de seguridad (TRANSEC, NETSEC, COMSEC), si la Plataforma SDR sigue una arquitectura estándar.

2.2.3.2 Arquitectura. [5]

La definición dentro del marco arquitectónico que especifica a los diseñadores de sistemas de comunicaciones debe definir lo siguiente:

- Cómo operan los elementos hardware y software entre sí.
- Cómo se controla el ciclo de vida de las aplicaciones.
- Cómo acceder a los recursos hardware de la radio a través de los Radio Dispositivos.
- Cómo acceder a los servicios de la radio a través de los Radio Servicios.

- Como hacer uso de la infraestructura de seguridad de la radio a través de los Radio Servicios de Seguridad.

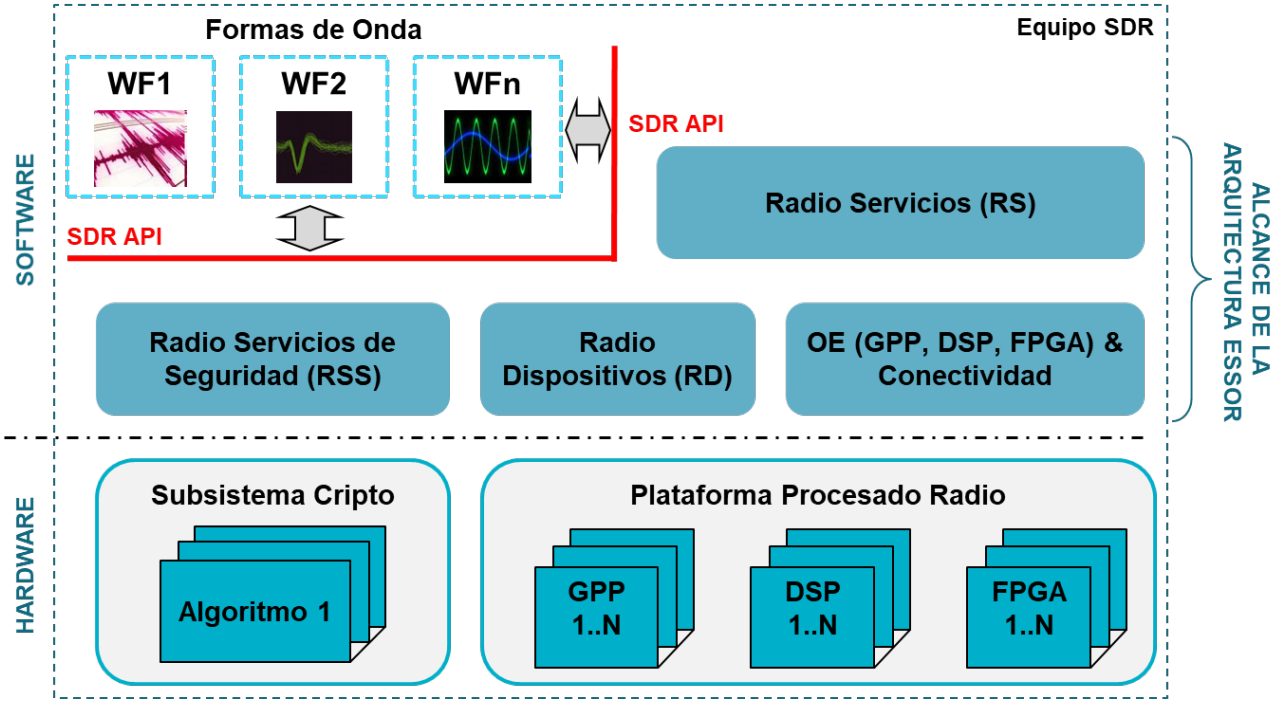


Figura 7 Fuente: ESSOR Architecture – Motivation and Overview (WInnF Technical Conference – December 2010). [4]

La arquitectura SDR ESSOR debe tener el siguiente alcance:

- **Permite la conectividad en un entorno operativo DSP (Digital Signal Processor), GPP (General purpose Processor) y FPGA (Field Programmable Gate Array).**

Donde desarrolla un entorno de ejecución para el software (firmware) de los elementos de procesado GPP, DSP y FPGA y mecanismos de conectividad entre componentes permitiendo Intra-procesador dentro del mismo elemento de procesado e Inter-procesador, entre diferentes elementos de procesado (o espacios de memoria), además de la Estandarización de API,s para el acceso a los mecanismos de conectividad y servicios del Sistema Operativo.

- **Radios dispositivos (RD).**

Elementos que proporcionan una abstracción de los elementos hardware de la radio, ofrecen un API SW/FW de alto nivel a las aplicaciones (formas de onda o servicios), y el API ofrecido está basado en las especificaciones del JTRS, complementándolo en aquellos puntos en los que resultaba incompleto.

Ejemplo: Transceiver Device.

- **Radios Servicios (RS).**

Elementos que proporcionan funcionalidades software que pueden ser útiles para el desarrollo de formas de onda, ofrecen un API SW/FW de alto nivel a las aplicaciones (formas de onda y otros servicios).Ejemplo: SNMP Service

- **Radios Servicios de Seguridad (RSS)**

Elementos que proporcionan una abstracción de los servicios de INFOSEC de la radio, ofrecen un API SW/FW de alto nivel a las aplicaciones (formas de onda o servicios), la primera estandarización multinacional del API de acceso a funciones de seguridad en SDR y el JTRS no han liberado la API de los servicios de seguridad, lo que imposibilita la realización de formas de onda multinacionales en estas plataformas.

2.2.4 Forma de Onda ESSOR HDRWF. [5]

Arquitectura ESSOR (ESSOR Architecture): consiste en la definición de una arquitectura de referencia SDR en el ámbito europeo. Para ello, partiendo de la parte pública de la "Arquitectura de comunicaciones mediante software (SCA)" norteamericana, desarrollada al amparo del programa JTRS (Joint Tactical Radio System) se han de elaborar las partes no publicadas de ésta: (1) la arquitectura de seguridad; (2) la capa de abstracción existente entre el software que define las diferentes formas de onda y el hardware de las plataformas.

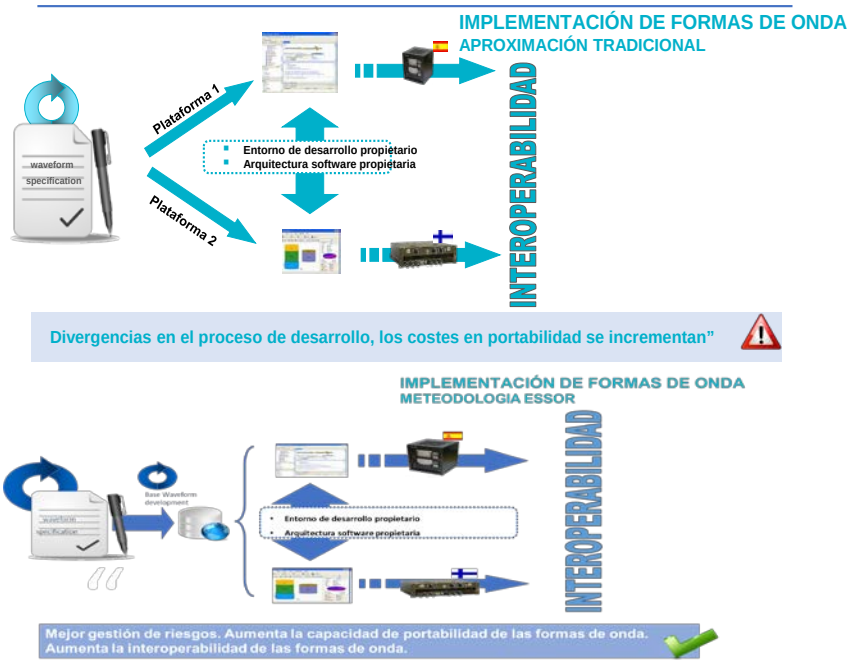


Figura 8 . Conferencia SDR en OTAN II CSUP CIS ET 2021.Coronel de Transmisiones EM Ignacio Javier Simón Andújar

Forma de onda de alta capacidad (HDR WF): abarca la definición y desarrollo de una forma de onda de comunicaciones militares tácticas con prestaciones avanzadas que servirá de enlace de alta capacidad en despliegues terrestres. Así mismo, se espera que la especificación de esta forma de onda adquiera la categoría de estándar internacional. Además, se ha podido demostrar que la arquitectura ESSOR es posible técnicamente y tiene capacidad para soportar una WF compleja como la HDR WF de ESSOR, forma de onda que cumple con los requisitos operacionales requeridos en el programa (capacidad MANET (Mobile Ad hoc Network), VoiP, video streaming, conexión con redes externas, gestión de la QoS (Quality of Service), etc.).

2.2.5 Soberanía en las Comunicaciones.

Ser soberano en comunicaciones significa tener control total sobre las comunicaciones propias y ser independiente.

Para ser independiente es necesario:

- Tener el **conocimiento** de los elementos que conforman las comunicaciones nacionales (i.e. especificación forma de onda, especificación plataforma, estándares utilizados, …)
- Tener **confianza** en los equipos y algoritmos que participan en las comunicaciones (i.e. mecanismos de Seguridad aprobados, algoritmos nacionales, …)
- Tener la **flexibilidad** de poder adaptar las comunicaciones a las necesidades operativas actuales y futuras (i.e. plataformas reconfigurables, formas de onda portables, …)

En el escenario tradicional mantener la soberanía en comunicaciones requiere tener el control total sobre el terminal hardware, ya que no existe una separación clara entre la capacidad de comunicaciones y el hardware que lo soporta. En un escenario con tecnología SDR, gracias a la estandarización, para mantener la soberanía en comunicaciones únicamente se requiere tener el control sobre ciertos elementos clave.

2.2.5.1 Elementos Clave a Controlar

i. Forma de onda

El elemento principal que proporciona la capacidad de comunicación, se debe evitar Comportamientos no especificados, Vulnerabilidades de Seguridad, problemas de interoperabilidad y se debe considerar, Especificación completa, Golden Reference disponible, Simulaciones, Definición de test de interoperabilidad, Caracterización de prestaciones requeridas y Funcionalidades de seguridad claramente diferenciadas y especificadas.

ii. Plataforma

Elemento responsable de las prestaciones y las capacidades finales del equipo radio en su conjunto.

Se debe evitar, las limitaciones de prestaciones y funcionalidad, la falta de flexibilidad y se debe considerar la Arquitectura HW, las capacidades de procesado digital, las prestaciones de RF, las capacidades de tiempo real, las cifras de prestaciones del middleware de comunicaciones entre los elementos de procesado, los framework estándar (ESSOR, SCA) y los servicios implementados (APIs)

iii. Seguridad

El Elemento responsable de las capacidades de seguridad del equipo radio debe de evitar, las limitaciones de prestaciones, las limitaciones de funcionalidad, la falta de flexibilidad y visibilidad y debe de considerar, la arquitectura del subsistema criptográfico (CS/S), la Capacidad de programación del CS/S, las prestaciones del CS/S, la Arquitectura lógica/física, los mecanismos anti-tamper, los motores criptográficos estándar soportado, el framework estándar (ESSOR, SCA) y los Servicios implementados (APIs)

iv. Portabilidad.

Elemento que garantiza la independencia de las comunicaciones y el hardware del equipo radio. Debe de evitar que la Documentación de diseño Software se encuentre incompleta o inexistente, los diseños Software deben de estar orientados a una plataforma concreta y se debe de considerar la utilización de marcos arquitectónicos estándar (e.j. ESSOR), limitar la utilización de extensiones opcionales de las APIs, utilización de lenguajes de codificación estándar (C/C++, VHDL, …), evitar la utilización de extensiones del lenguaje orientadas a procesadores concretos., definición de una implementación intermedia que sea agnóstica de plataforma (e.j. metodología ESSOR de Forma de Onda Base).

v. Estandarización.

Elemento que controla las interacciones entre el resto de los elementos clave. En la Plataforma existen estándares que definen las capacidades funcionales de plataforma (Radio Dispositivos y Radio Servicios), y que definen mecanismos para su interacción (e.j. middleware CORBA). Ejemplos: SCA, ESSOR. Actualmente existen limitaciones a la hora de caracterizar de una manera clara unificada las prestaciones de una plataforma.

Sobre la estandarización en la Seguridad, existen estándares que definen las capacidades funcionales de seguridad de la plataforma (Radio Servicios de Seguridad). Ejemplos: ESSOR, IRSS API.

Y sobre la estandarización Portabilidad, actualmente no hay un estándar para la portabilidad de forma de onda. El programa ESSOR define la aproximación de forma de onda base, y cuenta con un conjunto de lecciones aprendidas.

2.3 CONSTITUCIÓN DE GRUPOS DE TRABAJO PERMANENTES PARA LA IMPLANTACIÓN Y EMPLEO DE LA TECNOLOGÍA 5G Y DE LAS COMUNICACIONES DE RADIOS TÁCTICAS SDR EN EL MINISTERIO DE DEFENSA.

2.3.1 Grupo de Trabajo Permanente para la Implantación y Empleo de la tecnología 5G.

En la ya mencionada Resolución 307/08135/21 [2], de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa, en su apartado decimocuarto se establece su estructura de Gobierno y en concreto, “Se constituye un Grupo de Trabajo Permanente para la Implantación y Empleo de la Tecnología 5G en el seno de la Estructura de Gobierno de los CIS/TIC del Ministerio, dependiente del Comité de Telecomunicaciones del Ministerio de Defensa.”

Siguiendo con la Resolución 307/08135/21, en su capítulo V “Desarrollo e Implantación de la Estrategia 5G y Estructura de gobierno”, para cada proyecto se identificarán los siguientes aspectos:

- Necesidad operativa / funcional a la que se asocia.
- Objetivos esperados y plazos previstos de inicio y consecución.
- Dominio/s de aplicación, escenario/s de referencia y opción de despliegue y uso más adecuada.

- Actores implicados y matriz de responsabilidades (RASCI).
- Interdependencia con proyectos de desarrollo del PECIS (o integración en ellos).
- Interdependencia con proyectos y experiencias sobre redes y servicios 5G de la OTAN, la Unión Europea o de la AGE.
- Recursos implicados (humanos, materiales, financieros y formativos).

La definición y desarrollo de estos proyectos se adaptará, en todo caso, a la evolución en el contexto tecnológico y normativo que afecte al empleo de redes y servicios 5G.

2.3.2 Grupo de Trabajo de las comunicaciones de radios Tácticas. SDR.

El GT de Comunicaciones Tácticas de la JUPROAM (GTCOMTAC, presidido por JTEW[5], MCCE[6], EMAD[7]) elaboró el documento de Requisitos de Estado Mayor (REM) del Sistema Conjunto de Radio Táctica (SCRT), validado por el JEMAD[8] en FEB 2018 y cuyo DDV[9] se encuentra actualmente aprobado por la DGAM[10]. Su principal objetivo es la obtención de un SCRT, con tecnología SDR ("Software-Defined Radio"), con soberanía nacional y fundamentada en cuatro pilares esenciales:

- Foreign physical radio platform. (Plataforma radio física foránea, al no ser España un país productor de radios).

- Arquitectura radio software ESSOR ("European Secure SOftware Radio"), compatible con la SCA ("Software Communications Architecture") USA.

- Repositorio de formas de onda (WFs-"Waveforms", aplicaciones SW de Comms) estándares (NBWF, WBWF, UHF TACSAT, SATURN, etc.)

- Un subsistema de seguridad/ criptográfico que pueda ser nacional y, en un momento dado, que también pueda incorporar uno aliado.

En las comunicaciones tácticas, la interoperabilidad se sustenta en lograr una estandarización de soluciones para las formas de onda de la Radio Definida por Software, que permitan a los distintos fabricantes producir equipos radio interoperables que puedan portar las mismas WFs de coalición, permitiendo la colaboración en escenarios multinacionales (ámbitos de OTAN y UE principalmente).

Para conseguir la interoperabilidad no sólo es fundamental la estandarización de las WFs, sino también del componente COMSEC (sistema criptográfico embebido o externo) empleado por las radios, tanto en las comunicaciones como en el canal de control en algunas WF (por ejemplo, para UHF SATCOM). Los cifradores deben seguir los estándares definidos en OTAN para permitir esta interoperabilidad. Además hay que tener en cuenta el espectro de frecuencias (muy limitado por ejemplo en UHF para WBWF,s) y los "hopsets" disponibles para TRANSEC.

---

[5] JTEW. Jefatura de Telecomunicaciones y Guerra Electrónica del Mando Conjunto del Ciberespacio MCCE-JEMAD).

[6] MCCE. Mando Conjunto del Ciberespacio.
[7] EMAD. Estado Mayor de la Defensa.
[8] JEMAD. Jefe de Estado Mayor de la Defensa.
[9] DDV. Documento de Viabilidad.
[10] DGAM. Dirección General de Armamento y Material. Secretaría de Estado del MINISDEF.

La interoperabilidad en comunicaciones tácticas, en especial en el ámbito terrestre, sigue siendo una asignatura pendiente y muy importante en la situación internacional actual, con despliegue de Fuerzas españolas bajo mando OTAN, en Letonia, Lituania, en las SNMGs, etc.

España participa en iniciativas OTAN (NATO LoS Comms CaT, NATO BLoS Comms CaT, NATO SATCOM CaT, etc.) y UE (EDA PT CIS, Proyecto PESCO ESSOR, etc.) para el desarrollo de formas de onda interoperables de coalición.

En aras a alcanzar el grado de interoperabilidad deseado, los productos a incluir en los Programas de Adquisición deben cumplir los siguientes protocolos de comunicaciones y de cifrado:

a. La lista de Formas de Onda (WFs) de interés para el factor de forma vehicular V-UHF, handheld V-UHF, y Fijo de V-UHF queda conformada por las siguientes:

i. WFs SATCOM:

1. - IW (STANAG 4681 Ed1/Ed2).

2. - SCPC (Acceso dedicado).

ii. WFs de Banda Estrecha:

1. - SATURN (STANAG 4372 Ed4).

2. - NBWF EPM (STANAG 5630 Ed2 en definición).

3. -VHF legacy STANAG 4204.

4. - UHF legacy STANAG 4205.

5. - HQ-II STANAG 4246 (legacy).

6. - NEB, NATO Narrowband EPM Broadcast WF (STANAG 5652 en definición).

7. - ICAO ATC (Air Traffic Control).

iii. WFs de Banda Ancha:

1. - ESSOR HDRWF (como estándar internacional ESSOR).

2. - NATO HDRWF (STANAG 5651 en definición, en base a la ESSOR HDRWF).

3. - NATO HCDRWF (STANAG 5649 en definición).

iv. Compatibilidad con Links específicos:

1. - Link-11 (STANAG 5511).

2. - Link-22 (STANAG 5522).

3. - RVT (Remote Video Terminal for ISR Systems, STANAG 7085).

b. La lista de estándares de cifra queda conformada por los siguientes:

i. Cifrado de voz y datos serie:

1. - “Secure Communications Interoperability Protocol”, SCIP 214.6 (STANAG 5068), que incluye la Especificación STaC-IS (“Secure Tactical Communications Interoperability Specification”) que garantiza la interoperabilidad entre SCIP y TSVCIS.

2. - “Tactical Secure Voice Cryptographic Interoperability Specification”, TSVCIS 3.1.1, que incluye la Especificación STaC-IS que garantiza la interoperabilidad entre SCIP y TSVCIS.

ii. Cifrado de datos IP: - Protocolo NINE "Tactical Radio Profile" (“Networking and Information Infrastructure IP Network Encryptor”, STANAG 4787).

2.3.1 Redimensionamiento y priorización del Sistema Conjunto de Radio Táctica (SCRT-SDR).

En mayo del año 2022, debido a los últimos acontecimientos geoestratégicos ocurridos en el Flanco Este de la OTAN se han acelerado los trabajos para la obtención de los medios reflejados en el REM del SCRT, incluyendo la capacidad SATURN y TACSAT. En este estudio de dimensionamiento y priorización se ha tenido en cuenta las prioridades fijadas por el JEMAD en el Objetivo de Capacidades Militares y las nuevas posibilidades en Interoperabilidad que ofrecen los futuros equipos radio, como la posibilidad de que puedan ser integrados en la tecnología 5G.

. Por lo recogido en el punto anterior se ha clarificado algunos de los requisitos contenidos en el documento de Requisitos de Estado Mayor del SCRT y para establecer un punto de situación sobre la urgente adquisición de los equipos contenidos en el mismo. Dichos equipos se tienen que adquirir para cubrir diferentes necesidades, desde radios VHF/UHF a radios SATURN y TACSAT. La tecnología SDR (Radio Definida por Software) permite que un mismo equipo cubra diferentes necesidades, por lo que se han elaborado las tablas de dimensionamiento y su priorización para su posterior adquisición.Ver Figura 9 "Dimensionamiento de necesidades de Equipos para el programa SCRT. Dato JTEW-MCCE".

NECESIDADES EQUIPOS RADIO SDR PARA EL PROGRAMA SCRT													
TIPOS DE RADIOS													
Factor de Forma	Banda y Nº de canales	EJERCITO DE TIERRA			ARMADA			EJERCITO DEL AIRE			UME		
		2022-25	2026-30	Total	2022-25	2026-30	Total	2022-2025	2026-2030	Total	2022-25	2026-30	Total
HANDHELD	V/UHF - 1ch	4.623	2.105	**6.728**	900	420	**1.320**	169	126	**295**	0	426	**426**
	V/UHF - 2ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)	956	763	**1.719**	150	65	**215**	174	142	**316**	0	0	**0**
MANPACK	HF - 1Ch	58	177	**235**	15	50	**65**	26	22	**48**	0	0	**0**
	V/UHF - 2ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)	548	340	**888**	310	200	**510**	77	71	**148**	0	0	**0**
VEHICULAR	HF - 1Ch	0	359	**359**	18	20	**38**	17	3	**20**	31	0	**31**
	V/UHF - 2ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)	3.320	5.215	**8.535**	200	115	**315**	80	23	**103**	0	123	**123**
FIJO	HF - 1Ch	0	4	**4**	3	3	**6**	28	25	**53**	6	0	**6**
	V/UHF - 2ch / 2x 1ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)	19	2	**21**	8	2	**10**	393	0	**393**	0	2	**2**
AERO	HF - 1Ch	65	0	**65**	0	0	**0**	102	40	**142**			
	V/UHF - 2ch / 2x 1ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)	218	46	**264**	65	60	**125**	404	0	**404**			
NAVAL	HF - 1Ch				20	40	**60**						
	V/UHF - 2ch / 2x 1ch V/UHF 2ch (+SATURN) (SIN UHF TACSAT) V/UHF 2ch (+ UHF TACSAT) (SIN SATURN) V/UHF 2ch (+ UHF TACSAT)(+ SATURN)				80	35	**115**						
TOTALES		9.807	9.011	***18.818***	1.769	1.010	***2.779***	1.470	452	***1.922***	37	551	***588***

Figura 9 Dimensionamiento de necesidades de Equipos para el programa SCRT. Dato JTEW-MCCE.

2.1 NECESIDAD DE INTEGRACIÓN EN SISTEMAS DE GESTIÓN DE COMUNICACIONES EN LAS PEQUEÑAS UNIDADES DEL EJÉRCITO DE TIERRA.

El Sistema de Gestión de Comunicaciones en el Ejército de Tierra GESCOMET [5], es el sistema de gestión seleccionado por el Ejército de Tierra Español para coordinar y administrar las

comunicaciones de Voz y Datos en entornos tácticos a nivel de Batallón, alcanzando también el nivel de Brigada.

GESCOMET es una solución táctica definida por Software y personalizada para el Ejército de Tierra que incluye capacidades avanzadas para el encaminamiento de datos IP, telecontrol y gestión de la voz en las redes radio de combate. Ofrece integración de los medios en dotación de distintos fabricantes, herramientas avanzadas de priorización de tráfico, telecontrol de los principales equipos, servidor de Voz táctico e integración de Voz y Datos inteligentes.

El sistema GESCOMET se integra con los principales servicios y aplicaciones desplegados por Ejército de Tierra: BMS[11], SIMACET[12], etc. encaminando dinámicamente los flujos de datos y voz a través de los medios radio HF, VHF, UHF, SATCOM y Radioenlaces.

Figura 10. Logotipo de GESCOMET. RF Española. (GESCOMET - RFE).

GESCOMET es compatible con los siguientes equipos tácticos:

- INTERCOMUNICADOR TACTICO
- VMI (Voice Manager Integrado)
- RAU (Remote Access Unit)

Entre las principales características de GESCOMET destacan:

[11] BMS. Battlefield Management System. Sistema de Gestión del Campo de Batalla.
[12] SIMACET. Sistema de Mando y Control del Ejército de Tierra.

- Solución integrada de comunicaciones de voz y datos para escenarios militares.
- Enrutador táctico integrado para encaminamiento dinámico de tráfico de datos con priorización, QoS y Balanceo de Carga.
- Protocolo propietario de enrutamiento táctico dinámico.
- Transmisión de datos ARQ/NOARQ dinámica y adaptativa que incluye compresión y cifrado AES 256 en tiempo real.
- Intercomunicador táctico para la integración de voz CNR y servicios de VoIP sobre la red radio.
- Aplicación cliente de gestión completa de los servicios de voz desde cualquier punto de la red (Voice Manager).
- Gestión centralizada del escenario mediante un único fichero de misión.
- Visualización en pantalla del estado de los dispositivos de comunicaciones locales y remotas, así como del estado de la red.
- Integración de todo tipo de dispositivos de comunicaciones y redes independientemente de su fabricante y modo de trabajo.
- Control remoto de los dispositivos de comunicaciones.
- Completo servicio de correo electrónico y gestión de la mensajería.
- Sistema integrable con servidores de correo externos (modo MTA), como Microsoft Exchange ®, Lotus Notes ®, Merak Mail Server ®, etc.).
- Servicios tácticos avanzados para la adquisición de señal GPS y servidor GPS, NTP, gestión SNMP, etc.
- Soporte para cifradores (CIFPECOM, KG84, KY99…).
- Protocolo NATO STANAG 5066 para comunicaciones radio interoperables.

2.2 INTRODUCCIÓN A LA TECNOLOGÍA 5G.

2.2.1 Características de la arquitectura 5G.

La tecnología 5G, independientemente de las anteriores generaciones de redes móviles que simplemente ofrecían servicios de datos móviles rápidos y confiables a los usuarios de la red, esta ha ampliado este panorama para prestar una amplia gama de servicios inalámbricos a los usuarios finales a través de diversas plataformas de acceso y redes multicapa.

La tecnología 5G es un marco dinámico, coherente y flexible de varias tecnologías avanzadas que sustentan diversas aplicaciones. Se emplea una arquitectura más inteligente, con redes de acceso por radio (RAN) que ya no están constreñidas por la complejidad de la infraestructura o la proximidad de las estaciones base. La tecnología 5G lidera el camino hacia una red RAN virtual, flexible y descompuesta con interfaces nuevas que crean puntos de acceso de datos adicionales.

Como diferencia respeto otras arquitecturas móviles, cabe destacar que el uso de la conformación de haces, ha sido básica para la implementación de la tecnología. Con este método,

se emplea un algoritmo para centrar las señales inalámbricas en un haz dirigido. De esta manera, se evitan los obstáculos que interfieren con las transmisiones de alta frecuencia y se pueden también orientar de forma estratégica las transmisiones directamente al usuario final.

La conformación de haces puede ayudar a las matrices MIMO (del inglés Multiple-Input, Multiple-Output [múltiple entrada, múltiple salida]) masivas, que son estaciones base dispuestas con docenas o cientos de antenas individuales, a hacer un uso más eficiente del espectro que las rodea. El principal desafío para MIMO masivo es reducir la interferencia mientras se transmite más información desde muchas más antenas a la vez. En las estaciones base MIMO masivas, los algoritmos de procesamiento de señales trazan la mejor ruta de transmisión a través del aire para cada usuario. Luego pueden enviar paquetes de datos individuales en muchas direcciones diferentes, rebotándolos en edificios y otros objetos en un patrón coordinado con precisión. Al coreografiar los movimientos de los paquetes y el tiempo de llegada, la formación de haces permite que muchos usuarios y antenas en una matriz MIMO masiva intercambien mucha más información a la vez.

Otro concepto que hay que tener en cuenta en la tecnología 5G, es que el concepto de segmentación de redes se refiere al empleo inteligente de secciones del espectro según las necesidades específicas del dispositivo o la aplicación en cuestión. Por ejemplo, una operación quirúrgica de forma remota puede requerir una latencia extremadamente baja para un funcionamiento seguro, mientras que las aplicaciones del IoT pueden abarcar un elevado número de dispositivos con una demanda de capacidad muy baja. La red móvil gestionará automáticamente los recursos de ancho de banda para optimizar el flujo del tráfico y el uso de los mismos.

Tiene la capacidad de verificación del rendimiento de diversos elementos virtuales de las redes 5G en el mundo real, se puede ampliar realizando pruebas y validando diversos casos prácticos de segmentación de redes en el entorno del laboratorio. Las soluciones de extremo a extremo para las pruebas y la validación de redes RAN al núcleo pueden emular redes centrales 5G por completo y verificar la selección y la funcionalidad de los nodos de un segmento de red, antes de ponerlos en producción. Introduciendo sistemas de pruebas 5G escalables con servicios de datos integrados necesarios para medir el rendimiento completo de la red y simular el comportamiento de los usuarios en el mundo real en los ensayos de campo de la tecnología 5G. El software es capaz de emular y medir millones de flujos de datos únicos siendo otro elemento indispensable de la fase de verificación y validación (V&V) de la tecnología 5G, ya que puede mejorar las pruebas de carga y capacidad, y las funciones basadas en parámetros de referencia.

Figura 11. Fase para la implementación 5G.Diseño propio.

2.2.1 La importancia en Defensa de adquirir un 5G Core (5GC) en propiedad.

El 5G Core (5GC) es el corazón de una red móvil 5G. Establece una conectividad confiable y segura a la red para los usuarios finales y proporciona acceso a sus servicios independientemente del si hay o no proveedor de servicios. El dominio central maneja una amplia variedad de funciones esenciales en la red móvil, como la conectividad y la gestión de la movilidad, la autenticación y autorización, la gestión de datos de suscriptores y la gestión de políticas, entre otras. Las funciones de red 5G Core están completamente basadas en software y diseñadas como nativas de la nube, lo que significa que son independientes de la infraestructura de nube subyacente, lo que permite una mayor agilidad y flexibilidad de implementación.

El nuevo estándar 3GPP para redes centrales conocido como 5G Core (5GC), incluye nuevas funciones de red (NF) para la red central.

La nueva arquitectura 5GC es lo que se denomina una Arquitectura Basada en Servicios (SBA), que implementa los principios de red de TI y un enfoque de diseño nativo de la nube. En esta nueva arquitectura, cada función de red (NF) ofrece uno o más servicios a otros NF a través de interfaces de programación de aplicaciones (API). Cada NF está formado por una combinación de pequeñas piezas de código de software llamadas microservicios. Algunos microservicios incluso se pueden reutilizar para diferentes NF, lo que hace que la implementación sea más efectiva y facilita la gestión independiente del ciclo de vida, lo que permite implementar actualizaciones y nuevas funcionalidades sin ningún impacto en los servicios en ejecución.

Arquitectura central 3GPP 5G.Figura 12.

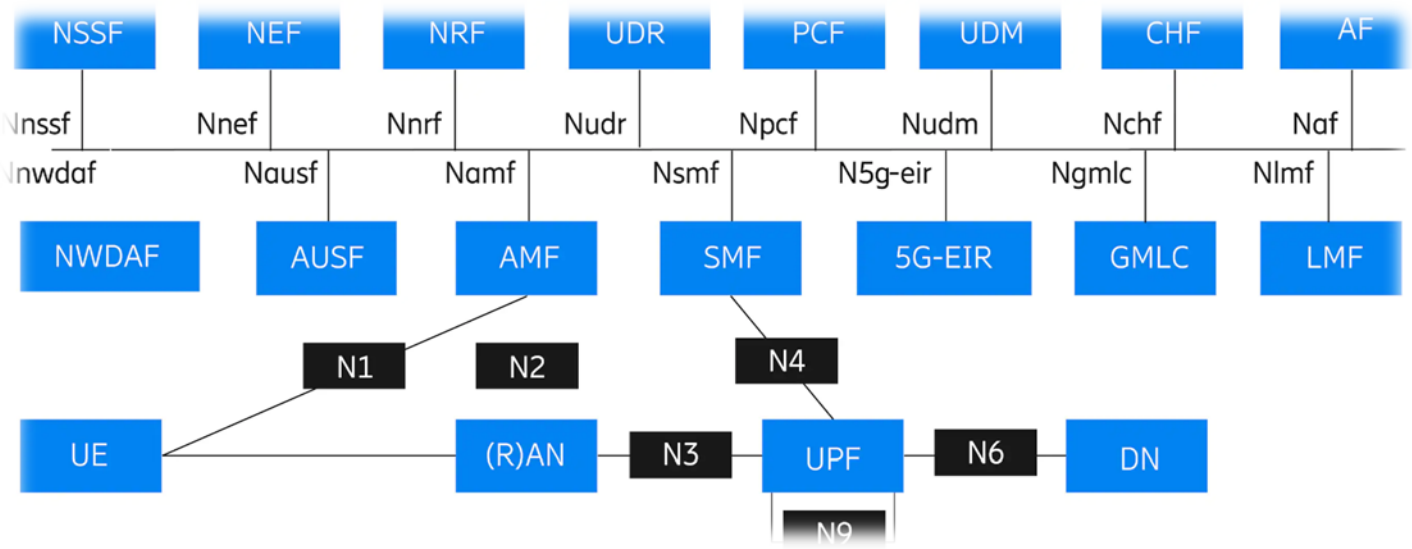


Figura 12. Arquitectura 3GPP 5G. Ejemplo CORE de ERICSSON.

Este diagrama no incluye todas las funciones de red (NF) en lugar de centrarse en las que están más asociadas a los dominios de administración de datos de usuario y núcleo de paquetes.

Todos los NF que se muestran en este diagrama forman parte de la cartera Cloud Core de Ericsson, excepto:

- CHF (cartera BSS de Ericsson).
- GMLC y LMF (cartera OSS de Ericsson).
- (R) AN (cartera RAN de Ericsson).
- AF que es una función fuera del dominio de los CSP.
- DN que es la red de datos a la que accede la UE (por ejemplo, Internet)

Siglas

5G-EIR	Registro de identidad de equipos 5G	**NSSF**	Función de selección de sectores de red
Af	Función de aplicación	**NWDAF**	Función de análisis de datos de red
AMF	Función de gestión de acceso y movilidad	**Pcf**	Función de control de directivas
AUSF	Función de servidor de autenticación	**(R) Un**	(Radio) Red de acceso
CHF	Función de carga	**SMF**	Función de gestión de sesiones
GMLC	Centro de ubicación móvil de Gateway	**LA UE**	Equipo de usuario
Lmf	Función de gestión de ubicación	**UDM**	Gestión unificada de datos
Dn	Red de datos	**Udr**	Repositorio de datos de usuario
Nef	Función de exposición de red	**UPF**	Función de plano de usuario
NRF (en inglés)	Función de repositorio NF		

Tabla 2-1. Arquitectura 3GPP 5G. [Red 5G Core (5GC): llegar al núcleo de 5G - Ericsson]

2.2.2 Núcleo de acceso múltiple: Núcleo 5G de modo dual.

5G Core ha implementado la nueva arquitectura de red 3GPP que liberará toda la potencia de 5G independiente, lo que permitirá velocidades de conectividad más rápidas, latencia ultrabaja y mayores tasas de bits y confiabilidad de la red. Estas capacidades, combinadas con la automatización de la red, la segmentación de red y la computación de borde, son fundamentales para abordar múltiples verticales y permitir un ecosistema para la innovación con casos de uso como: banda ancha móvil mejorada (eMBB), comunicación de baja latencia ultra confiable (URLLC), comunicación masiva de tipo máquina (mMTC) y comunicación de tiempo crítico (TCC).

Estas nuevas redes 5G deberán coexistir con las redes de 4G, mientras que al mismo tiempo es necesario mejorar las eficiencias para capturar nuevas oportunidades.

La solución 5G Core de modo dual es como implementar nueva arquitectura de red 5G Core a la vez que permite una coexistencia eficiente con las redes 4G Core implementadas, así como aprovechar los beneficios de las nuevas tecnologías, como la nube nativa de las redes heredadas. El núcleo 5G de modo dual se basa en tecnología nativa de la nube basada en microservicios y combina Evolved Packet Core (EPC) y las nuevas funciones de red 5G Core (5GC) en una plataforma común de acceso múltiple y nativa de la nube que admite 5G y generaciones anteriores para optimizar la huella y la eficiencia del TCO. Es una evolución virtualizada, diseñada para la implementación en la nube, que consiste con Cloud Packet Core, Cloud Unified Data Management (UDM) y Policy and Signaling Controller.

Para una mayor flexibilidad de implementación y eficiencia operativa, se han deben agrupar todas las funciones de red 5G y 4G en diferentes productos de acuerdo con los servicios que brindan a la red.

Esta solución también incluye una función de análisis de datos de red (NWDAF) incorporada y sondas de software para mejorar la experiencia del cliente de las redes basadas en datos que aprenden y mejoran, y un firewall integrado para aumentar la seguridad de la red 5G. También incluye capacidades de exposición a la red, incluido un módulo de administración de interfaces de programación de aplicaciones (API) integrado para permitir a los proveedores de servicios explorar nuevas oportunidades de negocio con una mayor programabilidad de la red.

El 5G Core de modo dual permite a los CSP[13]:

- Introducir 5G de forma rápida y eficaz mientras se protegen los servicios existentes.
- Tener una migración controlada y sin problemas a 5G alineada con las necesidades del negocio.
- Abordar nuevos segmentos con flexibilidad y agilidad.
- Reducir los costos y aumente el rendimiento con el diseño nativo de la nube.

[13] Content Security Policy (CSP). es una capa de seguridad adicional que ayuda a prevenir y mitigar algunos tipos de ataque, incluyendo Cross Site Scripting (XSS (en-US)) y ataques de inyección de datos. Estos ataques son usados con diversos propósitos, desde robar información hasta desfiguración de sitios o distribución de malware. Content Security Policy (CSP) - HTTP | MDN (mozilla.org).

• Introducir rápidamente nuevas funcionalidades y realizar actualizaciones de mantenimiento.

• Proporcionar compatibilidad óptima para implementaciones perimetrales y de segmentación de red.

2.3 INICIATIVAS PARA IMPLEMENTAR LA TECNOLOGÍA 5G EN OTAN Y PROYECTOS 5G MINISDEF- EJÉRCITO DE TIERRA.

2.3.1 Iniciativas OTAN. [6]

La controversia 5G llegó a un punto crítico a principios de 2019. Muchos aliados se preocuparon por la seguridad de las futuras comunicaciones comerciales y militares dentro de la Alianza, principalmente, pero no solo, debido a los riesgos planteados por proveedores no aliados. Después de meses de discusión y debate, los líderes de la OTAN reunidos en Londres en diciembre de 2019 destacaron la importancia de "la seguridad de las comunicaciones, incluida la 5G" y reconocieron "la necesidad de confiar en sistemas seguros y resistentes".

Entre todas las iniciativas solo se va a hacer mención la que conforma el grupo de trabajo IST-187 “5G Technologies Application to NATO Operations” del Science & Technology Organization de la OTAN por formar parte de ella España.

Este grupo de trabajo se encuentra enfocado en definir posibles casos de uso y la aplicación de las distintas funcionalidades que permite el 5G, estableciéndose 4 subgrupos de trabajo, que hago mención a continuación.

- Network Slicing & Multiaccess Edge Computing
- MIMO&Full Duplex
- Extreme Large Coverage
- Security Mecanisims

Los Objetivos Task Group (STO) IST-187 5G son los siguientes:

- Comprensión de la tecnología 5G para escenarios militares,
- Comprensión de las especificaciones subyacentes para soluciones 5G y
- Mejoras necesarias en la estandarización de 5G (Objetivo: Release 17).Ver Anexo III.

La NCIA[14], impulsa la creación de un programa multinacional 5G a petición de Letonia, siendo los países que han enviado una declaración de intenciones para participar: Alemania, Turquía, Hungría, Canadá, USA, Letonia y España.

Los siguientes pasos serían Establecer los Programas de Trabajos, financiación por los países y aprobación de un MoU[15].

En el mes de diciembre del 2020, se presentó el proyecto de crear un programa multinacional para realizar esfuerzos coordinados de las naciones y la OTAN para explotar y desarrollar el potencial de la tecnología 5G para su aplicación en operaciones militares / de defensa. Desde entonces se han celebrado

[14] NCIA. NATO Communications and Information Agency. Agencia de Comunicaciones e información de la OTAN.

[15] MoU. Memorandum de Entendimiento. Se define como un acuerdo entre las partes y puede ser bilateral (dos) o multilateral (más de dos partes). El memorando de entendimiento sirve como una expresión de voluntad alineada entre las partes en cuestión y describe la intención de una línea de acción común.

2 reuniones más que han resultado que varios países, entre ellos España, manifiesten su interés en participar.

Siendo el papel de la NCIA en estos momentos muy interesante ya que relaciona casos de uso concretos con las nuevas funcionalidades de 5G, incluso asignando las bandas de frecuencias para cada uno.

Figura 13. Logotipo de NCIA. [Agencia del NCI | Hogar (nato.int)](#).

Potential of 5G technologies for military application

Working paper, 15 Sep 2020 | Copyright 2020 NCI Agency

Luis Bastos, Germano Capela, Alper Koprulu
NATO Communications and Information Agency
{luis.bastos, germano.capela, alper.koprulu}@ncia.nato.int

Abstract–5G specifications and technologies implementing the International Telecommunications Union (ITU) IMT-2020 vision represent a paradigm shift in International Mobile Telecommunication (IMT) standards compared to previous IMT generations. 5G is poised to push the technology limits in many areas, particularly at the radio interface level. With the first 5G network rollouts taking place, a lot of attention to 5G is being given by many actors, including the military. As with any technological breakthrough, 5G is prone to significant hype and misconceptions. This paper provides an overview of 5G technologies and identifies key 5G technology enabling features for military applications. It then proposes a number of initial reference 5G military scenarios where the use of 5G systems or technologies could bring significant benefits to military users, either as private 5G implementations or as use of public 5G infrastructure. It then provides conclusions and recommendations to military communications stakeholders. Detailed rationales will be made available in a technical report. The authors intend

It developed the (communications) **usage scenarios** and (user) **applications** that are represented in Fig. 1.

Figura 14. NCIA. Potencial de la Tecnología 5G para Aplicaciones Militares.

2.3.1 Proyecto 5G del Ministerio de Defensa – Ejército de Tierra. [7].

Entre los proyecto 5G presentados al Ministerio de Defensa, se encuentra Red 5G ad-hoc de alta capacidad aérea y nube táctica distribuida: FANETC (Flying Ad-hoc 5G Network & Distributed Mobile Tactical Cloud) y el desarrollo de una Red Segura de Alta Velocidad y Baja Latencia 5G para la Base Logística del Ejército de Tierra. . A continuación, se realiza una breve descripción:

2.3.1.1 Red 5G ad-hoc de alta capacidad aérea y nube táctica distribuida: FANETC (Flying Ad-hoc 5G Network & Distributed Mobile Tactical Cloud).

La necesidad Operativa se base en que las comunicaciones empleadas por las unidades tácticas del Ejército de Tierra (ET) están soportadas por radios tácticas en las bandas de VHF y UHF. Este tipo de radios utilizan formas de onda de banda estrecha que proporcionan capacidades de transmisión muy bajas, del orden de Kbps. También se dispone de algunos equipos de comunicaciones satélite (con posibilidades reales de acceso muy limitadas) y radioenlaces desplegables obsoletos, que han dejado de emplearse.

La situación actual presenta la carencia de un medio de transmisión de alta capacidad en el ámbito táctico que permita una mayor flexibilidad, capacidad de reacción y dinamismo.

En consecuencia, se ha identificado la necesidad de aprovechar las capacidades de las comunicaciones 5G para proporcionar una mayor conciencia situacional y agilidad en la toma de decisiones en el ámbito táctico terrestre.

El objetivo de este proyecto es implantar un enjambre de *UAV (Unmanned Aerial Vehicle)* para crear una red 5G ad-hoc de alta capacidad aérea, *FANET (Flying Ad-hoc Network)*.

Esta red permite la capacidad de procesamiento y securización de los datos obtenidos a bordo de las aeronaves creando una nube táctica distribuida *FATC (Flying Ad-hoc Tactical Cloud).*

La red ad-hoc estaría compuesta por:

- Estaciones Base 5G con capacidad de *edge computing*, sobre vehículos militares facilitados por el ET para proporcionar la movilidad táctica necesaria (con capacidad de operar en dos bandas de frecuencia: 700/800/900 MHz y otra a partir de 3,5GHz, y con la posibilidad de emplear la banda 4,4-5GHz reservada para su empleo en comunicaciones terrestres militares por los países de la OTAN).
- Enjambre de UAV, con capacidad de procesado a bordo.

Para garantizar la confidencialidad de las comunicaciones, se empleará una arquitectura de seguridad acreditada por el Centro Criptológico Nacional (CCN), hasta nivel Difusión Limitada. En fases posteriores, con la incorporación de la arquitectura correspondiente y el equipamiento necesario se podría alcanzar el nivel RESERVADO NACIONAL / NATO SECRET.

El beneficio de este proyecto permitirá mejorar la conciencia situacional y agilizar la toma de decisiones en el campo táctico de las unidades del Ejército de Tierra, gracias a la implantación de una nube táctica que sólo se podrá llevar a cabo gracias a una tecnología que permita altos anchos de banda y economías de escala en dispositivos de usuario, como el 5G.

De esta forma se podrá incrementar la información con que se cuenta para el desarrollo de operaciones, derivada de los datos que se captan desde los sensores desplegados en vehículos o en el equipamiento del personal militar. Como un caso especialmente beneficioso, se podrían monitorizar las constantes vitales del personal militar para su seguridad (reacción a posibles armas químicas, control de niveles de estrés).

2.3.1.2 Red Segura de Alta Velocidad y Baja Latencia 5G para la Base Logística del Ejército de Tierra.

Actualmente los Órganos Logísticos Centrales del Ejército de Tierra, responsables de las actividades de sostenimiento al más alto nivel de los sistemas y materiales que este Ejército emplea, se encuentran desplegados en múltiples sedes repartidas a lo largo del Territorio Nacional. Estos centros están especializados por familias de apoyo, lo que implica múltiples movimientos de materiales para su reparación, aumentando los tiempos de inoperatividad.

La Base Logística del Ejército de Tierra (BLET) agrupará todas las actividades de sostenimiento de los sistemas terrestres en una única instalación reduciendo así los tiempos de servicio y aumentando la eficiencia de los recursos disponibles e incorporará, así mismo, nuevas tecnologías en un entorno de alta automatización y conectividad.

Para asegurar la integración y explotación en la BLET de las últimas tecnologías que ofrece la Industria 4.0[16], se hace necesario el despliegue en ella de una red de comunicaciones seguras de alta velocidad y baja latencia, basada en tecnología 5G.

El proyecto contempla el despliegue de una red multiservicio apoyándose principalmente en la tecnología 5G que permita crear un marco de trabajo para escenarios funcionales basados en Industria 4.0.

Se instalará una red multiservicio con 5G como principal método de conectividad, haciendo posible la entrega de un servicio de comunicaciones apropiado a cada sistema de información, priorizando la capacidad, la latencia o la movilidad según el caso (Network Slicing). Permitirá de esta forma unificar diferentes casos de uso bajo una misma tecnología e infraestructura.

El sistema deberá cubrir tanto el interior de las instalaciones como los espacios al aire libre, con el objetivo de dar respuesta a las posibles necesidades futuras de la BLET.

Se evaluará la implementación de sensorización (mMTC) y comunicaciones de alta fiabilidad y baja latencia (URLLC) principalmente.

2.3.1.3 Proyectos en desarrollo con tecnología LTE. (Long Term Evolution-4G).

A finales de 2016, se realizó en JCISAT[17] con el apoyo de la industria y una Brigada del E.T un ensayo con dos estaciones base LTE, una fija, para dar servicio a un Puesto de Mando Nivel Brigada (PCBRI) y otra móvil, para dar servicio a un Puesto de Mando Nivel Batallón (PCBON) y a pequeñas unidades dependientes.

El escenario de pruebas LTE se compuso del despliegue de dos Celdas en 700 MHz para los PCBRI y PCBON y una Celda de 2 GHz entre PCBRI y PCBON.

[16] Industria 4.0. "Sinónimo de manufactura inteligente, la Industria 4.0 es la realización de la transformación digital del campo, que brinda toma de decisiones en tiempo real, productividad mejorada, flexibilidad y agilidad". https://www.ibm.com/es-es/topics/industry-4-0.

[17] JCISAT- Jefatura de Sistemas de Información, Telecomunicaciones y Apoyo Técnico del Ejército de Tierra.

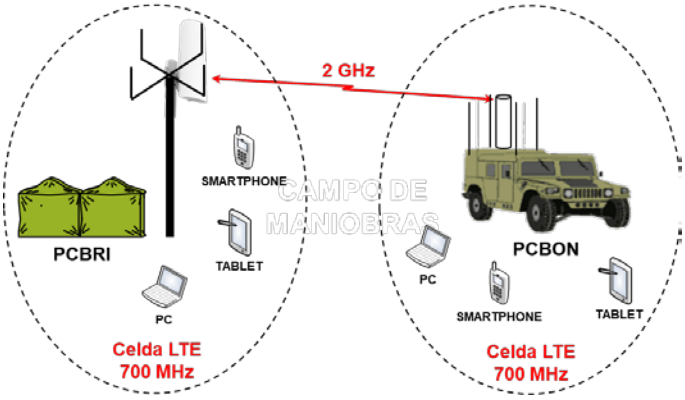


Figura 15 JCISAT. Despliegue LTE entre PC, s. Diseño propio.

Dentro del escenario de pruebas se instalaron los siguientes servicios de usuario:

- VoIP (con funcionalidad de PTT) más mensajería instantánea
- Videoconferencia, con una MTU en el PCBON y clientes "EZMeetup[18]".
- Streaming de vídeo, con una cámara IP instalada en el PCBON y clientes con el visor de video"RTSP Player".
- Transferencia de ficheros con las aplicaciones "FileZilla" y "vsnIPTransfer".
- Sistema de información C2 (BMS).
- Herramienta para medidas de capacidad de transmisión: LANTRAFFIC
- En el VCN (Virtual Core Network) del PCBRI con servicios de NTP y DHCP.

Resumen de las pruebas realizadas y resultados.

Pruebas realizadas:

Instalación, configuración y gestión de la infraestructura LTE.

Máximo throughput en celda a 700 MHz de PCBON y PCBRI.40 m/ UL: 15 Mbps DL: 34 Mbps.

Máximo throughput en enlace a 2 GHz entre PCBRI y PCBON. 185 m/ UL: 19 Mbps DL: 15 Mbps.

Cobertura en enlace a 2 GHz (10,7Km /UL: 512 Kbps DL: 512 Kbps).

Cobertura en celda a 700 MHz de PCBRI (4Km / UL: 512 Kbps DL: 512 Kbps).

Cobertura en celda a 700 MHz de PCBON (2Km / UL: 512 Kbps DL: 512 Kbps).

Configuración y explotación de servicios de voz, streaming de vídeo, VTC y Sistema C2.

[18] EZMeetup. Potente software de movilidad para iOS, Android, Mac y Windows. Es un práctico programa colaborativo diseñado específicamente para los sistemas de videoconferencia multipunto de AVer. Permite a los usuarios prolongar la videoconferencia de las salas de conferencia tradicionales a los equipos de sobremesa, portátiles, tabletas y smartphones. Como servidores SIP, los sistemas multipunto de AVer permiten que entre 3 y 9 usuarios de EZMeetup se registren y se comuniquen entre sí. Los usuarios accederán a sonidos e imágenes nítidas, de forma que las personas intervinientes puedan disfrutar de una videoconferencia de alta calidad independientemente de su ubicación.

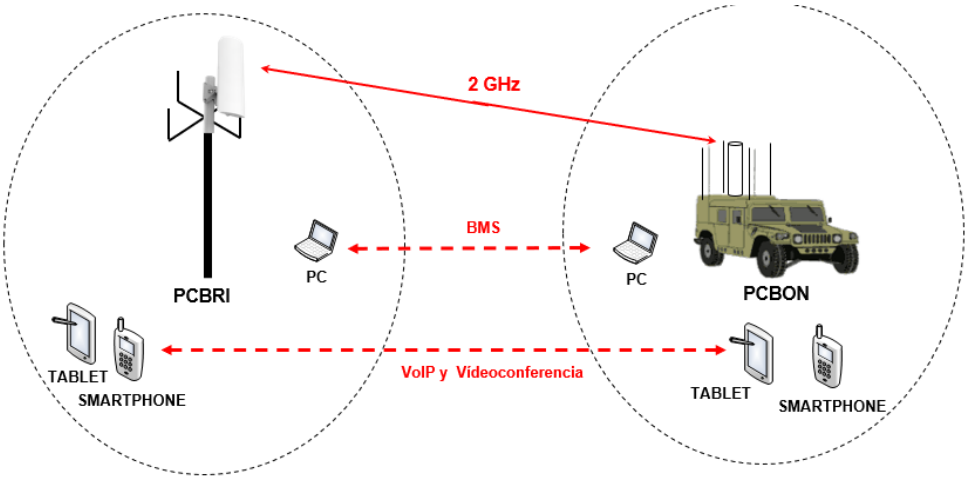


Figura 16. JCISAT. LTE. Pruebas de Servicios no simultáneas. Diseño propio.

Resultados:

El sistema de C2 de pequeñas Unidades BMS se probó conectando un nodo a la LAN PCBRI y otro nodo a la LAN PCBON, siendo el resultado satisfactorio, BMS no se pudo probar utilizando únicamente los dongle[19] LTE por problemas de licenciamiento de BMS, al estar asociado, entre otras cosas, a la MAC.

VoIP con PTT dio problemas 1 Servidor Virtual y 2 Servidores Físicos (1 PCBRI y 1 PCBON) a la hora de solicitar acceso al servidor del PCBRI perdía conexión siendo el servicio indisponible.

[19]Dongle-USB. es básicamente un dispositivo plug and play que te permite acceder a Internet mientras viajas. Algunos WiFi Dongles no se conectan a la computadora portátil o PC y funcionan independientemente para proporcionarle Internet Wi-Fi usando datos celulares.

3 PROYECTO DE INTEGRACIÓN.

Antes de desarrollar este capítulo, voy hacer un inciso, sobre el objetivo final del trabajo. Ya sabemos que técnicamente es viable la integración de la tecnología 5G en las SDR,s. De una forma simple se podría resumir que la integración sería una modificación del software de las radios el cual permitiera acceder a una BTS de 5G cercana o mediante la instalación de un CORE en propiedad 5G en las estaciones militares con cierta entidad. En capítulos anteriores se han presentado proyectos realizados por JCISAT en los cuales se han realizado prácticas de integración con tecnología LTE entre Puestos de Mando de entidad Brigada y Batallón, no utilizando radios tácticas ya que lo realizaron con mediante el uso de Tablet,s o smaphone,s. Actualmente ya hay empresas como Thales, Indra o Inster, que están desarrollado SDR,s que todas las funciones, modos y aplicaciones pueden ser configurados y reconfigurados por Software esto implica que los componentes tradicionalmente realizados con circuitos electrónicos tales como mezcladores, filtros, amplificadores, moduladores/demoduladores, detectores, etc. se implementan por software mediante algoritmos matemáticos.

Siendo las principales ventajas:

- Añadir flexibilidad al sistema, rápida reconfiguración del enlace y de sus parámetros de frecuencia, ancho de banda, modulaciones y potencia.
- Simplificar el número de circuitos y componentes reemplazándolos por Software.
- Permitir el trabajo simultáneo con varios esquemas o estándares.
- El Software es capaz de corregir imperfecciones del Hardware.
- La adición de nuevas funcionalidades o estándares como modulaciones, encriptaciones, etc. es inmediata cuando se realiza por software.
- Desarrollo, test y prototipo rápido.
- Reduce costes de desarrollo. Reducción de tamaño, peso y consumo.
- Permite rápida actualización de componentes (no necesita repuestos).

Es importante saber que existen en el mercado aplicaciones de diseño y prototipado de sistemas SDR como el MATLAB[20] y Simulink.

Otra forma de definir una radio definida por software (SDR), es como un dispositivo inalámbrico que consta de un extremo frontal de RF con una FPGA[21] o un sistema en chip (SoC)[22] programable para realizar funciones digitales. El hardware SDR disponible en el mercado puede transmitir y recibir señales en diferentes frecuencias para aplicar estándares inalámbricos, desde la radio FM hasta tecnología 5G, LTE y Wi-Fi.

---

[20] MATLAB es una plataforma de programación y cálculo numérico utilizada por millones de ingenieros y científicos para analizar datos, desarrollar algoritmos y crear modelos.

[21] Una **matriz de puertas lógicas programable en campo**[12] o **FPGA** (del inglés *field-programmable gate array*), es un dispositivo programable que contiene bloques de lógica cuya interconexión y funcionalidad puede ser configurada en el momento, mediante un lenguaje de descripción especializado. La lógica programable puede reproducir desde funciones tan sencillas como las llevadas a cabo por una puerta lógica o un sistema combinacional hasta complejos sistemas en un chip.

Las FPGA se utilizan en aplicaciones similares a los ASIC sin embargo son más lentas, tienen un mayor consumo de energía y no pueden abarcar sistemas tan complejos como ellos. A pesar de esto, las FPGA tienen las ventajas de ser reprogramables (lo que añade una enorme flexibilidad al flujo de diseño), sus costes de desarrollo y adquisición son mucho menores para pequeñas cantidades de dispositivos y el tiempo de desarrollo es también menor.

[22] Formalmente, se conoce a un SoC como un chip que **integra todas o la mayor parte de componentes necesarios para el funcionamiento de un ordenador.** Entre ellas se incluirá casi siempre una CPU, por lo que podemos hablar de un procesador que incluye más componentes en su interior que normalmente estarían relegados a chips externos a este.

Una vez considerado esto, y sobre todo teniendo en cuenta la distinta documentación de referencia para la implantación del 5G en el MINISDEF y la creación de Grupos de Trabajo sobre esta tecnología o sobre la adquisición de radios SDR para los distintos Ejércitos y Armada, lo que se va a desarrollar a continuación en una propuesta exclusivamente personal, sin haber tenido en cuenta las decisiones de los distintos grupos de trabajo creados para este fin, lo que quiero recalcar que esto seguramente no se lleve a cabo por distintas razones que no es el caso de comentar.

Se realizará una propuesta de los requisitos y necesidades operativas para poder hacer viable un proyecto en el cual se cumpla con la legislación vigente no solo marcada por el MINISDEF sino también con el CNI[23], con el fin de la poder conseguir una acreditación de Seguridad hasta nivel Difusión Limitada, que sería ideal para los puestos de mando de pequeñas unidades, ya que técnicamente esta integración es viable, como ya hemos visto en el ejemplo de LTE realizado por el personal de JCISAT.

3.1 Descripción de la solución para sistemas de Mando y Control. [8]

Dentro de los Escenarios Generales de empleo de las FAS, recogidos en la Estrategia Militar (CEFAS), la Directiva de Planeamiento Militar establece las Situaciones Operativas (SO,s) para la actualización de la Fuerza Conjunta. Para estas situaciones son fundamentales las Áreas de Capacidad de Mando y Control (C2) y de Conocimiento de la Situación.

El Área de Capacidad de Conocimiento de la Situación requiere unos sistemas de vigilancia, reconocimiento y obtención de datos tecnológicamente avanzados, integrados e interoperables que tras eficaces procesos de análisis proporcionen una inteligencia adecuada, precisa y oportuna.

Para el área de Mando y Control (C2), se requiere un sistema compuesto por personal adiestrado, procedimientos normalizados y un robusto, seguro y resistente Sistema de Información y Telecomunicaciones (CIS) con capacidad integración tanto en estructuras nacionales como multinacionales para su empleo

Estando relacionadas estas dos Áreas de Capacidad mencionadas al Sistema Conjunto de Radio Táctica (SCRT) que deberá proporcionar las capacidades de comunicaciones inalámbricas necesarias para las garantizar de forma segura y fiable el intercambio de información y que este sistema sea a vez interoperable con las nuevas tecnologías móviles.

El SCRT modernizará el sistema de comunicaciones radio tácticas al incluir dentro de sus capacidades a las Radios Definidas por Software y estas a su vez darán la posibilidad para interoperar con la tecnología móvil de 5G y futuras.

Esta modernización de los sistemas de comunicaciones tácticos proporcionará mayores capacidades a los Sistemas de Mando y Control y así como los Sistemas de Comunicaciones de las FAS.

Este estudio de aumento de las capacidades se desarrollará conforme a la documentación establecida por la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC)[24], para asegurar la interoperabilidad y el dominio de la información tanto en

[23] CNI. Centro Nacional de Inteligencia.

[24] La Orden DEF/2639/2015, de 3 de diciembre, establece la Política de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (Política CIS/TIC) y define la estructura de gobierno que permite su coordinación, control y seguimiento.

el ámbito nacional como aliado, cumpliendo con la establecido en las especificaciones de las Comunicaciones Tácticas que puedan derivarse de iniciativa de FMN (Federal Mission Networking).

El Planeamiento que debe guiar el desarrollo y obtención del SCRT debe estar acorde con los factores de Planeamiento de la Directiva de Política de Defensa 2020[25], así:

"La apuesta modernizadora de las Fuerzas Armadas emprendida recientemente tiene como objetivo añadido, además de la obtención de capacidades, el estimular y dar un entorno de confianza a la innovación en tecnologías de defensa. Así, los importantes proyectos y programas planteados contribuirán a los procesos de reorganización industrial para generar empleo, diversificar y acortar las cadenas de producción, garantizar el suministro, promover la innovación y consolidar la industria de defensa nacional en el marco de una base industrial y tecnológica europea cada vez más cooperativa y potente."

En relación con los objetivos de la Política de Defensa, recogido en la Política de Defensa 2020, el SCRT debe ser tener como principio:

"… Apoyar a la industria de defensa, contribuyendo a impulsar la economía y la base productiva nacional y a asegurar la resiliencia propia. Buscar el equilibrio entre desarrollos nacionales y programas con otras naciones -incluidos los acuerdos Gobierno a Gobierno- que aseguren la garantía de suministro y el desarrollo de una base industrial, tecnológica y de innovación nacional y europea en Defensa".

Por último, el SCRT deberá seguir las directrices para el planeamiento de la defensa, en el ámbito de las Capacidades militares, Tecnología e Industria.

"En el desarrollo de capacidades de defensa, se continuará apostando por mantenerse en la vanguardia tecnológica, reforzando la Base Tecnológica e Industrial (BTI) española, con una clara vocación europea e impulsando la Investigación, Desarrollo e Innovación de manera coordinada con otros ministerios, tratando de favorecer la dualidad de desarrollos siempre que las circunstancias lo permitan. Se favorecerá el empleo de alta cualificación y la competitividad de la industria nacional. El desarrollo de capacidades se basará en los siguientes criterios:

Asimismo, se potenciará la internacionalización de la industria nacional de defensa con las siguientes premisas:

- *Fomento de la cooperación industrial y tecnológica, como uno de los elementos principales de la Diplomacia de Defensa.*
- *Identificación de la Unión Europea y de la OTAN como escenarios prioritarios donde apoyar la internacionalización de la industria de defensa.*
- *Realizar un esfuerzo integrado y coordinado, buscando la colaboración de todos los departamentos ministeriales."*

En base a lo anteriormente expuesto, se significa que la obtención del SCRT debe basarse en el desarrollo de una base industrial, tecnológica y de innovación nacional y europea en Defensa. Esto obliga

[25] La Ley Orgánica de la Defensa Nacional 5/2005 y las directrices de la Directiva de Defensa Nacional 2020 promulgada por el Presidente del Gobierno el 11 de junio.

a un análisis y negociación muy exhaustiva de los planes industriales que deben de desarrollar los consorcios que opten a suministrar el SCRT en su totalidad o en parte.

La obtención del SCRT será muy dependiente de los recursos financieros comprometidos y de un escenario presupuestario estable.

En los actuales escenarios de operaciones, las unidades operativas se enfrentan a importantes amenazas en cuanto a la utilización de los sistemas de comunicaciones:

Ataques directos por parte del adversario o terceros actores para actuar en contra de la disponibilidad, confidencialidad, autenticidad e integridad de la información, así como de la integridad y disponibilidad de los sistemas de información, lo que obligará a la implantación de nuevas medidas de seguridad COMSEC, TRANSEC y NETSEC.

El colapso del sistema derivado del incremento del flujo de información en los momentos críticos de la operación, lo que obligará a gestionar la información de manera eficaz para evitar información redundante o innecesaria y asignar prioridades y perfiles de usuario en función de la fase en curso de la operación.

El efecto de estas amenazas se ve incrementado por la evolución tecnológica que incide sobre las vulnerabilidades técnicas de los equipos actuales y que agudizan otros aspectos como la falta de interoperabilidad o la necesidad creciente de mayores anchos de banda.

Los importantes avances tecnológicos en todos los campos de las telecomunicaciones han supuesto también un importante salto cualitativo en las capacidades militares, modificando la forma de empleo de la fuerza militar. Esto acentúa la importancia de continuar incorporando a las FAS aquellas tecnologías que permitan mantener la superioridad en el enfrentamiento dentro el espacio de batalla futuro. En este ámbito se encuadran los sistemas de Radio Definida por Software - SDR ("Software-Defined Radio") -.

El incremento notable del flujo de información en los momentos críticos de toda operación obliga a gestionar la información de manera eficaz. Asimismo, la flexibilidad necesaria para la reconfiguración de escenarios, planificación y rapidez de respuesta conlleva disponer de unas necesidades de comunicación para las cuales los sistemas radio SDR presentan notables ventajas técnicas por su reprogramabilidad de formas de onda operativas. Esto implica que esta capacidad de reprogramación de las formas de onda permita adaptarse e integrase a las frecuencias que utiliza la tecnología 5G, con unas simples modificaciones del Software.

En el entorno más amplio de los sistemas CIS, las operaciones conjuntas y combinadas, actuales y futuras, se desarrollan en ambientes que exigen un intercambio rápido y seguro de información entre fuerzas participantes, así como poder disponer de la misma en tiempo útil, en un ambiente dinámico, altamente móvil y lleno de riesgos y amenazas que dificultan la correcta operación de las comunicaciones y de los sistemas de información.

La necesidad de alta disponibilidad, confidencialidad, autenticidad e integridad de la información y de los sistemas que la intercambian, obliga también a actualizar las medidas de seguridad COMSEC, TRANSEC y NETSEC de los medios técnicos de comunicación sobre las que se sustentan. A este respecto, cobra vital importancia la capacidad de gestión y control del cifrado asociado a estas capacidades bajo soberanía Nacional, satisfaciendo los adecuados estándares de acreditación de seguridad para la gestión de la información a distintos niveles. Por ello, es necesario disponer del control,

conocimiento y acreditación de la arquitectura hardware y software interna de los equipos con objeto de adquirir además la capacidad de actualización y nacionalización de las formas de onda que se explotan sobre los mismos.

El potencial de la tecnología 5G en aplicaciones en el ámbito militar como son los sistemas de telecomunicaciones tácticas, mediante la utilización de las radios SDR, las cuales permiten la modificación de su configuración mediante software, permitirá la interoperabilidad de las distintas tecnologías ya sean desplegables o permanentes nacionales o multinacionales, proporcionado en ancho de banda deseado y la rápida transmisión de datos, que es lo que carecen hoy en día los medios radios de las unidades del Ejército de Tierra.

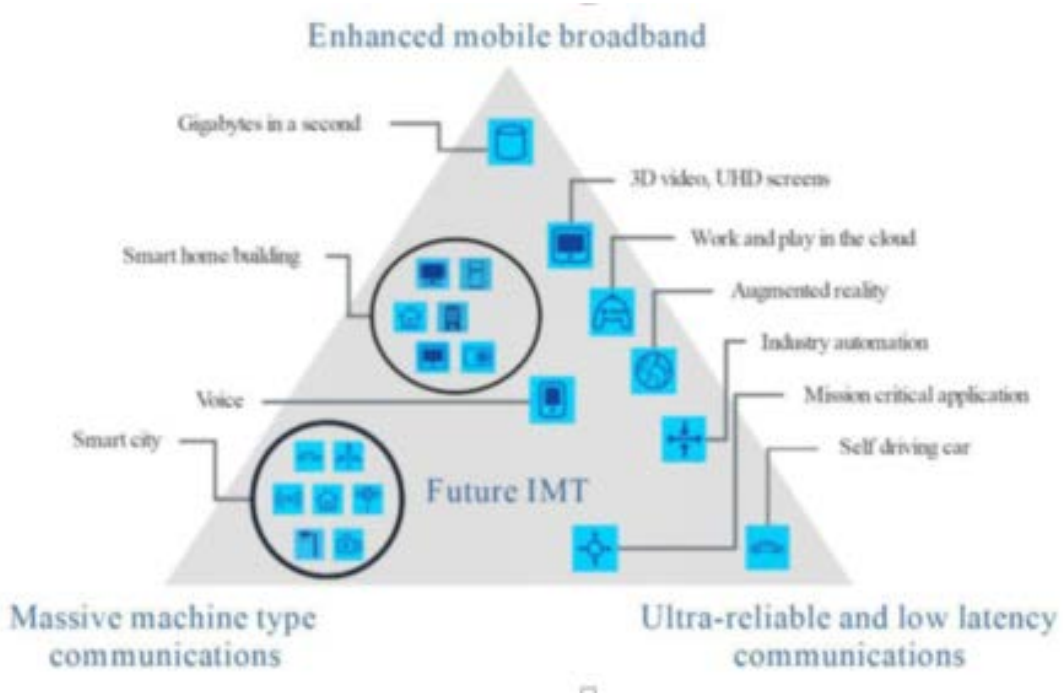


Figura 17 Casos de uso 5G en el MINISDEF. [El 5G transforma tu vida conectando el Internet de las cosas. - ARTÍCULO - YTTEK Technology Corp.]

Las redes 5G de próxima generación operarán en tres amplias bandas de radiofrecuencia, cada una de las cuales tienen diferentes características y aborda diferentes casos de uso. El espectro de baja frecuencia (sub-1GHz) es muy adecuado para la cobertura de área amplia e interior, y será importante para mejorar la cobertura móvil en áreas rurales desatendidas, así como en aplicaciones mMTC y URLLC. El espectro de frecuencia media (1-6GHz) admite una buena combinación de capacidad y cobertura, y es el enfoque inicial para eMBB y FWA, con mMTC a y URLLC a seguir. El espectro de alta frecuencia, también conocido como onda milimétrica o mmWave (>24GHz), admite velocidades muy altas y baja latencia dentro de áreas locales de "puntos calientes" y puede ofrecer eMBB "completo" y FWA de alta velocidad, aunque la cobertura en interiores es pobre.

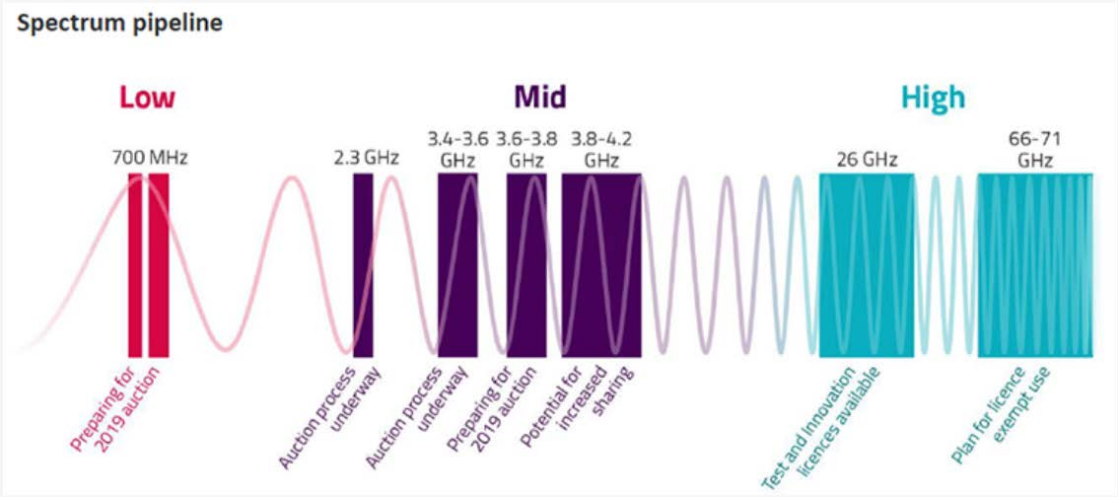


Figura 18 Espectro 5G. [La solución de diseño 5G se adapta al mercado real. - ARTÍCULO - YTTEK Technology Corp.]

Las frecuencias UHF (con capacidad de ser empleadas por las radios táctica) comprendidas entre 300 MHz y 3 GHz las cuales, se están readaptando para la tecnología 5G. La diversidad de frecuencias empleadas se puede adecuar a aplicaciones únicas dado que las frecuencias más altas se caracterizan por un ancho de banda mayor, aunque tienen un rango más corto. Las frecuencias de onda milimétrica son perfectas para zonas con una alta densidad de población, pero son ineficaces para las comunicaciones a larga distancia. Con estas bandas de frecuencias altas y más bajas destinadas a la tecnología 5G, las portadoras han comenzado a conformar sus pequeñas porciones propias de espectro 5G.

Otras características específicas para 5G de interés militar, son los denominados Proximity Services que permiten la comunicación entre terminales de usuario sin intervención de la estación base o la posibilidad de que 5G se extienda a redes no terrestres (SATCOM u otras como plataformas de alta altitud - HAPS u otras plataformas aéreas) , denominadas Non Terrestrial Networks (NTN,s) permitirá proporcionar estos servicios en zonas donde no exista esta infraestructura o permitirá la comunicación entre zonas distantes. El empleo de sistemas autónomos o semiautónomos facilitaría el desarrollo de esta capacidad.

Una vez tenido en cuenta los apartados anteriores sobre el empleo de la Tecnología 5G y las SDR,s en los posibles escenarios de interés en Operaciones Terrestres y Despliegue de Puestos de Mando (PC,s) en diferentes niveles permitiría el establecimiento rápido (aspecto particularmente critico en fases iniciales de despliegue) de redes de banda ancha inalámbrica de distinta cobertura (dependiendo de las bandas de frecuencias utilizadas y los requisitos de velocidad y ancho de banda así como el nivel de mando) posibilitando el enlace entre Puestos de Mando en el Área de Operaciones mediante sistemas aéreos o satélites aprovechando las posibilidades de 5G NTN. En cualquier caso, esta tecnología seria complementaria de las redes y medios tácticos (TACSAT, LOS, RRC) en el caso de despliegues de nivel Brigada o Batallón, en particular en ambiente de Guerra Electrónica (EW) favorable.

Las posibilidades proporcionadas por los servicios de Proximidad (Sidelink) que permiten utilizar las radios para comunicación entre ellas sin pasar por la estación Base también se aplican en este escenario, en particular para los escalones de Mando más bajos (ej Sección).

Cabe señalar que esto sería podría estar encuadrado la gestión de emergencias, en el caso de España en el seno de la UME que podría hacer uso de las posibilidades reseñadas incluyendo el Network Slicing para propósitos específicos extremo a extremo. En su caso sería una capacidad más, además de la disponible en SIRDEE y de sus medios tácticos.

Ejemplos de empleo 5G en Puestos de Mandos Desplegables:Figura 20. Empleo 5G en PC,s desplegables (Nivel Mando Componente o Nivel Operacional) y Figura 21 Empleo del 5G en PC,s desplegables (Nivel Brigada y Grupo Táctico)..

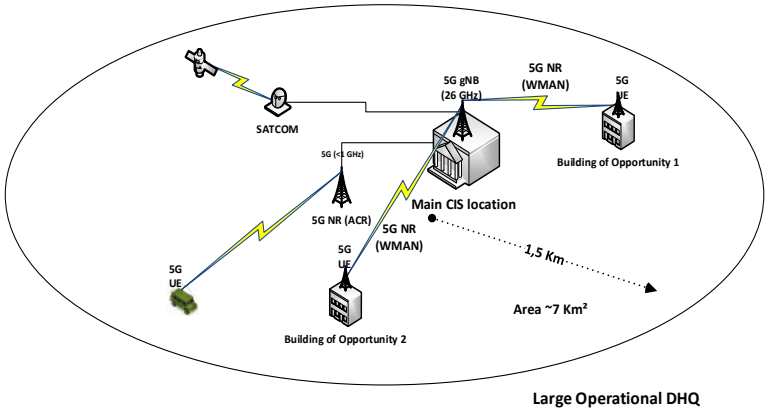


Figura 19. Empleo 5G en PC,s desplegables (Nivel Mando Componente o Nivel Operacional). **Diseño propio.**

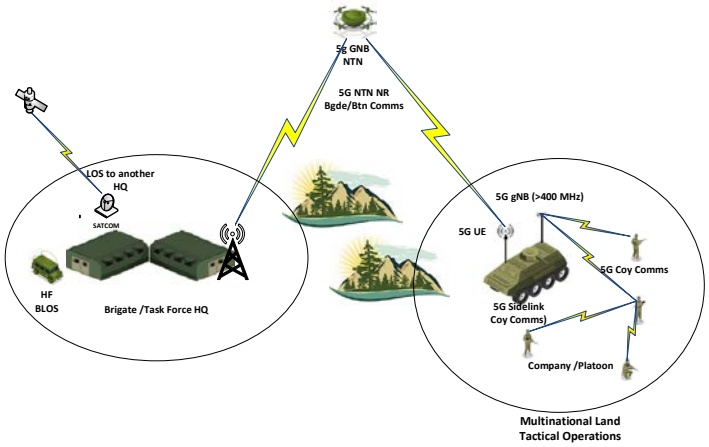


Figura 20 Empleo del 5G en PC,s desplegables (Nivel Brigada y Grupo Táctico). Diseño propio.

Se propone el siguiente modelo para su estudio, el cual implica la utilización del diseño por razones de seguridad en las comunicaciones de una nube privada en propiedad controlada por Defensa.

En los casos del ejemplo de las figuras 15 y 16, la nube privada será una infraestructura usada únicamente por las unidades implicadas en los despliegues, y a la cual solo tendrán acceso los usuarios designados por el Mando Operativo, además de que el acceso a los servicios que se tenga capacidad estará configurado según sus necesidades, lo cual permite tener una red a la medida y con unas condiciones de seguridad de la información óptimas.

Al requerirse un mayor control de la información, la administración de la nube privada debe de estar a cargo sólo de las propias unidades desplegadas, aunque en caso de ser necesario se puede recurrir a algún proveedor de confianza. Cabe recordar que su uso estará condicionado por la superioridad y el dominio sobre el enemigo del espectro electromagnético.

Se puede ejecutar en los PC, s de las unidades, para acceder a ella desde la web. Esto quiere decir que se puede abarcar, en un solo lugar, todos los procesos, servicios y aplicaciones del departamento de TI, lo cual facilita el rendimiento de los usuarios y su proactividad.

Los entornos que se ejecutan en la nube privada suelen brindar mayor seguridad, debido a que cuenta con recursos de acceso restringido. En el caso de un sistema como SAP[26] que maneja datos sensibles de las organizaciones, esto puede ser una gran ventaja. Siendo la probabilidad de filtración o perdida de datos menor.

Estará diseñada por los servicios que la unidad según su composición necesite, por lo tanto, es más personalizada y así las actualizaciones de SAP se programan de acuerdo con las necesidades de las misiones y del mandante de SAP.

Permite distribuir los recursos disponibles en tiempo real, en virtud de que las aplicaciones funcionan en todo momento.

El personal administrador de la nube privada tiene un mayor control sobre los servicios, recursos y las aplicaciones que se instalan.

El hardware estará acotado por las necesidades que se determinen y de los requerimientos técnicos de las soluciones de SAP.

La disponibilidad de la capacidad de procesamiento de datos o el uso de ciertas herramientas es exclusivo de los usuarios que tengan la necesidad de conocer.

Se pueden ejecutar de forma exclusiva ciertos protocolos o configuraciones, de acuerdo con las cargas de trabajo o los requerimientos de las soluciones de SAP.

3.2 Necesidad de diseño de una red definida por Software (SDN). [9]

Con el fin del diseño de una red propia para garantizar la seguridad en un despliegue se ha optado en este caso por la utilización de una red definida por software (SDN), ya que esta tecnología permite centralizar la lógica asociada al control de redes de comunicaciones, para el control de forma automatizada de los procesos operativos de red.

En SDN se separa físicamente el plano de encaminamiento de paquetes o plano de datos (forwarding o data plane) del plano de control (control plane). Esto difiere de las redes tradicionales, donde ambos planos coexisten en un mismo elemento de red. Donde el plano de control está compuesto por uno o varios componentes denominados controladores. Esto permite la gestión y el control de la red mediante

[26] El sistema SAP, acrónimo en inglés de “Systems, Aplications, Products in Data Processing” traducido al castellano como Sistemas, Aplicaciones y Productos Para el Procesamiento de Datos, son softwares de gestión empresarial que permiten la optimización de las tareas y los recursos con que disponen las empresas.

Fue inventado en Alemania en el año 1976, su nombre comercial fue SAP R/1 y fue ideado como un recurso de ayuda empresarial. Estaba estructurado a modo de capas. Dichas capas contaban con funciones que iban desde el diseño de presentaciones, hasta un software de control de negocios y una última capa dedicada a la gestión de datos.

Los sistemas SAP se componen de un soporte de software propio que es respaldado por un hardware. Basándose en estos dos elementos, permite tener un control más completo del personal humano, los recursos de la empresa, credenciales e inclusive otros programas informáticos utilizados por la empresa.

Con esto se busca centralizar las distintas dependencias de una empresa, lo que permite tener una visión general y detallada del estado de la compañía en tiempo real. Para lograrlo, los sistemas SAP están estructurados mediante distinto módulos, los cuales cuentan con herramientas y funciones para áreas específicas de cada empresa. Todas estas herramientas facilitan y reducen el tiempo necesario para cumplir las tareas. No obstante, estas herramientas no completan las tareas por sí mismas, sino que funcionan como un medio de apoyo para el personal humano que le use.

Por todo esto, los sistemas SAP guardan cierta relación con otros programas de asistencia empresarial como los ERP y los CRM. Aunque cada uno de estos cumplen tareas enfocadas a acciones específicas de un negocio (producción, atención al cliente, etc.).

software. Los equipos de red en el plano de datos únicamente se encargan de gestionar el tráfico en base a las órdenes recibidas del plano de control.

Un concepto muy relacionado con SDN es el de Virtualización de Funciones de Red (Network Function Virtualization) o NFV. Esta tecnología se basa en la virtualización de los diferentes elementos de una red (enrutadores, switches, cortafuegos, etc.), sirviéndose del hardware de red correspondiente a la capa de datos, para la implementación de dichos elementos o funciones de red.

Habitualmente, SDN y NFV se usan conjuntamente, con productos e infraestructuras basados en ambos paradigmas. Es común su integración con otros productos de virtualización, como hipervisores.

Esto nos daría acceso a las principales funcionalidades para el control y seguridad de nuestra red y así poder hacer frente a las vulnerabilidades de seguridad descritas en capítulos anteriores que puede presentar el uso de la tecnología 5G en nuestros sistemas de Mando y Control, que se relacionan a continuación:

1. Proporcionar a las aplicaciones una red de comunicaciones programable y configurable de forma centralizada, ofreciendo integración con elementos como hipervisores y orquestadores cloud, así como una API para el desarrollo de aplicaciones.
2. Proteger las máquinas y aplicaciones que hagan uso de la red, proporcionando servicios de protección de datos, cortafuegos, etc. Esto se lleva a cabo mediante la aplicación de políticas que prevengan ante actividad maliciosa, tanto para el tráfico intercambiado entre las máquinas conectadas a la red, como para el tráfico intercambiado con el exterior.
3. Definir grupos de máquinas en base a la aplicación o aplicaciones que ejecutan. Por ejemplo, una máquina que ejecute un servidor web con una máquina que contenga la base de datos asociada a esa aplicación web. Esto permite definir, a su vez, entornos de red para dichos grupos, como VLANs y redes privadas, aislándose del resto de máquinas conectadas a la red.
4. Automatizar procesos de gestión, despliegue y configuración de red, reduciendo la necesidad de realizar configuraciones manuales en los equipos que conforman la red.

Para nuestro caso en base a las funcionalidades y características del desarrollo que se quiere implantar para la integración de la tecnología 5G en las SDR, para el acceso a los sistemas de Mando y Control de Pequeñas Unidades debido a la poca disponibilidad de espacio en las plataformas móviles terrestres se va a hacer uso del producto basado en Software, compuesto por varios componentes que controlan el plano de datos, compuesto por equipos de red hardware, encargados del manejo del tráfico y que no forman parte del producto. Estos equipos pueden ser switches y routers tradicionales, o equipos diseñados para trabajar en entornos SDN, el producto también se integra con aplicaciones y servicios, o un hipervisor que soporta las máquinas virtuales donde se ejecutan las diferentes aplicaciones que hacen uso de la red. En muchos casos, el propio producto se puede ejecutar en una o varias máquinas virtuales soportadas por dicho hipervisor.

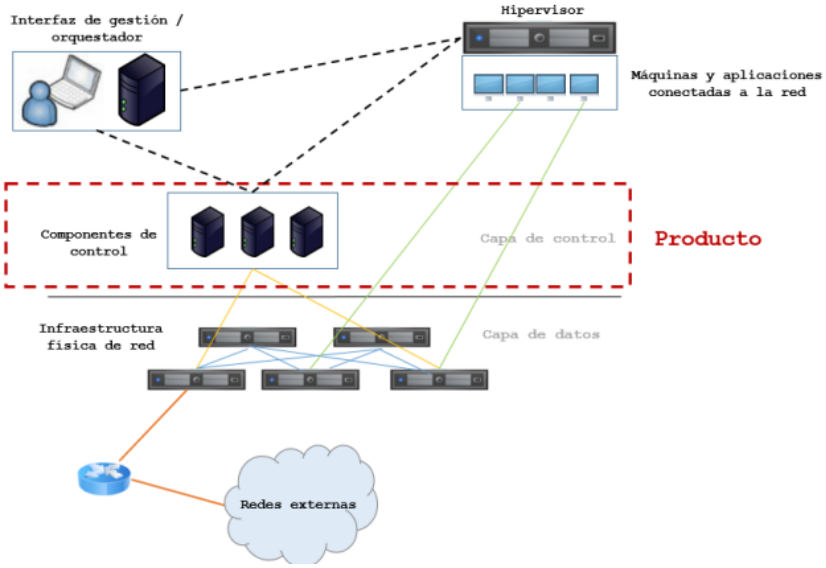


Figura 21 Producto Basado en Software. STIC 140 [9].

Estos productos son habitualmente usados en entornos de Centros de Datos (Data Centers) que en el caso que nos conlleva serán muy reducidos. Su uso proporciona una importante reducción de costes al operador del centro de datos, ya que permite un mejor aprovechamiento de los recursos, así como la automatización de procesos de despliegue, mantenimiento y configuración de red.

Para la utilización en condiciones óptimas de seguridad de los productos de Redes Definidas por Software (SDN), es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

Plataforma segura: El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.

Protección física: Los componentes del producto deberán instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.

Administración confiable: El administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la administración. Por ello, se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención maliciosa. Estará a cagar siempre de un militar con especialidad en Sistemas de Información y con las pertinentes acreditaciones de seguridad.

Flujo de información en red: El intercambio de información en la red deberá ser controlado por el producto, mediante la configuración y aplicación de políticas de filtrado de tráfico.

Actualizaciones periódicas: El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2[27] o superior (Evaluation Assurance Level), que contenga los SFR (Requisitos Fundamentales de Seguridad).

[27] EAL. El Nivel de Garantía de Evaluación de un producto o sistema de TI es una calificación numérica asignada después de completar una evaluación de seguridad de Common Criteria, un estándar internacional vigente desde 1999. Los crecientes niveles de garantía reflejan requisitos de garantía adicionales que deben cumplirse para lograr la certificación Common Criteria. La intención de los niveles superiores es proporcionar una mayor confianza en que las principales

A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC[28] en esta familia:

-Administración confiable. Podrán ser cubiertos por el producto o por su entorno operacional. Mitigando el Acceso a las funciones de seguridad donde un atacante podría acceder y modificar las funciones y datos de seguridad del producto.

-Identificación y autenticación. Mitigan el Acceso a información almacenada por la cual un atacante podría acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto y el Acceso a las funciones de seguridad.

-Auditoría. Mitiga la amenaza de Actividad no detectada donde un atacante podría acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.

Canal Seguro. Mitigan ataques a la red, por lo que un atacante, desde dentro o desde fuera de la red, podría acceder y/o modificar la información intercambiada entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.

Instalación y actualizaciones confiables. Mitigan ataques locales. Un atacante podría actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.

-Protección de credenciales y datos sensibles. Mitigan ataques al Acceso a información almacenada. Un atacante podría acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.

-Requisitos criptográficos. Mitigan ataque a la red y a la información almacenada.

---

características de seguridad del sistema se implementan de manera confiable. El nivel EAL no mide la seguridad del sistema en sí, simplemente indica a qué nivel se probó el sistema.

Para lograr un EAL particular, el sistema informático debe cumplir con *requisitos de garantía* específicos. La mayoría de estos requisitos implican documentación de diseño, análisis de diseño, pruebas funcionales o pruebas de penetración. Las EAL más altas implican documentación, análisis y pruebas más detalladas que las más bajas. Lograr una certificación EAL más alta generalmente cuesta más dinero y lleva más tiempo que lograr una más baja. El número EAL asignado a un sistema certificado indica que el sistema completó todos los requisitos para ese nivel.

Aunque cada producto y sistema debe cumplir con los mismos requisitos *de garantía* para alcanzar un nivel particular, no tienen que cumplir con los mismos requisitos *funcionales*. Las características funcionales de cada producto certificado se establecen en el documento *Security Target* adaptado para la evaluación de ese producto. Por lo tanto, un producto con un EAL más alto no es necesariamente "más seguro" en una aplicación en particular que uno con un EAL más bajo, ya que pueden tener listas muy diferentes de características funcionales en sus objetivos de seguridad. La idoneidad de un producto para una aplicación de seguridad determinada depende de la eficacia de las características enumeradas en el objetivo de seguridad del producto para cumplir los requisitos de seguridad de la aplicación. Si los objetivos de seguridad para dos productos contienen las características de seguridad necesarias, entonces el EAL más alto *debe* indicar el producto más confiable para esa aplicación.

EAL2 requiere la cooperación del desarrollador en términos de la entrega del diseño información y resultados de las pruebas, pero no debe exigir más esfuerzo por parte del desarrollador que es consistente con las buenas prácticas comerciales. Como tal, no debería requieren una inversión sustancialmente mayor de costo o tiempo. Por lo tanto, EAL2 es aplicable en aquellas circunstancias en las que los desarrolladores o usuarios requieren un Nivel bajo a moderado de seguridad garantizada independientemente en ausencia de Disponibilidad del registro de desarrollo completo. Tal situación puede darse cuando Protección de los sistemas heredados. Nivel de garantía de evaluación - Wikipedia, la enciclopedia libre.

[28] CPSTIC. Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones.

-Switching lógico. Esta funcionalidad de seguridad mitigan ataques a la red y al tráfico no autorizado (Uno o varios de los endpoints conectados a la red podrían realizar intercambios de tráfico no autorizado con otras máquinas y aplicaciones o con el exterior, lo que podría ser aprovechado por un atacante para explotar vulnerabilidades).

-Firewall Lógico. Esta funcionalidad mitiga las amenazas a la red y al tráfico no autorizado.

3.3 Desarrollo de una arquitectura de seguridad para el acceso en la nube [10].

En relación a la Resolución 307/08136/21 [1], de 17 de mayo de 2021, del Secretario de Estado de Defensa, por la que se establece la Estrategia de Explotación de la Nube en el Ministerio, en este apartado se va a definir una arquitectura de seguridad para el acceso a la nube definida en la STIC 499 [10].

La arquitectura planteada debe tomarse como una solución que dan respuesta a la necesidad de utilizar servicios en la nube cuando se maneja información que, por sus características, requiere de medidas especiales de protección. En ningún momento deben tomarse como un conjunto exclusivo y limitante de soluciones, ya que pueden existir otras alternativas igualmente válidas que cumplan con los requisitos establecidos por la normativa vigente para cada ámbito y que deberán analizarse caso por caso.

Los servicios en la nube adoptan un modelo de responsabilidad compartida en el que pueden existir diferentes actores con diferentes responsabilidades, resumiéndose en dos:

Usuario/Cliente y Administrador/Proveedor. Se asume que el primero es el organismo que consume el servicio y el segundo el que lo ofrece, total o parcialmente. En caso de existir más actores deberá analizarse qué medidas de las planteadas son responsabilidad de cada uno.

El usuario deberá implementar aquellas medidas que se definan bajo su responsabilidad y exigir al proveedor cuando contrata el servicio que cumpla con las definidas bajo responsabilidad del proveedor. Por lo tanto, no se han detallado aquellas medidas que debe implementar el proveedor sobre las cuales no tiene visibilidad el cliente, ya que se suponen garantizadas por las distintas auditorías de seguridad a las que se debe someter el proveedor del servicio y que el cliente debe exigir.

Por lo que se establecen los siguientes modelos de despliegue de la nube:

1. Nube pública. La infraestructura de esta nube está mantenida y gestionada por terceras personas no vinculadas con la organización proporcionando recursos de forma abierta a entidades heterogéneas, sin más que un contrato con el mismo proveedor que controla dicha infraestructura.
2. Nube privada. La infraestructura de esta nube o servicios provistos son completamente dedicados para un solo cliente que controla qué aplicaciones debe ejecutarse y dónde (infraestructura bajo demanda). Puede ser en propiedad, ser administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones. La nube pública presenta flexibilidad de contratación y la nube privada, en la mayoría de los casos, exige determinados compromisos de consumo o permanencia.
3. Nube híbrida. Los servicios se ofrecen de forma pública y privada. Un usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.
4. Nube comunitaria. La infraestructura de esta nube o servicios provistos son compartidos en comunidad cerrada por varias organizaciones relacionadas entre ellas y que comparten requisitos con la finalidad de servir a una función o propósito común (seguridad, política…). La nube

comunitaria puede ser propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas.

Dentro de estos modelos de nube, para nuestro proyecto nos centraremos en el modelo 2 Nube privada y el 4 Nube Comunitaria. No descartando los demás modelos ya que como se ha explicado anteriormente todo depende del entorno operativo donde se encuentren desplegadas nuestros medios CIS y sobre todo condicionado por el control del espectro electromagnético.

Sobre las categorías de servicio que ofrece el empleo de la nube, eligiéremos la infraestructura como servicio (IaaS) que es un tipo de servicio de informática en la nube que ofrece recursos esenciales de proceso, almacenamiento y redes a petición.

IaaS es uno de los cuatro tipos de servicios en la nube, junto con el software como servicio (SaaS), la plataforma como servicio (PaaS) y la tecnología sin servidor.

IaaS ayuda a reducir el mantenimiento de los centros de datos locales, a ahorrar dinero en los costes de hardware y a obtener información empresarial en tiempo real. Las soluciones de IaaS ofrecen la flexibilidad necesaria para escalar y reducir verticalmente los recursos de TI a petición. También ayudan a aprovisionar rápidamente nuevas aplicaciones y a aumentar la confiabilidad de la infraestructura subyacente.

IaaS permite evitar el coste y la complejidad de comprar y administrar servidores físicos e infraestructura de centro de datos. Cada recurso se ofrece como un componente de servicio aparte. El proveedor de servicios informáticos en la nube[29] administra la infraestructura, mientras que el administrador, instala, configura y administra el propio software (sistemas operativos, middleware y aplicaciones).

En la figura 23, se determina como quedaría definida y delimitada IaaS dentro de las categorías de servicio que nos puede proporcionar la nube, en caso de uso en el MINISDEF.

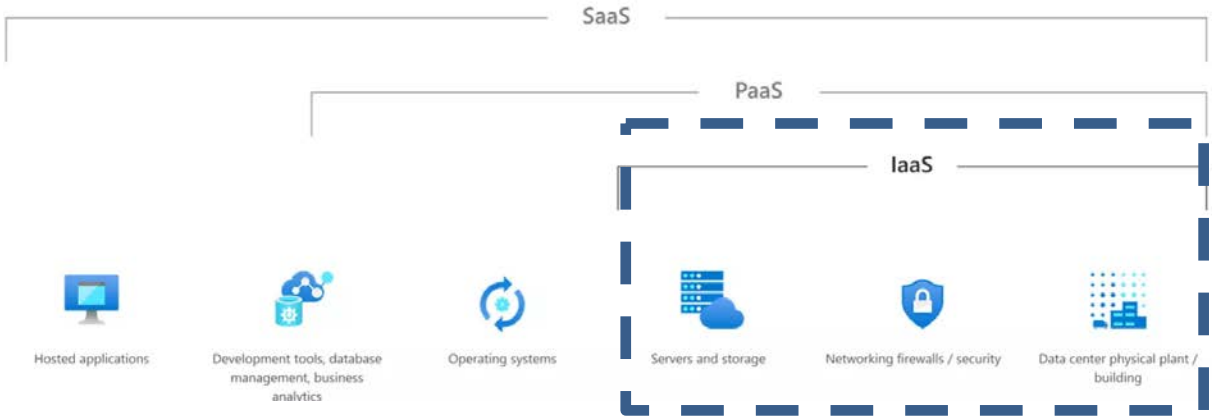


Figura 22. Tipos de Servicios en la Nube. AaaS, PaaS y IaaS. [https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iaas/ [9]](https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iaas/)

[29] El proveedor de servicios en la nube, en el caso del MINISDEF es el CESTIC. Por lo que los costes o adquisición de servicios no recae en el usuario. Además de tratarse de redes securizadas la administración de las aplicaciones, versionado de las existentes se realizan manualmente y no mediante plataforma Web.

3.3.1 Resposibilidad de seguridad "de" y "en".

En esta categoría de servicio, el proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red. Siendo los aspectos relacionados con la conformidad y la seguridad son una responsabilidad compartida entre proveedor o CSP (Cloud Service Provider) y el Cliente o CSC (Cloud Service Customer), tal como se muestra en la Figura 24. "Modelo de Responsabilidad compartida en IaaS".

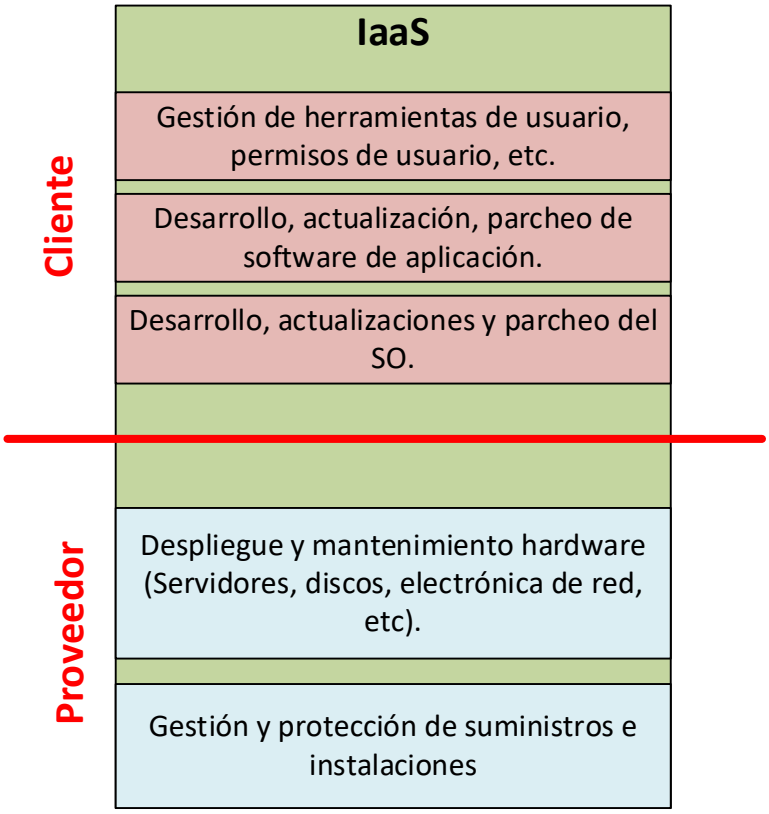


Figura 23. Modelo de Responsabilidad compartida en IaaS. [10]

Esta manera se puede distinguir seguridad "de" y seguridad "en" la nube, identificado los responsables en cada caso:

1. Seguridad "de" la nube. El proveedor o CSP será responsable de la seguridad de los servicios que provea al cliente, así como de cumplir aquellos acuerdos de nivel de servicio que establezca. Abarcará la seguridad del hardware, el software, las redes y las instalaciones que ejecutan servicios en la nube.
2. Seguridad "en" la nube. La responsabilidad del cliente o CSC estará limitada a la seguridad de los servicios que despliegue sobre la nube que no sean propietarios del CSP, así como de las configuraciones que establezca, en base a sus capacidades dependiendo de la categoría del servicio que haya contratado.

Los objetivos de seguridad de la arquitectura objeto del diseño serán los siguientes:

1. Control de la información: El servicio en la nube deberá tener la capacidad de manejar de manera segura información sensible o clasificada que demande protección en cualquiera de sus dimensiones de seguridad, en su almacenamiento, procesamiento y transmisión. Para ello, deberá implementar:
    a. Control de los flujos de información: Los flujos de información estarán restringidos, físicamente o mediante configuración software, a las interfaces habilitadas. Se protegerá la confidencialidad, integridad y autenticidad y se impedirá el establecimiento de canales encubiertos que faciliten la transmisión no autorizada de información.
    b. Aislamiento de datos. La tenencia múltiple y la compartición de recursos son características inherentes de la computación en la nube. El servicio deberá garantizar la separación de los recursos asignados al usuario, de forma que no se produzca trasvase de información entre recursos, salvo que esté debidamente autorizado, en cuyo caso deberán estar controlados y monitorizados.
    c. Acceso autorizado a la información. El servicio debe garantizar el acceso a la información.
2. Protección del servicio. El servicio deberá protegerse de ataques (actualizaciones no permitidas, malware, etc.) que puedan alterar su correcto funcionamiento y en especial sus funcionalidades de seguridad críticas, así como de ataques que puedan afectar a su disponibilidad.
3. Cumplimiento normativo. El Sistema deberá implementar medidas orientadas a comprobar la efectividad de las prácticas de gestión de datos del proveedor y verificar que dichas prácticas están de acuerdo a lo establecido en la ley.

Por la que establecerán las siguientes medidas de seguridad, en el cual se procederá a un modelo de responsabilidad compartida en dos niveles el CSC y CSP, estando asociadas al cliente, al proveedor o a ambos, sin impedir que otras medidas de seguridad que deban aplicarse según la normativa específica respecto a la información que se maneja. Se enumeran a continuación las medidas de seguridad a implementar en 17 dominios técnicos:

1. Dominio 1(D1). Auditoría y Aseguramiento.
    a. Auditoría del Sistema de Información. ASI.
    b. Sometimiento Jurisdiccional. SJD.
2. Dominio 2 (D2). Seguridad de aplicaciones e Interfaces.
    a. Cualificación del Servicio en la Nube. CSN y Cualificación de Producto. CPN.
    b. Aprobación Requisitos de Aprobación de Productos (ASN) y Requisitos de Aprobación de Servicios en la Nube (APN).
3. Dominio 3 (D3). Gestión de Continuidad y Resiliencia de Operaciones.
    a. Acuerdo de Servicio (SLA).
        i. Disponibilidad del Sistema.
        ii. Prestaciones.
        iii. Consecuencias de no cumplimiento.
        iv. Disposiciones que limiten los cambios implementados por el CSP que puedan impactar directamente en la infraestructura del CSC.
    b. Copias de Seguridad (BCK).
4. Dominio 4 (D4). Control de Cambios y Gestión de Configuración.

   a. Gestión de la Configuración. (GCF).
5. Dominio 5 (D5). Cifrado, Criptografía y Gestión de Claves.
   a. Protección de las Comunicaciones (PCM).
   b. Protección de Soportes (PSI).
   c. Gestión de Claves (GCK).
6. Dominio 6 (D6). Seguridad en el Centro de Procesamiento de Datos (CPD).
7. Dominio 7 (D7): Gestión de la Privacidad y la Seguridad del Dato. Confidencialidad, Integridad y Disponibilidad.
   a. Firewall de Aplicación Web (WAF).
   b. Prevención de Fuga de Datos (DLP).
   c. Cloud Access Security Broker (CASD).
   d. Borrado Seguro (BSD).
8. Dominio 8 (D8). Gobernanza, Riesgo y Cumplimiento.
9. Dominio 9 (D9). Recursos Humanos.
   a. Gestión de Usuarios. (GUS).
10. Dominio 10. (D10). Gestión de Identidad y Acceso.
   a. Control de Acceso (CAC).
   b. Identificación y Autentificación (I&A).
   c. Control de Sesión (CSS).
11. Dominio 11 (D11). Interoperabilidad y portabilidad.
12. Dominio 12 (D12). Infraestructura y Virtualización.
   a. Gestión de Infraestructura (GIV).
   b. Aislamiento de Datos y Recursos (ADR).
   c. Separación Hardware (SHW).
   d. Ubicación Hardware (UHW).
   e. Protección del Perímetro (PDP).
   f. Segregación de Redes (SGR).
13. Dominio 13. (D13). Registro y monitorización.
   a. Gestión de Eventos (GES).
14. Dominio 14 (D14). Gestión de Incidentes de Seguridad E-Discovery y Forense en la Nube.
15. Dominio 15 (D15). Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.
16. Dominio 16 (D16). Gestión de Vulnerabilidades y Amenazas.
   a. Gestión de Actualizaciones (GAC).

17. Dominio 17 (D17). Gestión del Endpoint.
   a. Gestión del Endpoint (GEP).

El Análisis de seguridad para arquitecturas Iaas como se ha indicado anteriormente en el caso de operación, mantenimiento y configuración de la capa de infraestructura es responsabilidad del CSP, quedando la parte de plataforma y servicios como responsable el CSC.

En la siguiente tabla se presenta un resumen de las medidas a implementar en el sistema dependiendo del nivel de clasificación de la información que se va a manejar. Siendo el nivel L1 el de un sistema sin clasificar y el L2 corresponde a Difusión Limitada.

Esta manera se puede distinguir de seguridad “de” y seguridad “en” la nube, identificado los responsables en cada caso:

3. Seguridad de la nube. El proveedor o CSP será responsable de la seguridad de los servicios que provea al cliente, así como de cumplir aquellos acuerdos de nivel de servicio que establezca. Abarcará la seguridad del hardware, el software, las redes y las instalaciones que ejecutan servicios en la nube.
4. Seguridad en la nube. La responsabilidad del cliente o CSC estará limitada a la seguridad de los servicios que despliegue sobre la nube que no sean propietarios del CSP, así como de las configuraciones que establezca, en base a sus capacidades dependiendo de la categoría del servicio que haya contratado.

Los objetivos de seguridad de la arquitectura objeto del diseño serán los siguientes:

4. Control de la información: El servicio en la nube deberá tener la capacidad de manejar de manera segura información sensible o clasificada que demande protección en cualquiera de sus dimensiones de seguridad, en su almacenamiento, procesamiento y transmisión. Para ello, deberá implementar:
    a. Control de los flujos de información: Los flujos de información estarán restringidos, físicamente o mediante configuración software, a las interfaces habilitadas. Se protegerá la confidencialidad, integridad y autenticidad y se impedirá el establecimiento de canales encubiertos que faciliten la transmisión no autorizada de información.
    b. Aislamiento de datos. La tenencia múltiple y la compartición de recursos son características inherentes de la computación en la nube. El servicio deberá garantizar la separación de los recursos asignados al usuario, de forma que no se produzca trasvase de información entre recursos, salvo que esté debidamente autorizado, en cuyo caso deberán estar controlados y monitorizados.
    c. Acceso autorizado a la información. El servicio debe garantizar el acceso a la información.
5. Protección del servicio. El servicio deberá protegerse de ataques (actualizaciones no permitidas, malware, etc.) que puedan alterar su correcto funcionamiento y en especial sus funcionalidades de seguridad críticas, así como de ataques que puedan afectar a su disponibilidad.
6. Cumplimiento normativo. El Sistema deberá implementar medidas orientadas a comprobar la efectividad de las prácticas de gestión de datos del proveedor y verificar que dichas prácticas están de acuerdo a lo establecido en la ley.

Por la que establecerán las siguientes medidas de seguridad, en el cual se procederá a un modelo de responsabilidad compartida en dos niveles el CSC y CSP, estando asociadas al cliente, al proveedor o a ambos, sin impedir que otras medidas de seguridad que deban aplicarse según la normativa específica respecto a la información que se maneja. Se enumeran a continuación las medidas de seguridad a implementar en 17 dominios técnicos:

18. Dominio 1(D1). Auditoría y Aseguramiento.
    a. Auditoría del Sistema de Información. ASI.
    b. Sometimiento Jurisdiccional. SJD.
19. Dominio 2 (D2). Seguridad de aplicaciones e Interfaces.
    a. Cualificación del Servicio en la Nube. CSN y Cualificación de Producto. CPN.
    b. Aprobación Requisitos de Aprobación de Productos (ASN) y Requisitos de Aprobación de Servicios en la Nube (APN).
20. Dominio 3 (D3). Gestión de Continuidad y Resiliencia de Operaciones.
    a. Acuerdo de Servicio (SLA).
        i. Disponibilidad del Sistema.
        ii. Prestaciones.
        iii. Consecuencias de no cumplimiento.

iv. Disposiciones que limiten los cambios implementados por el CSP que puedan impactar directamente en la infraestructura del CSC.

b. Copias de Seguridad (BCK).

21. Dominio 4 (D4). Control de Cambios y Gestión de Configuración.
    a. Gestión de la Configuración. (GCF).
22. Dominio 5 (D5). Cifrado, Criptografía y Gestión de Claves.
    a. Protección de las Comunicaciones (PCM).
    b. Protección de Soportes (PSI).
    c. Gestión de Claves (GCK).
23. Dominio 6 (D6). Seguridad en el Centro de Procesamiento de Datos (CPD).
24. Dominio 7 (D7): Gestión de la Privacidad y la Seguridad del Dato. Confidencialidad, Integridad y Disponibilidad.
    a. Firewall de Aplicación Web (WAF).
    b. Prevención de Fuga de Datos (DLP).
    c. Cloud Access Security Broker (CASD).
    d. Borrado Seguro (BSD).
25. Dominio 8 (D8). Gobernanza, Riesgo y Cumplimiento.
26. Dominio 9 (D9). Recursos Humanos.
    a. Gestión de Usuarios. (GUS).
27. Dominio 10. (D10). Gestión de Identidad y Acceso.
    a. Control de Acceso (CAC).
    b. Identificación y Autentificación (I&A).
    c. Control de Sesión (CSS).
28. Dominio 11 (D11). Interoperabilidad y portabilidad.
29. Dominio 12 (D12). Infraestructura y Virtualización.
    a. Gestión de Infraestructura (GIV).
    b. Aislamiento de Datos y Recursos (ADR).
    c. Separación Hardware (SHW).
    d. Ubicación Hardware (UHW).
    e. Protección del Perímetro (PDP).
    f. Segregación de Redes (SGR).
30. Dominio 13. (D13). Registro y monitorización.
    a. Gestión de Eventos (GES).
31. Dominio 14 (D14). Gestión de Incidentes de Seguridad E-Discovery y Forense en la Nube.
32. Dominio 15 (D15). Gestión de la Cadena de Suministro, Transparencia y Responsabilidad.
33. Dominio 16 (D16). Gestión de Vulnerabilidades y Amenazas.
    a. Gestión de Actualizaciones (GAC).
34. Dominio 17 (D17). Gestión del Endpoint.
    a. Gestión del Endpoint (GEP).

El Análisis de seguridad para arquitecturas Iaas como se ha indicado anteriormente en el caso de operación, mantenimiento y configuración de la capa de infraestructura es responsabilidad del CSP, quedando la parte de plataforma y servicios como responsable el CSC.

En la “Tabla 3-1 Medidas de Seguridad para la Arquitectura Iaas", se presenta un resumen de las medidas a implementar en el sistema dependiendo del nivel de clasificación de la información que se va a manejar. Siendo el nivel L1 el de un sistema sin clasificar y el L2 corresponde a Difusión Limitada.

		IaaS	
		SIN CLASIFICAR	DIF. LIMITADA
Dominio 1(D1). Auditoría y Aseguramiento.			
Auditoría del Sistema de Información. ASI	CPS	L1	L2
	CSC	L1	L2
Sometimiento Jurisdiccional. SJD.	CPS	L1	L2
	CSC	L1	L2
Dominio 2 (D2). Seguridad de aplicaciones e Interfaces.			
Cualificación del Servicio en la Nube. CSN.	CPS	L1	--
	CSC	L1	--
Cualificación de Producto. CPN.	CPS	--	--
	CSC	L1	--
Aprobación Requisitos de Aprobación de Productos (ASN)	CPS	--	L1
	CSC	--	L1
Requisitos de Aprobación de Servicios en la Nube (APN).	CPS	--	L1
	CSC	--	L1
Dominio 3 (D3). Gestión de Continuidad y Resiliencia de Operaciones.			
Acuerdo de Servicio (SLA).	CPS	L1	L1
	CSC	--	--
Copias de Seguridad (BCK).	CPS	--	--
	CSC	L1	L2
Dominio 4 (D4). Control de Cambios y Gestión de Configuración.			
Gestión de la Configuración. (GCF).	CPS	--	--
	CSC	L1	L2

		IaaS	
		SIN CLASIFICAR	DIF. LIMITADA
Dominio 5 (D5). Cifrado, Criptografía y Gestión de Claves.			
Protección de las Comunicaciones (PCM).	CPS	L1	L1
	CSC	L1	L2
Protección de Soportes (PSI).	CPS	--	--
	CSC	L1	L2
Gestión de Claves (GCK).	CPS	--	--
	CSC	L1	L2
Dominio 7 (D7): Gestión de la Privacidad y la Seguridad del Dato. Confidencialidad, Integridad y Disponibilidad.			
Firewall de aplicación Web (WAF).	CPS	--	--
	CSC	L1	L2
Prevención de Fuga de Datos (DLP).	CPS	--	--
	CSC	L1	L1
Cloud Access Security Broker (CASD).	CPS	--	--
	CSC	L1	L1
Borrado Seguro de datos (BSD).	CPS	L1	L2
	CSC	L1	L2
Dominio 9 (D9). Recursos Humanos.			
Gestión de Usuarios. (GUS).	CPS	--	L2
	CSC	L1	L2
Dominio 10. (D10). Gestión de Identidad y Acceso.			
Control de Acceso (CAC).	CPS	--	--
	CSC	L1	L2
Identificación y Autentificación (I&A).	CPS	--	--
	CSC	L1	L1
Control de Sesión (CSS).	CPS	--	--
	CSC	L1	L2

		IaaS	
		SIN CLASIFICAR	DIF.LIMITADA
Dominio 12 (D12). Infraestructura y Virtualización.			
Gestión de Infraestructura virtualizada (GIV).	CPS	L1	L1
	CSC	L1	L1
Aislamiento de Datos y Recursos (ADR).	CPS	--	--
	CSC	--	L1
Separación Hardware (SHW).	CPS	--	L1
	CSC	--	--
Ubicación Hardware (UHW).	CPS	L1	L2
	CSC	--	--
Protección del Perímetro (PDP).	CPS	L1	L2
	CSC	L1	L2
Segregación de Redes (SGR).	CPS	--	--
	CSC	L1	L2
Dominio 13. (D13). Registro y monitorización.			
Gestión de Eventos (GES).	CPS	--	--
	CSC	L1	L1
Dominio 16 (D16). Gestión de Vulnerabilidades y Amenazas.			
Gestión de Actualizaciones (GAC).	CPS	--	--
	CSC	L1	L1
Dominio 17 (D17). Gestión del Endpoint.			
Gestión del Endpoint (GEP).	CPS	--	--
	CSC	L1	L2

Tabla 3-1 Medidas de Seguridad para la Arquitectura Iaas.

En la siguiente se presenta un resumen de las medidas de seguridad asociadas a cada uno de los actores para implementar esta arquitectura en nuestros sistemas CIS para poder utilizar la tecnología 5G con garantías seguridad.

Se diferencia debido al nivel de clasificación de la información dos tipos de arquitecturas una sería la no clasificada y la otra con clasificación hasta “Difusión Limitada”.

Medidas de Seguridad en la IaaS en nube con información Sin clasificar. Véase **Figura 25. "Medidas de Seguridad en la IaaS Sin Clasificar. STIC 499" y Figura 26."Diagrama IaaS para manejar Información Sin Clasificar. STIC 499.** [10]

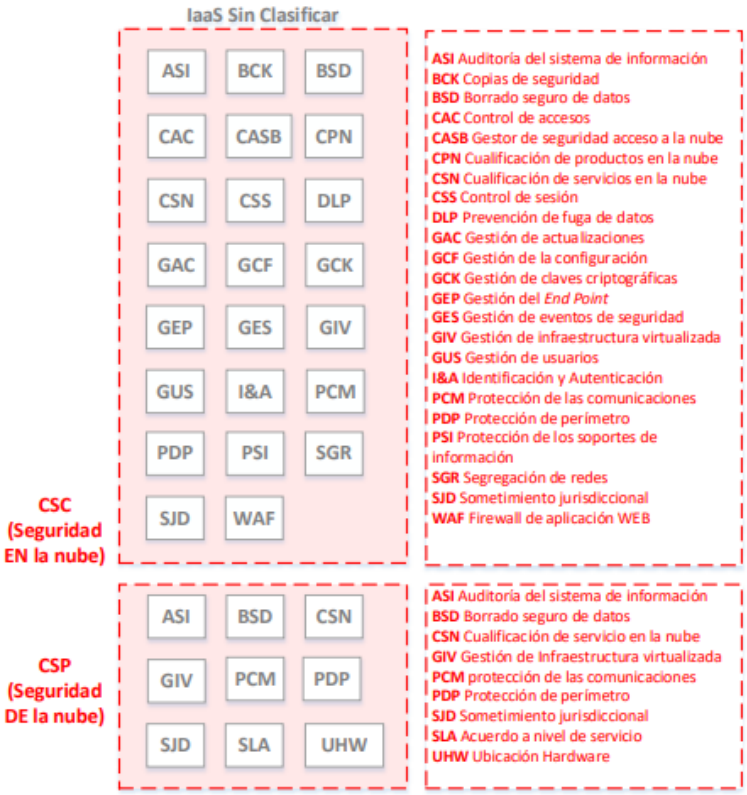


Figura 24. Medidas de Seguridad en la IaaS Sin Clasificar. STIC 499 [10]**.**

A continuación se expone un diagrama de red de alto nivel, de cómo debe ser la electrónica de red de Iaas para manejar información Sin Clasificar.

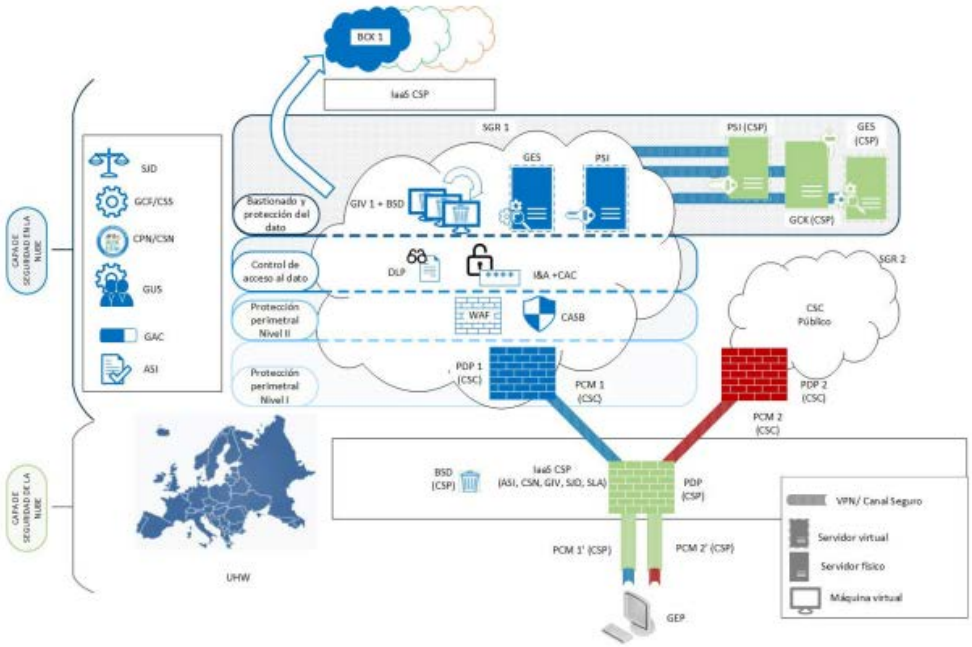


Figura 25.Diagrama IaaS para manejar Información Sin Clasificar. STIC 499 [10]**.**

Respecto a las medidas de seguridad IaaS en nube con información Difusión Limitada; es importante destacar que este es el caso de máxima clasificación que se va a manejar en los CIS desplegables de pequeñas unidades ya que en el caso de que se hubiera contemplado un sistema que manejara mayor clasificación deberán aplicarse las medidas correspondientes a ese máximo nivel.

Hay que tener en cuenta que para el manejo de información clasificada cifrada con herramientas aprobadas por el CNN, se podrá implementar la arquitectura descrita en el apartado anterior ya que la información cifrada anteriormente aunque esté cifrada no se considera información clasificada, a continuación se presenta un esquema donde se resumen las medidas necesarias de seguridad para implementar esta arquitectura.

Se han resaltado en gris aquellas medidas nuevas o que han sufrido modificaciones con respecto a la arquitectura de nube sin clasificar (medidas nivel L2). Estas medidas se describen a continuación. El resto de medidas permanecen invariables y será aplicable lo descrito anteriormente. Véase **Figura 27 "Medidas de Seguridad en nube para Difusión Limitada. STIC 499".**

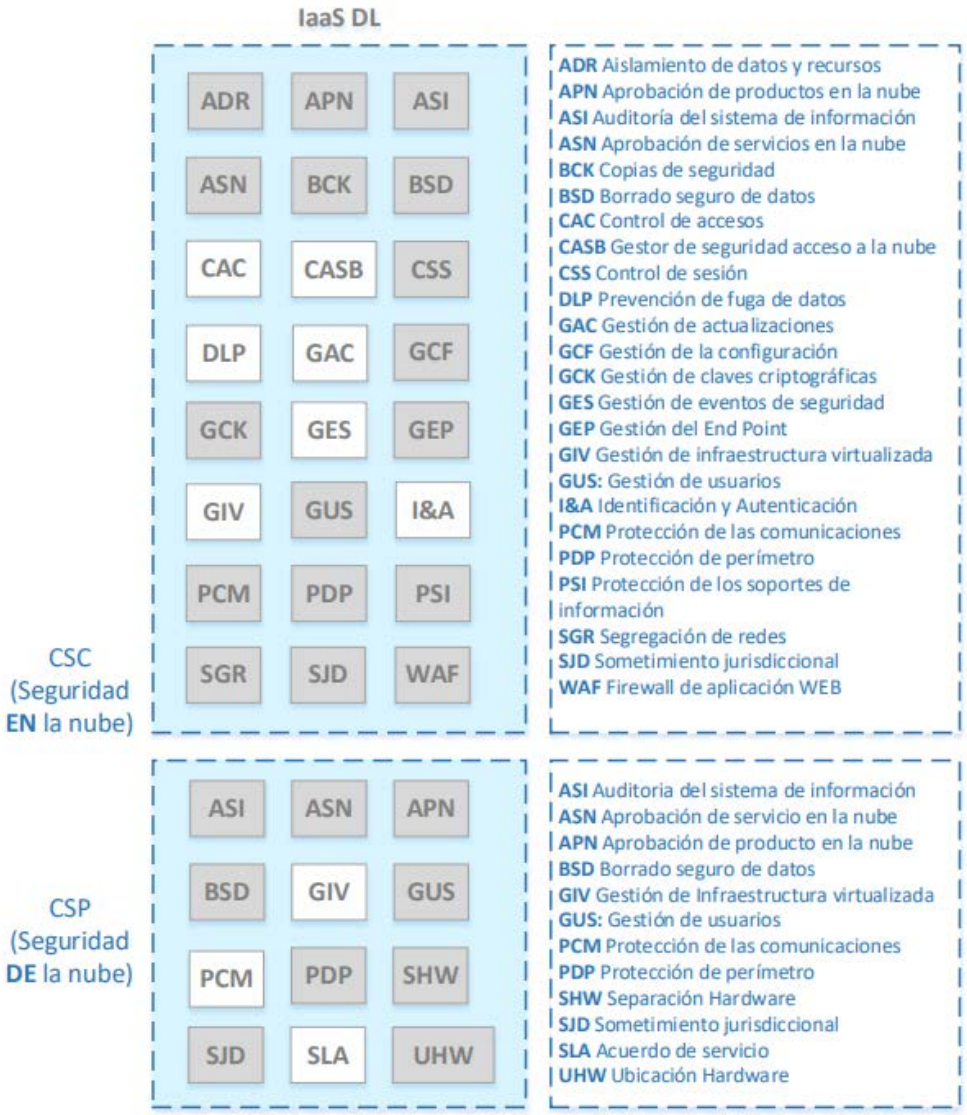


Figura 26 Medidas de Seguridad en nube para Difusión Limitada. STIC 499. [10]

Para implementar una arquitectura segura para el escenario en el que el/los sistemas manejen información clasificada DIFUSIÓN LIMITADA en la nube, se aplicarán todas las medidas del modelo de arquitectura descrita en los apartados anteriores y los elementos adicionales definidos a continuación.

Es importante destacar que el listado de medidas de seguridad establecido en el presente documento cumple con la guía CCN-STIC-301 [11] Medidas de Seguridad TIC a implementar en sistemas clasificados y parte de un escenario de uso genérico, que podrá ser modificado o refinado por los resultados del preceptivo análisis de riesgos para cada escenario de uso concreto.

En el siguiente diagrama de alto nivel se incluye las medidas de seguridad que se definen en la siguiente sección.

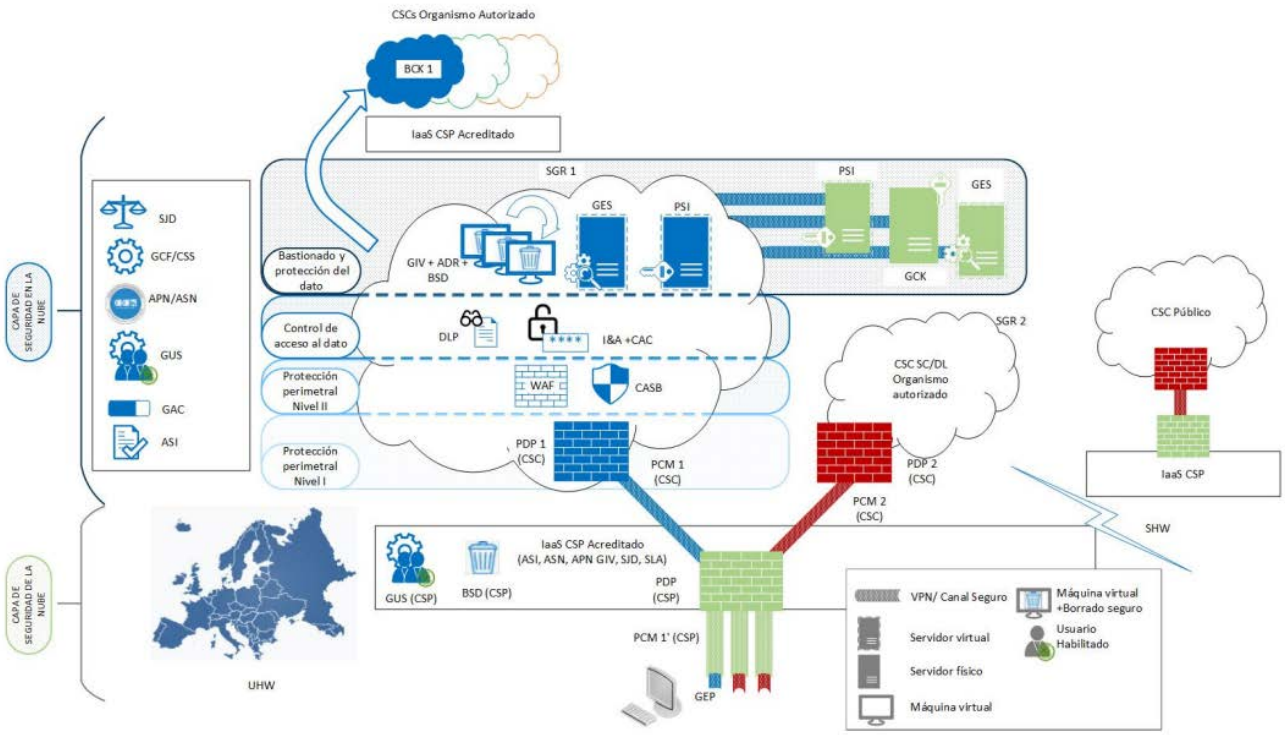


Figura 27. Diagrama de IaaS para manejar información de Difusión Limitada. STIC 499 [10].

Teniendo en cuenta las distintas categorías de servicio, así como las medidas contempladas en cada una de las arquitecturas planteadas, la siguiente tabla presenta un resumen de los modelos de despliegue que serían aplicables para cada una de ellas: Ver Tabla 8-2. Modelo de Despliegue. STIC 499. [10] [10].

	IaaS
SIN CLASIFICAR	Nube privada o Comunitaria
DIFUSIÓN LIMITADA	Nube privada o Comunitaria

Tabla 3-2. Modelo de Despliegue. STIC 499. [10]

4 DESARROLLO DEL PROYECTO

4.1 Viabilidad del Proyecto. Gestión del Proceso de Negocio. Business Process Management

4.1.1 Introducción BPM[30].

Para determinar la viabilidad del Proyecto y el éxito del mismo en su desarrollo Implementación de la Tecnología 5G para la Integración de las radios tácticas definidas por software se va a utilizar el método del Business Process Management (BPM).Es un procedimiento que se utiliza para diseñar, ejecutar, analizar y mejorar continuamente cada proceso de negocio de una organización en este caso el Ministerio de Defensa para orientarlo al objetivo concreto que en este caso es el título de este trabajo.

Con la utilización de BPM se definirán todos los procesos de negocio utilizando toda la información sobre disponible y alienarlos con la consecución del objetivo. Esto implica que si se conoce los procesos de principio a fin y su funcionamiento se pueden optimizar, adaptar específicamente a las necesidades operativas definidas y, en consecuencia, alcanzar sus objetivos operativos con mayor rapidez y eficacia.

Dado que los procesos y los objetivos cambian constantemente, la gestión de los procesos debe considerarse menos como un acontecimiento puntual y más como una actividad que propicia la mejora continua de cada proceso de negocio.

Los procesos de negocio constituyen el núcleo de toda organización. Deben funcionar de forma óptima para que se cumplan los objetivos definidos que en este caso es el dominio del espectro en el campo de batalla a largo plazo.

Los sistemas de control de procesos de negocio como base de la transformación digital son la clave del éxito: con una visión digital, se podrá revisar y mejorar continuamente sus estructuras y procesos, identificar nuevos potenciales y áreas de negocio, y utilizar la información obtenida para alinearse con los deseos de las unidades usuarias que este caso se les considerará como sus clientes, entre otras ventajas de las BPM.

De este modo, tras identificar cada proceso de negocio, se consigue una total transparencia en todos ellos, aumentando la velocidad de los procesos y reforzando su flexibilidad mediante la automatización. Esta mejora de la comprensión y la optimización y automatización continuas de los procesos reduce considerablemente los errores y ahorra tiempo.

Los nuevos retos y las tendencias del mercado en la industria pueden dominarse de forma estructurada con un sistema BPM y establecerse como nuevos modelos de negocio por ejemplo la utilización de la tecnología 5G en las redes de telecomunicaciones militares y su integración en las redes de radio de combate, y la capacidad de poder evolucionar los sistemas implementados en caso de tener adaptarse en un futuro no muy lejano a nuevas tecnologías (Ej: Tecnología 6G).

La gestión de los procesos de negocio representa la base elemental para una mayor productividad y eficiencia en la unidad de adquisición y, en consecuencia, es indispensable para estar al día y seguir teniendo éxito a largo plazo.

[30] La herramienta o aplicación que se va a usar para la realización de la viabilidad del proyecto es la proporcionada en la asignatura Gobierno, dirección y gestión TIC (COM1). BIZAGI MODELER.

En el ANEXO I, se presenta “La propuesta de desarrollo e implantación de la cobertura 5G en las SDR,s”.

4.1.1 Planificación del Proyecto.

En este apartado se va desarrollar la planificación del proyecto con el fin de conseguir una ordenación sistemática de las distintas tareas necesarias para lograr la integración no solo técnicas sino siguiendo las especificaciones que legales y operativas para la integración delas radios SDR en la tecnología 5G.

4.1.1.1 Planificación Previa.

Sin una planificación previa no es posible una acción correcta. El Project Management Institute (PMI) adoptó el ciclo de calidad PDCA en la forma de los grupos de proceso de inicio, planificación, ejecución, monitorización y control, y cierre.

Figura 28. Etapas del Ciclo PDCA.https:// public-library.safetyculture.io.

La planificación de un proyecto es la “ordenación sistemática de las tareas para lograr un objetivo, donde se expone lo que se necesita hacer y cómo debe llevarse a cabo”. “La planificación está compuesta por aquellos procesos que establecen el alcance total del esfuerzo, definen y refinan los objetivos y desarrollan la línea de acción requerida para alcanzar dichos objetivos”, en palabras del PMI.

En el siguiente apartado, se expone un posible análisis de viabilidad y definición de los objeticos, en su 1º Ciclo de adquisición, argumentando la necesidad operativa del proyecto.

4.1.1.2 Resumen de Análisis de viabilidad y definición de los objetivos

El presente trabajo tiene como objetivo principal el empleo de las Radios Definidas por Software SDR que van a formar parte del Sistema Conjunto de Radio Táctica de las Fuerzas Armadas (FAS) tengan la capacidad para su integración en la Tecnología 5G y en futuras, para la obtención de un “Sistema “, que permita y garantice el intercambio fiable y seguro de información táctica de las FAS.

Los equipos de comunicaciones tácticas actuales no permiten dar respuesta a las necesidades del presente ni del futuro en un entorno operativo en el ámbito de los actuales Sistemas de Comunicaciones e Información.

EL SCRT al emplear la tecnología de SDR, basada en arquitecturas (SCA) estandarizada y documentada que permitirá:

- La integración de las diferentes formas de onda (WFs) de coalición y el desarrollo, bajo el control nacional, de WFs nacionales específicas y de nuevas WFs de coalición, permitiendo obtener soberanía nacional en la evolución de las WFs y alcanzar el elevado grado de interoperabilidad requerido. Esto permite integrar a las WF,s que se emplean en 5G.
- La integración de algoritmos criptográficos nacionales, con el fin de obtener soberanía nacional en materia de cifra. Todos los aspectos relacionados con la seguridad criptológica del equipamiento susceptible de ser adquirido en el marco del SCRT.

A su vez la Tecnología 5G, permitirá aumentar la conectividad, bajar la latencia (entre otras cosas permitirá el empleo de la telemedicina en Zona de Operaciones, IOT, Industria 4.0, etc.,), la capacidad que ofrece el empleo de antenas Masive MIMO (creando redes malladas entre dispositivos), securización de la red (Permite la creación de VPN, segmentación de red) y mediante un CORE 5G en propiedad delimitará el acceso a la red de los usuarios.

Respeto a lo comentado, desde un punto de vista particular, para el desarrollo y análisis de esta capacidad en las FAS, sería viable siempre y cuando se cumplan los siguientes términos[31]:

- Las empresas líderes tecnológicas en el sector de las comunicaciones militares internacionales, y nacionales con acuerdos con fabricantes internacionales, deben responder satisfactoriamente a la solicitud de información[32] para la integración en la cobertura 5G en las SDR. Tras el análisis de las propuestas presentadas se confirma que el objetivo de capacidad asociado a los recursos materiales solicitados dentro del SCRT es viable, si bien:

i) Dependiendo de las propuestas industriales, determinadas formas de onda y factores de forma requeridos no están disponibles en la actualidad, si bien están contemplados en los planes de desarrollo a medio plazo presentados por la industria.

ii) No se dispone en el mercado internacional de un único proveedor que aporte todas las características exigidas a las SDR para su integración en la cobertura 5G, y que pueda satisfacer de manera inmediata los requisitos recogidos en los documentos.

iii) No existe un CORE 5G con las especificaciones de robustez exigidas en los entornos operativos más exigentes pero si hay empresas que han desarrollado prototipos.

iv) Se han identificado riesgos que no comprometen el desarrollo del SCRT y que se mitigarán desde las fases más tempranas del programa.

Las diferentes soluciones para disponer de soberanía nacional respecto a los sistemas criptográficos de las radios están analizadas y coordinadas con el CCN. El CCN considera que existen diferentes alternativas para lograr los objetivos del programa SCRT en materia de seguridad criptológica.

La adquisición de esta capacidad, se desarrollará en un marco de racionalización de esfuerzos y eficiencia en la gestión de Programas, tanto en la obtención como en el sostenimiento.

Durante la vida operativa del sistema, establecida en 15 años, se contemplarán las actividades de sostenimiento integrado de los equipos que constituyen este proyecto: mantenimiento, modernizaciones parciales, adquisición anual de repuestos, soporte de los Fabricantes de los elementos suministrados.

[31] Los términos referidos como una propuesta particular.

[32] Las empresas deben responder satisfactoriamente a la RFI,s (Request for Information), contemplando que puedan acometer todas las capacidades operativas requeridas, en el proyecto.

El tejido empresarial nacional relacionado con la Defensa y, en particular, en el sector TIC, necesita de acuerdos industriales con fabricantes extranjeros para abordar todas las fases del Programa (diseño, desarrollo, producción y sostenimiento) de obtención.

El desarrollo tecnológico asociado representa una oportunidad de impulso para la industria nacional en el sector de la Defensa, de cara a su proyección tanto interior como exterior, al fomentar colaboración industrial con fabricantes punteros extranjeros que facilitarán la transmisión de conocimiento y capacidad industrial a las empresas nacionales con las que firmen acuerdos de colaboración.

Se debe establecer una estrecha coordinación y colaboración con CESTIC y las distintas Oficinas de Programa que tengan relación con los sistemas de Telecomunicaciones y de Información de los Ejércitos, la Armada, EMAD y UME.

El Proyecto está alineado con la Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones del CESTIC del Ministerio de Defensa.

Desde el punto de vista financiero se considera viable, siempre y cuando se asigne al Proyecto la prioridad suficientemente elevada para que obtenga financiación su ciclo de vida.

La estrategia de adquisición debe plantear líneas de actuación tanto a corto plazo (dotación inmediata) como a largo plazo (capacitación industrial).

Desde un punto de vista industrial, esta capacidad deberá reforzar y desarrollar la Base Tecnológica e Industrial (BTI) española:

I. Aprovechando las capacidades nacionales SDR-5G y la inversión realizada, protegiendo y potenciando las habilidades y conocimientos ya adquiridos en este campo por la Industria Nacional.
II. Desarrollando el tejido industrial nacional y generando puestos de trabajo de nueva creación potenciando la capacidad de diseño, desarrollo, producción, mantenimiento y modernización de los nuevos sistemas SDR.
III. Garantizando el sostenimiento de las capacidades industriales que se desarrollen y los puestos de trabajo de nueva creación con soluciones con proyección a futuro y con posicionamiento internacional.
IV. Garantizando el máximo nivel de sostenimiento nacional de los sistemas adquiridos, capacitando a la industria española y las FAS en su mantenimiento, evitando la dependencia de terceros.

En la actualidad es esencial que haya necesidades concretas y urgentes para adquisiciones de equipos radio SDR programables para su integración en la tecnología 5G y equipos propios de las FAS las los sistemas de Mando y Control desplegables con la 5G. Las necesidades de equipamiento de estos equipos deberán estar incluidos en dichos programas estar alineadas y ser completamente interoperables tanto en lo referente a formas de onda como a sistemas criptológicos con el SCRT así como para su integración para poder integrase a la tecnología 5G, Las decisiones sobre las adquisiciones en dichos programas deberían coordinarse con la Oficina de Programa del Plan MC3/SCRT (JC4ISR) a establecer en la Subdirección de Programas de la DGAM.

Verificada la viabilidad de obtención de la capacidad solicitada a través de la solución propuesta, se considera como alternativa de obtención, según Instrucción SEDEF 67/11[33], la opción de adquirir sistemas disponibles en el mercado a la vez que se obtiene en su proceso el grado de capacitación industrial estratégica a nivel nacional que se determine necesario siendo un proceso de selección abierto a las principales empresas en el entorno SDR y la Tecnología 5G internacional y nacional, considerándose en este último caso la necesidad de ser apoyada por socios tecnológicos extranjeros.

Asimismo, dicho proceso de adquisición deberá ser complementado en aspectos puntuales con desarrollos específicos para el sistema, bien por parte de la industria nacional, bien con socios tecnológicos extranjeros.

También se considera la posibilidad de colaboración con otros países para la obtención conjunta de determinadas capacidades optimizando su proceso de adquisición, o con adquisiciones puntuales de sistemas ya disponibles en Fuerzas Armadas de otros países.

El desarrollo de un Programa como el contemplado en este trabajo, debe garantizar la soberanía y control nacional del mayor porcentaje de elementos que lo integran, con especial interés en los aspectos que afectan a la seguridad de las comunicaciones y a la capacitación para establecer el adecuado soporte de sostenimiento.

En el siguiente cronograma se muestra la estimación temporal de la alternativa seleccionada, en la que se ha tenido en cuenta una eventual disponibilidad presupuestaria a partir del año 2022, y las propuestas de calendario presentadas por la industria como respuesta a la RFI elaborada por la Oficina de Programas de las DGAM.

Figura 29. Estimación temporal del proyecto.

Dentro del Primer Ciclo de Adquisición (2022-2024), se ha realizado a su vez una división por prioridades para la disponibilidad de los equipos SDR y 5G, con la siguiente justificación:

[33] SEDEF 67/11.

a. Instrucción 67/2011, de 15 de septiembre, del Secretario de Estado de Defensa, por la que se regula el Proceso de Obtención de Recursos Materiales.

b. C*oncepto de Empleo de las FAS (CEFAS), JEMAD 14OCT2021 (*representa la Estrategia Militar para el Ciclo de Planeamiento 2017-2024).*

c. Orden de Servicio de marzo de 2015, del Director General de Armamento y Material, por la que se adaptan las instrucciones 67/2011 y 72/2012 del SEDEF en su aplicación a los recursos de I+D y armamento y material.

- La Primera prioridad se establece para los sistemas y plataformas en misiones permanentes, que previsiblemente serán puestas a disposición de las OISD[34], principalmente de la OTAN.
- La Segunda prioridad se establece para otras plataformas de los Ejércitos y Armada susceptibles de ser alistadas en Operaciones OTAN.
- La Tercera prioridad se establece para el resto de las plataformas.

En la siguiente tabla se muestra la división por prioridades dentro del primer ciclo de adquisición de equipos SDR, para cada factor de forma y para las bandas y número de canales disponibles dentro de esos factores de forma. También se muestra, para la banda V/UHF, la priorización de las necesidades de adquisición de radios con forma de onda SATURN y TACSAT. La Tercera prioridad se establece para el resto de las plataformas.

EQUIPOS RADIO SDR				
TIPOS DE RADIOS		Usuarios y Número de Equipos		
Factor de Forma	Banda y Nº de canales	PRIMER CICLO ADQUISICIÓN 2022-2025		
		1ª Prioridad	*2ª Prioridad*	*3ª Prioridad*
HANDHELD, MANPACK, VEHICULAR, FIJO	V/UHF - 2ch	20	20	
	V/UHF 2ch (+SATURN) (SIN UHF TACSAT)	10	10	
	V/UHF 2ch (+ UHF TACSAT) (SIN SATURN)	10	10	10
	V/UHF 2ch (+ UHF TACSAT) (+ SATURN)	20	20	20

Figura 30. Equipos radio SDR por prioridades del 1º ciclo de adquisición.

Una evaluación ficticia la evaluación estimada, el coste más probable del programa es: Costes de adquisición 3,5 M€, de sostenimiento 350 K€, para modernización 1 M€ para y coste de baja 100 K€, estimado para 15 años de vida útil.

Por lo tanto, el coste total del programa SCRT se estima en 4,95 M€.

En la Figura 33. "Costes generales". Es una tabla se resumen los costes generales del proyecto, desagregados por los conceptos de Adquisición, Sostenimiento y Modernización del Sistema.

[34] OISD. Organismos internacionales de Defensa y Seguridad.

ESTIMACIÓN GENERAL COSTES	
	Importe € Constantes `22
ADQUISICIÓN	*3.500.000 €*
SOSTENIMIENTO	*350.000 €*
MODERNIZACIÓN	*1.000.000 €*
BAJA	*100.000 €*
TOTAL (21% IVA incl.)	**4.950.000 €**

Figura 31. Costes generales.

Como argumento para la adquisición de estos medios de integración en una red de combate, hay que señalar que en la situación actual en que se encuentran los medios radio en las FAS, se requiere de manera urgente la sustitución de estos medios de comunicaciones tácticas actuales que se encuentran en dotación en las unidades, por su obsolescencia y falta de acreditación de seguridad, el riesgo inferido de la no satisfacción de esta capacidad a corto plazo, conllevaría a la imposibilidad de poder cumplir las misiones derivadas de la Directiva de Planeamiento Militar en vigor (DPM) [12] así como con los acuerdos suscritos por España para la participación en organizaciones y operaciones internacionales.

4.1.1.2.1 Definición del alcance del Proyecto.

En el ANEXO II se define cada una de las posibles tareas y actividades en que se divide el proyecto y las prioridades para su realización, así como la distribución de responsabilidades entre todos los participantes (matriz de responsabilidad, RASCI), estableciéndose los vínculos de interdependencia en cada actividad para asegurar el flujo de trabajo para garantizar los productos y servicios comprometidos para la viabilidad del proyecto.

Siguiendo con la Resolución 307/08135/21 [1], en su capítulo V “Desarrollo e Implantación de la Estrategia 5G y Estructura de gobierno”, para cada proyecto se identificarán los siguientes aspectos:

- Necesidad operativa / funcional a la que se asocia.

- Objetivos esperados y plazos previstos de inicio y consecución.

- Dominio/s de aplicación, escenario/s de referencia y opción de despliegue y uso más adecuada.

- Actores implicados y matriz de responsabilidades (RASCI).

- Interdependencia con proyectos de desarrollo del PECIS (o integración en ellos).

- Interdependencia con proyectos y experiencias sobre redes y servicios 5G de la OTAN, la Unión Europea o de la AGE.

- Recursos implicados (humanos, materiales, financieros y formativos).

La definición y desarrollo de este proyecto se adaptará, en todo caso, a la evolución en el contexto tecnológico y normativo que afecte al empleo de redes y servicios 5G. En el desarrollo de este trabajo se ha hecho mención y desarrollado los tres primeros apartados, por lo que se comienza por el apartado siguiente:

i. Actores implicados y matriz de responsabilidades (RASCI)

Responsible, "R", (responsable de la ejecución): es quien ejecuta una tarea. Su función es "HACER". Lo más habitual es que exista sólo un encargado R por cada tarea.

Accountable, "A", (responsable del proceso en conjunto): es quien vela porque la tarea se cumpla, aún sin tener que ejecutarla en persona. Su función es "HACER QUE SE HAGA". Support, "S", (apoyo): Alguien que apoya un rol ejecutivo en un proceso, contribuyendo a la implementación de una tarea en un proceso. Bien podría ser un substituto. (Backup)

Consulted, "C", (consultado): Persona que debe ser consultada para la realización de una tarea.

Informed, "I", (Informado): Persona que debe ser informada de la realización de una tarea.

ii. Interdependencia con proyectos 5G, PECSI, OTAN y UE [6]**. Iniciativas 5G en OTAN y proyectos 5G MINISDEF- Ejército de Tierra** [7]**.**

Red 5G ad-hoc de alta capacidad aérea y nube táctica distribuida: FANETC (Flying Ad-hoc 5G Network & Distributed Mobile Tactical Cloud).

Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS) MINISTERIO DE DEFENSA.

El objetivo de este proyecto es implantar un enjambre de UAV (Unmanned Aerial Vehicle) para crear una red 5G ad-hoc de alta capacidad aérea, FANET (Flying Ad-hoc Network).Esta red permitiría capacidad de procesamiento y securización de los datos obtenidos a bordo de las aeronaves creando una nube táctica distribuida FATC (Flying Ad-hoc Tactical Cloud).

La red ad-hoc estaría compuesta por:

- Estaciones Base 5G con capacidad de edge computing, sobre vehículos militares facilitados por el ET para proporcionar la movilidad táctica necesaria (con capacidad de operar en dos bandas de frecuencia: 700/800/900 MHz y otra a partir de 3,5GHz, y con la posibilidad de emplear la banda 4,4-5GHz reservada para su empleo en comunicaciones terrestres militares por los países de la OTAN).
- Enjambre de UAV, con capacidad de procesado a bordo.
- Para garantizar la confidencialidad de las comunicaciones, se empleará una arquitectura de seguridad acreditada por el Centro Criptológico Nacional (CCN), hasta nivel Difusión Limitada. En

fases posteriores, con la incorporación de la arquitectura correspondiente y el equipamiento necesario se podría alcanzar el nivel RESERVADO NACIONAL / NATO SECRET.

iii. Identificación de costes y recursos.

Incluye los financieros, humanos, materiales y tecnológicos, necesarios para realizar las actividades y tareas definidas en el ANEXO II y III. Es importante señalar que, NO SE HAN TENIDO en cuenta los riesgos que podría afectar al proyecto y cómo se gestionarían. La identificación de costes y recursos necesarios para el desarrollo del proyecto no tiene ninguna valoración documentada, ya que para esto es necesario realizar una evaluación de costes por un organismo que dentro del MINISDEF es el Grupo de Evaluación de Costes, perteneciente a un departamento de la Dirección General de Armamento y Material, que elevarían un documento de viabilidad de costes.

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones.

Este proyecto está relacionado con el resto de programas actuales y futuros relacionados con distintos tipos de plataformas de las FAS (Ej: Equipación de SDR,s en Vehículos 8X8). Por lo tanto, podría ser una alternativa de obtención de gran relevancia y tendría una gran repercusión sobre futuros programas, especialmente en aquellos programas del MINISDEF que contemplan la integración de sistemas radio SDR y utilización de la tecnología 5G.

Independientemente a todo esto, la implementación de este tipo de tecnología daría las siguientes posibilidades de que ahora no disponen las FAS:

5.1.1 Adquisición de las SDR,s.

i. Permitiría la capacidad de poder implementar las formas de onda que son utilizadas en 5G.
ii. Adquisición de un módulo cripto integrado, proporcionando seguridad en las comunicaciones y posibilidad de acreditación de la red hasta un nivel de Difusión Limitada.
iii. Al ser radios IP, capacidad de integrase en las aplicaciones como el GESCOM, implementado en el ET, para la gestión de comunicaciones.
iv. Capacidad de integración con medios radios legados.
v. Capacidad de transmisión de datos hasta 100 Mbps.

5.1.2 Adquisición de equipos con tecnología 5G.

i. CORE 5G de telecomunicaciones en propiedad, con el fin de gestionar y administrar a propia red de telecomunicaciones en los Puestos de Mando Desplegables, con capacidad de acceso a la I3D, mediante la capacidad que les proporcionaría las radios TACSAT (Terminales Satélite Tácticos).Securización de la red, control de acceso total sobre los usuarios. Establece una conectividad confiable y segura a la red para los usuarios finales y proporciona acceso a sus servicios independientemente si hay o no proveedor de servicios.
ii. Integración a la “Nube de Combate” [13], entendiendo como Nube de Combate“ *La aplicación de una solución tecnológica avanzada a las capacidades militares que habilita su empleo, especialmente el mando y control, en el multidominio y que permite mediante la captura , procesamiento y distribución de datos, incluidos los que proporcionan sensores y sistemas e intercambio de información de datos, así como la prestación de servicios, que cada usuario, plataforma o nodo autorizado contribuya y reciba información esencial a tiempo para que sea capaz de utilizarla para la toma de decisiones y la ejecución de operaciones militares dentro de un espacio de batalla”*.
iii. Aumento notable de la capacidad de transmisión de datos, aumento de ancha de banda, acceso a sensores con garantías de recibir información en tiempo real, disminución de latencia, etc.
iv. Otro concepto que hay que tener en cuenta en la tecnología 5G, es que permite la segmentación de redes, referido al empleo inteligente de secciones del espectro según

las necesidades específicas del dispositivo o la aplicación en cuestión.

v. Tiene la capacidad de verificación del rendimiento de diversos elementos virtuales de las redes 5G en el mundo real, se puede ampliar realizando pruebas y validando diversos casos prácticos de segmentación de redes en el entorno del laboratorio.

5.1.3 Implantación de Redes Definidas por Software. SDN.

i. Capacita a los usuarios finales (combatientes) que puedan hacer uso de las redes de forma remota, segura fácil y productiva, dándoles mayor capacidad de recursos para ejercer el Mando y Control de sus Unidades. La SDN permiten conectar cualquier dispositivo o usuario a cualquier aplicación en cualquier lugar, ya sea en la nube, en el perímetro o en el centro de datos, con análisis y seguridad de red profundos.

ii. Se simplifican las implementaciones de nodos y sitios remotos con la visibilidad, agilidad y escalabilidad globales de la WAN a través de una plataforma automatizada.

iii. La seguridad de la nube de la SDN, se logra mediante la segmentación integral y funciones de red virtual (VNF) de seguridad a través de la plataforma SDN. La SDN combina los servicios de seguridad y Edge Compute en una sola plataforma, controlado desde una sola interfaz de usuario, lo que permite que los usuarios y organizaciones se conecten de forma segura a múltiples nubes sin consumir recursos de los centros de datos. Además, garantiza la calidad de las aplicaciones llevando el tráfico directamente a la nube y a las aplicaciones SaaS sin backhaul a través del centro de datos tradicional.

5.1.4 Capacidad de acreditación de la red, hasta Difusión Limitada.

Relativo, al cumplimiento de la STIC 499 “Arquitectura de Seguridad en la Cloud”, hay que señalar que tendría sus limitaciones sobre todo para las acreditaciones de locales o zonas de acceso restringido o “ZAR”, ya que para este caso estarían supeditado a la localización de los mismos, al entorno operativo, la degradación del espectro electromagnético, etc., sobre todo si se trata de medios desplegables. Esto es independiente de que la información se pueda encontrar segura.

5.1.5 Viabilidad del proyecto.

i. Este proyecto se adapta a la normativa para la implantación del 5G en el ámbito del MINISDEF.

ii. El Proyecto está alineado con la Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones del CESTIC del Ministerio de Defensa.

iii. Respecto al presupuesto económico que se ha puesto como ejemplo, aquí es importante hacer un inciso, ya que no está documentado por GEC (Grupo de Evaluación e Coste) ni por Organismo competente en la materia, esta valoración no tiene valor legal. En todo caso y se acepta esta cantidad de unos 5 millones de €, en el ámbito de MINISDEF, sería viable.

5.2 Líneas futuras.

5.2.1 Implantación del 5G, en redes y servicios del MINISDEF.

La 5G es una tecnología de redes de comunicaciones de quinta generación que ofrece una mayor velocidad, capacidad y conectividad que las tecnologías de comunicaciones anteriores. Esto tendrá un

gran impacto en la mejora de la eficacia de las comunicaciones en las operaciones militares, desarrollo de nuevas aplicaciones y tecnologías para inteligencia, vigilancia y defensa. Sin embargo, también existen preocupaciones sobre la seguridad de la tecnología debido a posibles ataques y espionaje como consecuencia el MINISDEF ha desarrollado por la "Resolución 07/08135/21 [2], de 17 de mayo de 2021, de la Secretaria de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa", donde especifica que los desarrollos y definiciones de los proyectos se adaptaran a la evolución del contexto tecnológico y normativo que afecte al empleo de redes y servicios 5G, sobre todo en su seguridad en operaciones.

En definitiva, la implantación del 5G a corto plazo puede ser una realidad en los CIS del MINISDEF.

5.2.2 Seguridad del 5G [14] [15].

Tanto en la OTAN como en nuestras FAS, la seguridad cibernética de la 5G necesita algunas mejoras significativas para evitar los crecientes riesgos de hackeo. Algunas de las preocupaciones de seguridad son resultado de la propia red, mientras que otras tienen que ver con los dispositivos que se conectan a la 5G. Pero ambos aspectos ponen en peligro a los consumidores, los gobiernos y las empresas.

El investigador principal Felix Arteaga perteneciente al "Real Instituto Elcano", en su artículo "Las medidas de la UE para proteger las redes 5G (EU Toolbox): se dice el pecado, pero no el pecador" [16], realiza una análisis sobre la evolución de las medidas de seguridad en las redes 5G en la UE. En marzo del 2019, la Comisión Europea propuso una "Recomendación sobre Ciberseguridad de las redes 5G"[35] para la evaluación conjunta de los riegos y en octubre del mismo año el Grupo de Cooperación NIS[36], presenta un "Informe de coordinación de las valoraciones nacionales", identificado, riesgos, actores, vulnerabilidades y activos críticos, solo identificando activos y no los responsables de las amenazas, como se presenta en la Figura 33. Panorama de amenazas de EINSA para las redes 5G. Fuente EINSA[37]. Este informe presenta una visión general de los desafíos de seguridad del 5G.

[35] Comisión Europea (2019), "Cybersecurity of 5G Networks", COM (2019) 534, de 26 de marzo, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534&from=GA.

[36] NIS Cooperation Group (2019), "EU coordinated risk assessment of the cybersecurity of 5G networks", 9 de octubre, https://www.europeansources.info/record/eu-coordinated-risk-assessment-of-thecybersecurity-of-5g-networks

[37] **EINSA: European Union Agency For Cybersecurity. Panorama de amenazas de ENISA para redes 5G — ENISA (europa.eu).**

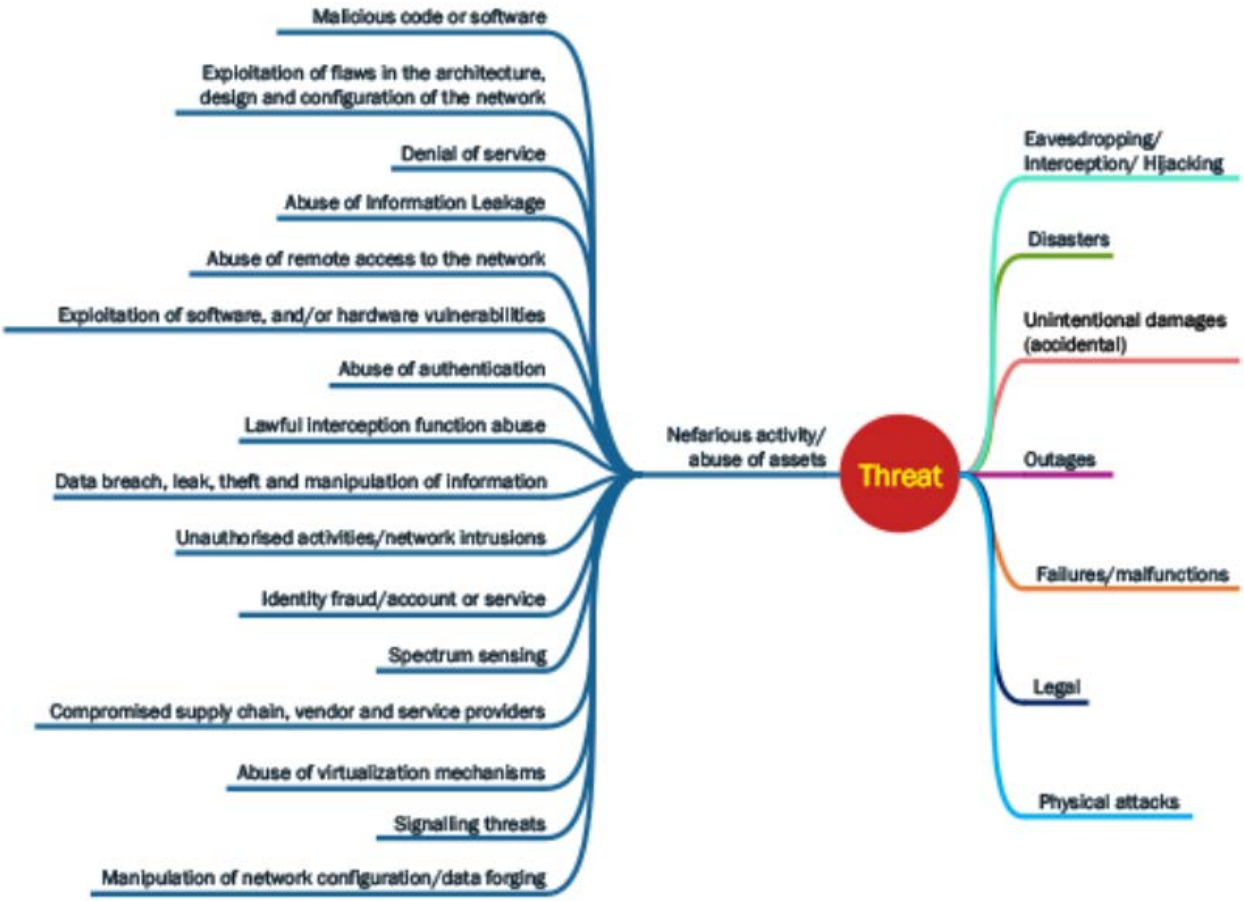


Figura 32. Panorama de amenazas de EINSA para las redes 5G. Fuente EINSA.

Esta evaluación de riesgos refleja un aumento considerable de las amenazas con respecto a la tecnología 4G, en la Tabla 5-1 Escenarios y categorías sobre riesgos principales en las redes 5G.”EU Coordinated Risk Assessment Report” [15], se identifican los siguientes escenarios y los riesgos que se presentan.

Escenarios	**Categorías de Riesgos (R)**
Medidas de seguridad insuficientes	R1 Desconfiguración de las redes
Cadena de suministros	R3 Baja calidad de los productos

Modus operandi de los actores detrás de los riesgos (amenazas)	R7 Disrupción relevante de las infraestructuras o servicios críticos
Interferencia entre redes y otros sistemas críticos	R8 Fallo masivo de las redes debido a la falta de electricidad o de los sistemas de apoyo
Dispositivos de los usuarios finales	R9 Alteración de los dispositivos IoT

Tabla 5-1Escenarios y categorías sobre riesgos principales en las redes 5G."EU Coordinated Risk Assessment Report" [15]

Para hacer frente a los riegos de seguridad presentados en la Tabla 5-1, las líneas de acción propuestas serán las siguientes:

5.2.2.1 Adquision de CORE 5G.

Las funciones básicas de la red 5G generalmente se consideran críticas. En efecto afectar a la red central puede comprometer potencialmente la confidencialidad y la disponibilidad y la integridad de todos los servicios de red (mientras que los compromisos de otros pueden tener un impacto más limitado, por ejemplo, afectar solo a una función específica o área).

Uno de los principales hándicaps del 5G, es la seguridad, en este proyecto se ha hecho hincapié en la adquisición y desarrollo de un CORE 5G portátil, con capacidad de escalabilidad y flexibilidad para la interconexión con otros CORE,s, el fin es el control total de la red, administrando en todo momento el acceso a usuarios, la monitorización de la red, etc...

5.2.2.2 Desarrollo 5G Non-Public Networks. [17]

Esta capacidad permitiría la implementación de 5G Non-Public Networks (NPN-Red no publica de 5G) [17], que permitiría a las unidades tanto de nivel táctico como operacional tener su propia red de datos, que además posibilitaría el acceso a la red publica o ISP, mediante la colocación firewars o la instalación de su correspondiente DMZ[38]. Como se muestra en la figura 33, en este escenario se ha implementado una red que solo pueden acceder los puesto de mando ahí despeglados, encontrándose todas las funciones de red en un perímetro lógico, siendo la NPN independiente de la red publica, la única via de comunicación entre NPN y la red pública es a través de la DMZ.

La NPN se basa en tecnologías definidas por 3GPP, teniendo su propio ID NPN dedicado, además tiene la opción de conexión a los servicios de la red pública a través de cortafuegos, como el que se muestra el la figura 33, permitiendo el acceso en determinados entornos operativos el acceso a internet, además de permitir el acceso a la I3D, mediante la creación de una VPN (Vitual Private Net).

[38] DMZ. Zona desmilitarizada (demilitarized zone) es una red perimetral que protege la red de área local (local-area network, LAN) interna contra el tráfico no confiable. Es una subred que separa las redes privadas de las redes públicas de internet.

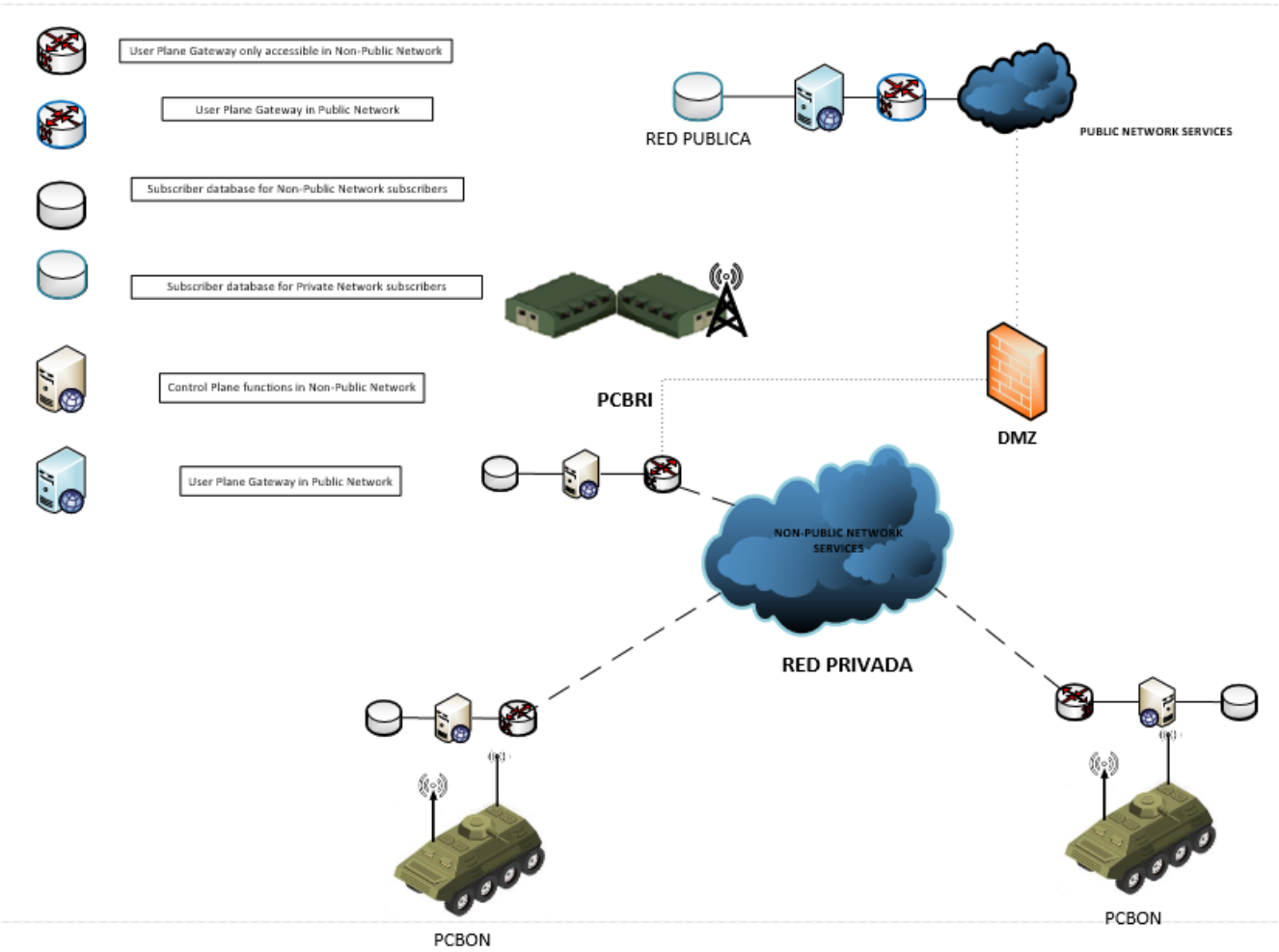


Figura 33. NPN. Non-Public Network. Diseño propio.

5.2.2.3 Implantación de SDN.

La arquitectura de una red definida por software introduce un increíble potencial que sus controladores están basados en software y los interfaces de programación de aplicaciones (API), de innovación en el uso de la red. La red definida por software proporciona una nueva forma de controlar el enrutamiento de los paquetes de datos a través de un servidor centralizado. La combinación de la vista global de la red y la programabilidad de la red respalda el proceso de recopilación de inteligencia de los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) existentes, seguido de la reprogramación y el análisis centralizado de la red. Por lo que las SDN puedan ser más robustas para los ataques maliciosos que las redes tradicionales. En la STIC 140 [9], como es su arquitectura.

5.2.3 Equipación de SDR para las FAS.

La DGAM y MALE[39] [17], han realizado ambos expedientes para la adquisición de SDR para el combatiente y se lo han adjudicado a la UTE[40] Telefónica y Aicox. Por otro lado la JCISAT del ET., en

[39] MALE. Mando de Apoyo Logístico del Ejército.
[40] UTE. Unión Temporal de Empresas.

el año 2021 ha realizado "Pruebas de la radio SDR para Batallón" [18], de las SDR TGOR-V de Tecnobit – Grupo Odesia.

La adquisición de estos tipos de radios, siguen las especificaciones marcadas en el proyecto, a continuación se expone todas las especificaciones técnicas de la radio presentada por Tecnobit [18].

"La radio TGOR trabaja con un ancho de banda de hasta 100 Mbps, en la banda VHF, UHF y la banda L, realiza asignación dinámica del espectro, permite la recepción multicanal, y la priorización de comunicaciones simultáneas. Todo ello, además de otras ventajas obvias, hace posible, en sus versiones vehiculares, disminuir las necesidades de equipos y de espacio dentro de los vehículos.

*Como dos de sus características más destacables podríamos mencionar su carácter de "radio cognitiva", gracias a su capacidad de análisis del espectro electromagnético y de detección de posibles perturbadores (*jammers*). Así como su capacidad de enviar video de muy alta calidad en las bandas mencionadas, y simultáneamente a otras comunicaciones que tengan lugar en paralelo. Además permite también la utilización de una Red Móvil Ad-Hoc (MANET) para que cada uno de los nodos / radios puedan comunicarse entre sí; ya que todos pueden actuar como emisores, receptores y encaminadores permitiendo la retransmisión.*

Capacidades de la radio TGOR - V como SDR MANET IP, entre las cuales figuran:

- ***Recepción de Canales Multi-Frecuencia (MCR)**, lo que le permite recibir y analizar la información de numerosos canales de frecuencia simultáneamente, utilizando una cabecera de RF única.*
- ***Red MANET (Red Móvil Ad-Hoc)** escalable hasta 1000 usuarios. La capacidad MANET de TGOR permite establecer redes con nodos de radio en movimiento. Lo cual, hace posible establecer redes radio con topología y tamaño dinámico. Cada radio puede actuar como retransmisor, reenviando tráfico destinado a otros dispositivos. Las rutas entre nodos pueden contener potencialmente múltiples saltos. El continuo movimiento conduce a variar la conectividad entre los dispositivos, dando lugar a cambios de la topología de red y en el número de nodos en la red.*
- ***Formas de onda MANET de banda ancha** para transmisión simultánea de voz, datos y video en movimiento. Con capacidad de recepción de hasta 100 Mbps. Así mismo, también se probaron **formas de onda MANET de banda estrecha** para la transmisión simultánea de voz y datos.*
- ***Capacidad de gestionar de forma autónoma el espectro electromagnético (Capacidad de Radio Cognitiva)** congestionado. Pudiendo manejar simultáneamente un gran número de transmisiones, procesarlas y fusionarlas en una única red IP de banda ancha con altas velocidades de datos, elevado número de usuarios y retrasos mínimos.*
- *Empleo de cifrado mediante módulo cripto nacional (CIFPECOM)."*
- *Capacidad de operación en entornos con GPS restringido o denegado mediante el empleo de su sistema MCR.*
- *Integración con el Gestor de Comunicaciones del Ejército de Tierra (GESCOMET), así como con el sistema de mando y control BMS.*
- *Kit para Desarrollo de Formas de Onda para que el usuario pueda desarrollar autónomamente sus propias formas de onda. El kit está compuesto por las*

aplicaciones BDK, SDK y FDK. Estas herramientas permiten desarrollar formas de onda mediante software y/o firmware. Permiten una forma sencilla de implementar, configurar y depurar las formas de onda.

Además, TGOR permite personalizar sus formas de onda nativas. Es decir, el usuario de TGOR puede customizar (definir, modificar) los parámetros de sus formas de onda. Con la adquisición de TGOR, el usuario recibe además de la aplicación NMS, el kit para desarrollo de formas de onda.

Por otra parte, Tecnobit – Grupo Oesía dispone de una pasarela que garantiza la interoperabilidad con las radios legadas.”.

En consonancia con el proyecto presentado, al existir en el mercado SDR,s con aplicaciones software que tienen herramientas para desarrollar sus propias formas de onda, nos permite que el desarrollo se agilice, siendo el único bastión que quedaría por superar, el desarrollar equipos con tecnología 5G desplegables.

6 BIBLIOGRAFÍA

[1] S. D. E. D. DEFENSA, «Estrategía de Explotación de la Nube en el Ministerio.,» 21.

[2] S. D. E. D. DEFENSA, Estategía de comunicaciones móviles de quinta generación (Estrategía 5G) del Ministerio de Defensa., 21.

[3] T. y. A. D. El Ministerio de Energía, «https://avancedigital.mineco.gob.es/5G/Documents/plan_nacional_5g.pdf,» 2020. [En línea]. [Último acceso: 17 JULIO 2022].

[4] I. J. S. Andujar, *Conferencia SDR en OTAN II CSUP CIS ET 2021,* Madrid, 2018.

[5] «ESSOR Architecture – Motivation and Overview (WInnF Technical Conference – December 2010,» 2010. [En línea]. Available: https://www.wirelessinnovation.org/assets/work_products/winnf_tc10_essor%20architecture-contribution_02dec10.pdf.

[6] NCIA, «https://ieeexplore.ieee.org/document/9486402/authors#authors,» 2021. [En línea]. Available: https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html.

[7] CESTIC, «PROYECTOS 5G DEL MDEF PARA LA FINANCIACIÓN EN EL MARCO DEL MECANISMO DE RECUPERACIÓN Y RESILIENCIA Y LE PROGRAMA ÚNICO -INTERCONEXIÓN DEL MINISTERIO DE ASUNTOS ECONOMICOS Y TRANSFORMACIÓN DIGITAL,» 2022.

[8] «CONCEPTO DE EMPLEO DE LAS FUERZAS ARMADAS 2017,» 2017. [En línea]. Available: https://emad.defensa.gob.es/en/Galerias/emad/files/CEFAS_2017_total.pdf#:~:text=El%20CEFAS%20representa%20laEstrategia%20Militarpara%20cada%20Ciclo%20de,objeto%20de%20garantizar%20unas%20FAS%20eficaces%20y%20sostenibles..

[9] CENTRO CRIPTOLOGICO NACIONAL, «CNN STIC 140. REDES DEFINIDAD POR SOFTWARE.,» Junio. 2021. [En línea]. [Último acceso: Diciembre 2022].

[10] Centro Criptologico Nacional, «STIC 499. Arquitectura de Seguridad en la Cloud.,» [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6807-ccn-stic-499-arquitecturas-de-seguridad-cloudaW5zaWQ9NTE2OQ&ptn=3&hsh=3&fclid=220faa04-92c7-64ff-23d2-b89d93ec65ae&psq=stic+499&u=a1aHR0cHM6Ly93d3cuY2NuLWNlcnQuY25pLmVzL3Nlc.

[11] Centro Criptologico Nacional, «La Guía CCN-STIC-301 de Medidas de Seguridad TIC a Implementar en Sistemas Clasificados es una instrucción técnica de obligado cumplimiento para todos los Sistemas que manejen información clasificada.,» 2020. [En línea]. Available: ticias/Anio2020/Enero/Noticia-2020-01-22-Nueva-Guia-CCN-STIC-implementar-Sistemas-Clasificados.html.

[12] M. d. Defensa, «Directiva de Política de Defensa - Ministerio de Defensa de España,» 2020.[Enlínea].Available: https://www.defensa.gob.es/defensa/politicadefensa/directivapolitica/.

[13] EMAD, «Visión del JEMAD de la "Nube de Combate",» 2022.

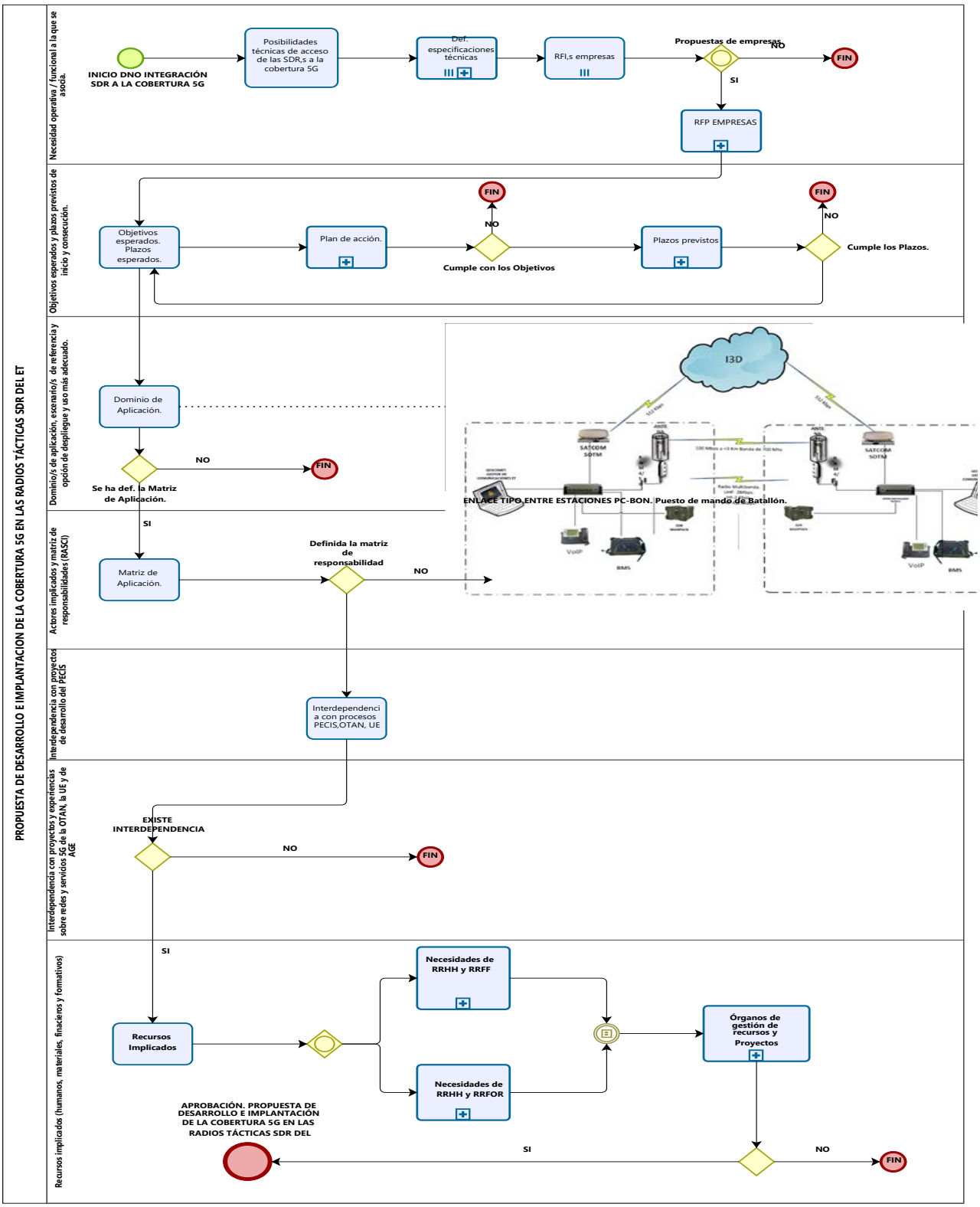
[14] «Web de La Moncloa,» [En línea]. Available: http://www.lamoncloa.gob.es. [Último acceso: 13 enero 2015].

[15] J. Rodríguez y V. Fernández, Cómo redactar el estado del arte de un trabajo, Editorial Genios, 2010.

[16] P. Martínez y A. García, Cómo escribir una buena memoria de TFG, Publicaciones del 2000, 2013.

[17] A. Pérez, Cómo escribir una bibliografía, Nuevas publicaciones.

ANEXO I: PROYECTO PARA LA INTEGRACIÓN DE LA COBERTURA 5G EN LAS SDR,S



ANEXO II: PLANIFICACIÓN DEL PROYECTO

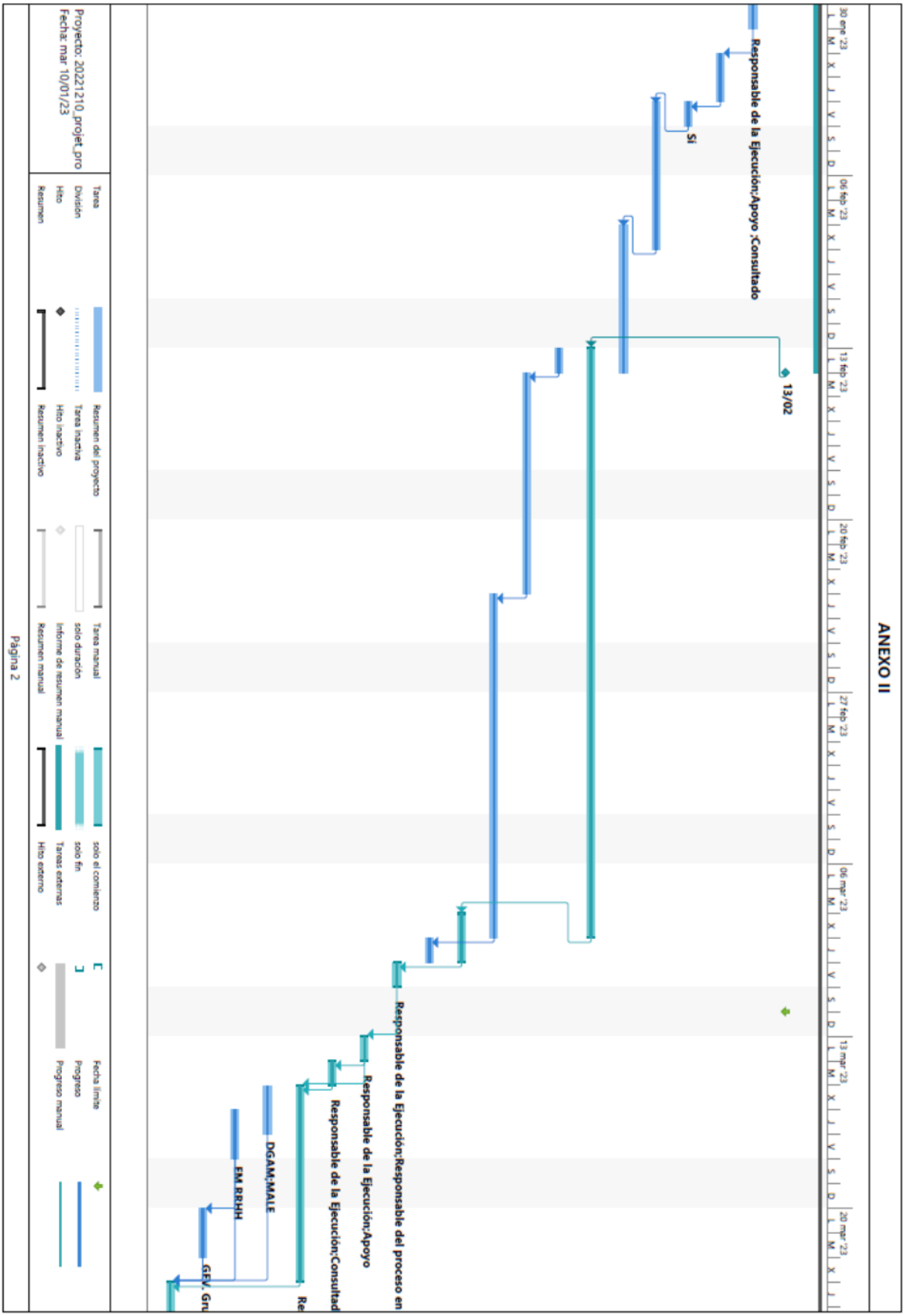
ANEXO II

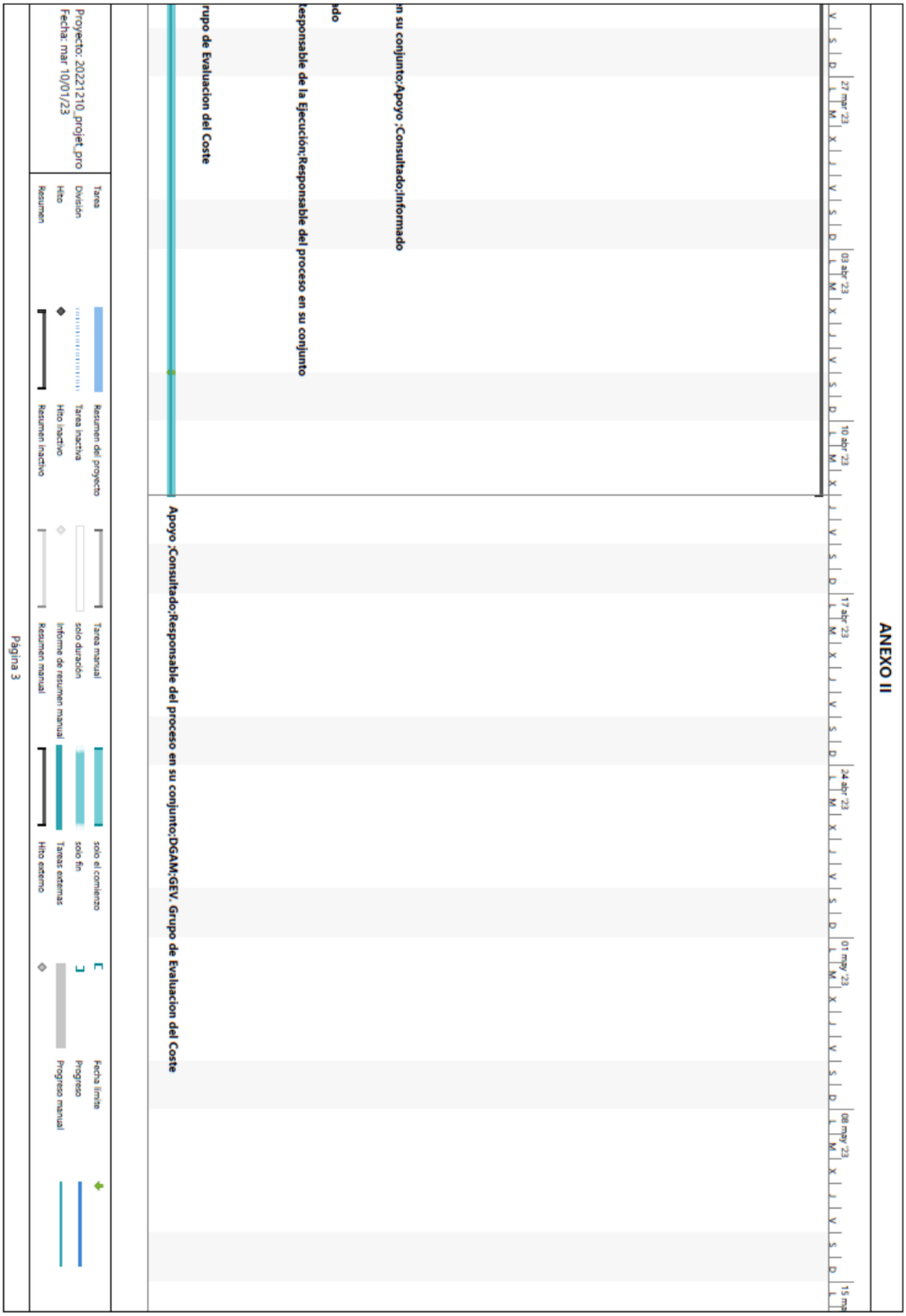
Id	% compl	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	**10...**		**<Resolución 307/08135/21, en su capítulo V "Desarrollo e Implantación de la Estrategia 5G y Estructura de gobierno">**	**53 días**	**lun 30/01/23**	**mié 12/04/23**		
2	100%		<Necesidades Operativas funcionalidad a la que se asocia>	11 días	lun 30/01/23	lun 13/02/23		
3	100%		Posibilidades técnicas de las SDR a la Tecnología 5G	1 día	lun 30/01/23	lun 30/01/23		Responsable de la Ejecución;Apoyo ;Consultado
4	100%		Definición de especificaciones tecnicas.	2 días	mié 01/02/23	jue 02/02/23	3	
5	100%		Request For Information a empresas	1 día	vie 03/02/23	vie 03/02/23	4	
6	100%		Request For Proposal	4 días	vie 03/02/23	mié 08/02/23	5	
7	100%		Request For Quote	4 días	mié 08/02/23	lun 13/02/23	6	
8	100%		<Objetivos esperados y Plazos previstos de Inicio y Comercialización>	18 días	lun 13/02/23	mié 08/03/23	2	
9	100%		Objetivos esperados y Plazos previstos	1 día	lun 13/02/23	lun 13/02/23		
10	100%		Plan de Acción	7 días	mar 14/02/23	mié 22/02/23	9	
11	100%		Plazos previstos	10 días	jue 23/02/23	mié 08/03/23	10	
12	100%		<Dominio de aplicación, escenarios de referencia y opción de despliegue y uso más adecuado.>	2 días	mié 08/03/23	jue 09/03/23	8	
13	100%		<Definicion del dominio de aplicación>	1 día?	jue 09/03/23	jue 09/03/23	11	
14	100%		Actores implicados y matriz de responsabilidades (RASCI)	1 día	vie 10/03/23	vie 10/03/23	12	Responsable de la Ejecución;Responsable del proceso en su conjunto;Apoyo ;Consultado;Informado
15	100%		Interdependencia con proyectos 5G, PECSI,OTAN y UE	1 día	lun 13/03/23	lun 13/03/23	14	Responsable de la Ejecución;Apoyo
16	100%		interdependencia con proyectos y experiencias sobre redes y servicios 5G, PECSI,OTAN y UE	1 día	mar 14/03/23	mar 14/03/23	15	Responsable de la Ejecución;Consultado
17	100%		<Recursos implicados (humanos, materiales y formación)>	6 días	mié 15/03/23	mié 22/03/23	15;16	Responsable de la Ejecución;Responsable del proceso en su conjunto
18	100%		<Necesidades de Recursos Humanos>	2 días	mié 15/03/23	jue 16/03/23		DGAM;MALE
19	100%		<Necesidades de recursos materiales>	2 días	jue 16/03/23	vie 17/03/23		EM RRHH
20	100%		<Necesidades de recursos finacieros>	2 días	lun 20/03/23	mar 21/03/23	19	GEV. Grupo de Evaluacion del Coste
21	100%		<Organos de Gestión de recursos y proyectos	15 días	jue 23/03/23	mié 12/04/23	17FC+1 día;18;1	Apoyo ;Consultado;Responsable del proceso en su conjunto;DGAM;GEV. Grupo de Evaluacion del Coste

Proyecto: 20221210_projet_pro
Fecha: mar 10/01/23

Tarea · Resumen del proyecto · Tarea manual · solo el comienzo · Fecha límite
División · Tarea inactiva · solo duración · solo fin · Progreso
Hito · Hito inactivo · Informe de resumen manual · Tareas externas · Progreso manual
Resumen · Resumen inactivo · Resumen manual · Hito externo

Página 1


ANEXO II
30 ene '23
06 feb '23
13 feb '23
20 feb '23
27 feb '23
06 mar '23
13 mar '23
20 mar '23
Responsable de la Ejecución;Apoyo ;Consultado
Sí
13/02
Responsable de la Ejecución;Responsable del proceso en
Responsable de la Ejecución;Apoyo
Responsable de la Ejecución;Consultad
DGAM;MALE
FM RRHH
GEV, Gru
Proyecto: 20221210_projet_pro
Fecha: mar 10/01/23
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
sólo duración
Informe de resumen manual
Resumen manual
sólo el comienzo
sólo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 2


ANEXO II
27 mar '23
03 abr '23
10 abr '23
17 abr '23
24 abr '23
01 may '23
08 may '23
15 may
n su conjunto;Apoyo ;Consultado;Informado
do
esponsable de la Ejecución;Responsable del proceso en su conjunto
rupo de Evaluacion del Coste
Apoyo ;Consultado;Responsable del proceso en su conjunto;DGAM;GEV. Grupo de Evaluacion del Coste
Proyecto: 20221210_projet_pro
Fecha: mar 10/01/23
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Página 3

ANEXO II

1 <Resolución 307/08135/21, en su capítulo V "Desarrollo e Implantación de la Estrategia 5G y Estructura de gobierno">

Siguiendo con la Resolución 307/08135/21, en su capítulo V "Desarrollo e Implantación de la Estrategia 5G y Estructura de gobierno", para cada proyecto se identificarán los siguientes aspectos:

- Necesidad operativa / funcional a la que se asocia.
- Objetivos esperados y plazos previstos de inicio y consecución.
- Dominio/s de aplicación, escenario/s de referencia y opción de despliegue y uso más adecuada.
- Actores implicados y matriz de responsabilidades (RASCI).
- Interdependencia con proyectos de desarrollo del PECIS (o integración en ellos).
- Interdependencia con proyectos y experiencias sobre redes y servicios 5G de la OTAN, la Unión Europea o de la AGE.
- Recursos implicados (humanos, materiales, financieros y formativos).

La definición y desarrollo de estos proyectos se adaptará, en todo caso, a la evolución en el contexto tecnológico y normativo que afecte al empleo de redes y servicios 5G.

14 Actores implicados y matriz de responsabilidades (RASCI)

Responsible, "R", (responsable de la ejecución): es quien ejecuta una tarea. Su función es "HACER". Lo más habitual es que exista sólo un encargado R por cada tarea.
Accountable, "A", (responsable del proceso en conjunto): es quien vela porque la tarea se cumpla, aún sin tener que ejecutarla en persona. Su función es "HACER QUE SE HAGA".
Support, "S", (apoyo): Alguien que apoya un rol ejecutivo en un proceso, contribuyendo a la implementación de una tarea en un proceso. Bien podría ser un sustituto. (Backup)
Consulted, "C", (consultado): Persona que debe ser consultada para la realización de una tarea.
Informed, "I", (Informado): Persona que debe ser informada de la realización de una tarea.

15 Interdependencia con proyectos 5G, PECSI,OTAN y UE

2.6 INICIATIVAS DE 5G EN OTAN Y PROYECTOS 5G MINISDEF- EJÉRCITO DE TIERRA.

Red 5G ad-hoc de alta capacidad aérea y nube táctica distribuida: FANETC (Flying Ad-hoc 5G Network & Distributed Mobile Tactical Cloud).
Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS) MINISTERIO DE DEFENSA.

El objetivo de este proyecto es implantar un enjambre de UAV (Unmanned Aerial Vehicle) para crear una red 5G ad-hoc de alta capacidad aérea, FANET (Flying Ad-hoc Network).

Esta red permitiría capacidad de procesamiento y securización de los datos obtenidos a bordo de las aeronaves creando una nube táctica distribuida FATC (Flying Ad-hoc Tactical Cloud).

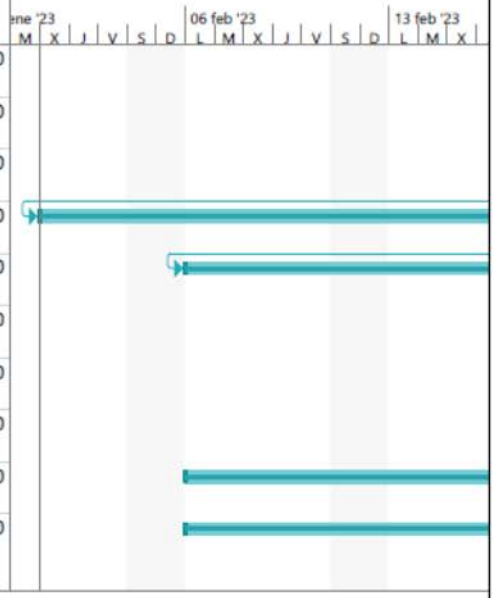
La red ad-hoc estaría compuesta por:

- Estaciones Base 5G con capacidad de edge computing, sobre vehículos militares facilitados por el ET para proporcionar la movilidad táctica necesaria (con capacidad de operar en dos bandas de frecuencia: 700/800/900 MHz y otra a partir de 3,5GHz, y con la posibilidad de emplear la banda 4,4-5GHz reservada para su empleo en comunicaciones terrestres militares por los países de la OTAN).
- Enjambre de UAV, con capacidad de procesado a bordo.

Para garantizar la confidencialidad de las comunicaciones, se empleará una arquitectura de seguridad acreditada por el Centro Criptológico Nacional (CCN), hasta nivel Difusión Limitada. En fases posteriores, con la incorporación de la arquitectura correspondiente y el equipamiento necesario se podría alcanzar el nivel RESERVADO NACIONAL / NATO SECRET.

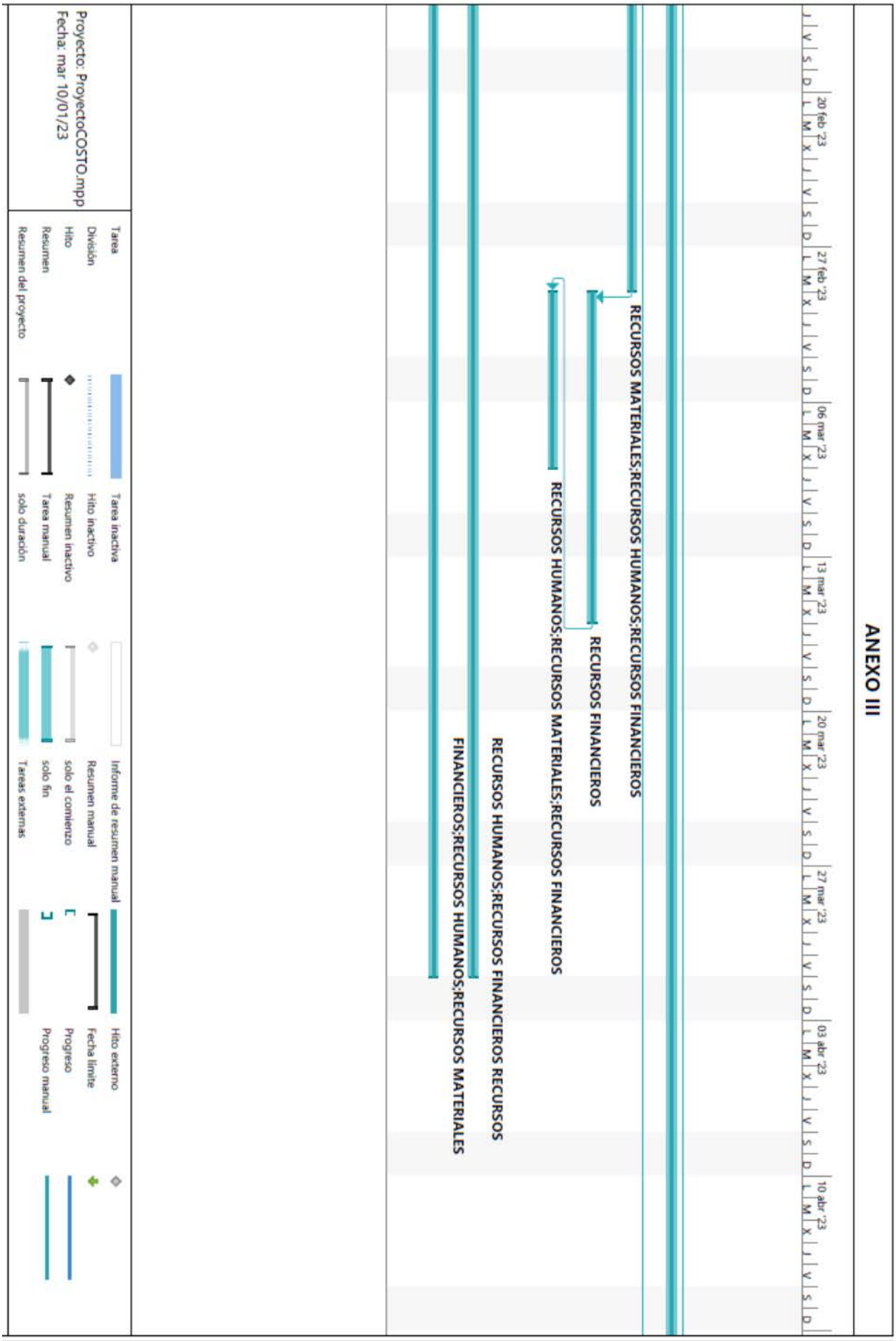
ANEXO III

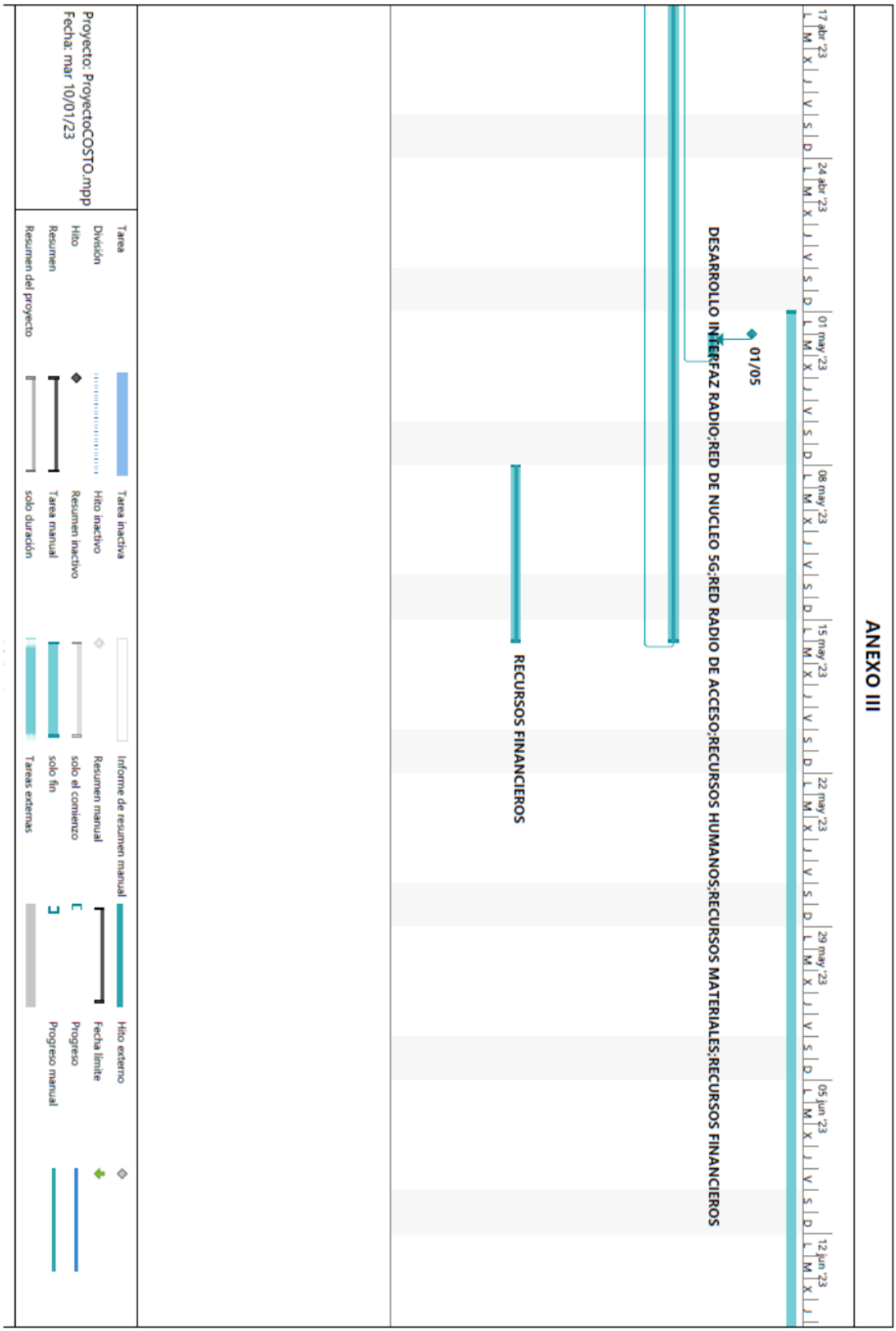
Id	Predecesoras	Nombres de los recursos	Acumulación de costos fijos previstos	Comienzo de la entrega previsto	Fin de la entrega	Costo1
1		DESARROLLO SW 5G INTEGRACION SDR;DESARROLLO DE COMPONENTES	Comienzo	lun 01/05/23	NOD	€100.000,00
2		PROPUESTA DE EMPRESAS DESARROLLO COMPONENTES 5G;PROPUESTA DE	Prorrateo	lun 16/01/23	NOD	€100.000,00
3	2	DESARROLLO INTERFAZ RADIO;RED DE NUCLEO 5G;RED RADIO DE	Prorrateo	lun 16/01/23	NOD	€200.000,00
4	3		Prorrateo	lun 16/01/23	NOD	€100.000,00
5	4	RECURSOS MATERIALES;RECURSOS HUMANOS;RECURSOS FINANCIEROS	Prorrateo	lun 16/01/23	NOD	€50.000,00
6	5	RECURSOS FINANCIEROS	Prorrateo	lun 16/01/23	NOD	€2.000.000,00
7	6	RECURSOS HUMANOS;RECURSOS MATERIALES;RECURSOS FINANCIEROS	Prorrateo	lun 16/01/23	NOD	€900.000,00
8		RECURSOS FINANCIEROS	Prorrateo	lun 16/01/23	NOD	€1.000.000,00
9		RECURSOS HUMANOS;RECURSOS FINAN(	Prorrateo	lun 16/01/23	NOD	€100.000,00
10		RECURSOS FINANCIEROS;RECURSOS HUMANOS;RECURSOS MATERIALES	Prorrateo	lun 16/01/23	NOD	€500.000,00

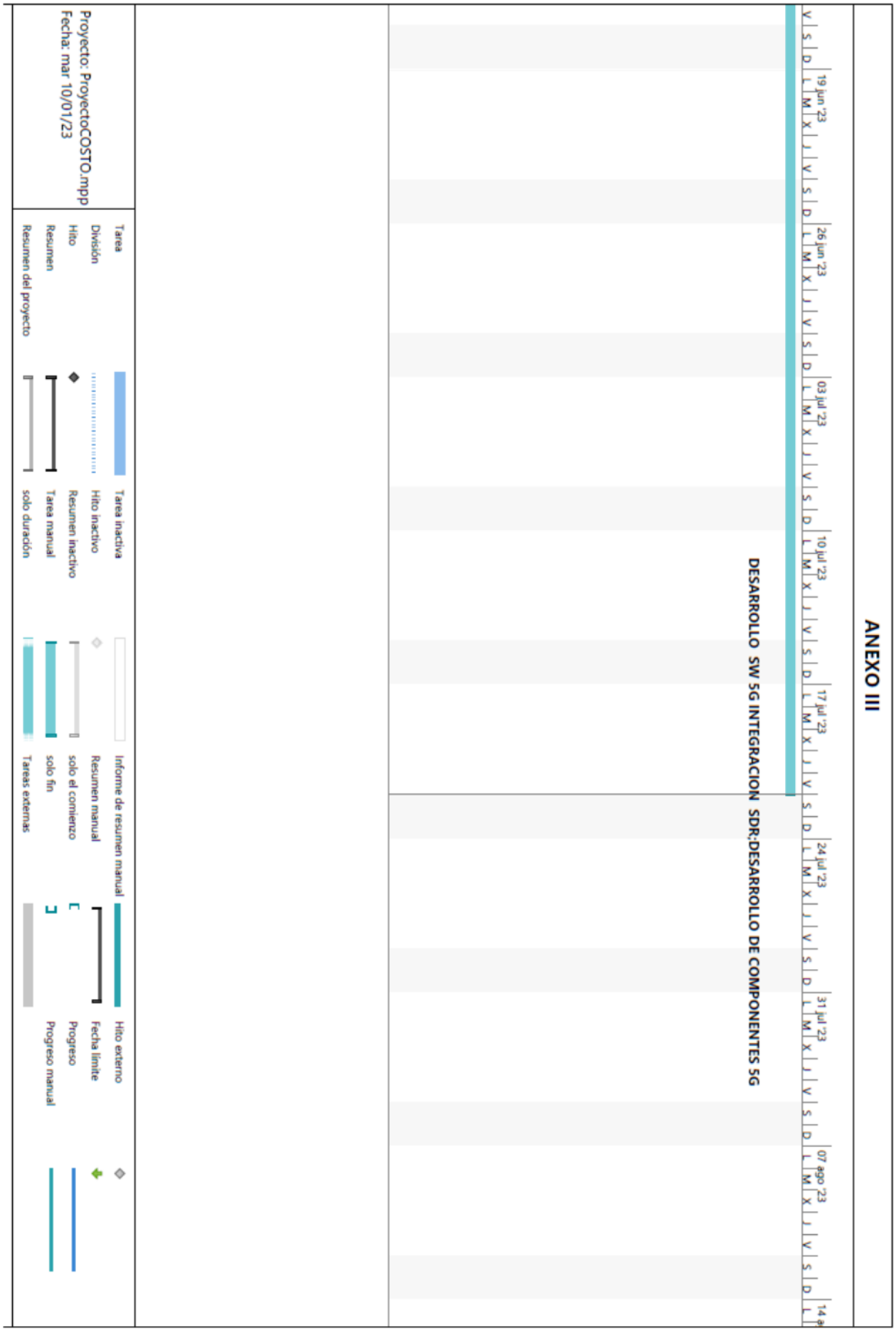


Proyecto: ProyectoCOSTO.mpp
Fecha: mar 10/01/23

Tarea	Tarea inactiva	Informe de resumen manual	Hito externo
División	Hito inactivo	Resumen manual	Fecha límite
Hito	Resumen inactivo	solo el comienzo	Progreso
Resumen	Tarea manual	solo fin	Progreso manual
Resumen del proyecto	solo duración	Tareas externas	


ANEXO III
20 feb '23
27 feb '23
06 mar '23
13 mar '23
20 mar '23
27 mar '23
03 abr '23
10 abr '23
RECURSOS MATERIALES;RECURSOS HUMANOS;RECURSOS FINANCIEROS
RECURSOS FINANCIEROS
RECURSOS HUMANOS;RECURSOS MATERIALES;RECURSOS FINANCIEROS
RECURSOS HUMANOS;RECURSOS FINANCIEROS RECURSOS
FINANCIEROS;RECURSOS HUMANOS;RECURSOS MATERIALES
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Proyecto: ProyectoCOSTO.mpp
Fecha: mar 10/01/23


ANEXO III
17 abr '23
24 abr '23
01 may '23
08 may '23
15 may '23
22 may '23
29 may '23
05 jun '23
12 jun '23
01/05
DESARROLLO INTERFAZ RADIO;RED DE NUCLEO 5G;RED RADIO DE ACCESO;RECURSOS HUMANOS;RECURSOS MATERIALES;RECURSOS FINANCIEROS
RECURSOS FINANCIEROS
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual
Proyecto: ProyectoCOSTO.mpp
Fecha: mar 10/01/23


ANEXO III
19 jun '23
26 jun '23
03 jul '23
10 jul '23
17 jul '23
24 jul '23
31 jul '23
07 ago '23
DESARROLLO SW 5G INTEGRACION SDR;DESARROLLO DE COMPONENTES 5G
Proyecto: ProyectoCOSTO.mpp
Fecha: mar 10/01/23
Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual