Universidad Zaragoza
1542

Trabajo Fin de Grado

LA INTEROPERABILIDAD ENTRE LOS SISTEMAS DE MANDO Y CONTROL DEL EJÉRCITO DE TIERRA (SIMACET) Y DEL EJÉRCITO DEL AIRE (SC2N-EA) EN EL MARCO DE LAS OPERACIONES CONJUNTAS

Jesús Izquierdo Conesa

Director académico: María Teresa Sánchez Rúa

Director militar: Víctor Rafael López Sánchez

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

La realización del presente Trabajo Fin de Grado es fruto de la guía, sugerencias y disposición de la profesora Dña. María Teresa Sánchez Rúa, quien, desde el comienzo de este manuscrito hasta su finalización, ha estado a mi disposición en todo momento para solventar las dudas surgidas, así como para orientarme de manera excelente.

Por otro lado, agradecer al Capitán D. Víctor Rafael López Sánchez su disposición, vía telefónica, para orientarme y solventarme las dudas surgidas a lo largo de toda la realización del TFG, a pesar de su estancia durante todo el periodo en Turquía de misión.

Deseo agradecer profundamente a todo el personal militar del Regimiento de Artillería Aérea Nº73, en especial al Comandante D. Julián David Alcázar López, a la Capitán Dña. Natalia Eugenia Gómez Gabás, al Capitán D. Fco. Javier Mancebo Plaza y al Teniente D. Adrián Sánchez Carrillo, su disposición para ayudarme a realizar este trabajo, dado que sin ellos no habría podido adquirir los conocimientos necesarios.

Además, agradecer al Capitán D. Daniel Álvarez de Pablos y a la Capitán Dña. Elena Fátima Martin Jomse, destinados en el GRUCEMAC, ya que gracias a ellos he podido adquirir los conocimientos necesarios relativos al escalón superior en lo que al Ejército del Aire se refiere.

Y, por supuesto quería agradecérselo a toda mi familia y a mi pareja, dado que han sido los que me han apoyado en todo momento durante estos últimos 7 años de academia. Gracias a ellos he superado todos los obstáculos que se han puesto en el camino, logrando salir adelante y llegar a este punto de culminación de la carrera con este TFG.

RESUMEN

El objetivo principal del presente TFG es conseguir la **interoperabilidad** del Sistema de Mando y Control del Ejército de Tierra (SIMACET) y de la red del Sistema de Mando y Control Nacional del Ejército del Aire (SC2N-EA).

Se pretende buscar una solución a la problemática que tiene actualmente el regimiento al establecer una Unidad de Defensa Antiaérea (UDAA) en la que opera conjuntamente el Ejército de Tierra y el Ejército del Aire. En la situación actual la célula de inteligencia se enfrenta a 2 usuarios, por lo que se trabaja con dos terminales, uno el usuario del SIMACET y otro del SC2N-EA. La solución buscada es unir ambos usuarios en uno, un único portátil, de tal manera que sólo hubiera un operador especializado en ambos sistemas de mando y control.

Para conseguir este objetivo, se proponen 2 soluciones: por un lado, una primera solución, económica, con la que se reciclarían todos los componentes posibles, aunque varios elementos hardware serían sustituidos para que SIMACET pueda recibir la información, tanto del Ejército de Tierra como del Ejército de Aire, manteniendo los niveles de seguridad de cada uno, "*NATO confidential*" y "*NATO secret*", respectivamente. Además, se sustituiría el programa geográfico ANTARES (actualmente en SIMACET) por TALOS Táctico. De esta manera se tendría toda la información unificada y un único operador especializado. Por otro lado, la segunda solución, óptima pero poco económica, en la que se propone el desarrollo de un nuevo sistema que una SIMACET y SC2N-EA llamado SIMACTA (Sistema de Mando y Control Tierra Aire), con el que estarían perfectamente integrados ambos sistemas de mando y control, tanto táctica como técnicamente.

Una vez presentadas las dos soluciones se ha aplicado la metodología AHP para determinar cuál de las dos propuestas es la óptima para llevar a desarrollo, para la cual, los operadores del SIMACET y del SC2N-EA del Regimiento de Artillería Antiaérea Nº73 del primer grupo han contestado dos cuestionarios relativos a la metodología. Con los resultados de los cuestionarios, la metodología AHP ha mostrado que la opción que habría que poner en práctica es la segunda, la creación de un nuevo sistema de mando y control (SIMACTA).

PALABRAS CLAVE

Interoperabilidad

Mando y Control (C2)

Seguridad de la información

ABSTRACT

The main aim of this work is to reach the interoperability of command-and-control system of the Army (SIMACET) and the command-and-control national net of the Air Force (SC2N-EA).

The objective is to look for a solution to the problem that the regiment has to face regarding to the anti-aircraft defence unit (UDAA), in which the Army and the Air Force work jointly. Currently, the intelligent cell must face two users; due to that, this cell works with two laptops and two operators, the first with the SIMACET´s user and the second with the SC2N-EA´s user. The solution for this problem is to join both users in a unique laptop. So, the intelligent cell would only have a specialized user in both command-and-control systems.

To reach this aim, two solutions are proposed: on the one hand, the first solution, economical, is based in recycling all the possible components, although, some elements would be changed to allow that SIMACET can receive the information of the Army and the Air Force, keeping the security levels in which one, “NATO confidential” and “NATO secret”, respectively. Moreover, the geographic program ANTARES (in SIMACET) would be changed by Tactic TALOS. Thus, the system would have all the information in a unique software and with one specialized operator. By the other hand, the second solution, optimal but less economic, consists of the development of a new command and control system that would join SIMACET and SC2N-EA, called SIMACTA (command and control land air). With this system, both command and control systems would be perfectly integrated, such tactically as technically.

After both solutions have been presented, the AHP method is applied to determine which of both solutions is the best to implement. For that, the operators of the SIMACET and SC2N-EA of the anti-aircraft artillery regiment number 73, both first and second groups, have answered two questionnaires. With the results of these questionnaires, the AHP method has shown that the best option to develop is the second one, the creation of a new command and control system (SIMACTA).

KEYWORDS

Interoperability

Command and Control (C2)

Information security

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

Se han elaborado dos columnas, una en español y otra en inglés. Si se encuentran rellenadas las dos columnas, significa que se puede encontrar en los libros, o en la documentación, tanto de una forma como de la otra.

Siglas	Español	Inglés
AAA	Artillería Antiaérea	
ACM	Medidas de control aéreo	*Airspace Control Means*
ACO	Orden de control del espacio aéreo	*Airspace Control Orders*
AD	Defensa aérea	*Air Defence*
ADS	Sistema de defensa aéreo	*Air Defence System*
AHP	Proceso analítico jerárquico	*Analytic Hierarchy Process*
AIRCOM	Mando Aéreo	*Air Command*
ANPIC	Autoridad Nacional para la Protección de la Información Clasificada	
AOAD	Defensa aérea del componente terrestre	*Army Organic Air Defence*
AOC	Centro de operaciones aéreas	*Air Operations Centre*
AOC-D	Centro de operaciones aéreas desplegable	*Air Operation Centre Deployable*
ARS	Agencia de control subordinada a CAOC/AOC	*Air Control Center/ RAP Production Centre/ Sensor Fusion Post*
ARS-D	ARS desplegable	*ARS Deployable*
ASACS	Sistema de vigilancia aéreo	*Air Surveillance and Control System*
ATO	Orden de misión aérea	*Air Tasking Order*
BDT	Base de Datos Técnica	
BMS		*Battlefield Management System*
BOC-D	Base de operaciones aéreas desplegable	*Base Operation Centre Deployable*
C2	Mando y Control	*Command and Control*
CAOC	Centro de operaciones aéreas combinado	*Centre Air Operations Centre*
CG	Cuartel General	*Head quarter*
CIO	Centro de Información y Operaciones	
CIS	Sistema de mando e información	*Command Information System*
CNI	Cuerpo Nacional de Identidad	
COAAAS-M	Centro de Operaciones de Artillería Antiaérea Semiautomático Medio	
CPL	Centro de Personal y Logística	
CRC	Centro de información y control	*Control and Reporting Centre*
CT	Centro de Trasmisiones	
DAA	Defensa Antiaérea	
DACCC	Centro de mando y control aéreo desplegable	*Deployable Air Command and Control Center*
DAFO	Debilidades, Amenazas, Fortalezas, Debilidades	
DPS	Declaración Personal de Seguridad	
DTU	Unidad de terminación de datos	*Database Transaction Unit*
EA	Ejército del Aire	*Army of air*
EBM	Módulos de batería extra	*Extra Battery module*
ET	Ejército de Tierra	*Land army*
EVA	Escuadrón de Vigilancia Aérea	
EW	Guerra electrónica	*Electronic War*
FDC	Centro director de fuegos	*Fire Director Centre*
GAAA	Grupo de Artillería Antiaérea	
GACA	Grupo de Artillería Antiaérea	
GIS	Sistema de información geográfica	*Geographic Information System*
GRUALERCON	Grupo de Alerta y Control	
GRUCEMAC	Grupo Central de Mando y Control	
GRUNOMAC	Grupo Norte de Mando y Control	
GU	Gran Unidad	
HD	Alta definición	*High Definition*

HDD	Unidad de disco duro	*Hard Disk Drive*
HP		*Hewlett Packard*
HPS	Habilitación Personal de Seguridad	
HQ	Cuartel general	*Head Quarter*
ICC		*Integrated Command and Control*
IFF	Identificación amigo-enemigo	*Identification Friend or Foe*
IP		*Internet Protocol*
JADTAGES	Sistema geográfico táctico de defensa aérea conjunta	*Joint Air Defence Tactical Geographic System*
JCHAT	Chat conjunto	*Joint Chat*
JEMAD	Jefe de Estado Mayor de la Defensa	
JFAC	Componente aéreo de la fuerza conjunta	*Joint Force Air Command*
JFLC	Componente terrestre de la fuerza conjunta	*Joint Force Land Command*
LAN	Red de área local	*Local Area Network*
LCC	Mando componente terrestre	*Land Component Command*
MAAA	Mando de Artillería Antiaérea	
MACANA	Mando de Canarias	
MACOM	Mando Aéreo de Combate	
MAPSIT	Mapa de situación	*Map Situation*
MCEA	Medidas de Control del Espacio Aéreo	
MIXCHAT	Chat mixto	*Mixed Chat*
MOA	Mando Operativo Aeroespacial	
NAT	Traducción de direcciones de red	*Network Address Translation*
OC	Centro de operaciones	*Operations Centre*
OPTASK EW	Mensaje operativo de guerra electrónica	*Operational Tasking of Electronic War*
OPTASK LINK	Mensaje operativo de enlace	*Operational Tasking of Link*
OTAN	Organización del Tratado Atlántico Norte	
PC	Puesto de mando	*Planning Cell*
PU	Pequeña Unidad	
RAAA	Regimiento de Artillería Antiaérea	
RAM	Memoria de acceso aleatorio	*Random Access Memory*
RAP	Imagen de situación aérea	*Recognized Air Picture*
RI	Razón de Inconsistencia	
S-1	Sección de Personal	
S-2	Sección de Inteligencia	
S-3	Sección de Operaciones	
S-4	Sección de Logística	
SA	Designador de AAA	*SAM Allocator*
SAI	Sistema de Alimentación Ininterrumpida	
SAM	Misil superficie-aire	*Surface to Air Missile*
SBAD	Defensa Aérea basada en superficie	*Surface Based Air Defence*
SC2N-EA	Sistema de Mando y Control Nacional del Ejército del Aire	
SHPS	Solicitud de la Habilitación Personal de Seguridad	
SIMACET	Sistema de Mando y Control del Ejército de Tierra	
SIMACTA	Sistema de Mando y Control Tierra Aire	
SO	Sistema Operativo	
TDO	Oficial director táctico	*Tactic Officer Director*
TFG	Trabajo Fin de Grado	
TN	Territorio Nacional	
UCE	Unidad de Control de Empeños	
UDAA	Unidad de Defensa Antiaérea	
UE	Unión Europea	
UMG	Unidad Mínima de Generación	
UT	Unidad de Tiro	
UTMAAA	Unidad de Transmisiones de Artillería Antiaérea	
VJTF	Fuerza conjunta de muy alta disponibilidad	*Very High Readiness Joint Task Force*

VPN	Red virtual privada	*Virtual Private Network*
WA		*Weapons Allocator*
WAN	Red de área amplia	*Wide Area Network*

1 Introducción

Este Trabajo de Fin de Grado (TFG), se ha realizado en el Regimiento de Artillería Antiaérea Nº73 (RAAA 73), en el Acuartelamiento Tentegorra situado en la ciudad portuaria de Cartagena.

El Regimiento citado lleva a cabo a lo largo del año numerosos ejercicios en los que interopera con el Ejército del Aire (EA), en lo que a Mando y Control (C2) se refiere, ejercicios tales como la generación de una Unidad de Defensa Antiaérea (UDAA), el ejercicio Mando Operativo Aeroespacial (MOA)[1], o formando parte de la fuerza conjunta de muy alta disponibilidad (*Very high readiness Joint Task Force*, VJTF)[2], entre otros.

El Ejército de Tierra (ET) cuenta con el Sistema de Información para el Mando y Control del Ejército de Tierra (de ahora en adelante SIMACET), y el Ejército del Aire con la red del Sistema de Mando y Control Nacional del Ejército del Aire (de ahora en adelante SC2N-EA). Si bien ambos sistemas de C2 muestran información sobre la operación en curso a desarrollar, el SIMACET se limita a las Unidades del ET y el SC2N-EA a la información del espacio aéreo.

A la hora de establecer un Puesto de Mando (*Planning Cell*, PC) de una UDAA, la visualización de la información proveniente de ambos sistemas de C2 se realiza en distintos terminales por parte de dos usuarios distintos, uno para cada usuario. Esto limita el conocimiento global del campo de batalla y de la operación en sí, al resultar difícil el trasvase de información entre ambos operadores, dado que no existe una forma de explotar la información de ambos sistemas de forma conjunta en un único usuario.

Por tanto, este trabajo se centrará en dar solución a la problemática citada. Para ello, se llevará a cabo un rediseño de los actuales sistemas de C2, uniendo la información de ambos en un único terminal, consiguiendo así su **interoperabilidad**.

2 Objetivos y Metodología

2.1 Objetivos y Alcance

El alcance de este trabajo es rediseñar el actual SIMACET para que pueda **interoperar** con la red del SC2N-EA.

Para ello se plantean los siguientes objetivos:

1. Determinar las capacidades del SIMACET.
2. Determinar las capacidades del SC2N-EA.
3. Determinar el método de **interoperabilidad** entre ambos y los elementos necesarios para ello.
4. Determinar qué solución sería la más adecuada a la hora de solventar el problema.

[1] MOA: es una misión permanente en la que cooperan el ET, el EA y la Armada para llevar a cabo la vigilancia, control y policía aérea, con el fin de proteger el espacio aéreo español.

[2] VJTF: Es una brigada multinacional de maniobra con apoyos vía aérea, marítima y fuerzas especiales, que se formará sobre un núcleo principal de fuerzas aportado por nación que la lidera, al que se suman elementos de otras naciones. El mando de la VJTF lo ejercerán, con carácter rotatorio, los Cuarteles Generales de Alta Disponibilidad de la estructura de fuerzas de la alianza [33].

2.2 Metodología

Para llevar a cabo la memoria de este TFG, se ha realizado un estudio prospectivo del estado del arte de ambos sistemas de C2, SIMACET y SC2N-EA.

Inicialmente, se llevó a cabo una investigación exhaustiva en el RAAA 73 para conocer todo lo referente a ambos sistemas de C2. A continuación, se realizaron entrevistas con expertos en la materia, tanto presencialmente en el regimiento como telemáticamente con aquellos destinados en otras unidades.

La asistencia al ejercicio “Dardo”, llevado a cabo en el regimiento durante la semana del 13 al 17 de septiembre de 2021, permitió comprobar de primera mano cómo se utiliza el SIMACET, sus capacidades y debilidades. En este ejercicio interactuaban los sistemas de C2 de todos los grupos de todos los regimientos de artillería antiaérea integrados en el mando de artillería antiaérea (ubicado en Fuencarral, Madrid).

Para profundizar en el conocimiento acerca del SC2N-EA, se estableció contacto con un Capitán y una Capitán de Artillería Antiaérea (AAA) especialistas en el sistema, ambos destinados como figuras del ET en el ARS, el centro de control aéreo.

Con vistas a estudiar la **interoperabilidad** de los dos sistemas de C2, se llevó a cabo un *Focus Group*, con el que se trató de conocer las opiniones de los especialistas en ambos sistemas, relativas a sus fortalezas y limitaciones, así como posibles mejoras. También se realizó un *Brainstorming*, con el que se trataba de conocer el punto de vista de los operadores en cuanto a qué elementos debería poseer imprescindiblemente un nuevo sistema de C2 que integre al SIMACET y al SC2N-EA.

Por último, se llevó a cabo entre todos los operadores de los sistemas de C2 de los dos grupos de artillería antiaérea del regimiento, donde se han realizado las prácticas, una encuesta.

Una vez analizados todos los resultados obtenidos, se propusieron dos posibles soluciones. Una de ellas está basada en la mejora de SIMACET para subsanar el problema actual, conectando de modo seguro la red del SC2N-EA al nodo del SIMACET, y sustituyendo la aplicación geográfica utilizada, por otra más adecuada que permita visualizar tanto la información de las unidades propias del ET como la información recibida del EA. Para determinar la aplicación adecuada, se realizaron análisis DAFO entre las dos opciones posibles. La segunda solución es la creación de un nuevo sistema de C2, así como el desarrollo de algunas de las aplicaciones necesarias para ejercer el mando de la operación, denominado Sistema de Información para el Mando y Control Tierra Aire (SIMACTA).

Por último, se realizó un análisis AHP de ambas soluciones, donde los criterios de selección fueron determinados gracias a la colaboración de operadores del SIMACET y del SC2N-EA de la batería de plana del Grupo de Artillería Antiaérea I/73. De este modo, se determinó la opción más viable para implementar en el puesto de mando de una UDAA.

3 Antecedentes y Marco Teórico

En esta sección, se explican los conceptos necesarios para el desarrollo y análisis del trabajo en base a la Unidad de Defensa Antiaérea (UDAA).

3.1 Artillería Antiaérea y Mando de Artillería Antiaérea

Según el Manual de Empleo de la artillería antiaérea PD4-300 Tomo I: “La Artillería Antiaérea (AAA) está formada por un conjunto de unidades especialmente concebidas,

organizadas, adiestradas y equipadas para llevar a cabo acciones de Defensa Antiaérea (DAA). Estas unidades se organizan con el personal y el material adecuado para llevar a cabo la preparación y generación de organizaciones operativas." [28, Pág. 1-1]

Por ello, la AAA es el órgano fundamental del ET encargado de la DAA, cuya misión es la protección de las unidades e instalaciones sensibles o vitales contra cualquier acción aérea hostil.

A nivel peninsular, el escalón superior de la AAA es el Mando de Artillería Antiaérea (MAAA), ubicado en Fuencarral (Madrid), encargado de emitir las órdenes a todas las unidades de artillería antiaérea bajo su mando.

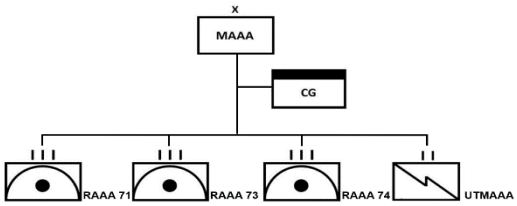


Figura 2 Organigrama del MAAA. Fuente: elaboración propia.

El MAAA es el órgano del ET responsable de la generación de las organizaciones operativas de defensa antiaérea necesarias para proporcionar un control del espacio aéreo y una defensa antiaérea de las distintas zonas o puntos de interés del Territorio Nacional (TN), integrando sus unidades en el sistema de defensa aérea (*Air Defence System,* ADS), así como en las organizaciones operativas de nivel superior. El MAAA está compuesto por tres Regimientos de Artillería Antiaérea (RAAA), el Cuartel General (CG) y la Unidad de Transmisiones del Mando de Artillería Antiaérea (UTMAAA) (véase Figura 1). En la Figura 2 se muestra la distribución de las unidades del MAAA en el TN [10].

Figura 1 Organización estratégica del MAAA. Fuente: elaboración propia a partir de [10].

Además, fuera de la península se encuentra otra unidad de AAA, el RAAA 94, ubicado en Las Palmas de Gran Canaria (Islas Canarias). Esta unidad no depende del MAAA, sino del Mando de Canarias (MACANA), localizado en Santa Cruz de Tenerife [11].

3.1.1 Unidad de Transmisiones del Mando de Artillería Antiaérea

La Unidad de Transmisiones del Mando de Artillería Antiaérea (UTMAAA), como parte integrante del MAAA, presta los servicios de transmisiones que requiere el ET. Esta Unidad tiene entidad batallón y como se puede observar en la Figura 2, consta de una compañía en El Pardo (Madrid) y otra en Dos Hermanas (Sevilla). Para coordinar su funcionamiento dispone de una Plana Mayor de Mando, ubicada en Madrid.

"La misión principal de la UTMAAA es establecer, mantener y en su caso explotar, un sistema de telecomunicaciones e información para favorecer el C2 del MAAA en su misión permanente de defensa aérea. Esta misión permanente se transforma en una integración en tiempo real[3] de todos los sistemas de armas de artillería en el sistema conjunto/combinado de defensa aérea nacional." [12]

[3] Tiempo real: dícese del periodo temporal en el que se desarrollan acciones de fuego real, así como las órdenes de C2 pertinentes para ello, a través del centro director de fuegos. En cambio, tiempo no real es aquel periodo en el que se llevan a cabo labores de C2 referentes a personal, logística, información y operaciones, a través del Centro de Información y Operaciones (CIO) y del Centro de Personal y Logística (CPL).

3.1.2 Defensa Aérea, Sistema de Defensa Aérea y Defensa Antiaérea

"La Defensa Aérea (*Air Defence*, AD) se define como el conjunto de todas las medidas diseñadas para anular o reducir la eficacia de la acción hostil. Las operaciones de defensa aérea conjuntas buscan lograr el nivel apropiado de control del espacio aéreo y, así, la protección de la fuerza. Integra capacidades de defensa aérea de los componentes terrestre, naval y aéreo, y en su caso, aquellos otros que se pudiera constituir y puedan contar con capacidades de AD." [28, Pág. 1-1]

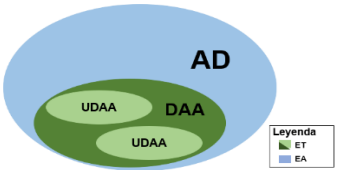


Figura 3 Representación de una UDAA en una AD. Fuente: elaboración propia.

La Figura 3 muestra cómo se integran las UDAA dentro de una DAA en una AD.

Estas operaciones de AD son gestionadas por el sistema de defensa aérea (*Air Defence System*, ADS), que consta por un lado de todas estas medidas de AD, y por otro, está equipado con los sistemas de C2, sistemas de armas superficie-aire y medios de apoyo logístico, necesarios para el sostenimiento de las operaciones durante el tiempo que sea necesario. De esta manera, el ADS se materializa con la **interoperabilidad** del ET y del EA, aunque en ejercicios específicos también interopera la Armada, en lo que a sistemas de C2 para la defensa del espacio aéreo se refiere.

"La Defensa Antiaérea (DAA) es la contribución de las unidades de superficie a la defensa aérea y comprende el conjunto de actividades desarrolladas por la fuerza terrestre para anular o reducir la eficacia de cualquier acción aérea hostil, lo que incluye todo el espectro de la amenaza aérea." [28, Pág. 1-1]

La DAA se basa en una serie de principios: principio de masa, principio de armas convencionales, principio de movilidad y principio de integración. De todos estos, para este TFG, el más importante será el principio de integración: "Comprende las actividades, medios y procedimientos encaminados a sincronizar y coordinar las operaciones militares en todos sus niveles." [28, Pág. 2-5]

3.1.3 Concepto de Unidad de Defensa Antiaérea

"La Unidad de Defensa Antiaérea (UDAA) es la unidad fundamental de empleo de la AAA, en la que se ven materializados los principios de la defensa antiaérea." Es una unidad eventual organizada por el MAAA con el fin de hacer frente a una amenaza, cumplir unos objetivos, etc., y "se organiza sobre la base de una unidad orgánica de tipo grupo o batería de AAA a la que se incorporan o detraen módulos de capacidades de C2, de fuego, de apoyo logístico, Sistemas de Información y Comunicación (CIS), de protección de fuerza, etc.," para generar Unidades Mínimas de Generación (UMG) "de la organización operativa que se requiere. Cuenta con todos los medios necesarios para cumplir la misión." [28, Pág. 3-4]

La UMG es "aquella unidad por debajo de la cual no debe emplearse el sistema para hacer fuego sin peligro de degradar sus capacidades operativas. Las UMG son diferentes para cada sistema de armas y nunca serán inferiores a la Unidad de Tiro (UT). Se le pueden incluir núcleos logísticos, de mando y control, de fuego, etc." [28, Pág. 3-5]

"Una UT es la mínima unidad de artillería capaz de ejecutar una acción de fuego, cuenta con todos los medios necesarios para realizar la secuencia de fuego completa: detección, identificación, adquisición, seguimiento y fuego." [28, Pág. 3-5]

En el caso de los sistemas de armas que tiene el RAAA 73, la UMG tanto del Grupo de Artillería Antiaérea número uno (GAAA I/73) como el GAAA II/73, cuyos sistemas de armas son el cañón 35/90 y el Nasams respectivamente, es de entidad batería. Por otro lado, la UT del

GAAA I/73 es de entidad sección, y la UT del GAAA II/73 es de entidad batería.

La Figura 4 muestra de manera esquemática el proceso de creación de una UDAA.

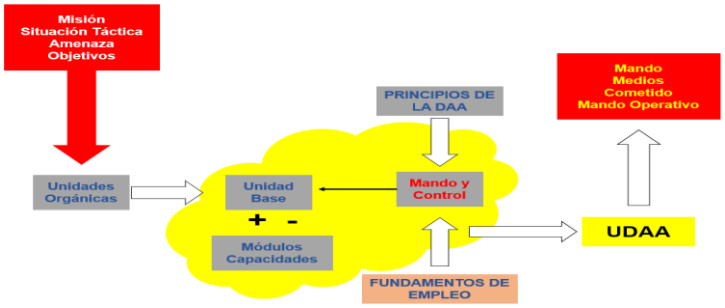


Figura 4 Proceso de generación de una UDAA. Fuente: readaptación propia a partir de [28].

A modo de ejemplo, en la Tabla 1 se muestra la creación de una UDAA en base al RAAA 73 y se detallan a continuación todos los elementos que la forman.

Tabla 1 Organización operativa de una UDAA del RAAA 73. Fuente: elaboración propia.

NÚCLEO DE MANDO Y CONTROL	NÚCLEO DE FUEGO	NÚCLEO LOGÍSTICO
1. Batería de Plana Unidad Base Generadora:	1. Batería de Armas Unidad Base Generadora:	1. Batería de Servicios Unidad Base Generadora:
1.1. Puesto de Mando: 1.1.1. CIO 1.1.2. CPL 1.1.3. FDC	1.1. UMG GAAA I/73 1.2. UMG GAAA II/73	1.1. Mantenimiento 35/90 1.2. Mantenimiento Nasams
1.2. RAC 3-D		
2. Centro de Transmisiones (UTMAAA)		

Como se puede apreciar en la Tabla 1, el núcleo de C2 está formado por una batería de plana del Grupo de AAA (GAAA) tomada como unidad base generadora, y por un Centro de Transmisiones (CT). En la batería de plana, nos encontramos con: el puesto de mando (PC UDAA) o Centro de Operaciones de Artillería Antiaérea Semiautomático Medio (COAAAS-M), que engloba al Centro de información y Operaciones (CIO), al Centro de Personal y Logística (CPL) y al centro director de fuegos (*Fire Director Center*, FDC). También cuenta con un radar RAC 3-D.

En la Figura 5 se puede observar cómo se adoptaría el despliegue del núcleo de C2 del ejemplo de UDAA anterior. En todos los casos, el radar RAC 3-D estaría situado a unos 1000m del puesto de mando. En el PC UDAA se llevan a cabo todas las tareas de C2, tanto en tiempo real como en tiempo no real.

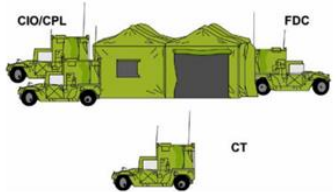


Figura 5 Concepto de PC UDAA. Fuente: [28, Pág. 5-5].

El FDC es el órgano del PC UDAA que lleva a cabo la distribución y control de los fuegos durante la conducción del combate antiaéreo de la UDAA en tiempo real. En éste se recibe la información por datos y fonía del escalón superior de fuegos (el ARS) para realizar la AD con sus sistemas de armas, además de la información generada por el RAC-3D. Por otro lado, tiene comunicación en tiempo no real por fonía con el CIO de la UDAA. "Su funcionamiento estará dirigido por el oficial director táctico (*Tactic Director Officer*, TDO), responsable de tomar, en representación del jefe de la UDAA, las decisiones concernientes al control táctico de las armas y de los fuegos de la unidad." [28, Pág. 5-9]

El escalón superior de la UDAA, en lo que a tiempo real se refiere, siempre es el ARS (detallado en el Apartado 3.2), el cual manda por datos toda la información, relativa a las trazas aéreas y a las órdenes de fuego, al FDC de la UDAA. Además, por fonía se corrobora que esas órdenes han sido correctamente recibidas. En caso de tiempo no real, el escalón superior de la

UDAA sería: un Teniente General del EA, jefe del Mando Aéreo de Combate (MACOM) si de ambiente SBAD (*Surface Based Air Defence,* defensa aérea basada en superficie) se tratase; o un Teniente General del ET, jefe del mando de componente terrestre (*Land Component Command*, LCC), si de ambiente AOAD (*Army Organic Air Defence*, defensa aérea del componente terrestre) se tratase. En el Apartado 3.2, se explican en profundidad ambos ambientes.

En el CIO se planean, coordinan y conducen las actividades de la UDAA relacionadas con el C2 táctico de la batalla antiaérea en tiempo no real tanto con el ET como con el EA. Por otro lado, el CPL es el encargado de planear y conducir las actividades destinadas a las funciones logísticas de la UDAA y sus unidades subordinadas, así como llevar un control del personal.

Todo el personal perteneciente al PC UDAA debe de estar acreditado con la Habilitación Personal de Seguridad (HPS) correspondiente (véase Anexo A), para lo que habrá tenido que realizar la Solicitud de Habilitación Personal de Seguridad (SHPS) (véase Anexo A). Cabe destacar que el operador del SIMACET requiere de una HPS de "Confidencial" (a nivel nacional), equivalente a "*NATO confidential*" (a nivel OTAN), mientras que el personal que tenga acceso a información proveniente del EA deberá estar acreditado con un nivel superior de seguridad, correspondiente a "Secreto", equivalente a "*NATO secret*".

Hay que distinguir dos figuras: el jefe de operaciones de la UDAA, un Comandante, que se encuentra junto al CIO y el CPL, encargado de que la operación se desarrolle satisfactoriamente; y el jefe de la UDAA, el Teniente Coronel jefe de la Unidad Base Generadora que forma la UDAA. Este último suele estar junto al jefe de operaciones, pero en ambiente AOAD, se encontrará junto al LCC, para su asesoramiento del empleo de la AAA.

"La UDAA debe disponer de un sistema de transmisiones seguro y fiable que permita el enlace con: el ADS; el puesto de mando de la unidad o elemento apoyado o protegido; el Puesto de Mando de Artillería Antiaérea (PC AAA) superior; elementos integrados en la propia UDAA (unidades de fuego y unidades de tiro, elementos de apoyo logístico…); y con los sistemas de vigilancia de la propia UDAA (sensores y puestos de observación)." [28, Pág. 5-11]

Por ello, la UDAA dispone de un CT que materializa ese enlace, integrado por la UTMAAA. Es la encargada, cuando se está desarrollando una operación, de proveer todo enlace necesario a los diferentes puestos de mando: por cable (RJ45 de datos y fonía) o asignando unas direcciones IP específicas a los sistemas para la conexión por satélite.

El núcleo de fuego está compuesto por un número variable de UT de uno o varios sistemas de armas, provenientes de una unidad base generadora.

Por último, el núcleo logístico se crea a partir de la unidad de servicios de la unidad base generadora de la UDAA. Normalmente dispone de los apoyos logísticos generales, así como de los específicos de cada sistema de armas.

3.2 ARS

El ARS es el centro de control aéreo encargado de generar imágenes relativas a la información de las aeronaves que sobrevuelan el TN, como el código de la aeronave, altura de vuelo y su trayectoria, etc., a través de la información proporcionada por todos los radares (tanto civiles como militares) desplegados a lo largo del TN.

La Figura 6 muestra la cadena orgánica que existe desde el más alto escalón hasta los ARS, en lo que a vigilancia y control del espacio aéreo se refiere. En la cúspide de la cadena orgánica se encuentra el cuartel general del *Allied Air Command* (AIRCOM), ubicado en Ramstein (Alemania). Éste es el mando de componente aéreo de la OTAN, del cual depende el C2

responsable de planear y conducir las actividades que con carácter permanente se desarrollan por el poder aéreo en el territorio de la alianza.

"La estructura permanente del AIRCOM comprende de: el cuartel general (*Headquarters*, HQ) antes citado, que incluye un centro de operaciones (*Operations Centre*, OC) y el núcleo del mando componente aéreo (*Core Joint Force Air Component*, Core-JFAC); dos CAOC, uno ubicado en Uedem (Alemania) y otro ubicado en Torrejón de Ardoz (Madrid); y un centro de mando y control aéreo desplegable (*Desployable Air Command and Control Center*, DACCC), ubicado en Poggio Renatico (Italia)." [29, Pág. G-1]

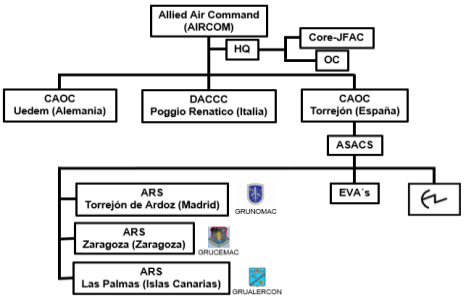


Figura 6 Organigrama AIRCOM. Fuente: elaboración propia basada en [28].

En el centro de operaciones aéreas (*Combined Air Operations Centre*, CAOC, o *Air Operation Center*, AOC) se encuentra el Mando Aéreo de Combate (MACOM). Desde aquí se lleva a cabo el planeamiento y conducción de la AD, así como su coordinación con las operaciones terrestres en tiempo no real. En este centro se elaboran las órdenes de misión aérea (*Air Tasking Order*, ATO), así como el plan de AD de la ATO, las órdenes de control del espacio aéreo (*Air Airspace Control Order*, ACO), la gestión de enlaces tácticos (OPTASK LINK)[4], guerra electrónica (OPTASK EW)[5], plan de comunicaciones del CAOC, etc.

El ACO es el documento con las órdenes de control del espacio aéreo. En estos documentos se recoge la información relativa a las Medidas de Control del Espacio Aéreo (MCEAs o *Air Control Management*, ACM). Asimismo, recoge los criterios que debe reunir una traza para ser considerada como amiga (*friend*), enemiga (*hostile*) o desconocida (*unknown*), los criterios de autodefensa y el IFF[6] modo 1 para cada espacio temporal.

El ATO es el documento relativo a las órdenes de misión aérea, donde se incluyen las rutas, salidas y destinos de los desplazamientos de las aeronaves de las que tenemos conocimiento, el indicativo de cada aeronave y el IFF modo 3 para cada aeronave.

Tanto el ATO como el ACO se generan diariamente; de esta manera, se podrá identificar por procedimiento si una nave es amiga o enemiga durante la vigilancia y control del espacio aéreo.

"El sistema de vigilancia y control aéreo (*Air Surveillancce and Control System*, ASACS) está compuesto esencialmente por sensores (en España, la red de escuadrones de vigilancia aérea [EVAs]), agencias de mando y control (los ARS) y otros medios fijos o desplegables que contribuyen a las labores permanentes de vigilancia y control de los espacios aéreos del TN y aliado, así como a la dirección táctica de las operaciones aéreas en su zona de responsabilidad." [29, Pág. G-1]

El ASACS obtiene la información del espacio aéreo de los medios fijos o desplegables que contribuyen a la vigilancia y control, tanto civiles como militares. La función del ASACS en

[4] OPTASK LINK (*Operational Tasking of Link*, mensaje operativo de enlace): mensaje con instrucciones para el establecimiento de los enlaces automáticos de datos [29].

[5] OPTASK EW (*Operational Tasking of Electronic Warfare*, mensaje operativo de guerra electrónica): mensaje con instrucciones de guerra electrónica [29].

[6] IFF (*Identification Friend or Foe*, identificación amigo o enemigo): Sistema de identificación criptográfica para distinguir aeronaves enemigas de las que no lo son. Tiene hasta 4 modos [29].

definitiva es poner a disposición de los ARS toda la información que se ha recibido de todos los sensores, cargándola en la base de datos de la red del SC2N-EA destinada a ello, para así transformarla en lo que se relata a continuación.

Las siglas "ARS" significan: A: *Air Control Center*, R: RAP (*Recognised Air Picture*) *Production Center*, S: *Sensor Fusion Post*.

Según el Manual de Empleo de la artillería antiaérea PD4-300 Tomo II: "Los ARS o también llamados CRC (*Control and Reporting Centre*), son elementos del sistema de mando y control de la defensa aérea cuya misión principal es la producción de la RAP (*Recognised Air Picture*) en su área de responsabilidad y el control táctico centralizado de las aeronaves de la defensa aérea y los sistemas SBAD." [29, Pág. G-12]

El ARS es el encargado de transformar la información proporcionada por el ASACS en imágenes de situación aérea (RAP), donde aparecen todas las trazas aéreas detectadas. Las RAP creadas se recogen en otra base de datos de la misma red, así el ARS podrá explotarla para llevar a cabo la AD. La base de datos en la que el ARS recoge todas las RAP, es la NATO-ICC (*NATO Integrated Command and Control*).

Cabe destacar, que la RAP se actualiza constantemente, segundo tras segundo. Es una imagen aérea en tiempo real, en la que se visualizan todas las trazas de todas las aeronaves que hay sobrevolando el espacio aéreo. Ésta es la información del espacio aéreo enviada al operador de S-2 del CIO en una UDAA.

En España hay tres ARS: uno próximo al CAOC en la base aérea de Torrejón de Ardoz (Madrid); otro ubicado dentro del aeropuerto de Zaragoza (Zaragoza) y el tercero en Las Palmas (Islas Canarias). En cada uno de ellos, está integrado el Grupo Norte de Mando y Control (GRUNOMAC), Grupo Central de Mando y Control (GRUCEMAC) y Grupo de Alerta y Control (GRUALERCON), respectivamente.

En el ARS se encuentra el *Weapons Allocator* (WA), responsable de la asignación de trazas y la distribución de información sobre la situación aérea a las UDAAs que se encuentren bajo su responsabilidad. Además, es el responsable de decidir qué sistemas de armas (aeronaves propias del EA o sistemas de AAA del ET) combaten a cada objetivo, y, por lo tanto, asigna a cada *SAM* (*Surface to Air Missile*) *Allocator* los objetivos que debe combatir.

EL *SAM Allocator* (SA), también situado en el ARS, es el experto en operaciones de DAA; está en contacto permanente con el WA informándolo de todo lo que ocurre en la UDAA, siendo responsable ante éste de todas sus decisiones. Se encarga de controlar el combate de las UDAAs que tenga asignadas, así como de aceptar las trazas recibidas del WA y mandarlas al FDC correspondiente para combatirlas. Para aumentar la seguridad de la información, tiene que confirmar por voz con el FDC todas las órdenes de control de fuegos que se transmitan mediante enlace de datos. Tanto este elemento como el WA son operadores pertenecientes al ET, en concreto del arma de AAA [29].

Se diferencian dentro de la AD, dos ambientes: el SBAD, desarrollado cuando se lleva a cabo la protección y defensa antiaérea de objetivos de interés conjunto, que suelen ser puntos vitales en los que se establece una defensa estática; y el AOAD, que se materializa cuando se destina esa AD a la protección de las fuerzas y organizaciones operativas terrestres o unidades de maniobra desplegadas y otros objetivos de interés en el área de responsabilidad LCC.

Ambos ambientes, a la hora del desarrollo de la operación se diferencian en que: en el SBAD es el componente aéreo de la fuerza conjunta (*Joint Force Air Component*, JFAC) el que lleva a cabo el planeamiento de cómo y dónde se posicionarán las UDAAs, donde el jefe es el MACOM; y en el ambiente AOAD, es el componente terrestre de la fuerza conjunta (*Joint Force Land*

Component, JFLC) el que lleva a cabo tal planeamiento, siendo el LCC el jefe de la operación. En este caso, el Teniente Coronel jefe de la UDAA, estará en contacto con el LCC para asesorar sus decisiones, y llevar a cabo el C2 de su UDAA.

En ambos casos el ARS es el responsable del control de la DAA y de las órdenes de fuego. Por lo tanto, en tiempo real siempre mandará el ARS las órdenes de fuego, y la única potestad que varía en un ambiente u otro es el planeamiento de la UDAA dentro de la AD.

En la Figura 7 puede observarse cómo varía el flujo de información, sea en tiempo real o no, a la hora de llevar a cabo el combate aéreo, tanto en ambiente AOAD como en SBAD.

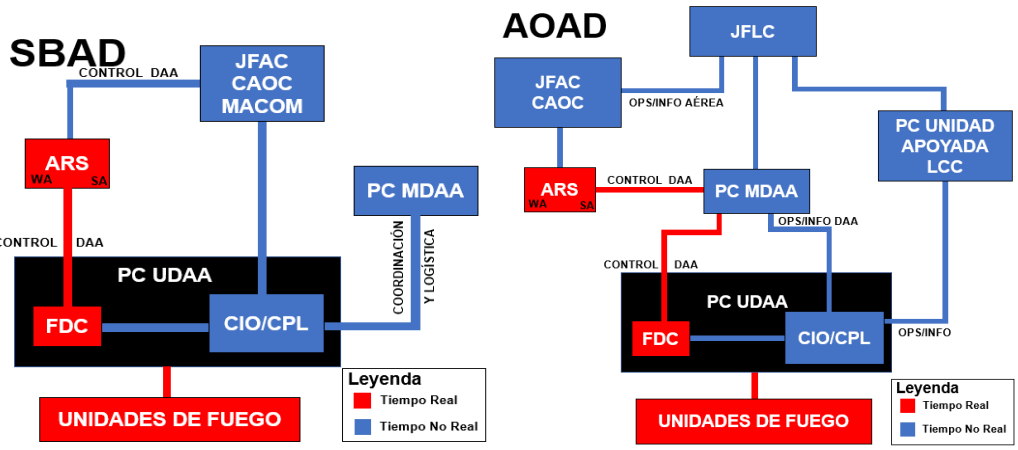


Figura 7 Flujo de información en ambiente SBAD y AOAD. Fuente: readaptación propia a partir de [28].

Para hacer frente a esta diversidad de misiones, escenarios y elementos a defender, la AAA debe ser modular, polivalente e **interoperable** con el sistema de C2 de la AD y, en su caso, con el C2 correspondiente a la organización operativa terrestre protegida. Más adelante el desarrollo de este TFG recogerá el estudio realizado sobre la posible interoperabilidad entre el C2 del ET y el del EA.

3.3 Sistemas de Información para el C2

3.3.1 Sistema de información para el Mando y Control del Ejército de Tierra

Según el Manual de Establecimiento y Empleo de SIMACET (PD3-602): “El Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) es la herramienta que permite al jefe la dirección, planeamiento y la conducción de las operaciones militares, así como obtener una visión coherente y homogénea del escenario terrestre. Asimismo, facilita la toma de decisiones, su difusión y el intercambio de información entre los diferentes escalones.” [26, Pág. 1-1]

Es un sistema de C2 cuya seguridad a nivel OTAN es “*NATO confidential*”, con personal operando en tiempo no real, llevando a cabo lo relativo a mensajería, posicionamiento de unidades, personal, logística, conducción de la operación, etc. Para que el personal pueda operar el SIMACET deben poseer una HPS del mismo grado que la seguridad que del sistema.

Este sistema lo utilizan todas las armas del ET, pero en este TFG se tratará su empleo por parte de la AAA, el MAAA y las UDAAs.

SIMACET incluye a nivel funcional diferentes aplicaciones de gestión táctica, de información geográfica, de mensajería y para otras utilidades que facilitan el C2 de la UDAA.

3.3.1.1 Estructura virtual del SIMACET

El sistema consiste en una serie de nodos de Pequeña Unidad (PU)[7] y uno de Gran Unidad (GU)[8] interconectados entre sí. Todos ellos están conectados a la Base de Datos Táctica (BDT)[9], que se encuentra en el nodo de GU, situado en Fuencarral (Madrid), junto al MAAA. Toda la información introducida al sistema por cualesquiera de los nodos, así como su modificación será visible de inmediato en cualquiera de ellos gracias al sistema de réplica [25].

El sistema de réplica se basa en la existencia de una base de datos en cada nodo, cuyas modificaciones se comparten (réplicas) mediante distintos sistemas de transmisión, de tal modo que, las bases de datos de todos los nodos contengan la misma información.

Una red lógica de réplica sería la formada por una serie de terminales con sus determinados usuarios conectados a un nodo de PU, mediante una conexión de área local (Local Area Network, LAN). Este nodo ejerce de nodo pasarela, para interconectarse con otros nodos pasarela con sus propias redes lógicas de réplica, creando así una red de redes lógicas de réplica [26].

Para que se materialice esta conexión de redes es necesaria la acción de la UTMAAA. Ésta es la encargada de la conexión por satélite de todos los nodos creando una red de área extensa (*Wide Area Network*, WAN).

Cabe destacar que cada nodo de PU está integrado en una red VPN (*Virtual Private Network*) propia, gracias a la cual se garantiza la seguridad mientras se intercambia información a través de la red WAN.

En la Figura 8 se muestra cómo está formado virtualmente SIMACET, desde el nodo de GU con su BDT hasta las simples redes lógicas de réplica, poniendo de ejemplo al MAAA con sus regimientos.

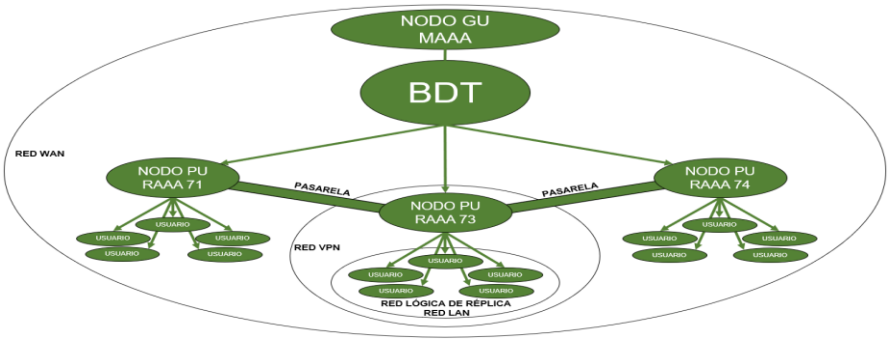


Figura 8 Organización de la red del SIMACET desde GU hasta PU. Fuente: elaboración propia.

Los usuarios de cada nodo son responsables de introducir y gestionar la información dentro del sistema. Normalmente hay 6 usuarios por nodo, cada uno de ellos diferente y con funciones específicas a su puesto: un usuario pertenece al jefe de operaciones, otro al personal de primera sección (S-1), dos de ellos al de S-2, otro al de S-3 y el último al de S-4. Todos los usuarios tienen acceso a las distintas aplicaciones de mensajería, cada uno con su perfil de usuario y contraseña.

S-2 y S-3 forman el CIO (Centro de Inteligencia y Operaciones). S-2 corresponde a la sección de inteligencia y debe estar integrado por dos operadores: uno para operar el terminal

[7] PU: Una pequeña unidad es aquella de entidad regimiento o menor.
[8] GU: Una gran unidad es aquella de entidad brigada o superior, con mando y órganos de mando.
[9] BDT: Conjunto de datos base de iconografía, plantillas, perfiles de usuario y datos planeados de usuarios, etc.

con el usuario del SIMACET y otro para utilizar el terminal proporcionado por el CAOC, para acceder a la red permanente del SC2N-EA. Cabe destacar, que tanto este segundo operador de S-2 como S-3 y el jefe de operaciones, debido al alto nivel de confidencialidad, serán los únicos con acceso a la información recibida desde la red del SC2N-EA. Deben tener, por tanto, la acreditación "*NATO secret*" de la HPS. Además, el CAOC le proporciona al operador de la red del SC2N-EA de S-2 un usuario y contraseña necesarios para poner en funcionamiento el sistema. El jefe operaciones y S-3 visualizan de este terminal la información cargada relativa al espacio aéreo (la RAP), para su explotación y conducción de la operación. El operador S-2 de la red del SC2N-EA es el encargado de poner en funcionamiento el sistema, y de intercambiar mensajería con el EA.

Por otro lado, S-3 es operaciones, encargado de cargar las unidades participantes en la UDAA, así como la posición geográfica en la que están en cada momento y la conducción de la operación (junto al jefe de operaciones), además de enlazar por fonía con el FDC.

En cuanto a S-1 y S-4, forman el CPL (Centro de Personal y Logística), donde S-1 realiza labores de personal, y S-4 es el encargado de las labores logística, tales como el suministro de las necesidades de las unidades.

3.3.1.2 Enlace

Para materializar la conexión entre los distintos nodos de PU y el nodo de GU, así como el con el ARS, CAOC u otros organismos, el MAAA dispone de la UTMAAA, proveniente del CT. La UTMAAA es la encargada de permitir la conexión por satélite de todos ellos, dando unas determinadas direcciones IP a cada sistema, tanto al router como a los distintos terminales de los usuarios del nodo. Además, cuando está desplegada una UDAA es la encargada de proveer de los enlaces por RJ-45 al PC UDAA.

3.3.1.3 Estructura física del SIMACET

Físicamente un nodo SIMACET está formado por un conjunto de medios hardware y por cinco terminales conectados a éste donde se llevan a cabo las labores de C2. En la Figura 9 se recoge un esquema del flujo de información. También se describe cada uno de los hardware del sistema.

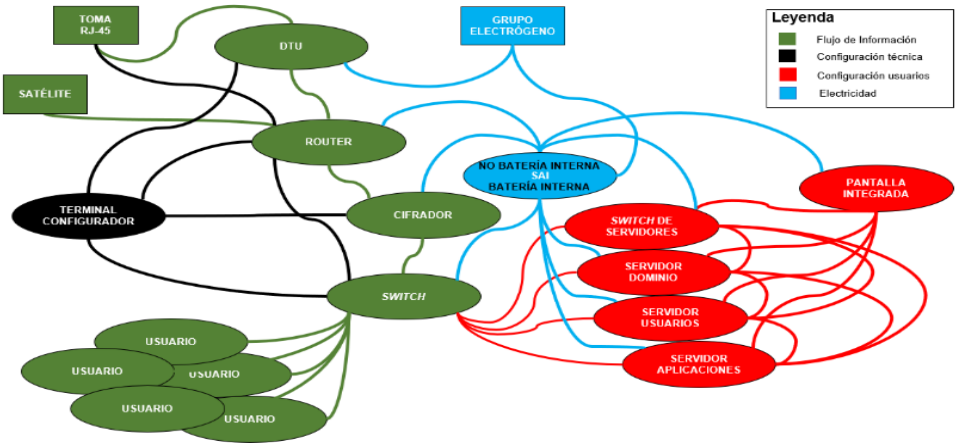


Figura 9 Flujo de información de un nodo del SIMACET. Fuente: elaboración propia.

3.3.1.3.1 DTU

La *Database Transaction Unit* (DTU), o unidad de terminación de datos, es el modelo NEWBRIDGE 2753E. Es un hardware que proporciona un acceso seguro, de todos los terminales

de la red LAN creada, a la red WAN, mediante la tecnología *frame-relay* o *newbridge*[10] [3].

3.3.1.3.2 Router

El router modelo CISCO 2801 se encarga de la recepción de la información [7]. Para ello tiene una determinada dirección IP asignada por la UTMAAA. Toda la información recibida en el router se envía directamente al cifrador. Además, el router está conectado a un *switch* para materializar la red interna creada por el servidor de dominio.

3.3.1.3.3 Cifrador

El cifrador EPICOM 430, según la OTAN: "es un equipo de cifrado IP de alta velocidad que permite un despliegue de redes privadas virtuales (VPN) de forma completamente segura. Fue especialmente diseñado para la protección de las redes de la OTAN." [36]

En cuanto a la seguridad que aporta, tiene aprobado su uso a redes de la OTAN hasta nivel de seguridad "*NATO secret*", así como de clasificación inferior. Se encarga de desencriptar la información para su posterior explotación; por ello, recibe toda la información encriptada del router, para transformarla y enviarla al *switch* para su posterior difusión por la red LAN. De igual modo, recibe toda la información de los distintos usuarios del nodo, para cifrarla y mandarla al router para su posterior difusión por la red WAN de manera segura.

3.3.1.3.4 *Switch*

El *switch*, modelo Allied Telesis x610-24Ts-POE+, es un hardware de alto rendimiento con el que se consigue la creación de una red LAN de alta seguridad. A éste van conectados los cinco terminales de los usuarios, los tres servidores que configuran la red, y el *switch* de servidores, además del cifrador y el router [1]. Gracias al *switch*, l*a* información que llega al nodo una vez traducida por el cifrador puede enviarse por la red LAN. Además, el *switch* se puede configurar de modo que por cada puerto ethernet se envíe una determinada información en función de los operadores o usuarios.

3.3.1.3.5 *Switch* de servidores

El otro *switch*, modelo CV-S801 KVM, es un sistema utilizado para proporcionar una ayuda eficaz al administrador a la hora de configurar el anterior *switch* y los tres servidores [24].

3.3.1.3.6 Servidores

Para crear, modificar o eliminar usuarios y aplicaciones, así como su organización están los tres servidores siguientes, cuyo modelo es Dell PowerEdge 210 II: servidor de dominio, con el que se configura la estructura de la que dependerá la red LAN del nodo, en definitiva, el número de usuarios; servidor de usuarios, con el que se configura el software de cada usuario, así como su acceso a las distintas aplicaciones y permisos, la información que reciben, etc.; y el servidor de aplicaciones, según el cual se establece qué aplicaciones estarán disponibles [8].

3.3.1.3.7 Monitor con teclado

El monitor con teclado es una pantalla integrada modelo KVM CyberView N-1417, que está conectada al *switch* CV-S801 KVM y a los tres servidores. Se utiliza para la configuración citada

[10] *Frame relay* o *newbridge* es una tecnología de protocolo de red de conmutación de paquetes digital de enlace de datos diseñada para conectar redes de área local (LAN) y transferir datos a través de área amplia (WAN) [22].

en el apartado anterior de los tres servidores, así como del *switch* de los servidores [23].

3.3.1.3.8 SAI

Conectado al grupo electrógeno se encuentra el proveedor de energía, modelo SAI EATON Ellipse MAX1500. Dispone de una batería interna con la que, en caso de fallo en suministro eléctrico, se mantendrían encendidos y conectados hasta cuatro equipos hasta la finalización de su reserva de energía. Presenta 4 conexiones a la batería interna, y otras 4 conexiones que no están conectadas a la batería interna, solo proporcionan electricidad si está conectado al grupo electrógeno. Este SAI posee una potencia de 1500VA/900W, y es capaz de suministrar corriente eléctrica, a cada uno de los cuatro sistemas conectados a la batería interna, durante como máximo 90 minutos [14].

Por un lado, se conectan a la batería interna los tres servidores y el *switch*. Por otro lado, a los otros cuatro enchufes se conectan la pantalla integrada, el router, el cifrador y el *switch* de servidores dado que, si estos se quedan sin flujo energético, no conllevaría la pérdida de información, al igual que la DTU que va conectada al grupo electrógeno.

3.3.1.3.9 Terminales

En el sistema hay 6 terminales, cinco de ellos pertenecen a los operadores (jefe operaciones, S-1, S-2, S-3, S-4 y S-5) y el sexto terminal se utiliza como configurador de la DTU, del router, del cifrador, y del *switch*. Para llevar a cabo estas configuraciones se conecta el terminal con los distintos elementos mediante conexión por cable.

Todos ellos son portátiles modelo HP ELITEBOOK 8460 [19]. Este modelo posee un procesador Intel-Core i5 de 2ª Generación, memoria RAM de 4 GB, memoria interna en disco duro HDD de 250 GB y tarjeta gráfica Intel HD 3000; además el sistema operativo (SO) presente es el *Windows 7 Pro*.

3.3.1.4 Aplicaciones

Se detallan las aplicaciones disponibles en el SIMACET, objeto de estudio de este trabajo.

3.3.1.4.1 Antares

ANTARES es una aplicación de usuario que proporciona el plano de situación y diferentes funcionalidades tácticas. Se divide en dos partes: MAPSIT (mapa de situación), que recoge las funcionalidades tácticas de ANTARES; y GIS (*Geographic Information System*), que recoge la parte técnica del tratamiento geográfico [27].

3.3.1.4.2 OUTLOOK

Es una aplicación de mensajería que tiene múltiples funcionalidades adicionales como crear una lista de distribución a la que enviar un mensaje, trabajar con el calendario, etc. Sólo se emplea para mensajería formal [27].

3.3.1.4.3 JCHAT

La aplicación JCHAT (*Joint Chat*) es una aplicación de mensajería instantánea, en la que se permite dialogar en una sala virtual de manera escrita, tanto con un grupo de usuarios, como con uno en concreto en una sala privada. Para hacer uso de ésta, el administrador técnico del nodo habrá creado una o varias salas con distintos privilegios de acceso a los usuarios del sistema. Esta configuración se lleva a cabo con el servidor de aplicaciones y a través del monitor integrado del nodo [27].

3.3.1.4.4 XoMail

La aplicación XoMail es un sistema de mensajería oficial que cumple ciertos requisitos de la OTAN, tanto de seguridad (posibilidad de cifrado, información clasificada…) como operacionales (estandarización, control de sobretiempos…). Su lógica de empleo se basa en una jerarquía de organizaciones y una jerarquía de usuarios [27]. Se utiliza para el intercambio de mensajería confidencial relativa a las operaciones en curso.

3.3.1.4.5 SHAREPOINT

Es una herramienta colaborativa, pensada para trabajar en grupo, que permite compartir y modificar información y documentos. Es la aplicación más empleada por los usuarios [27].

3.3.1.4.6 JEMM

JEMM es una aplicación que permite crear incidencias, y hacer su seguimiento de una manera muy eficiente. No es, por tanto, una aplicación de mando y control [27].

3.3.2 Sistema de Mando y Control Nacional del Ejército del Aire

"El Sistema de Mando y Control Nacional del Ejército del Aire (SC2N-EA) permite a los mandos del Ejército del Aire ejercer el planeamiento, dirección, ejecución y control de sus actividades de la forma más eficiente posible." [40]

El SC2N-EA, además permite el planeamiento, dirección, ejecución y control en tiempo real de todas las misiones aéreas y de vigilancia, además del control aeroespacial, la asignación de objetivos y la generación y difusión de una única RAP.

"Conecta el Centro de Operaciones Aéreas (AOC) del Mando Aéreo de Combate con las principales unidades de la fuerza del Ejército del Aire, el componente desplegable (AOC-D[11], BOC-D[12] y ARS-D[13]), y las unidades conjuntas y del Ejército de Tierra y la Armada que interactúan con el Mando Operativo Aeroespacial (MOA), ejercido por el general jefe del Mando Aéreo de combate." [39]

A diferencia del SIMACET, el SC2N-EA es una red virtual permanente para ejercer el C2, a diferentes escalas de mando. En esta red se encuentran las bases de datos de cada una de las aplicaciones que tiene disponibles, entre las que podemos destacar la base de datos del ASACS, encargada de recoger toda la información relativa al espacio aéreo, de todos los sensores disponibles; la base de datos de la ICC-NATO, donde se encuentran las RAP creadas por el ARS; o la base de datos de la división de adiestramiento y ejercicios del CAOC.

Además, la seguridad a nivel OTAN de este sistema es "*NATO secret*", un nivel superior a la seguridad del SIMACET.

3.3.2.1 Estructura virtual del SC2N-EA

La Figura 10 recoge un esquema de la red del SC2N-EA, mostrando las distintas bases de datos, la conexión entre el CAOC y el ARS, y el canal que sigue el flujo de información hasta el FDC y el CIO, del núcleo de C2. Este esquema está basado en la generación de una UDAA por el RAAA 73.

[11] AOC-D: *Air Operation Centre Deployable* (centro de operaciones aéreas desplegable).
[12] BOC-D: *Base Operation Centre Deployable* (base de operaciones aéreas desplegable).
[13] ARS-D: *ARS Deployable* (ARS desplegable).

El SC2N-EA virtualmente consiste en una red de alta seguridad, a la que se encuentran unidos diferentes terminales para llevar a cabo el C2 de la AD. Estos terminales son ordenadores portátiles, con un alto nivel de seguridad y que sólo pueden ser utilizados para acceder a dicha red.

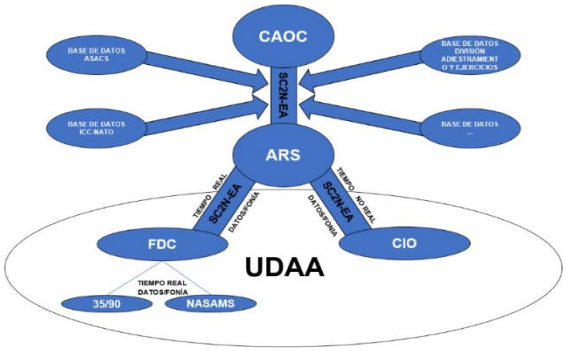


Figura 10 Red del SC2N-EA. Fuente: elaboración propia.

Al estar cada una de las bases de datos dentro de la red permanente, toda la información que se requiera de la misma estará constantemente actualizada. El acceso a cada base de datos se realiza mediante programas específicos, instalados en el terminal conectado a la red. A modo de ejemplo, el programa informático utilizado para visualizar la RAP creada por el ARS, que se encuentra en la base de datos ICC-NATO, tiene ese mismo nombre: ICC-NATO.

El CAOC es el encargado de proveer los terminales, con acceso a la red del SC2N-EA, a todo aquel que los necesite para llevar a cabo la AD, proporcionando también el usuario y contraseña al personal que lo opera y activando el acceso a las bases de datos de la red que se considere necesario para cada usuario. En una UDAA, es el operador de S-2 del SIMACET el encargado de recibir dicho usuario y contraseña, por ser el personal encargado de operar dicha red, y estar acreditado con la HPS necesaria para ello.

El CAOC, el ARS, el CIO y el FDC consiguen un intercambio constante de información gracias a esta red del SC2N-EA, permitiendo que estén actualizados con respecto a todas las novedades relativas a la UDAA y al control de la DAA. El enlace entre ARS y FDC es en tiempo real, mientras que, todos los enlaces restantes son en tiempo no real.

El ARS y el CIO están conectados por datos y fonía en tiempo no real. De esta manera, S-2 mantiene intercambio de mensajería con el escalón superior del EA y recibe la RAP del espacio aéreo en el que está establecida la UDAA, para que el jefe de operaciones y S-3 puedan conducir la operación de manera satisfactoria.

Cabe destacar que para poder cargar los documentos ACO y ATO en el software de ICC-NATO, en el terminal con acceso a la red del SC2N-EA, es necesario que el operador de S-2 los descargue previamente. Para ello, mediante un ordenador securizado[14], S-2 procede a la descarga de dichos documentos, de una base de datos del CAOC, y los introduce en un pendrive, también securizado, para así cargarlos en ICC-NATO del terminal y que sean visibles. De esta manera, al visualizar la RAP con toda la información de las trazas aéreas, el sistema podrá determinar si una aeronave es amiga, enemiga o desconocida.

Los terminales conectados a esta red sirven a los tres ejércitos para que en el puesto de mando de cada uno se conozca la situación del espacio aéreo, y se pueda llevar a cabo una conducción de la operación lo más acertada posible.

[14] Ordenador securizado. Ordenador portátil que posee un nivel de seguridad superior, con el que únicamente se pueden realizar determinadas acciones. Cualquier uso indebido o la introducción de cualquier memoria externa (pendrive) que no esté securizada pondría en riesgo la seguridad del sistema.

3.3.2.2 Enlace

Al igual que en el SIMACET, la UTMAAA es la encargada de proveer a todos los elementos de la red del SC2N-EA de determinadas IPs para ese intercambio de información.

3.3.2.3 Estructura física del SC2N-EA

Físicamente el conjunto de hardware que permite el acceso a la red del SC2N-EA está compuesto por una DTU NEWBRIDGE 2753E, un router CISCO 2801, un cifrador EPICOM 430 y un ordenador portátil, cuyos modelos son los mismos que posee el nodo del SIMACET. Además, está compuesto por un teléfono IP[15], cuyo software se configura por el EA para desarrollar sus funciones específicas. En la Figura 11 se puede observar su estructura.

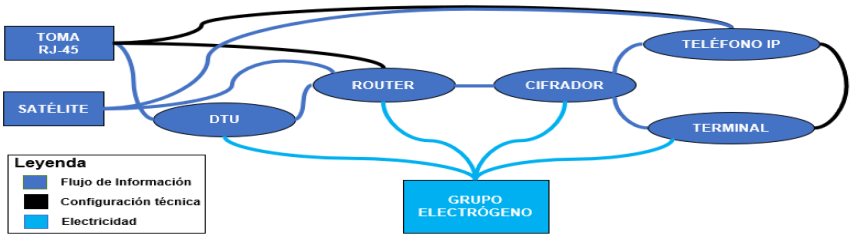


Figura 11 Estructura física de los elementos hardware que permiten el acceso a la red del SC2N-EA. Fuente: elaboración propia.

El teléfono modelo IP Digium D40, es un teléfono que con un software interno configurable por un terminal. De esta manera, el EA lo configura para que los usuarios que lo explotan puedan operar en la red del SC2N-EA.

Tiene varias funciones en este sistema: en primer lugar, es el que determina si el circuito cifrador-teléfono-terminal está cerrado, es decir, si todas las conexiones son óptimas y es posible la explotación de la red del SC2N-EA. El estado del circuito se indica mediante una silueta de color negro en el *display* del teléfono: si dicha silueta no aparece, el sistema está inoperativo. En segundo lugar, sirve de enlace telefónico con el ARS.

3.3.2.4 Aplicaciones

Análogamente al SIMACET, el terminal con acceso al SC2N-EA, a nivel UDAA, presenta una serie de aplicaciones utilizadas para el C2 de las unidades de AAA encuadradas en una defensa aérea (AD). Por el nivel de confidencialidad, sólo podrán ser explotadas por el operador de S-2, S-3 y el jefe de operaciones. Sin embargo, las aplicaciones que debe visualizar el personal de S-3 y el jefe de operaciones serán aquellas destinadas a la visualización del espacio aéreo, y el operador de S-2 será el encargado de la mensajería. Dado que sólo hay un terminal en el puesto de mando de la UDAA, estos dos últimos deberán desplazarse para acceder a la información, dificultando la toma de decisiones.

3.3.2.4.1 Mensajería e incidencias

Las aplicaciones del terminal que opera en la red del SC2N-EA utilizadas para el intercambio de información con el escalón superior del EA, tanto con el ARS, como con el CAOC son: JCHAT, Outlook, JEMM, Sharepoint y XoMail. Son las mismas aplicaciones utilizadas en el SIMACET, pero poseen un nivel mayor de seguridad.

[15] Teléfono IP: Es un teléfono creado para funcionar sobre IP. A diferencia de los teléfonos analógicos, los IP son miniordenadores que disponen de software.

3.3.2.4.2. ICC-NATO

Una de las aplicaciones clave en el terminal con acceso a la red del SC2N-EA es la aplicación de información geográfica ICC-NATO (*NATO Integrated Command and Control)*, que permite visualizar la información del espacio aéreo, es decir, las trazas. Además, permite cargar los documentos ATO y ACO. Dicha aplicación se llama ICC-NATO, al igual que la base de datos donde se encuentran las RAP. Esta aplicación es la encargada de proveer de la RAP, cargada en la base de datos del SC2N-EA, al terminal del CIO.

3.4 Aplicaciones de Información Geográfica

En este apartado, se dará una breve descripción de dos aplicaciones de información geográfica disponibles en el ET.

3.4.1 TALOS Táctico

TALOS se utiliza en todas las unidades de artillería de campaña y está dividido en TALOS Técnico y TALOS Táctico. El primero se utiliza para enviar órdenes de fuego a las piezas de artillería subordinadas, mientras que el segundo se utiliza a nivel puesto de mando para el planeamiento y conducción de la operación.

Según el Manual de TALOS Táctico de GMV [17]: “El Subsistema Táctico TALOS permite el planeamiento de una operación y su apoyo de fuegos, con capacidades de planeamiento conceptual y detallado, hasta la obtención de la orden de operaciones y la conducción de esta”.

A través del presente sistema, el operador tiene la capacidad de coordinar y dirigir directamente todas las piezas, así como enviar órdenes. Permite conocer datos de interés como la munición disponible, personal presente o la posición de todos los elementos de forma exacta y la situación en la que se encuentran: asentados en una posición fija o en transporte.

Presenta muchas funciones específicas, en lo que a conducción de una operación se refiere, tales como: establecer una jerarquía de operadores, situar unidades y crear despliegues militares sobre una cartografía tipo *ráster*[16], conducir el planeamiento, control de personal y material, así como la creación y gestión de peticiones de fuego. Además, tiene la posibilidad de recibir información GPS ya sea de los vehículos, sistemas de armas o personal que lleve consigo un geo localizador, para así plasmar automáticamente su posición en el sistema geográfico. Permite también la carga de los documentos ATO y ACO procedentes del ARS para el control del espacio aéreo.

Para ser instalado en un terminal TALOS Táctico requiere un SO *Windows 7* o superior, un espacio libre mínimo de 25 MB en la memoria interna y una memoria RAM mínima de 2GB [17].

3.4.2 Carta Digital

Carta Digital es una aplicación GIS (*Geographic Information System*), y según su propio manual (Carta Digital V8.1): “Se trata de un sistema de información capaz de analizar y mostrar información geográficamente referenciada. Dicho de otro modo, es una herramienta que permite a los usuarios crear consultas interactivas, analizar la información espacial, editar datos, mapas

[16] Cartografía tipo *raster*: se trata de fotografías aéreas digitales, imágenes de satélite, imágenes digitales o incluso mapas escaneados. Los datos representan dos tipos de datos: los datos temáticos, que representan entidades como datos de la tierra o uso de la tierra; los datos continuos representan la temperatura, elevación del terreno o datos espectrales, entre otros [4].

y presentar los resultados de todas las operaciones. En el corazón de la Carta se encuentran los componentes de SIGMIL (Sistema de información Geográfica Militar). Estos componentes son los que dotan a la aplicación de las operaciones GIS.” [4]

Carta Digital presenta una extensión denominada APP-6, la cual permite crear despliegues militares y situar unidades, dando, la posibilidad de introducir el personal presente y el material utilizado. Además, tiene la posibilidad de posicionar automáticamente la situación de las unidades, siempre y cuando estas tengan integrado un GPS. Su función principal es la de estudiar la geografía mediante capas vectoriales y ráster, a través de todo tipo de consultas.

Para ser instalado este software en un terminal, es necesario disponer de un SO *Windows 10* o superior, un espacio libre de 50Mb de memoria interna y una memoria RAM mínima de 128 MB, además de una tarjeta gráfica dedicada [4].

4 Desarrollo: Análisis y Resultados

El objetivo principal de este TFG es buscar una solución a la problemática presente en el RAAA 73 al generar una UDAA en la que el ET y el EA operen conjuntamente. Actualmente, la célula de inteligencia (S-2) se enfrenta a dos usuarios en dos terminales diferentes, lo que requiere a dos operadores: uno encargado de manejar el terminal con el SIMACET, y otro dedicado a operar el terminal que permite el acceso a la red del SC2N-EA.

La solución buscada en este TFG es unir ambos usuarios en uno, un único terminal, de manera que sea necesario sólo un operador especializado en ambos C2. Con esta unión, se optimizaría la toma de decisiones. Además, se evitaría la duplicidad de información, enviar la misma mensajería por dos cadenas diferentes (la del ET y la del EA), y se ahorraría personal.

Para conseguir este objetivo se proponen dos soluciones, en las que se conecta la red del SC2N-EA al SIMACET. Por un lado, una primera solución que resultaría económica al Ejército, con la que se sustituye el programa geográfico ANTARES (actualmente en SIMACET) por TALOS Táctico o Carta Digital, y se añaden varios elementos hardware para que SIMACET pueda soportar la carga extra de información recibida desde el EA. De esta manera tendríamos toda la información unificada y con un único operador especializado. Por otro lado, una segunda solución, que sería la óptima, pero también la menos económica, en la que se propone el desarrollo de un nuevo sistema de C2 que integre al SIMACET y al SC2N-EA, bautizado como SIMACTA (Sistema de Información para el Mando y Control Tierra Aire), con el que estarían perfectamente integrados ambos sistemas de C2.

A continuación, se exponen las soluciones propuestas, en base a las opiniones de los operadores de ambos sistemas de C2, materializadas en la realización de un *Focus Group*, un *Brainstorming* y una encuesta a personal especialista.

4.1 Focus Group

Para determinar los posibles problemas y limitaciones, así como posibles soluciones al problema se realizó un *Focus Group* [18,35] el pasado 28 de septiembre de 2021. A continuación, se expone el informe final de esta metodología, donde se recogen las ideas clave y conclusiones de ésta. Además, en el Anexo B se muestra una breve descripción de lo que es el *Focus Group*, así como el guion utilizado para el desarrollo de la reunión.

En primer lugar, los expertos en ambos sistemas de C2 coinciden en que son totalmente aptos para conducir la operación de una UDAA, sin embargo, los operadores de SIMACET detallan que en S-2 debería haber un único operador. De este modo, se reduciría la posibilidad

de error y se podría informar mejor al mando de la situación. Por ello, S-2 debería tener acceso a todo lo relativo al intercambio de información entre el ET y el EA, mientras que el jefe de operaciones y S-3 deberían poder visualizar la información del espacio aéreo (RAP), en lo que a información del C2 del aire se refiere.

A la hora de unir ambos sistemas de C2, los operadores de la red del SC2N-EA resaltaron que es necesario que se mantengan los niveles de seguridad establecidos, dado que el SC2N-EA posee un nivel de seguridad "*NATO secret*" superior al del SIMACET, cuyo nivel de seguridad es "*NATO confidential*". Al unir ambas redes, la seguridad del SC2N-EA estaría siendo violada, por lo tanto, los técnicos del EA que tienen que aprobar el uso de la red en estas condiciones, no lo aprobarían y no se podrían integrar ambos sistemas de C2.

Con respecto a la parte informática de los sistemas de C2, los participantes resaltaron que el software de los terminales es sencillo y no da ningún problema. Sin embargo, en lo relativo a los medios hardware coincidían en que deben disponer de mayor velocidad de procesamiento, y en palabras de los asistentes, tanto la memoria RAM como el procesador "están obsoletos". Estos dos aspectos son importantes de cara a la velocidad en la decisión, necesaria a la hora de dirigir una operación. Como propuesta de mejora, indicaron que es necesaria una renovación de los terminales, por otros con hardware más moderno.

Con respecto al SC2N-EA, los especialistas presentes resaltaron la necesidad de incorporar un SAI, como en el SIMACET.

Por último, haciendo referencia a las distintas aplicaciones de los terminales que posibilitan el C2, lo más destacable es la opinión de los operadores del SIMACET con respecto a la aplicación geográfica ANTARES, que en sus palabras:

> *"ANTARES es una aplicación que nos permite posicionar las unidades en el terreno, llevar un control de la operación, introducir al personal participante y dirigir las labores logísticas, sin embargo, es difícil de operar, se queda pillada constantemente y es antigua."*

A partir de estas palabras, se discutió sobre posibles aplicaciones que podrían sustituir a ANTARES, entre las que surgieron: BMS (*Battlefield Management System*), TALOS Táctico, TALOS Técnico y Carta Digital. BMS fue descartado inmediatamente porque no es una aplicación geográfica, sino un conjunto de aplicaciones, al igual que se descartó TALOS Técnico por ser una aplicación para enviar órdenes de fuego, que no se realiza en el PC UDAA.

Las dos aplicaciones que se compararon en el *Focus Group* por sus posibilidades fueron TALOS Táctico y Carta Digital. Con respecto a la primera, se destacó que tenía posibilidad de tratamiento geográfico y posicionamiento de unidades. Por otro lado, Carta Digital también posee esas funcionalidades, aunque, al ser una aplicación especializada en tratamiento geográfico, suele ralentizar los ordenadores en los que está instalada. Pero según los expertos, la gran diferencia radica en que TALOS Táctico es capaz de cargar en el sistema los documentos ATO y ACO, y Carta Digital no.

Por otro lado, los operadores de la aplicación ICC-NATO del SC2N-EA destacaron su facilidad de uso, no presentando problemas a la hora de operarla. Haciendo referencia a la adhesión de la red del SC2N-EA, han considerado que ICC-NATO no podría ser utilizada para presentar la información del ET y del EA, dado que no tiene las posibilidades de ANTARES de posicionamiento de unidades en el terreno, o de realizar labores de personal y logística.

Con respecto a las aplicaciones destinadas al intercambio de mensajería, todos estaban de acuerdo en que son todas aceptables, pero se podría considerar la opción de integrar JCHAT y Outlook en una única aplicación. De esta manera, se podría explotar el intercambio de mensajería formal (oficial) e informal en una única aplicación. Además, los participantes hicieron

hincapié en la mejora que supondría la posibilidad de envío a través de JCHAT de documentación adjunta, además de simple texto. Respecto a la aplicación XoMail, se destacó que únicamente se utiliza para recibir documentación confidencial del ejercicio u operación.

De las dos aplicaciones restantes, JEMM y SHAREPOINT, los operadores del SIMACET comentan simplemente que son muy útiles de cara a facilitar el intercambio de documentación pesada entre distintos usuarios, así como el control de incidencias. Por otro lado, por parte de los operadores de la red del SC2N-EA, destacan que no las han usado en ningún momento, dado que únicamente se dedican a intercambiar mensajería o recibir la RAP.

4.2 Brainstorming

Para determinar los requisitos que debería poseer un nuevo sistema de C2 que integrase a los dos sistemas actuales (el ya mencionado SIMACTA), se realizó un *Brainstorming* [42] con el personal especializado en ambos sistemas.

El presente informe recoge las ideas clave y conclusiones destacadas de la reunión del 8 de octubre de 2021, fecha en la que se realizó este *Brainstorming*. El Anexo C recoge una breve introducción acerca de la metodología, así como el guion utilizado en esta reunión.

Las principales ideas recogidas en la realización de esta sesión son las siguientes:

- El software de los terminales debería ser el más actual posible, para así tener el mayor grado de seguridad. De esta manera, tardará más en quedarse obsoleto.
- Con respecto a los elementos hardware internos de los terminales, consideraron que deberían ser potentes para asegurar la velocidad de procesamiento necesaria a la hora de conducir una operación. La memoria RAM debería tener como mínimo 12GB, y el procesador debería ser un Intel i5 de al menos 11ª generación.
- A la hora de la creación de SIMACTA, los operadores de la red del SC2N-EA coincidían en que hay que conectar también el teléfono al sistema, ya que éste es el que cierra el circuito cifrador-teléfono-terminal, que permite la unión a la red del SC2N-EA. Además, también sirve de enlace por fonía con los mismos.
- Estos mismos operadores, daban una gran importancia a que el nivel de seguridad que posee la red del SC2N-EA ("*NATO secret*") debe mantenerse, y no mezclarse con la red del SIMACET cuyo nivel de seguridad es un escalón inferior ("*NATO confidential*").
- Según los expertos las aplicaciones más necesarias serían las siguientes:
    - Aplicación geográfica, cuyos requisitos mínimos serían:
        - Cargar, posicionar y modificar, durante la operación, unidades.
        - Introducir personal involucrado.
        - Planificación de labores logísticas.
        - Realizar tratamiento geográfico.
        - Cargar documentos ACO y ATO.
    - Aplicación para mensajería oficial y formal, así como para mensajería informal. Se ha recalcado que hasta ahora hay dos aplicaciones para la mensajería, que se diferencian en que una es un chat informal (JCHAT) y la otra se utiliza para mensajería oficial (Outlook). Hay dos aspectos que han considerado mejorables: en primer lugar, que el chat informal debería tener la posibilidad de enviar documentos (Excel, Word, PDF), en sus palabras "ser más parecido a *WhatsApp*"; por otro lado, han planteado la posibilidad de unir ambas aplicaciones, de manera que en una única aplicación existiese la posibilidad de tener ese chat individual o grupal y, además, enviar mensajería oficial.
    - Aplicación para mensajería confidencial-secreta, en lo que al ET y EA concierne.
- Para acabar la reunión, en la última cuestión sobre los usuarios que debería tener el sistema de C2 se propuso que deberían ser cinco: jefe de operaciones, S-1, S-2, S-3 y S-4, dándole

la mayor importancia a que en S-2 únicamente debería haber un único operador, y no dos como hasta ahora.

4.3 Encuesta

Para completar la información recabada en los dos apartados anteriores, se ha realizado una encuesta (véase Anexo D), a través de la extensión de formularios de Google, a un total de doce operadores del CIO y del CPL que componen las UDAAs tanto GAAA I/73 como del GAAA II/73. La encuesta se ha dividido en cuatro secciones: una primera sección destinada a conocer el puesto del operador que realiza la encuesta; una segunda sección destinada a conocer la opinión de los operadores con respecto a la unión de ambos sistemas de C2 (ET y EA); una tercera sección destinada a conocer la opinión sobre los elementos hardware y software de terminales que utilizan; y una última sección en la que se pregunta acerca de la creación de un nuevo sistema de C2 que integre ambos sistemas.

Los resultados de la misma se encuentran en el Anexo E. A continuación, se hace referencia a las conclusiones más importantes de la encuesta, que han ayudado al presente alumno a desarrollar esta investigación:

- Todos los operadores consideran que es un problema que la información del SIMACET y la de la red del SC2N-EA llegue a terminales diferentes con una puntuación de 4,5/5.
- Un 66,7% de los operadores consideran que la red del SC2N-EA debe adherirse al nodo SIMACET.
- Un 75% considera beneficiosa la creación de un nuevo sistema de C2 que integre a ambos, además, el 25% restante escoge la opción “Tal vez”, no estando nadie en contra.

4.4 Análisis de las Aplicaciones de Información Geográfica

Para integrar la red del SC2N-EA en el nodo de PU del SIMACET, y que la RAP sea visible en el mismo terminal del nodo, es necesaria la sustitución de la actual aplicación geográfica ANTARES por otro software. Este nuevo software debe permitir la visualización de toda la información de las unidades del ET y RAP proveniente del ARS.

Figura 12 Análisis DAFO Carta Digital. Fuente: elaboración propia.

Figura 13 Análisis DAFO de TALOS Táctico. Fuente: elaboración propia.

En el Apartado 3.4 se presentaron dos aplicaciones que podrían satisfacer las necesidades propuestas: TALOS Táctico y Carta Digital. Para evaluar cuál de ellas es la mejor opción, se ha realizado un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades) para cada opción. De esta manera, se conocerán a nivel interno de cada aplicación sus fortalezas y debilidades, y a nivel externo sus oportunidades y amenazas. Al comparar los análisis DAFO de ambos softwares, representados en la Figura 12 y 13, la principal diferencia radica en que TALOS

Táctico presenta la posibilidad de cargar en el sistema los documentos ACO y ATO. Ahora bien, para que sean efectivos estos datos en el sistema, éste debería ser capaz de presentar las RAP recibidas por la red del SC2N-EA, procedentes del ARS.

Figura 14 Trazas aéreas en TALOS Táctico. Fuente: cortesía CAC Pablo Casal Martínez.

Si bien es cierto que TALOS Táctico aún no ha proporcionado la visualización de la RAP, sí que otras unidades del ET, como el Grupo de Artillería de Campaña número siete (GACA VII), ubicado en Pontevedra, han experimentado la implementación en TALOS Táctico de trazas aéreas de forma satisfactoria como se puede apreciar en la Figura 14. Éstas eran recibidas desde la Unidad de Control de Empeños (UCE)[17], que a su vez recibía la información del radar RAC-3D, se puede observar como el rombo rojo con el avión es el enemigo, y las azules son las unidades propias. Por lo tanto, TALOS Táctico es una potente posibilidad para conseguir la interoperabilidad buscada, y se considera una gran oportunidad de cara a su posible uso en C2 de una UDAA.

Entre los requerimientos mínimos necesarios en el terminal para que TALOS Táctico lleve a cabo sus funciones sin problemas, podemos destacar como oportunidades que únicamente requiere de 25 MB de espacio libre en el disco duro, además de que, podría ejecutarse en un SO Windows 7 o inferior. En cuanto a sus amenazas hay que resaltar que requiere una memoria RAM mínima de 2GB.

En el caso de Carta Digital, hay que resaltar como oportunidad que la mayoría del personal del ET está familiarizado con esta aplicación; por otro lado, con respecto a los hardware necesarios en el terminal desde el que se opere, únicamente requiere una memoria RAM de 128 MB, aunque la recomendada es de 512 MB. En cuanto a las amenazas, también a nivel software, necesitaría el SO *Windows 10*, una memoria libre en el disco duro mínima de 50 MB y una tarjeta gráfica dedicada, al ser un software especializado en tratamiento geográfico.

Por último, en la encuesta, el 83,3% de los operadores ha considerado que la mejor opción para sustituir a ANTARES es TALOS Táctico, calificando a este con una puntuación de 4,33/5 a la hora de cumplir con las necesidades tras la unión de ambos sistemas.

Como conclusión a la comparativa de los análisis DAFO realizados, TALOS Táctico sería el software más adecuado para sustituir a ANTARES. En primer lugar, por presentar la posibilidad de incluir los documentos ACO y ATO, imprescindibles para el C2 de una UDAA; y, en segundo lugar, por requerir el SO *Windows 7*, presente actualmente en los terminales.

4.5 Objetivos Internos para la Interoperabilidad entre los Sistemas de C2

Tanto el *Focus Group* como el *Brainstorming* y la encuesta (véase Apartados 4.1, 4.2 y 4.3) realizados han proporcionado las ideas clave sobre las necesidades del personal que opera en el CIO y el CPL. Aunque el *Brainstorming* se realizó en base a la creación de un nuevo sistema de C2, también recoge ideas de mejora. Gracias a las conclusiones obtenidas, se han extraído

[17] UCE: La Unidad de Control de Empeños de una batería mistral es lo equivalente al FDC de una batería de armas de AAA.

una serie de objetivos principales y secundarios. Los principales serían aquellos que hay que cumplir irremediablemente para conseguir que la unión de ambos sistemas de C2 sea efectiva. Los secundarios corresponderían a propuestas de mejora.

Como bien se ha explicado hasta ahora, el objetivo principal es que únicamente se necesite un operador en S-2. Para ello, el nodo de PU del SIMACET debe ser capaz de recibir la información procedente de la red del SC2N-EA y comprenderla, dado que sin ser esto posible, la unión no estaría materializada. Una vez conseguida la **interoperabilidad** entre sistemas de C2, la consecuencia directa sería que S-2 sólo necesitaría un operador.

Los objetivos secundarios están enfocados a mejorar el C2, y no todos se podrán conseguir en las dos soluciones propuestas. Entre estos destacan:

a. Una aplicación geográfica capaz de representar la información relativa al ET y al EA.
b. El jefe de operaciones y S-3 han de ser capaces únicamente de visualizar toda la información procedente de ambos ejércitos.
c. S-2 será el único con capacidad de intercambiar mensajería con el ET y el EA.
d. Renovación de los hardware de los ordenadores portátiles (memoria RAM, procesador).
e. Incorporación de suficientes SAI, evitando así interrupciones del suministro eléctrico.
f. Unión de las capacidades de JCHAT y Outlook.

4.6 Arquitectura virtual buscada

La arquitectura virtual buscada sería la representada en la Figura 15, relativa a la información proveniente del EA y del ET.

En ella se pueden apreciar los cauces que seguiría la información, así como los derechos de cada usuario. Toda la información llegaría al router, después pasaría por el cifrador, para una vez descifrada, llegar al *switch* o al teléfono en su defecto. El *switch*, previamente configurado según las necesidades propuestas, permitiría las siguientes acciones: al jefe de operaciones y S-3 un intercambio de información del ET, y únicamente la recepción de la RAP; a S-1 y S-4 el intercambio de todo lo relativo al ET; y S-2 tendría autorizado enviar y recibir mensajería de ambos sistemas de C2. El teléfono, al igual que en la red del SC2N-EA, sirve de enlace telefónico con el ARS, cuyo operador es también de S-2.

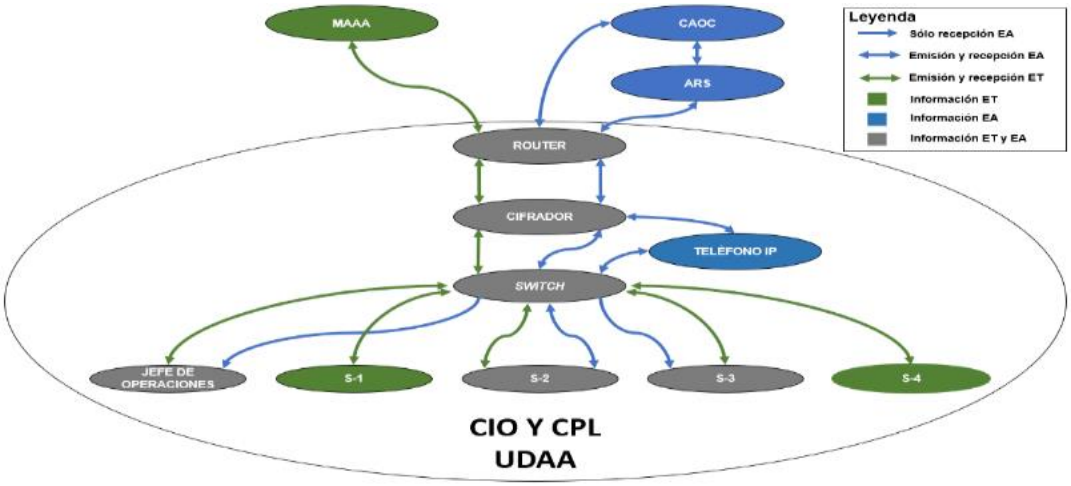


Figura 15 Arquitectura virtual buscada. Fuente: elaboración propia.

Para conseguir el objetivo principal, la unión de ambos sistemas de C2 y que en S-2 únicamente haya un operador, bastaría simplemente la sustitución del router, como se verá en el Apartado 4.7. Con esta propuesta, también se han conseguido dos objetivos secundarios (b y c), relativos a la información que llega a cada operador.

Hay que destacar que para materializar este flujo de información entre el CAOC, el ARS, S-2, S-3 y el jefe de operaciones, físicamente será necesaria la conexión de un teléfono IP del EA al nodo SIMACET existente. Es imprescindible esta adhesión dado que tiene dos funciones: en primer lugar, determina si el circuito cifrador-teléfono-terminal está cerrado, es decir, si todas las conexiones son óptimas y es posible la explotación de la red de SC2N-EA; y, en segundo lugar, sirve de enlace telefónico con el ARS.

Respecto a las acreditaciones HPS necesarias, para los operadores del CIO y CPL se mantiene el requerimiento de "*NATO confidential*" para S-1 y S-4, y de "*NATO secret*" para el operador de S-2, S-3 y el jefe de operaciones.

4.7 Solución a la comunicación entre los Sistemas de C2

Hay presentes varios problemas a la hora de llevar a la práctica la unión de los dos sistemas. A continuación, se detallan dichos problemas y se proponen soluciones:

- Conseguir que ambas redes se entiendan, dado que integran diferentes protocolos de red: habría que aplicar una pasarela[18] entre redes, para que la información de la red del SC2N-EA pueda ser recibida y entendible por el nodo del SIMACET.

- Que se mantengan los niveles de seguridad a nivel OTAN de ambas redes de C2: habría que asegurar que la información recibida de ambos Ejércitos no se mezcle, para no violar los niveles de seguridad de ambas redes. Para ello se necesitaría: que el router tenga la capacidad de discriminar la información proveniente de cada red, tanto en la recepción como en la emisión; y que el switch tenga la misma habilidad.

- Que se materialice la conexión a la red del SC2N-EA: simplemente bastaría con conectar al sistema el teléfono IP, que el mismo EA provee, para cerrar el circuito cifrador-teléfono-terminal.

En definitiva, lo que se necesita conseguir para que no se mezclen ambos flujos de información, es tener la posibilidad de mantener dos redes VPN dentro del nodo bien diferenciadas, en vez de una como hasta ahora. En una red se encontraría todo lo relativo al ET y en la otra lo relativo al EA. Sólo de esta manera se podrían mantener ambas cadenas de información con su mismo nivel de seguridad. En la Figura 16 se puede apreciar lo que se necesita conseguir.

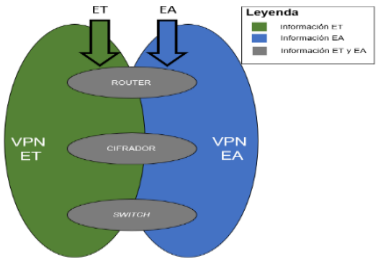


Figura 16 Redes VPN en el nodo. Fuente: elaboración propia.

Por lo tanto, el objetivo principal para conseguir la **interoperabilidad** entre el SIMACET y la red del SC2N-EA es la recepción por parte del nodo de PU del SIMACET de la información procedente de la red del SC2N-EA, así como mantener los niveles de seguridad de cada una de las redes, "*NATO confidential*" lo que concierne al ET, y "*NATO secret*" lo que concierne al EA.

[18] Pasarela: Dispositivo que permite conectar dos redes incompatibles por usar cada una un protocolo diferente.

Para conseguir el propósito establecido, será necesario la utilización de:

- Un router que tenga la capacidad de hacer de pasarela entre dos redes incompatibles, y que permita integrar dos redes VPN distintas.
- Un cifrador que también tenga la capacidad del router citada en el punto anterior.
- Un *switch* que permita, al igual que el router, integrar dos redes VPN distintas, así como su difusión a los distintos operadores del nodo.

A continuación, se explican los elementos hardware que serán incorporados a ambas propuestas. En primer lugar, se hará referencia a los propuestos para poner solución a los problemas de comunicación entre los sistemas de C2 y, en segundo lugar, a los que serán incorporados para mejorar las capacidades existentes.

4.7.1 Router

"Una pasarela o puerta de enlace (del inglés *gateway*) es un dispositivo que permite interconectar dos redes distintas, con protocolos de red[19] y arquitecturas diferentes, a todos los niveles de comunicación. Básicamente, es un sistema hardware o software que hace de puente entre dos aplicaciones o redes incompatibles para que los datos puedan ser transferidos entre distintos ordenadores. Así, su propósito es traducir la información del protocolo utilizando en una red al protocolo usado en la red de destino." [5]

La red del SC2N-EA utiliza protocolos de red diferentes a los del SIMACET, a los cuales no se puede hacer referencia debido a su alta confidencialidad, y para que este último comprenda a la red del SC2N-EA es necesario un *gateway*, capaz de materializar la unión de ambos sistemas de C2. Ésta es la problemática que hay que solucionar, como se ha podido observar en el apartado anterior, para conseguir el objetivo principal del presente TFG: que sea necesario un único operador de inteligencia (S-2).

Para solucionar este problema, se ha elegido el router modelo TC MGUARD RS4000. Este router es un componente de red que proporciona una seguridad y disponibilidad de las redes máxima, tanto LAN como WAN. Además, posee la función NAT (*Network Address Translation*), que permite el intercambio de información, así como la traducción de los protocolos utilizados, entre redes incompatibles. Por último, presenta la capacidad de soportar hasta 10 redes VPN, así como un cortafuegos inteligente [38].

Al realizar la sustitución del router existente en el nodo SIMACET por esta propuesta, se consigue una conexión entre los dos sistemas de C2 actuales, añadiendo mayor seguridad a las redes involucradas, así como el mantenimiento del nivel de seguridad de ambos sistemas, gracias al soporte de varias redes VPN.

4.7.2 Cifrador

El cifrador modelo EPICOM 430, al tener aprobado su uso en redes de la OTAN con la certificación de seguridad de "*NATO secret*" y clasificación inferior, es capaz de recibir la información tanto del EA como del ET, para su posterior des-encriptación y difusión por la red

[19] Protocolo de red: "Es un término utilizado en el mundo de la informática, para dar nombre a una serie de normas y criterios, los cuales, son utilizados para mantener una comunicación entre ordenadores que forman parte de una red informática, es decir, entre los ordenadores que se encuentren conectados entre sí por cualquier sistema de comunicación, sea alámbrico o inalámbrico." [6]

VPN del nodo [36]. Además, es capaz de recibir información de dos redes distintas, y mantener separadas las dos redes VPN, una del ET y otra del EA, diferenciándolas en áreas rojas y negras. El área roja estaría con seguridad "*NATO confidential*", en la que se encontraría la VPN del ET; y el área negra con seguridad "*NATO secret*", en la que se encontraría la VPN del EA.

4.7.3 Switch

Gracias al nuevo router propuesto, una vez configurado, al recibir la información de ambos sistemas de C2 permitiría la convivencia de ambas redes VPN. Pero ahora, es necesario un *switch* que, gracias a sus especificaciones técnicas y su configuración, sea capaz de mantener estas redes VPN, y de garantizar el nivel de seguridad de la red del SC2N-EA ("*NATO secret*"). Por ello se propone la sustitución del actual *switch* modelo Allied Telesis x610-24Ts-POE+ por el modelo Allied Tellesis x530L-28GPX [2].

El Allied Tellesis x530L-28GPX reúne las características imprescindibles para la interoperabilidad de ambas redes. Se trata de un *switch* inteligente, capaz de recibir información de dos redes diferentes y de enviarla sin romper esa diferenciación, permitiendo así la coexistencia de dos redes VPN.

En la Figura 17 se muestra como estarían conectados los distintos elementos hardware al *switch*, así como la información que se recibe y envía por cada puerto.

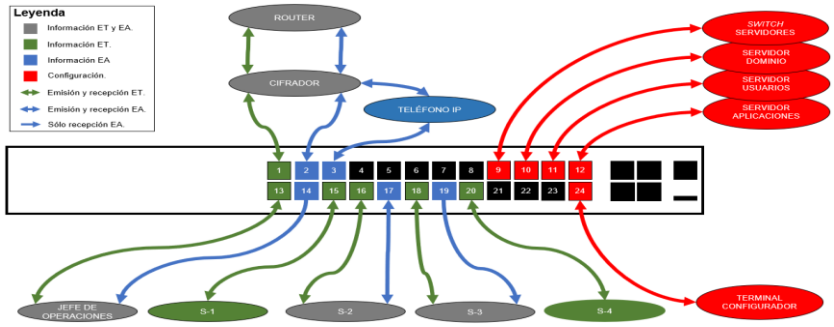


Figura 17 Conexiones de los diferentes elementos al switch. Fuente: elaboración propia

En primer lugar, se puede apreciar en la Figura 18 la presencia de un teléfono, este es el perteneciente al sistema que permitía el acceso a la red del SC2N-EA hasta ahora.

Si se observan los cauces de información, en vez de unirse router, teléfono y *switch* por una única conexión como hasta ahora, se unen por dos conexiones, una por la que circula la información del ET y por la otra la del EA. En ningún momento se mezcla la información de ambos sistemas de C2. Los terminales que reciben la información de ambos Ejércitos (jefe de operaciones, S-2 y S-3) llevarían conectados dos RJ-45 (uno perteneciente a la red VPN del ET, y otro perteneciente a la red VPN del EA) provenientes del *switch*, y el resto que únicamente recibe del ET llevaría conectado un RJ45. De esta manera, se garantiza la existencia de dos redes VPN diferentes y operables por los terminales, manteniendo cada una su propia seguridad.

4.7.4 Teléfono IP

El teléfono, modelo IP Digium D40, que se añadiría al nodo es el usado anteriormente en el conjunto de sistemas para operar en la red del SC2N-EA, con la salvedad de que en vez de estar conectado directamente al cifrador y al terminal para cerrar el circuito (cifrador-teléfono-terminal), ahora se coloca un *switch* entre el terminal y el teléfono (véase Figura 15). Esto no debería ser un problema, dado que puede configurarse el *switch* para establecer qué tipo de información recibe y envía a través de los distintos puertos. Así, se establecería que los puertos X e Y reciben

la información del cifrador y del teléfono, y por el puerto Z dicha información se dirige al operador de S-2.

En la Figura 17, se puede observar un ejemplo de cómo estaría cerrado el circuito "cifrador-teléfono-usuario S-2" para obtener acceso a la red del SC2N-EA, así como el flujo de información en lo que a EA se refiere. El *switch* se configuraría de tal modo que la información del EA recibida a través de los puertos número dos y tres, se envíe y se reciba únicamente por el puerto diecisiete. Además, se configuraría para que la RAP sea enviada a los puertos trece y diecisiete, sin posibilidad de envío de información por la cadena del EA.

4.7.5 SAI

El SAI presente actualmente en el nodo del SIMACET, modelo EATON Ellipse Max1500, está sin existencias. La presente necesidad de añadir otro SAI al nodo para prevenir un corte eléctrico, y la consecuente pérdida del C2 de la operación conlleva la necesidad de adquirir un modelo diferente y el posible desecho del existente.

Se propone como sustituto el hardware SAI modelo EATON 9SX6KiRT, un modelo relativamente nuevo. Éste posee un total de 10 conexiones, todas ellos conectados a la batería interna del SAI. De potencia posee 6000VA/5400W, con la posibilidad de añadir módulos de batería extra (*Extra Battery module*, EBM), hasta un máximo de 4. Si no se incorpora ningún EBM, el tiempo que puede soportar el SAI el suministro de energía, a cada uno de los 10 sistemas, sería de 57 minutos. Ahora bien, si se incorporan los 4 EBM este periodo de tiempo aumentaría hasta los 755 minutos [15].

Al SAI irían conectados todos y cada uno de los hardware, dado que tiene 10 tomas de corriente y tenemos 9 elementos hardware. Con esta incorporación, en caso de apagarse el grupo electrógeno, se conseguiría tener todos los sistemas conectados a su batería interna, así como un mayor tiempo de suministro energético para no perder las capacidades de C2 de la operación.

Los componentes que irían conectados al SAI, en ambas propuestas serían los mismos, dado que únicamente se sustituyen los hardware por otros con mejores prestaciones; además, se añade el teléfono IP, el cual no requiere estar conectado al SAI dado que únicamente se conecta a la toma RJ-45.

4.8 Primera Solución

En los apartados anteriores, se han detallado los elementos imprescindibles para interconectar ambos sistemas de C2, así como la estructura virtual deseada.

A continuación, se muestra la primera propuesta de las dos presentes en este TFG, con la que se trata de proveer al Ejército de una solución económica y rápida al actual problema. Por ello, la solución se basa primordialmente en el reciclaje del mayor número posible de elementos pertenecientes a ambos sistemas de C2, tanto hardware como software. También se detalla el coste de desarrollo de esta primera solución.

4.8.1 Arquitectura física

En la Figura 18 se muestra cómo sería la arquitectura física del sistema con todos los enlaces entre los elementos hardware, una arquitectura que materializaría la unión de ambos sistemas de C2, así como la estructura virtual mostrada en el Apartado 4.6.

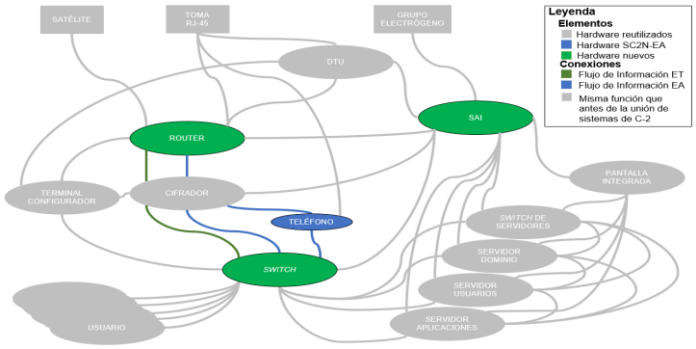


Figura 18 Arquitectura física de la primera solución. Fuente: elaboración propia.

La estructura sería muy similar a la del actual nodo SIMACET de PU, con la salvedad de que se han cambiado tres dispositivos, además de, la incorporación de un hardware procedente del SC2N-EA. Asimismo, al contar ahora el nodo con dos redes VPN, el router, el cifrador y el *switch*, disponen de dos conexiones cada uno. De esta manera, por una conexión circularía la información del ET y por la otra la del EA (véanse los cables de color verde y azul que unen router-cifrador-*switch*).

La DTU, los tres servidores, el *switch* de los servidores, la pantalla integrada, el cifrador, así como los distintos terminales de los usuarios serían los mismos modelos que los usados actualmente en el SIMACET (véase Apartado 3.3.1.3.). Por otro lado, el teléfono también es el mismo que el presente en el sistema que accede a la red del SC2N-EA. Por último, como se ha explicado en el Apartado 4.7, han sido sustituidos el router, el *switch*, y el SAI.

4.8.1.1 Servidores

Para garantizar que el nivel de seguridad de la red del SC2N-EA no sea violado, los tres servidores serán los encargados de establecer los límites a los que pueden llegar los usuarios con sus terminales. Para ello, se llevaría a cabo la configuración de todos ellos del siguiente modo: el servidor de aplicaciones establecería cómo llega la información y cómo la almacena cada aplicación para que no se mezcle la información del ET con la del EA; el servidor de usuarios dictaría qué usuarios tienen derecho a acceder a cada aplicación, así como a qué extensiones de esta puede acceder; y el servidor de dominio sería el encargado de materializar la red LAN creada.

4.8.1.2 Terminales

Con respecto a los 6 terminales necesarios, modelo HP ELITEBOOK 8460, cabe destacar que a nivel hardware tienen lo imprescindible (véase Apartado 3.3.1.3.9) para operar las aplicaciones necesarias.

Sin embargo, el soporte técnico del SO *Windows 7 Pro* finalizó el pasado 14 de enero de 2020, lo que conlleva que, aunque siga funcionando, es mucho más vulnerable a los riesgos de seguridad y virus dado que no tiene actualizaciones de seguridad por parte de la compañía Microsoft [32].

Se propone para subsanar este gran riesgo de seguridad la modernización del SO del *Windows 7 Pro* al *Windows 10 Pro*. Los requerimientos mínimos del sistema son: un procesador compatible a 1GHz mínimo, una memoria RAM mínima de 1GB, espacio libre en disco duro de 20GB [31], los cuales son cumplidos por el HP EliteBook 8460 [19].

Como bien se ha explicado en el Apartado 4.7.3, relativo al nuevo *switch* para operar con las dos redes VPN bien diferenciadas en el nodo, se necesitará conectar dos cables RJ-45,

provenientes del propio *switch,* a los terminales que requieran de la recepción de información tanto del ET como del EA. Para ello, se necesitaría adquirir tres duplicadores de RJ-45, uno para cada operador, que posean un extremo macho para insertar en el terminal, y 2 hembras en el otro extremo para conectar los dos RJ-45 [37].

Por último, en la Figura 19 se muestra cómo sería el flujo de información en lo que a direcciones IP se refiere.

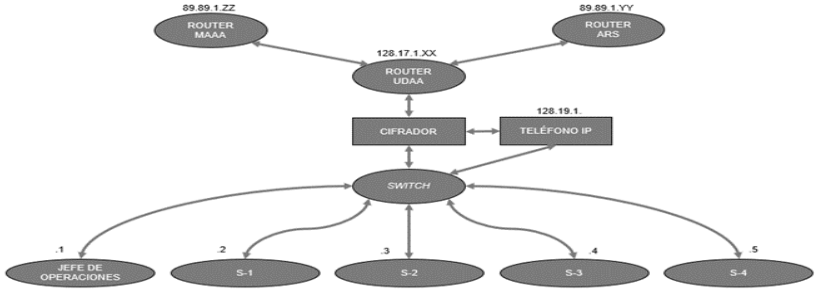


Figura 19 Configuración de direcciones IP de los distintos router y terminales del jefe de operaciones, CIO y CPL. Fuente: elaboración propia.

Como se puede observar, cada router posee una determinada dirección IP, así como el teléfono IP del EA, proporcionada por la UTMAAA. Por otro lado, dentro del router de destino del nodo, cada usuario se identifica con una extensión de la IP del router. A modo de ejemplo, el jefe de operaciones poseerá la IP del router con la extensión .1, quedando de la siguiente manera: 128.17.1.1.

Gracias a la IP de cada hardware, tanto de los router como de los terminales y el teléfono, el *switch* es capaz de discriminar la información recibida dependiendo de cuál es la IP desde la que se envió la información. De esta manera, se puede enviar a cada usuario la información correspondiente, ya sea a un usuario del CIO o del CPL, o a un terminal del ET o del EA externo a la red LAN.

4.8.2 Aplicaciones

Tanto la realización del *Focus Group* como la encuesta (véase Apartados 4.1 y 4.3), han proporcionado un conocimiento bastante amplio sobre las opiniones de los operadores acerca de las distintas aplicaciones que poseen ambos sistemas de C2.

Con respecto a las aplicaciones geográficas, de la encuesta se puede destacar que los operadores del SIMACET califican ANTARES con una puntuación media de 4,1/5, y los operadores de la red del SC2N-EA, así como el operador de S-3 y el jefe de operaciones, califican al ICC-NATO con una puntuación de 5/5. Sin embargo, ANTARES no puede representar las trazas aéreas de la RAP, ni permite cargar los documentos ACO y ATO (imprescindibles para el C2 de la UDAA), mientras que ICC-NATO no ofrece la posibilidad de posicionamiento de las unidades del ET, ni de introducción de datos de personal o logística presentes en la operación (imprescindible para el C2 de las unidades del ET). Y, por otro lado, ICC-NATO no es capaz de llevar a cabo ninguna tarea relativa al C2 del ET.

Por lo tanto, es necesaria la sustitución de ANTARES (utilizada en SIMACET) y de ICC-NATO (en SC2N-EA) por una nueva aplicación que englobe todas las capacidades anteriores.

En base a los resultados obtenidos en la encuesta del Apartado 4.3 y a los análisis DAFO realizados en el Apartado 4.4, la aplicación geográfica más adecuada para esta primera propuesta es TALOS Táctico.

Cabe destacar que, haciendo referencia a los requerimientos del sistema para poder operar esta aplicación, el terminal HP EliteBook 8460 reúne las características necesarias (véase Apartado 4.4).

Se detallan también las aplicaciones a las que tendrá acceso cada operador para ejercer un correcto C2:

- El jefe de operaciones y S-3 tendrían acceso a TALOS Táctico (ET y EA), JCHAT (ET), Outlook (ET), XoMail (ET), Sharepoint (ET) y JEMM (ET). Con la salvedad de que únicamente podrán recibir información del EA, y enviar y recibir del ET.
- S-2 tendría acceso únicamente a las aplicaciones de mensajería, tanto para enviar como recibir información: JCHAT (ET y EA), Outlook (ET y EA), XoMail (ET y EA), Sharepoint (ET) y JEMM (ET y EA).
- S-1 y S-4 tendrían acceso, tanto para recibir como enviar información a TALOS Táctico (ET), JCHAT (ET), Outlook (ET), XoMail (ET), Sharepoint (ET) y JEMM (ET).

Haciendo referencia a la seguridad en la información, no habría problema ante la posibilidad de violar la seguridad de la red del SC2N-EA, dado que el servidor de usuarios es el encargado de establecer los permisos que tiene cada usuario en cada aplicación.

Con respecto a las aplicaciones de mensajería, en la encuesta, los operadores de SIMACET y de la red del SC2N-EA otorgan una calificación de entre cuatro y cinco a las aplicaciones de mensajería JCHAT, Outlook y XoMail. Estos resultados junto con las conclusiones del *Focus Group* conducen a mantener en el sistema las tres aplicaciones de mensajería, con las mismas funciones que presentaban hasta ahora.

Además, también se ha hecho referencia a la necesidad de una aplicación de mensajería en la que se puedan intercambiar mensajes con ambos ejércitos. Dado que los dos sistemas de C2 poseen las mismas aplicaciones (JCHAT, Outlook y XoMail), la solución propuesta es reutilizar los tres softwares, con la salvedad de que habría que conseguir que el terminal de S-2 pueda enviar y recibir mensajería de ambos Ejércitos. Esto no sería un problema, dado que únicamente habría que asignar los permisos correspondientes a esas aplicaciones para que permitan el envío y recepción de información de ambos Ejércitos en las mismas aplicaciones.

JEMM y Sharepoint han obtenido en la encuesta calificaciones de entre tres y cuatro, pero teniendo en cuenta el informe final del *Focus Group*, se llega a la conclusión de que son aptas para realizar sus funciones específicas y se mantienen en esta propuesta, con la salvedad de que el usuario de S-2 tendrá la posibilidad de utilizar JEMM con ambos ejércitos, y Sharepoint únicamente con el ET.

4.8.3 Coste

El coste que conllevaría el desarrollo de esta primera propuesta sería de 10.405,34€. En el Anexo F se puede ver un desglose detallado del mismo.

Con este gasto se consigue materializar la **interoperabilidad** de ambas redes de C2, pero no así conseguir un sistema lo más eficiente posible para llevar a cabo el C2 de la operación de una UDAA.

4.9 Segunda Solución: SIMACTA

Una vez conocida la primera solución, se va a presentar la segunda propuesta de este trabajo, basada en la creación de un nuevo sistema de C2. Éste ha sido nombrado como

SIMACTA, cuyas siglas significan: Sistema de Información para el Mando y Control Tierra Aire.

A diferencia de la anterior propuesta, su desarrollo conllevaría un largo periodo de tiempo, además de un gran desembolso económico, mucho superior a la primera solución.

El nodo SIMACTA de PU tendría la misma arquitectura física que su predecesor, pero con la mayoría de los sistemas hardware de última generación. Su arquitectura virtual sería la misma que se presentó en el Apartado 4.6, mientras que las aplicaciones utilizadas para ejercer el C2 serían renovadas en su mayor parte (excepto tres de ellas, que serán reutilizadas).

La realización del *Brainstorming* (apartado 4.2) permitió recabar un considerable número de ideas sobre las necesidades y requisitos de cara a la implementación de un sistema de C2 que englobase a los anteriores. Además, la encuesta (véase Apartado 4.3) también ayudó considerablemente.

En los siguientes apartados se detalla cómo sería la arquitectura física del nodo de PU del SIMACTA, así como una explicación de cada uno de los hardware que lo integrarían y sus aplicaciones, que permitirían ejercer de manera eficiente el C2 de la UDAA.

Por último, se detalla el coste que conllevaría el desarrollo de este nuevo sistema de C2.

4.9.1 Arquitectura física

La Figura 20 muestra cómo sería la arquitectura física del nodo SIMACTA de PU.

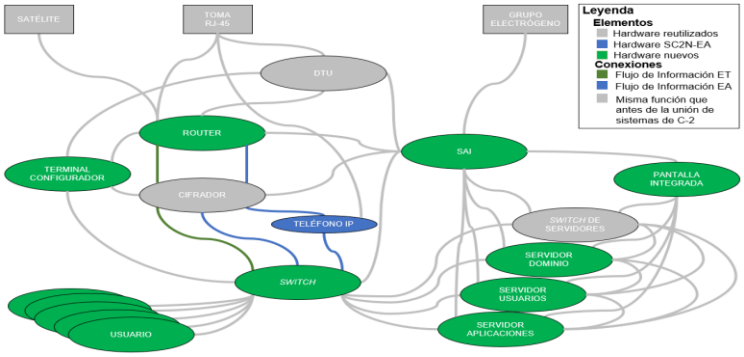


Figura 20 Arquitectura física del nuevo nodo SIMACTA de PU. Fuente: elaboración propia.

Por un lado, como bien se ha explicado en el Apartado 4.7.: se ha añadido el teléfono IP del anterior conjunto de elementos que permitían el acceso a la red del SC2N-EA; el cifrador se mantiene en el SIMACTA; y el router, el *switch* y el SAI han sido sustituidos, tanto para conseguir la independencia de la red VPN correspondiente al ET, de la red VPN del EA, como para conseguir el suministro energético ininterrumpido tan necesario para el correcto C2.

Por otro lado, se han reciclado del SIMACET la DTU y el *switch* de servidores, dado que, realizan sus labores eficientemente y no tienen sistemas sucesores con mejores prestaciones.

4.9.1.1 Servidores

En los actuales sistemas, los tres servidores necesarios (uno para el servidor de dominio, un segundo para el de aplicaciones y el último para el servidor de usuario), son el modelo Dell PowerEdge 210 II. Este modelo ha realizado de manera muy eficiente su labor, pero hoy en día está ya descatalogado. Por ello, se propone la adquisición del modelo Dell PowerEdge R 350, que aporta un plus de seguridad a la red virtual creada, manteniendo unas características similares al anterior [9].

De manera análoga a la primera propuesta, estos tres servidores deberían ser configurados

de igual forma para garantizar que el nivel de seguridad de la red del SC2N-EA no es violado (Apartado 4.8.1.1).

4.9.1.2 Pantalla integrada

La pantalla integrada, modelo Cyberview N-1417, debido a que es un modelo descatalogado en la actualidad [23], se sustituye por el modelo CyberView N119. Se trata de un monitor LCD de 19", con teclado y un panel táctil, con el que se configura todo lo relativo a los servidores de aplicaciones, dominio y usuario, así como el *switch* de servidores. De esta manera, además, se mejoraría la capacidad de visualización y configuración del nodo [25].

4.9.1.3 Terminales

Como se ha podido observar en el informe final del *Brainstorming* y del *Focus Group* (véanse Apartados 4.1 y 1.2), los componentes que integran los terminales son la mayor limitación que presentan los sistemas de C2. Los especialistas destacaron que la falta de velocidad de procesamiento y la lentitud del sistema era debida tanto a la baja capacidad de memoria RAM como al procesador.

Además, en los resultados de la encuesta (véase Anexo E) se puede apreciar que los operadores calificaron con una puntuación media de 1,66/5 el procesador de los terminales, también con un 1,66/5 la memoria RAM, con un 2,58/5 la memoria interna, y con un 2,41/5 el sistema operativo (SO) presente en los terminales.

El modelo HP ELITEBOOK 8460 es el utilizado hasta ahora (véase Apartado 3.3.1.9.), pero debido a la necesidad de unas especificaciones técnicas, acordes a las necesidades de velocidad de procesamiento de información y para poder hacer frente a las necesidades del C2 de una UDAA, es necesaria su sustitución.

El modelo propuesto es el HP ELITEBOOK 840 G8, que posee un procesador Intel-Core i7 de 11ªGeneración, una memora RAM de 16 GB, un disco duro HDD de 512GB y una tarjeta gráfica Intel Iris Xe, con un SO modelo *Windows 10 Pro* [20]. Con las prestaciones presentes en este terminal todas las debilidades que presentaba su antecesor serían subsanadas, garantizando esa velocidad en el procesado de datos para un C2 rápido y efectivo.

Nótese que las versiones seleccionadas para todos los hardware del terminal no son de última generación, sino de una anterior. Esto se hace para asegurar que tanto el SO como los hardware que componen SIMACTA presenten un rendimiento estable y testeado, sin posibles conflictos en sus capacidades de respuesta. Por lo tanto, para SIMACTA se dispondrá de medios de última generación en lo que a estabilidad y seguridad en su respuesta se refiere.

Por último, al igual que en la anterior solución, dado que los terminales únicamente poseen una hembra de RJ-45, se necesitaría adquirir tres duplicadores de RJ-45, uno para cada operador (jefe de operaciones, S-2 y S-3) [37].

4.9.2 Aplicaciones

De los resultados obtenidos en el *Brainstorming* (Apartado 4.2) y en la encuesta (Anexo E) se concluye que es totalmente necesaria la creación de una nueva aplicación para la explotación del sistema geográfico. También es imprescindible contar con una aplicación de intercambio de mensajería, tanto formal como informal, y de documentos, entre el ET y el EA.

Por otro lado, se mantendrán aplicaciones como XoMail, Sharepoint o JEMM, que no se utilizan tan frecuentemente y realizan sus funciones satisfactoriamente.

4.9.2.1 JADTAGES

El nuevo software propuesto para la explotación de un sistema de información geográfico por el SIMACTA ha sido apodado como: Sistema Geográfico Táctico de Defensa Aérea Conjunta (JADTAGES: *Joint Air Defense Tactical Geographic System*).

Mediante el nuevo software se pretende reunir todas las capacidades presentes de sus dos predecesores: ANTARES e ICC-NATO. Deberá ser capaz de presentar en un mapa geográfico toda la información que llegue del ARS, la RAP, así como mostrar las posiciones de las unidades del ET. Para ello la interfaz del sistema, a modo de capas superponibles, mostrará tres posibilidades de visualización de la información: visualizar únicamente la RAP, visualizar la posición de las unidades del ET, o la visualización de ambas capas a la vez.

JADTAGES deberá ofrecer la posibilidad de realizar un estudio del terreno, que facilitaría la labor del personal de S-3 y del jefe de operaciones. Con esta extensión se puede conocer cuál es el estado del terreno para determinar si es accesible a las unidades, o si por el contrario es necesario buscar un itinerario o asentamiento diferente. Además, permite al operador de S-4 realizar un planeamiento adecuado para llevar a cabo el abastecimiento logístico al personal de la operación. Con respecto al operador de S-1, la nueva aplicación deberá tener la posibilidad de introducir toda la información relevante al personal presente en la operación.

Además, deberá ser capaz de leer los documentos ATO y ACO, dado que, sin estos, no se podría determinar por procedimiento si una nave es amiga, enemiga o desconocida.

Las funciones nombradas anteriormente equivalen a las especificaciones mínimas que deberá reunir el JADTAGES. Si falta alguna de ellas, no se podría llevar a cabo el C2 de la UDAA.

Tanto en el *Brainstorming* como en la encuesta se propuso una función extra, considerada beneficiosa por parte de todos los operadores: la incorporación de una extensión destinada a la detección de la señal GPS. De esta manera, el sistema geo-posicionaría a las unidades o sistemas de armas, que dispongan de dispositivo GPS, automáticamente en el sistema.

JADTAGES estará presente en los terminales de los operadores S-1, S-3, S-4 y del jefe de operaciones. Además, cada uno de ellos tendrá permisos diferentes: S-1 y S-4 únicamente operarán con la capa relativa a las unidades del ET, y el jefe y S-3 tendrán permitida además la recepción de la RAP.

Es importante destacar que con esta aplicación no se violaría la seguridad que posee la red del SC2N-EA de "*NATO secret*" dado que, como se ha podido observar a lo largo de este apartado, en ningún momento se mezcla la información, estando diferenciada en capas una vez entra en el terminal por el RJ-45.

4.9.2.2 MIXCHAT

MIXCHAT hace referencia a *Mixed Chat*, o lo que en español significa: chat mixto. Es un software de nueva creación, con el que se pretende conseguir los siguientes objetivos de mensajería: interconexión entre el EA y el ET para enviar y recibir mensajería; posibilidad de comunicación mediante un chat informal individual o en grupo; posibilidad de comunicación mediante mensajería formal; y capacidad de envío y recepción de archivos en distintos formatos por medio de cualquier chat de la plataforma, ya sea formal o informal.

MIXCHAT dará al operador la posibilidad de, utilizando una única aplicación, dialogar informalmente en una interfaz tipo "*WhatsApp*", de forma privada o en grupo, así como el intercambio de mensajería formal mediante un formato similar al de Outlook.

Además, permitirá el intercambio de archivos, siendo aceptados un amplio abanico de

formatos como: Word, Excel, PDF, PowerPoint, JPEG, MP3, MP4, etc. Haciendo referencia a la mensajería formal, también permitirá enviar y recibir archivos en los formatos recién citados, con la salvedad de que existirá un límite de peso del archivo.

Todos los operadores del CIO y el CPL, así como el jefe de operaciones, tendrán este software instalado en sus terminales, con la salvedad de que al igual que JADTAGES, cada uno poseerá unos permisos de envío y recepción de información diferente. De este modo, S-2 será el único con los permisos pertinentes para el intercambio de mensajería con el escalón superior del EA, así como, con el del ET. El resto únicamente tendrá permitido el flujo de información con el ET.

Al igual que JADTAGES, MIXCHAT tampoco violaría la seguridad de la red del SC2N-EA, porque la información llegaría a S-2 por cauces diferentes, siendo diferenciada al llegar y recogido cada flujo por separado. A la hora de recibir y enviar, aunque se envíen mensajes a los dos Ejércitos a la vez, cada mensaje llevará asignada una IP o dirección de correo electrónico, por lo que seguirá su camino sin entremezclarse.

4.9.2.3 XoMail

XoMail ya está presente en los sistemas de C2 tanto del ET como del EA, permitiendo el envío y recepción de información sensible con distintos niveles de seguridad. Es un software de especial seguridad, usado únicamente para el propósito descrito.

En el nuevo C2 continuará estando presente, con la salvedad de que S-2 accederá a un XoMail con permiso para el intercambio de documentación sensible con ambos Ejércitos, mientras que el resto de personal dispondrá del mismo XoMail, pero con permiso únicamente para el intercambio de información con el ET. Con respecto a la seguridad en la información de ambos Ejércitos, esta aplicación estaría configurada de igual forma que MIXCHAT.

4.9.2.4 Sharepoint

La nueva aplicación MIXCHAT permitirá el intercambio de archivos. A pesar de esto, se mantendrá en el nodo SIMACTA la aplicación SHAREPOINT. La diferencia radica en que este software permite cargar en una nube un archivo para que otros usuarios puedan visualizarlo, manipularlo y modificarlo quedando guardado en esa nube todo cambio realizado.

Este software lo poseerán todos y cada uno de los usuarios del nodo del SIMACTA en el ámbito del ET, sin la posibilidad de que S-2 lo utilice en el ámbito del EA (en esta red S-2 no usa esta aplicación).

4.9.2.5 JEMM

Ésta es la única aplicación disponible hoy en día destinada a la creación y seguimiento de incidencias, dentro de los sistemas de C2. Como ha realizado sus cometidos con satisfacción, se considera apropiado volver a utilizarla en el nuevo sistema.

Cabe destacar que el operador de S-2 será el único que poseerá los permisos para operar esta aplicación tanto cuando del EA se trate como del ET, para ello tendrá dos pestañas bien diferenciadas, una de cada Ejército para garantizar la seguridad en la información necesaria.

4.9.3 Coste

El coste que conllevaría el desarrollo de este nuevo sistema de C2, SIMACTA, sería de aproximadamente 234.780,00€. En el coste se incluyen tanto los nuevos elementos hardware, como el desarrollo de los dos softwares que tendrían que ser desarrollados, JADTAGES y

MIXCHAT. En el Anexo G se encuentra desglosado todo el coste que conllevaría el desarrollo de SIMACTA.

El coste de los diferentes hardware se ha hallado de las diferentes páginas web de venta oficiales de los productos.

El coste de desarrollo de los softwares JADTAGES y MIXCHAT se fija en un valor de 100.000€ cada uno. Tomando como referencia que el precio del desarrollo de un software personalizado varía entre los 400€ y los 120.000€, se ha considerado el valor anterior debido a la complejidad que conlleva, se trata del desarrollo de un software con alto nivel de seguridad e interconexión con otros softwares, así que su coste sería muy alto.

Con esta última propuesta, se consigue materializar la **interoperabilidad** de ambas redes de C2, además de la perfecta integración de toda la información recibida de ambos Ejércitos, facilitando en gran medida el C2 de una UDAA.

4.10 Metodología AHP

Para determinar qué propuesta de solución es la óptima para obtener la **interoperabilidad** del C2 entre el ET y el EA, se utiliza el proceso analítico jerárquico (*Analytic Hierarchy Process*, AHP), desarrollado por Thomas L. Saaty [41]. Es un método multicriterio diseñado para resolver problemas complejos con múltiples criterios. Para que el método sea satisfactorio, requiere que quien toma las decisiones proporcione evaluaciones subjetivas respecto a la importancia relativa de cada uno de los criterios y que especifique su preferencia con respecto a cada una de las alternativas de decisión. El resultado del AHP es una jerarquización de prioridades que muestran la preferencia global de cada una de las alternativas de decisión [16, 21].

La metodología AHP es una técnica que se utiliza ante la imposibilidad de cuantificar algunas características de los sistemas, como puede ser la viabilidad de llevar a cabo un proyecto. Mediante este método se permite asignar una medida cuantitativa a esas características que se quieren analizar. Se usa habitualmente en la toma de decisiones de las empresas y organizaciones, cuando necesitan elegir entre varias alternativas posibles [44].

Se ha elegido este método de decisión multicriterio para encontrar cuál de las dos soluciones presentadas en este TFG es la más apropiada para unir la red del SC2N-EA al SIMACET, dado que ambas satisfacen las necesidades de los operadores, pero hay diferencias significativas entre los distintos aspectos que dan lugar a su desarrollo o mantenimiento. Para llevar a cabo el método AHP se han seguido las siguientes fases mostradas en la Figura 21.

Figura 21 Fases en el desarrollo del método AHP. Fuente: elaboración propia a partir de [34].

A continuación, se detalla la ejecución de las cuatro fases anteriores.

1. Primera etapa: Presentación del problema

El objetivo de esta primera etapa del método AHP es presentar el problema a debatir en la toma de decisiones, en este caso, la elección de una de las soluciones propuestas para conseguir la **interoperabilidad** del SIMACET y la red del SC2N-EA [21].

La obtención de los criterios y subcriterios se ha basado en los informes finales del *Focus Group* y del *Brainstorming* (véanse Apartados 4.1 y 4.2), así como en los resultados de la encuesta (véase Apartado 4.3).

El problema en cuestión ha sido representado en un diagrama de árbol (véase Figura 22), donde se pueden observar tanto los criterios de decisión, como sus propios subcriterios.

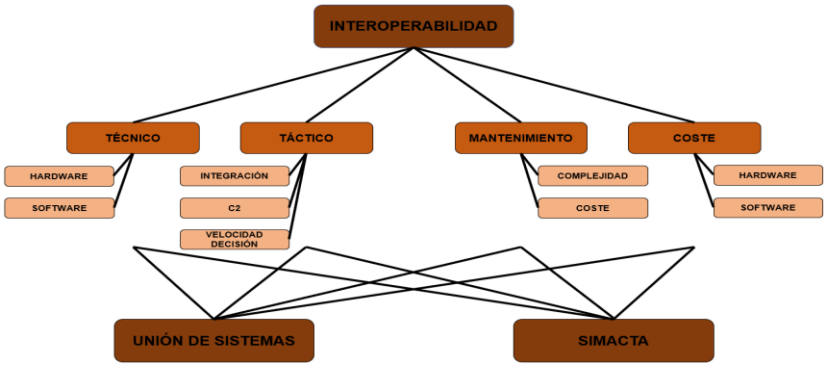


Figura 22 Diagrama de árbol de decisión del método AHP. Fuente: elaboración propia.

La celda superior corresponde al fin que se quiere conseguir, mientras que las dos inferiores corresponden a las dos soluciones propuestas para alcanzar ese fin. Por otro lado, la segunda fila de celdas (de arriba hacia abajo) corresponde a los criterios que se evalúan para llevar a cabo la decisión, y las celdas de color más claro, son los subcriterios.

- Criterio Técnico. Este criterio está relacionado con los aspectos técnicos necesarios en el sistema, así como la viabilidad de materializar las propuestas de interoperabilidad entre sistemas. Hace referencia a la importancia que tienen los elementos tanto hardware como software para mantener los niveles de seguridad de cada red de C2.
  - Hardware. Este subcriterio hace referencia a la importancia o necesidad de renovar los elementos hardware para mantener los niveles de seguridad de ambas redes de C2.
  - Software. Este subcriterio hace referencia a la importancia o necesidad de renovar los elementos software para mantener los niveles de seguridad de ambas redes de C2.
- Criterio Táctico. Este criterio está relacionado con la importancia que tienen los aspectos tácticos, necesarios en el sistema para llevar a cabo el C2 de la UDAA de forma eficiente.
  - Integración. Este subcriterio hace referencia a la importancia que tiene la integración de la información proveniente del C2 de ET como del C2 del EA en un único sistema.
  - C2. Este subcriterio hace referencia a la importancia que tiene que el C2 de la operación de la UDAA se pueda hacer de la manera más eficiente posible.
  - Velocidad de decisión. Este subcriterio hace referencia a la importancia que tiene que el sistema posea una velocidad suficiente para que la toma de decisiones sea rápida.
- Criterio Mantenimiento. Este criterio está relacionado con la importancia que tiene el mantenimiento a la hora de desarrollar las propuestas.
  - Complejidad. Este subcriterio hace referencia a la importancia de la complejidad para llevar a cabo las tareas de mantenimiento.
  - Coste. Este subcriterio hace referencia a la importancia del coste del mantenimiento.
- Criterio Coste. Este criterio está relacionado con la importancia que se le da al coste a la hora de desarrollar las propuestas.
  - Hardware. Este subcriterio hace referencia a la importancia que se le asigna al coste de los elementos hardware.
  - Software. Este subcriterio hace referencia a la importancia que se le asigna al coste del

desarrollo de aplicaciones nuevas.

2. Segunda Etapa. Evaluación de los criterios de valoración

Una vez obtenidos los criterios y subcriterios, se procede a la valoración de estos. Esta valoración es necesaria dado que no todos los criterios/subcriterios tendrán la misma importancia para los expertos. Por ejemplo, unos considerarán más importante conseguir unos buenos aspectos tácticos, que mejoren considerablemente el C2, que mantener la seguridad técnica.

Para evaluar los criterios/subcriterios se ha contado con la participación de los seis operadores pertenecientes al CIO y CPL (jefe de operaciones, S-1, S-2 del SIMACET, S-2 de la red del SC2N-EA, S-3 y S4) de la batería de plana del GAAA I/73 que dirigen el combate en tiempo no real de una UDAA. Para ello,

Se han realizado dos cuestionarios, donde en el primer cuestionario se evalúa cada criterio y subcriterio haciendo comparaciones por parejas (véase Anexo I), cuyos resultados se encuentran en el Anexo K. En el segundo cuestionario se evalúan las dos propuestas en base a cada subcriterio de cada criterio (véase Anexo J), cuyos resultados se encuentran en el Anexo L.

Todos los criterios/subcriterios son medidas cualitativas, y para que sean medibles de forma cuantitativa y poder determinar cuál de las dos propuestas es la mejor opción, se ha utilizado la escala de Saaty (véase Tabla 2). Como se puede apreciar en la Tabla 2, mediante la escala de Saaty se valoran dos criterios, A y B. Si se le asigna por ejemplo un valor de 5 al criterio A, al criterio B se le asignaría el inverso, 1/5. Esta escala ha sido suministrada, al igual que la encuesta, al personal participante para valorar las diferentes preguntas acerca de la comparación de los criterios y subcriterios.

Tabla 2 Escala de Saaty. Fuente: [41 y 45].

VALOR	DEFINICIÓN	COMENTARIO
1	Igual importancia	A y B tienen la misma importancia
3	Importancia moderada	A es ligeramente más importante que B
5	Importancia grande	A es más importante que B
7	Importancia muy grande	A es mucho más importante que B
9	Importancia extrema	A es extremadamente más importante que B

La Tabla 3 muestra un ejemplo de la encuesta realizada para la comparación de dos criterios. La manera de proceder sería: marcar con una “X” a la derecha del criterio/subcriterio elegido, y posteriormente en el hueco en blanco, de la columna “VALOR”, asignar la valoración correspondiente, en base a los valores de la Escala de Saaty (véase Tabla 2).

Tabla 3 Ejemplo de tabla del cuestionario.

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el criterio Técnico con el Táctico:	Técnico		Táctico		3

Una vez obtenidos los valores del cuestionario (véase Anexo K) relativo a la comparación entre criterios y subcriterios, se llevó a cabo un método cualitativo (véase Anexo H) para conseguir un resultado final en base a los valores cualitativos de cada una de las respuestas de cada uno de los operadores. Una vez conseguidos estos resultados finales, se introdujeron los datos en el programa AHP elaborado por el Teniente Coronel D. Carlos L. Ruiz López, el cual nos proporciona las matrices de comparación de criterios con sus pesos correspondientes (W) (véase Tabla 4) [45].

Tabla 4 Matriz de resultados de la comparación de criterios.

CRITERIOS	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	PESO(W)	RI
TÉCNICO	1	3	9	3	0,51	
TÁCTICO	1/3	1	7	3	0,29	0,0658
MANTENIMIENTO	1/9	1/7	1	1/5	0,04	
COSTE	1/3	1/3	5	1	0,16	

Como se puede observar en la Tabla 4, los criterios Técnico y Táctico obtienen los mayores pesos, con un 51% y un 29% respectivamente. A estos dos le sigue el Coste con un 16%, y por último el Mantenimiento con un 4%. Como conclusión, se puede apreciar que los operadores han dado una mayor importancia a conseguir que el sistema sea capaz de mantener los niveles de seguridad de cada sistema de C2, por encima de los aspectos técnicos que proporcionan las capacidades de conducción de la operación, y muy por encima del coste. Por lo tanto, los expertos consideran que, si no se pudieran mantener los niveles de seguridad necesarios, seguramente no se podría llevar a desarrollo las propuestas.

La Razón de Inconsistencia (RI) (véase Tabla 4) es un coeficiente, calculado en cada tabla de comparaciones, que informa del grado de coherencia o incoherencia presente en los valores asignados a la importancia de cada criterio, subcriterio o propuestas. Saaty estableció que el valor de la RI debe de estar por debajo del 10%, de este modo se garantiza la coherencia del análisis realizado. En este caso, adquiere un valor de 0,0658 (6,58%), inferior al valor umbral establecido por Saaty, por lo que se puede continuar con el estudio dada su coherencia [21,41,45]. Cabe destacar, que cuando los valores de la matriz son todo 1, o cuando la matriz es 2x2 (únicamente hay dos elementos a comparar), el valor de RI será de 0.

De manera análoga, se comparan los subcriterios. La tabla 5 muestra la tabla correspondiente a la comparación entre subcriterios del criterio Técnico. En el Anexo H se pueden consultar las tablas correspondientes al resto de criterios.

Tabla 5 Matriz de resultados de la comparación entre los subcriterios del criterio Técnico.

TÉCNICO	HARDWARE	SOFTWARE	PESO(W)	RI
HARDWARE	1	7	0,87	0,0000
SOFTWARE	1/7	1	0,13	

3. Tercera etapa: Evaluación de alternativas

En este paso, se realizan tantas tablas o matrices como subcriterios haya en cada criterio, donde en cada matriz se lleva a cabo la comparación entre las alternativas con respecto al subcriterio en cuestión. Para ello, se ha realizado otro cuestionario a los mismos operadores (véase Anexo J), cuyos resultados finales obtenidos del método cualitativo seguido (Anexo H) se encuentran en el Anexo L.

Este segundo cuestionario es muy similar al anterior, con la salvedad de que para contestarlo los operadores deberán conocer cuáles son las dos propuestas a comparar (unión de ambos sistemas y SIMACTA). En el cuestionario, previo a las preguntas, se detalla cuáles son las dos propuestas, así como los criterios y subcriterios a evaluar, los cuales también se detallan en el Anexo H.

Las Tablas 6 y 7 muestran las matrices obtenidas de la comparación de los subcriterios del criterio Táctico. Las tablas correspondientes al resto de criterios se incluyen en el Anexo H.

Tabla 6 Matriz final con los resultados de la comparación del subcriterio Hardware, del criterio Técnico, con ambas propuestas.

HARDWARE	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1	0,5	0,0000
SIMACTA	1	1	0,5	

Tabla 7 Matriz final con los resultados de la comparación del subcriterio Software, del criterio Técnico, con ambas propuestas.

SOFTWARE	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1/3	0,25	0,0000
SIMACTA	3	1	0,75	

4. Cuarta etapa: Jerarquización de alternativas

Finalmente, después de todos los pasos anteriores, en la cuarta y última etapa, se determina cuál de las dos propuestas es la óptima. Para discriminar la mejor propuesta se reúne toda la información, relativa a los pesos de la segunda etapa (valoración de los criterios de evaluación) y de la tercera etapa (evaluación de alternativas) en una tabla para la toma de la decisión, como se puede apreciar en la Tabla 8.

Tabla 8 Matriz final con los resultados de la aplicación del método AHP.

CRITERIOS/ SUBCRITERIOS	PESOS (W)	UNIÓN DE SISTEMAS	SIMACTA
TÉCNICO	0,51	0,47	0,53
HARDWARE	0,87	0,50	0,50
SOFTWARE	0,13	0,25	0,75
TÁCTICO	0,29	0,29	0,71
INTEGRACIÓN	0,33	0,25	0,75
C2	0,33	0,50	0,50
VELOCIDAD DECISIÓN	0,33	0,13	0,87
MANTENIMIENTO	0,04	0,25	0,75
COMPLEJIDAD	0,25	0,25	0,75
COSTE	0,75	0,25	0,75
COSTE	0,16	0,88	0,12
HARDWARE	0,83	0,87	0,13
SOFTWARE	0,17	0,90	0,10
RESULTADO		0,47	0,53

4.10.1 Interpretación de resultados

Al observar la Tabla 8, la columna de pesos muestra que el criterio principal y más importante es el Técnico, con un peso del 51%. El siguiente criterio con más peso es el Táctico con un 29%. Estos resultados son lógicos por diversos motivos: en primer lugar, porque la seguridad en las redes a nivel OTAN es lo más importante a la hora de materializar la **interoperabilidad** de ambos sistemas; en segundo lugar, porque los elementos hardware y software que presentan las propuestas deben de permitir esa seguridad.

El hecho de que el segundo criterio sea el Táctico es totalmente lícito, dado que la **interoperabilidad** de ambos sistemas de C2 debe dar como resultado esa integración de informaciones, un C2 eficaz y una velocidad en la toma de decisiones.

Por último, se puede destacar que los operadores han considerado que tanto el mantenimiento como el coste son criterios menos importantes que el conseguir una seguridad y un C2 efectivo.

En la Tabla 8 también se recogen los resultados de la comparación entre ambas propuestas. Se puede apreciar como la propuesta “SIMACTA” ha quedado por encima de la propuesta “Unión de sistemas” por la mínima, con 53% y un 47% respectivamente.

De esta manera, podemos finalizar concluyendo que, en función de los resultados obtenidos a través del método AHP, la propuesta más apropiada para llevar a cabo la **interoperabilidad** del SIMACET y de la red del SC2N-EA es el desarrollo de un nuevo sistema de C2, apodado como SIMACTA (Sistema de Información para el Mando y Control Tierra Aire).

5 Conclusiones

Con este trabajo se han conseguido aportar dos propuestas con las que mejorar el mando y control en tiempo no real de los puestos de mando de una UDAA.

Para presentar las dos posibilidades, se ha realizado un estudio de las capacidades y limitaciones que presenta el mando y control en tiempo no real de un puesto de mando de una UDAA. Por otro lado, se han determinado las capacidades y limitaciones presentes en el

SIMACET y en el SC2N-EA, para después determinar cómo subsanarlas.

Las dos propuestas presentadas consiguen el objetivo principal de este TFG, la **interoperabilidad** de ambos sistemas de mando y control. Sin embargo, no aportan las dos las mismas capacidades, pues la propuesta basada en la creación de un nuevo sistema de mando y control consigue integrar perfectamente ambos sistemas, además de conseguir una velocidad de procesamiento con una consecuente velocidad en la toma de decisiones muy superior a la primera propuesta.

Cabe destacar, que para que se lleven a cabo cualesquiera de las dos soluciones, sería necesario que la nueva topología/estructura de red sea homologada por ambos ejércitos. De esta manera, tanto el ET como el EA darían el visto bueno a las propuestas, habiendo realizado un estudio minucioso sobre el mantenimiento de la seguridad, tanto "*NATO confidential*" como "*NATO secret*" del ET y del EA, respectivamente.

El método multicriterio AHP, ha permitido determinar, gracias a los cuestionarios rellenados por los operadores del SIMACET y del SC2N-EA, cuál de las dos propuestas es la adecuada para llevar a desarrollo, determinando que debería de ser la segunda propuesta, la creación de un nuevo sistema de mando y control, apodado como SIMACTA (Sistema de Mando y Control Tierra Aire).

6 Líneas Futuras

La **interoperabilidad** del sistema de Mando y Control del Ejército de Tierra y del sistema de Mando y Control del Ejército del Aire, es uno de los puntos recogidos en el archivo "Tendencias 2018-2019. Volumen II", de uso oficial, creado por el Mando de Adiestramiento y Doctrina.

En este documento se recogen todas las tendencias futuras que tiene la Artillería, relacionadas con el concepto "Fuerza 35"[20]. En lo que a C2 de una DAA se hace referencia a conseguir para el año 2035 una "capacidad de integración del sistema de C2 de la defensa aérea y de la organización operativa terrestre. Para ello sería necesario que el sistema de Mando y Control terrestre (SIMACET), y aéreo (SC2N-EA) sean **interoperables** y compartan información, tanto las acciones de DAA como la gestión del espacio aéreo." [30]

Además, de igual modo, se quiere conseguir una **interoperabilidad** de los sistemas de C2 españoles con los sistemas de C2 de otros ejércitos extranjeros. [30]

Los resultados recogidos en este trabajo proporcionan una primera fase para conseguir dicha interoperabilidad. Las líneas futuras, en base a las perspectivas de "Fuerza 35", son:

- Mantener los niveles de seguridad de todos y cada uno de los sistemas de C2 que intervengan.
- Conseguir que el C2 mejore considerablemente, tanto en integración de la información como en velocidad de decisión.
- Lograr una **interoperabilidad** con los sistemas de C2 de los países de la OTAN para mejorar así considerablemente la defensa del espacio aéreo de la alianza.

[20] "Fuerza 35" es la solución del ET para dar respuesta al proceso de planeamiento militar que lidera el Jefe de Estado Mayor de la Defensa (JEMAD), con la finalidad de mantener unas Fuerzas Armadas eficaces y proporcionadas al nivel de ambición establecido. [13]

7 Referencias Bibliográficas

[1]Allied Tellesis (2017). Switch x610-24Ts-POE+. Disponible en: x610-24Ts-POE+ | Allied Telesis [Consultado 7-10-2021].

[2]Allied Tellesis (2020). Switch x530L-28GPX. Disponible en: https://www.alliedtelesis.com/es/es/products/switches/x530L-series/x530l-28gpx [Consultado 7-10-2021].

[3]Carritech Telecommunications (2015). Alcatel Mainstreet 2753 DTU. Disponible en: https://www.carritech.com/item/Newbridge/90-4093-02/ [Consultado 8-10-2021].

[4]Centro Geográfico del Ejército (1998). ***Manual de Usuario de la Carta Digital.*** Madrid: CEGET.

[5]Centro Integrado de Formación Profesional de Aprendizajes Virtuales y Digitalizados (2009). Pasarelas (Gateways): El Router. Disponible en: https://ikastaroak.ulhi.net/edu/es/IEA/ICTV/ICTV09/es_IEA_ICTV09_Contenidos/website_64_pasarelas_gateways_el_router.html [Consultado 5-10-2021].

[6]Centro Integrado de Formación Profesional de Aprendizajes Virtuales y Digitalizados (2009). Protocolo de comunicación. Disponible en: https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/DAMDAW/SI/SI03/es_DAMDAW_SI03_Contenidos/website_22_protocolo_de_comunicacin.html [Consultado 5-10-2021].

[7]Cisco Worldwide. Cisco 2801 Integrated Services Router (2016). Disponible en: https://www.cisco.com/c/en/us/obsolete/routers/cisco-2801-integrated-services-router.html [Consultado 22/09/2021].

[8]Dell (2009). Dell PowerEdge R210. Disponible en: https://www.dell.com/es-es/work/shop/productdetailstxn/poweredge-r210 [Consultado 22-09-2021].

[9]Dell (2020). Dell PowerEdge R350. Disponible en: https://www.dell.com/es-es/work/shop/cty/pdp/spd/poweredge-r350/emea_r350 [Consultado 7-10-2021].

[10]Departamento de comunicación del Ejército de Tierra (2012). Cuartel General del Mando de Artillería Antiaérea. Disponible en: https://ejercito.defensa.gob.es/unidades/Madrid/cgmaaa/Organizacion/index.html [Consultado 19/09/2021].

[11]Departamento de comunicación del Ejército de Tierra (2012). Regimiento de Artillería Antiaérea 94. Disponible en: https://ejercito.defensa.gob.es/unidades/Las_Palmas/raaa94/ [Consultado 19/09/2021].

[12]Departamento de comunicación del Ejército de Tierra (2012). Unidad de Transmisiones del Mando de Artillería Antiaérea. Disponible en: https://ejercito.defensa.gob.es/unidades/Madrid/utmaaa/ [Consultado 19/09/2021].

[13]Departamento de comunicación del Ejército de Tierra (2019). Resumen ejecutivo “Fuerza 35”. Disponible en: .:Ejército de tierra - Resumen ejecutivo 'FUERZA 35':. (defensa.gob.es)

[Consultado 28/10/2021].

[14]EATON Powering Business Worldwide (2009). SAI EATON Ellipse Max 1500. Disponible en: http://powerquality.eaton.com/68558.aspx?cx=97&GUID=377781F3-4FA5-446F-B384-F1F8FB5977F6 [Consultado 22-09-2021].

[15]EATON Powering Business Worldwide (2020). SAI EATON 9SX6KiRT. Disponible en: https://www.eaton.com/es/es-es/catalog/backup-power-ups-surge-it-power-distribution/eaton-9sx--5-11kva--ups.html [Consultado 7-10-2021].

[16]Escobar Urmeneta, M.T. y Moreno Jiménez, J.M (1997). ***Problemas de gran tamaño en el proceso analítico jerárquico.*** *Estudios de Economía Aplicada*, 8, pp. 25-40. Disponible en: https://www.researchgate.net/publication/28088594_Problemas_de_gran_tamano_en_el_Proceso_Analitico_Jerarquico

[17]GMV Aerospace and Defence S.A.U. (2020). ***Manual de Usuario TALOS Táctico.*** Zaragoza: GMV Aerospace and Defence S.A.U.

[18]Hernández Salazar, P. (2008). ***Métodos cualitativos para estudiar a los usuarios de la información.*** México: Centro Universitario de Investigaciones Bibliotecológicas.

[19]Hewlett-Packard (2011). Notebook HP EliteBook 8460p. Disponible en: https://support.hp.com/es-es/document/c03289311 [Consultado 22-09-2021].

[20]Hewlett-Packard (2021). Notebook HP EliteBook 840 G8. Disponible en: https://www.hp.com/es-es/shop/product.aspx?id=336D6EA&opt=ABE&sel=NTB [Consultado 8-11-2021].

[21]Hurtado, T. y Bruno, G. (2005). ***El Proceso de Análisis Jerárquico (AHP) como herramienta para la Toma de Decisiones en la Selección de Proveedores.*** Universidad Nacional Mayor de San Marcos. Disponible en: https://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/toskano_hg/cap3.PDF

[22]IBM (2014). Redes frame relay. Disponible en: https://www.ibm.com/docs/es/i/7.2?topic=standards-frame-relay-networks [Consultado 25/09/2021].

[23]KVM Switches Online (2002). Cyberview N-1417. Disponible en: https://www.dell.com/es-es/work/shop/productdetailstxn/poweredge-r210 [Consultado 22-09-2021].

[24]KVM Switches Online (2017). Cyberview CV-S801 KVM. Disponible en: CV-S801 - Cyberview KVM USB de 8 puertos - con 8 cables (kvm-switches-online.com) [Consultado 22-09-2021].

[25]KVM Switches Online (2020). Cyberview N119. Disponible en: https://www.kvm-switches-online.com/n119.html [Consultado 7-10-2021].

[26]Mando de Adiestramiento y Doctrina (2009). ***PD3-602: Establecimiento y Empleo del SIMACET***. Granada: MADOC.

[27]Mando de Adiestramiento y Doctrina (2010). ***Manual Básico de Usuario de SIMACET***. Granada: MADOC.

[28]Mando de Adiestramiento y Doctrina (2016). ***PD4-300 Tomo I: Empleo de Artillería Antiaérea***. Granada: MADOC.

[29]Mando de Adiestramiento y Doctrina (2016). ***PD4-300 Tomo II: Empleo de Artillería Antiaérea***. Granada: MADOC.

[30]Mando de Adiestramiento y Doctrina (2018). ***Tendencias 2018-2019. Volumen II. Artillería***. Granada: MADOC.

[31]Microsoft (2015). Windows 10 Pro. Disponible en: https://www.microsoft.com/es-es/d/windows-10-pro/df77x4d43rkt/0002?rtc=1&activetab=pivot%3aoverviewtab [Consultado 7-10-2021].

[32]Microsoft (2020). El soporte de Windows 7 finalizó el 14 de enero de 2020. Disponible en: https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finaliz%C3%B3-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962 [Consultado 7-10-2021].

[33]Ministerio de Defensa de España (2016). Fuerza de Respuesta OTAN España, punta de lanza VJTF. Disponible en: https://www.defensa.gob.es/brigada-vjtf/index.html [Consultado 19/09/2021].

[34]Moreno Jiménez, J.M. (2002). ***El Proceso Analítico Jerárquico (AHP). Fundamentos, Metodología y Aplicaciones.*** *Rect@: Revista Electrónica de Comunicaciones y Trabajos de ASEPUMA,* Extra_____1, pp. 28-77. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7886562

[35]Morgan, D. L. (1998). ***The Focus Group Guidebook, Focus Group kit 1.*** Portland: SAGE publications.

[36]NATO Information Assurance (2015). EP430GN. Disponible en: NIA - NATO Information Assurance [Consultado 22/09/2021].

[37]PC Componentes (2021). Duplicador conector RJ-45. Disponible en: Duplicador Conector de red RJ45 Cat 5e | PcComponentes.com [Consultado 27-10-2021]

[38]Phoenix Contact (2018). TC MGUARD RS4000 3G VPN. Disponible en: https://www.phoenixcontact.com/online/portal/es?uri=pxc-oc-itemdetail:pid=2903440&library=eses&tab=1 [Consultado 5-10-2021].

[39]Redacción (2021). "El Ejército del Aire estrena sistema de mando y control". ***Infodefensa***, 29 de septiembre. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3212883/ejercito-aire-espanol-estrena-sistema-mando-control [Consultado 3-10-2021].

[40]Redacción (2021). "Entra en funcionamiento el nuevo el nuevo sistema de mando y control del Ejército del Aire SC2N-EA". ***La Noción***, 29 de septiembre. Disponible en: https://www.lanocion.es/espanya/20210929/entra-en-funcionamiento-el-nuevo-sistema-de-m-12884.html [Consultado 3-10-2021].

[41]Saaty, R.W. (1987). ***The analytic hierarchy process – what it is and how it is used. Mathematical Modelling***, 9 (3-5), pp. 161-176. DOI: 10.1016/0270-0255(87)90473-8

[42]Sancho Val, J. J. (2016). ***Apuntes de Calidad.*** Zaragoza: Centro Universitario de la Defensa.

[43]Secretaría General Técnica-Secretariado del Gobierno-Centro de Publicaciones (2016). Normas de la Autoridad Nacional para la Protección de la Información Clasificada. Disponible en: Normas de la autoridad nacional para la protección de la información clasificada (cni.es) [Consultado 17-10-2021].

[44]Subías Canals, P. (2015). ***Toma de Decisiones en la Adquisición de un Sistema de Guiado para el Lanzamiento de Cargas con Precisión para las Fuerzas Armadas: Empleo de la Metodología Multicriterio AHP.*** Trabajo Fin de Grado. Centro Universitario de la Defensa.

[45]Tcol. Ruíz López, C. L. (2014). ***Manual de Usuario del Programa Ayuda a la Decisión AHP***. Zaragoza: Centro Universitario de la Defensa.

ANEXOS

ANEXO A. HPS y SHPS

"La habilitación personal de seguridad (HPS) es la resolución positiva de la Agencia Nacional para la Protección de la Información Clasificada (ANPIC) por la que, en nombre del Gobierno del Reino de España, reconoce formalmente la capacidad e idoneidad de una persona para tener acceso a la información clasificada en el ámbito y grado autorizado, al haber superado el proceso de investigación de seguridad y haber sido concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento, resolución que se materializa en un documento firmado por la ANPIC." [43]

Hay distintos tipos de HPS, clasificadas según el tipo y el grado que posea, donde el tipo corresponde al ámbito al que pertenece la información (OTAN, UE, NACIONAL), y el grado corresponde a la máxima clasificación de la información a la que se le habilita el acceso con una HPS determinada. De este modo, en la Tabla 9 se pueden apreciar los distintos tipos y grados de las HPS, así como sus equivalencias entre los tipos.

Tabla 9 Diferentes tipos y grados de la información clasificada, y sus equivalencias. Fuente: elaboración propia a partir de CNI [43].

NACIONAL	UNIÓN EUROPEA (UE)	OTAN
Secreto	UE top secret	Cosmic top secret
Reservado	UE secret	NATO secret
Confidencial	EU confidential	NATO confidential
Difusión limitada	EU restricted	NATO restricted
Sin clasificar	EU sensitive information	NATO unclassified

Toda persona que necesite manipular información de grado "Confidencial", o equivalente o superior, deberá disponer de la HPS necesaria. Para solicitar la HPS habrá para el uso de información clasificada se deben rellenar los siguientes formularios, que se pueden encontrar en este mismo anexo.:

- Rellenar el formulario denominado "Solicitud de Habilitación Personal de Seguridad (SHPS), debiendo firmar este documento el superior jerárquico que acredita la necesidad de la solicitud.
- Rellenar el formulario denominado "Declaración Personal de Seguridad (DPS)"

En relación con este TFG, la HPS es la acreditación necesaria en los componentes del puesto de mando de una UDAA para poder manipular tanto la información relativa al ET como al EA, dado que la información del C2 del ET es de grado "Confidencial" y la del EA es de grado "Secreto".

SOLICITUD DE HABILITACIÓN PERSONAL DE SEGURIDAD (SHPS)

FORMULARIO A CUMPLIMENTAR POR LOS ÓRGANOS QUE TRAMITAN LA SOLICITUD DE HPS

AUTORIDAD NACIONAL PARA PROTECCIÓN IC

SOLICITUD DE HABILITACIÓN PERSONAL DE SEGURIDAD — **SHPS-100 (2018)**

1.- IDENTIFICACIÓN DEL INTERESADO [1] (datos EXACTOS extraídos del documento de identidad)		
Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	**(FOTOGRAFÍA)** [3]
PRIMER APELLIDO:	NOMBRE:	
SEGUNDO APELLIDO:	SEXO: **MASCULINO**	
FECHA DE NACIMIENTO:	NACIONALIDAD:	
LUGAR DE NACIMIENTO:	PROVINCIA/PAÍS NAC.:	
LUGAR DE DOMICILIO:	PROVINCIA/PAÍS DOM.:	
NOMBRE PADRE (A):	NOMBRE MADRE (B):	
Datos Pasaporte [2] (internacional) – Número:	Número de Identificador:	

DATOS DE EMPLEO/DESTINO [4] El interesado es personal laboral ajeno que trabaja eventualmente como ASESOR en el Sector Público: ☐

Organismo, Unidad o Empresa:	Cargo o empleo:
Correo electrónico oficial propio:	Teléfono de contacto:

2.- INICIO DEL EXPEDIENTE DE SOLICITUD POR EL JEFE DE SEGURIDAD (JS) DEL ÓRGANO DE SEGURIDAD [5]

NOMBRE (JS):	ÓRGANO DE SEGURIDAD:
Correo electrónico oficial:	Teléfono de contacto:

HPS SOLICITADA PARA EL INTERESADO [6]

GRADO DE LA HPS [7] BORRAR		TIPO	ESPECIALIDADES por TIPO	CARÁCTER DE LA SOLICITUD [8]
NACIONAL	INTERNACIONAL	NACIONAL ☐	CRIPTO (C) ☐ SIGINT (B) ☐	
CONFIDENCIAL ☐	CONFIDENTIAL ☐	OTAN ☐	CRYPTO (C) ☐ BOHEMIA (B) ☐ ATOMAL (A) ☐	INICIAL (I) ☐
RESERVADO ☐	SECRET ☐	UE ☐	CRYPTO (C) ☐	RENOVACIÓN (R) ☐
SECRETO ☐	TOP SECRET ☐	ESA ☐	CRYPTO (C) ☐	AMPLIACIÓN (A) ☐

DECLARACIÓN [9]: Certifico que el interesado ha sido: 1) **identificado correctamente**, a la vista del documento de identidad original y verificación de validez de la firma electrónica, en su caso, 2) **concienciado** en la protección de la información clasificada y 3) **instruido en las especialidades** siguientes, estando motivada la solicitud por las razones que se indican:

☐ Cripto/Crypto (C)
☐ Bohemia/Sigint (B)
☐ Atomal (A)

JUSTIFICACIÓN DETALLADA DEL MOTIVO DE SOLICITUD DE LA HPS [10]

FECHA: (sello / firma) FIRMAR

DOCUMENTACIÓN QUE SE ACOMPAÑA [11] (cumplimentar por los escalones de tramitación responsables en cada caso)

FORMULARIO DPS-101 COMPLETO ☐	APARTADO 7 DEL DPS-101 ☐	CERTIFICADO DE INVESTIGACIÓN DE SEGURIDAD AUTORIZADA ☐
PP-103 (Empresas) ☐	ACTA DE NACIONALIZACIÓN (copia compulsada) ☐	CERTIFICADO DE INSTRUCCIÓN BOHEMIA/SIGINT ☐
OTROS (especificar):		

3.- DECLARACIÓN DEL MANDO O RESPONSABLE DE LA UNIDAD, CENTRO, ORGANISMO O EMPRESA, SOLICITANTE DE LA HABILITACIÓN PARA EL INTERESADO, QUE AUTORIZA LA SOLICITUD [12]

NOMBRE:	CARGO:
ORGANISMO O EMPRESA:	UNIDAD/CENTRO:

DECLARACIÓN: Autorizo el inicio de la tramitación de la solicitud de HPS para la persona interesada identificada arriba, en este documento, basado en su "necesidad de conocer" y en la veracidad y exactitud de dichos datos de identidad, y declaro que, **tras haber realizado averiguaciones básicas** [13], **(marcar una)**:

☐ Hasta donde razonablemente se conoce, no se tiene información alguna que haga dudar de la idoneidad del interesado para la solicitud.
☐ No se tiene conocimiento de las condiciones de seguridad del interesado o se aprecian circunstancias adversas, no siendo éstas lo suficientemente significativas como para adoptar una decisión previa al respecto.

FECHA: (sello / firma) FIRMAR

4.- AUTORIZACIÓN DE TRAMITACIÓN A LA ONS DEL ÓRGANO SUPERIOR DE PROTECCIÓN DE LA IC [14]		**SOLICITUD FINAL** [15]
El Jefe de Seguridad del Servicio de Protección, Subregistro Principal, Área de Seguridad, u Oficina de Seguridad autoriza la tramitación, una vez revisado el expediente y solicitud final.		
NOMBRE:	FECHA: (sello / firma) FIRMAR	

(Código de presentación por la Sede Electrónica del CNI) [16]	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Formulario ONS/SHPS-100/2018.02 - 1 -

INSTRUCCIONES DE CUMPLIMENTACIÓN

INSTRUCCIONES GENERALES

- El proceso de habilitación de seguridad del personal se rige conforme a la norma NS/02 de las Normas de la Autoridad Nacional para la Protección de la Información Clasificada.
- La responsabilidad sobre la veracidad, necesidad y conveniencia de los datos remitidos en el presente formulario es del responsable del inicio de la tramitación, auxiliado por su Órgano de Control/Servicio de Protección/Área u Oficina de Seguridad. En ningún caso es responsabilidad del interesado, quien únicamente deberá presentar la información que le sea requerida, y que podrá ayudar, en su caso, en su confección, conforme a los criterios e instrucciones precisos recibidos de los primeros. **Es obligatoria la identificación positiva del interesado con su documento de identidad original**.
- Los datos se cumplimentarán electrónicamente. No se admitirán formularios rellenos a mano, salvo en la firma, fechado y sellado oficial (en tanto no se sustituyan por una firma electrónica autorizada), y salvo marcas posteriores necesarias en el apartado "Documentación que se acompaña". Para ello únicamente se precisa disponer de un ordenador con la aplicación Adobe Acrobat Reader instalada (disponible gratuitamente en Internet). El formulario es editable y grabable, por lo que, hasta el momento de su firma, podrá circular como fichero electrónico, hasta su impresión.
- Las correcciones o anotaciones que se quieran hacer por parte del Subregistro Principal, Servicio Central/General de Protección o Área-Oficina de Seguridad, último escalón de la tramitación, se indicarán en el escrito de remisión que preparen al efecto.
- Este formulario está disponible en la página WEB de la Oficina Nacional de Seguridad (ONS), en la Sede Electrónica del CNI y en aquellas Intranet corporativas en que se haya instalado dicha funcionalidad.

ACLARACIONES AL IMPRESO (ADJUNTAR FOTOCOPIA DNI O PASAPORTE – O INTEGRAR COMO IMAGEN – Pegar con opción sello -)

1. Los datos del interesado serán copia exacta de los que aparecen en el documento de identidad del mismo. Se deberán confrontar con el original de dicha documentación de identificación. Utilizar en este apartado siempre caracteres en MAYÚSCULAS.
2. En caso de **extranjeros, y de españoles que hayan residido en el extranjero**, será obligatorio rellenar los datos adicionales de Pasaporte, por ser el único documento válido internacionalmente. Para el resto de personas, aunque no obligatorio, se estima conveniente el añadirlo, si se posee.
3. Foto tipo carnet (rostro), en color, reciente. Podrá ir integrada como imagen en el propio documento (pegar con opción Sello).
4. Datos de identificación y localización en el empleo actual. Si el interesado pertenece a una Empresa o es autónomo, y ha sido contratado temporalmente por la Administración como Asesor, se marcará en la casilla establecida al efecto.
5. Se darán todos los datos de identificación y contacto precisos para poder contactar con el responsable correspondiente, para solventar cualquier tipo de duda existente sobre esta solicitud.
6. Se indicarán **todos los accesos** a información clasificada que se necesita que posea el interesado tras la nueva solicitud. Aún en el caso de ampliación, se deberán señalar los anteriores que son ampliados. Por ejemplo, si el interesado posea ahora NATO SECRET y necesita disponer también de SECRET UE, en la solicitud se deberán marcar ambos tipos. Los que no figuren se cancelarán, al entenderse que ya no son necesarios.
7. El grado será único para todos los accesos a información clasificada internacional. **El grado nacional podrá diferir del internacional.**
8. Sólo se marcará una casilla. Se deberán tener en cuenta la HPS previa, su fecha de caducidad y los criterios que se marcan en los apartados 5.4.12 y 5.4.13 de la norma NS/02.
9. La Concienciación de Seguridad se define en el apartado 2.3 de la norma NS/02, e incluye la lectura y comprensión de dos documentos: el "Decálogo de la Protección de la Información Clasificada" y las "Leyes que amparan la disciplina del secreto". Las Especialidades exigen una instrucción específica, **impartida por personal con formación y experiencia** en dichas materias. No se admitirán solicitudes de especialidades si no se ha impartido la instrucción correspondiente y así se certifica en este apartado.
10. **No se admitirán declaraciones de tipo general o poco concreto**, que no aportan ninguna información relevante, como "Necesidad de acceder a información clasificada", "Por razón de su cargo", "Ordenado por la superioridad", etc. Especialmente necesaria es la justificación detallada para las solicitudes de grado "SECRETO o equivalente", o las que incluyan Especialidades. Indicar las circunstancias que determinan la **necesidad de conocer**.
11. Toda la documentación que se señale es la que acompañe físicamente a este impreso. Cualquier documento que sea entregado por otra vía (por ejemplo, el DPS enviado por vía telemática a la Sede Electrónica del CNI), **no se marcará**. Hay que tener en cuenta que el expediente de solicitud se va completando durante su tramitación por lo que, aquellos escalones que añadan documentos al mismo, deberán anotarlo en este apartado.
12. Se aportarán en su totalidad los datos solicitados del mando o responsable que acredita la necesidad de habilitación del interesado, pudiendo establecerse contactos directos para solicitar aclaraciones sobre dicho interesado.
13. Las averiguaciones se basarán principalmente en el conocimiento directo del interesado, o a través de sus responsables directos, así como en la revisión de los expedientes personales de que se disponga. En caso de observarse aspectos que pudieran ser relevantes y de estimarse preciso, se podrá contactar confidencial y directamente con la Oficina Nacional de Seguridad (ONS) para informar sobre la existencia de los mismos.
    (*Nota: conforme se marca en el apartado 5.1 de la norma NS/02, por parte de la ONS se podrán solicitar los datos adicionales que se estimen necesarios para determinar el riesgo*)
14. Conforme se indica en el apartado 5.4.5.1 de la norma NS/02, el último escalón de cada cadena jerárquica de protección (Jefe de Seguridad del Servicio de Protección, Subregistro Principal, Área de Seguridad responsable de empresas ,u Oficina de Seguridad), responsable de la remisión del expediente de solicitud a la Oficina Nacional, certificará con el sello oficial y firma, estampados en este cuadro, que todo el proceso se ha efectuado conforme a la normativa y que la documentación que se entrega está revisada y completa. Se identificará con su nombre completo.
15. En **SOLICITUD FINAL** se confirmará lo que se solicita para cada tipo. Si el grado nacional es distinto al internacional es absolutamente necesario marcar aquí lo solicitado, o se concederá con grado único. La selección para grado internacional deberá coincidir con el grado único internacional marcado en la casilla correspondiente.
16. Este código de identificación debe **coincidir exactamente** con el generado al presentar el interesado la Declaración Personal de Seguridad (DPS) por la Sede Electrónica del CNI, y servirá para relacionar ambos documentos. **Si no se ha presentado por dicha vía el DPS, entonces figurará todo con "1".**

DECLARACIÓN PERSONAL DE SEGURIDAD (DPS)

ESTE FORMULARIO DEBE SER CUMPLIMENTADO EXCLUSIVAMENTE POR EL INTERESADO

AUTORIDAD NACIONAL PARA PROTECCIÓN IC

DECLARACIÓN PERSONAL DE SEGURIDAD

DPS-101 (2018)

1.- DATOS DEL INTERESADO

BORRAR FORMULARIO COMPLETO

IDENTIFICACIÓN DEL INTERESADO Y DATOS PARTICULARES DE CONTACTO DIRECTO

Tipo de Documento de Identidad: DNI / NIF		Número de Identidad:	País de Expedición:
NOMBRE:		PRIMER APELLIDO:	SEGUNDO APELLIDO:
Estado civil:	Sexo: M	Número de hijos:	Fecha de nacimiento:
País de nacimiento:		Provincia de nacimiento:	Lugar de nacimiento:
Nacionalidad de origen:		Nacionalidad actual:	Fecha de adquisición de la nacionalidad:
Doble nacionalidad: ☐	Segunda nacionalidad:	Tiene o ha tenido Habilitación Personal de Seguridad: ☐	Fecha Caducidad:
Correo electrónico (E-mail):		Teléfono móvil:	Teléfono fijo:

DATOS DE RESIDENCIA *(Indique aquí su domicilio habitual y no alguno que pudiera estar ahora ocupando de forma eventual, que irá debajo)*

País:		Provincia:	Municipio:
C.P.:	Dirección:	Teléfono:	Fecha inicio de residencia:

RESIDENCIAS DEL INTERESADO DURANTE LOS ÚLTIMOS DIEZ AÑOS *(no son precisas fechas exactas, pueden ser aproximadas)*

Desde:	Hasta:	País	Provincia	Municipio	Dirección

DATOS DE EMPLEO/DESTINO ACTUAL

Cargo o Empleo:	Organismo, Unidad o Empresa:		Fecha de antigüedad:
País:	Provincia:	Municipio:	
C.P.:	Dirección:	Tfno. Oficial:	E-mail oficial:

EMPLEOS/DESTINOS PREVIOS DEL INTERESADO DURANTE LOS ÚLTIMOS DIEZ AÑOS *(fechas aproximadas)*

Desde:	Hasta:	Organismo, Unidad o Empresa	País / Lugar / Dirección	Cargo o Empleo

TITULACIÓN O FORMACIÓN ACADÉMICA *(fechas aproximadas)*

Titulación o formación:		Centro docente:	
País:	Fecha del Título:	Fecha de inicio de estudios:	Fecha de fin de estudios:

OTROS ESTUDIOS REALIZADOS POR EL INTERESADO *(fechas aproximadas)*

Desde:	Hasta:	Centro docente / País	Titulación obtenida

ESTANCIAS EN EL EXTRANJERO - de duración superior a 3 meses, en los últimos diez años - *(fechas aproximadas)*

Desde:	Hasta:	País/Lugar	Motivo detallado

Formulario CNI/DPS 101/2018.01 Pg.1

Firma semiseria interesada o huella electrónica)

RELACIONES O TRABAJO CON GOBIERNOS EXTRANJEROS, O EN ORGANIZACIONES/PROGRAMAS INTERNACIONALES O MULTINACIONALES		
Gobierno, Organismo o Programa	**País**	**Tipo de relación**

RELACIÓN DE CONVIVENCIA DEL INTERESADO RESPECTO A SU PAREJA ACTUAL (identificada en el apartado 2)		
Vínculo actual de convivencia: **Sin pareja actual**	Año de inicio de la relación:	Datos adicionales:

IDENTIFICACIÓN DE PAREJAS ESTABLES ANTERIORES DEL INTERESADO - en los últimos diez años - *(fechas aproximadas)*			
NOMBRE Y APELLIDOS	**NACIONALIDAD**	**PERÍODO DE CONVIVENCIA**	**EXPLICAR GRADO DE RELACIÓN ACTUAL**
		De: a:	
		De: a:	
		De: a:	

2.- DATOS DE SU PAREJA ACTUAL

IDENTIFICACIÓN DE LA PAREJA ACTUAL Y DATOS PARTICULARES DE CONTACTO DIRECTO			
Tipo de Documento de Identidad: **DNI / NIF**		Número de Identidad:	País de Expedición:
NOMBRE:		PRIMER APELLIDO:	SEGUNDO APELLIDO:
Estado civil:	Sexo: **M**	Número de hijos no comunes:	Fecha de nacimiento:
País de nacimiento:		Provincia de nacimiento:	Lugar de nacimiento:
Nacionalidad de origen:		Nacionalidad actual:	Fecha de adquisición de la nacionalidad:
Doble nacionalidad: ☐	Segunda nacionalidad:	Tiene o ha tenido Habilitación Personal de Seguridad ☐	Está aún en vigor: ☐
Correo electrónico (E-mail):		Teléfono móvil:	Teléfono fijo:

DATOS DE RESIDENCIA *(indique aquí el domicilio habitual y no alguno que pudiera estar ahora ocupando de forma eventual, que irá debajo)*			
País:	Provincia:	Municipio:	
C.P.:	Dirección:	Teléfono:	Fecha inicio de residencia:

RESIDENCIAS DE LA PAREJA ACTUAL DURANTE LOS ÚLTIMOS DIEZ AÑOS *(fechas aproximadas)*					
Desde:	**Hasta:**	**País**	**Provincia**	**Municipio**	**Dirección**

DATOS DE EMPLEO/DESTINO DE LA PAREJA ACTUAL			
Cargo o Empleo:	Organismo, Unidad o Empresa:		Fecha de antigüedad:
País:	Provincia:	Municipio:	
C.P.:	Dirección:	Tfno. Oficial:	E-mail oficial:

EMPLEOS/DESTINOS PREVIOS DE LA PAREJA ACTUAL DURANTE LOS ÚLTIMOS DIEZ AÑOS *(fechas aproximadas)*				
Desde:	**Hasta:**	**Organismo, Unidad o Empresa**	**País / Lugar / Dirección**	**Cargo o Empleo**

TITULACIÓN O FORMACIÓN ACADÉMICA DE LA PAREJA ACTUAL *(fechas aproximadas)*			
Titulación o formación:		Centro docente:	
País:	Fecha del Título:	Fecha de inicio de estudios:	Fecha de fin de estudios:

OTROS ESTUDIOS REALIZADOS POR LA PAREJA ACTUAL *(fechas aproximadas)*			
Desde:	**Hasta:**	**Centro docente / País**	**Titulación obtenida**

INDICAR ESTANCIAS EN EL EXTRANJERO DE LA PAREJA ACTUAL - de duración superior a 3 meses, en los últimos diez años - *(fechas apraximadas)*			
Desde:	Hasta:	País/Lugar	Motivo detallado

RELACIONES O TRABAJO DE LA PAREJA ACTUAL CON GOBIERNOS EXTRANJEROS, O CON ORGANIZACIONES/PROGRAMAS INTERNACIONALES		
Gobierno, Organismo o Programa	País	Tipo de relación

3.- DATOS DE LOS PROGENITORES (del interesado y de la pareja actual)

PADRE o PROGENITOR "A" DEL INTERESADO (FALLECIDO: ☐)		(Convive con el interesado en su domicilio habitual: ☐)	
Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:	Nivel de estudios:	
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:	
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:	
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:	
Doble nacionalidad ☐	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

MADRE o PROGENITOR "B" DEL INTERESADO (FALLECIDO: ☐)		(Convive con el interesado en su domicilio habitual: ☐)	
Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:	Nivel de estudios:	
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:	
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:	
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:	
Doble nacionalidad ☐	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

PADRE o PROGENITOR "A" DE LA PAREJA ACTUAL (FALLECIDO: ☐)		(Convive con el interesado en su domicilio habitual: ☐)	
Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:	Nivel de estudios:	
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:	
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:	
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:	
Doble nacionalidad ☐	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

MADRE o PROGENITOR "B" DE LA PAREJA ACTUAL (FALLECIDO: ☐)		(Convive con el interesado en su domicilio habitual: ☐)	
Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:	Nivel de estudios:	
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:	
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:	
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:	
Doble nacionalidad ☐	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

Firma completa interesado o huella electrónica)

4.- DATOS DE PERSONAS CONVIVIENTES (familiares o no, mayores de edad, no incluidos anteriormente, que habitan de forma fija o temporal, o que trabajan como servicio doméstico, en el domicilio habitual del interesado)

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Tipo de Documento de Identidad: **DNI / NIF**	Número de Identidad:	Relación familiar o de convivencia: **Otros**
NOMBRE:	PRIMER APELLIDO:	SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:	Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad de origen:	Nacionalidad actual:
Doble nacionalidad ☐	Profesión, empleo u ocupación:	Estudios:

Formulario ONS/DPS-101/2018.01-Pg.4

Firma completa Interesado o huella electrónica)

5.- DATOS DE REFERENCIAS. Señale dos personas de su entorno, mayores de edad, no incluidas en otros apartados anteriores de esta declaración, que puedan dar referencias sobre usted. (Recuerde informar a estas personas de que se han dado sus datos para referencias)

Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:		Relación con el interesado:
NOMBRE:	PRIMER APELLIDO:		SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:		Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad:	E-mail de contacto:	
Teléfono contacto:	Nivel de estudios:	Profesión, empleo u ocupación:	

Tipo de Documento de Identidad: DNI / NIF	Número de Identidad:		Relación con el interesado:
NOMBRE:	PRIMER APELLIDO:		SEGUNDO APELLIDO:
Fecha de nacimiento:	País de nacimiento:		Provincia de nacimiento:
Lugar de nacimiento:	Nacionalidad:	E-mail de contacto:	
Teléfono contacto:	Nivel de estudios:	Profesión, empleo u ocupación:	

6.- CUESTIONARIO AVANZADO DE SEGURIDAD

INSTRUCCIONES

Lea con atención el siguiente cuestionario. Las situaciones que se le plantean deberán ser analizadas con la mayor precisión y sinceridad. En el caso de que, alguna de las cuestiones planteadas, le afecte de alguna forma, bien a usted o a alguna de las personas que convivan con usted, deberá remitir un escrito por correo electrónico, a la dirección: ons-hps@cni.es , en la forma que se indica a continuación:

a. Un primer mensaje, sin datos personales, con un código alfanumérico de 8 caracteres que usted elija, aportando toda la información, de forma detallada.
b. Un segundo mensaje con su nombre completo, DNI y el código alfanumérico elegido.

La falta de aportación de la información se podría interpretar como una ocultación y puede tener como consecuencia la denegación de la solicitud de HPS. Si ninguna cuestión le afecta, no remita mensaje alguno.

CUESTIONARIO

1. Existencia de algún antecedente o proceso judicial, aunque sea leve y en el pasado.
2. Relación con grupos radicales o terroristas.
3. Relación con personas de países que no sean miembros de OTAN/UE o con gobiernos/servicios de inteligencia extranjeros.
4. Pertenencia a organizaciones en contra del orden constitucional de España o que impidan las libertades y derechos de los demás.
5. Existencia de dificultades económicas o deudas con la Administración Pública.
6. Consumo de alcohol/drogas o existencia de trastornos emocionales.
7. Aspectos susceptibles de ser usados como objeto de presión.
8. Infracción de normas de seguridad o del manejo de sistemas de información y comunicación.
9. Cualquier aspecto no contemplado y que considere que pudiera afectar a la seguridad de la información clasificada.

Firma completa interesado o huella electrónica)

7.- DECLARACIÓN PERSONAL DEL INTERESADO

El interesado:
con documento de identificación número: , declara:

A.- SOBRE LA CUMPLIMENTACIÓN DEL CUESTIONARIO

Quedo enterado de la obligatoriedad de responder a todas las preguntas que sean precisas para la gestión de las HPS solicitadas.

Todo lo manifestado por mí en este cuestionario es la verdad completa y exacta en cuanto sé y conozco, tras haber recabado, de forma razonable, la información solicitada de los afectados.

En particular declaro conocer que cualquier falsedad (por omisión deliberada, engaño o tergiversación de algún dato), será motivo suficiente para la denegación o retirada de la habilitación de seguridad, sin perjuicio de otras responsabilidades de cualquier tipo.

Cualquier modificación posterior de mi situación personal que, por cualquier motivo, pudiere alterar de forma sustancial los datos recogidos en este cuestionario y, por tanto, modificar las condiciones de seguridad actuales, será obligatoria y oportunamente comunicada por los cauces reglamentarios a la Oficina Nacional de Seguridad (ONS).

B.- AUTORIZACIÓN PARA LA INVESTIGACIÓN Y SOLICITUD DE DATOS

Conozco que los datos por mí aportados puedan ser, si ello fuere preciso, investigados por la Autoridad Nacional para la Protección de la Información Clasificada, con los medios y órganos que la legislación vigente pone a su alcance.

Asimismo, presto mi consentimiento expreso para que estos mismos órganos puedan recabar física o electrónicamente cualquier dato o documento que, sobre mi persona, obre en poder de las administraciones públicas, con las restricciones que la normativa de aplicación a los datos y documentos recabados imponga.

C.- LECTURA Y CONOCIMIENTO DEL DECÁLOGO

He leído y comprendido el documento **"Anexo I - Decálogo de la Protección de la Información Clasificada"**, en el entendido de que la lectura de dicho Decálogo no me exime de recibir la posterior Instrucción de Seguridad[1] en materia de protección de la información clasificada, ni del conocimiento de cuantas normas referentes a la protección de la información clasificada del Reino de España, OTAN, Unión Europea, Agencia Espacial Europea, u otras organizaciones de los que España sea parte, sean de aplicación[2].

1 La Instrucción de Seguridad se le deberá impartir una vez concedida la Habilitación Personal de Seguridad, por el responsable de la protección de la información clasificada, antes de que pueda tener acceso a la información clasificada. Si no la recibe, deberá reclamarla.
2 La Instrucción de Seguridad, obligatoria para cualquier tipo de HPS, deberá complementarse con otros documentos dependiendo de la HPS que se trate (p. e. Decisión 2013/488/UE de 23.09.2013 del Consejo y Decisión 2015/444/EU, EURATOM de 13.03.2015 de la Comisión, para HPS de la Unión Europea).

D.- COMPROMISO DE SEGURIDAD

Me comprometo a mantener la debida reserva, y a no revelar ningún dato, sobre la información clasificada a la que pudiera tener o haber tenido acceso con motivo del cumplimiento de mis obligaciones o por otro motivo cualquiera, siendo consciente de que dicho deber de reserva permanecerá vigente de forma permanente.

Asimismo declaro que conozco perfectamente las responsabilidades penales y disciplinarias en que pudiera incurrir por la divulgación no autorizada de esta clase de informaciones, bien sea voluntariamente o por negligencia, por acción u omisión, con arreglo a las disposiciones legales y administrativas vigentes, habiendo leído y comprendido el documento **"Anexo II - Leyes que amparan la disciplina del secreto"**.

Y para que conste y surta los debidos efectos ante la Autoridad Nacional, firmo la presente declaración:

En , a de **diciembre** de

ACTIVAR FIRMA DIGITAL

(Firma del interesado)

CERTIFICACIÓN TELEMÁTICA

Formulario ONS/DPS-101/2018.01-Pg.6

Firma completa interesado o huella electrónica)

Anexo I
Decálogo de la Protección de la Información Clasificada

(Este decálogo servirá de referencia para la concienciación de seguridad sobre protección de Información Clasificada del solicitante de una HPS)

1. La información clasificada es aquella información o material sobre el que se ha decidido que requiere un grado de protección para evitar su revelación o acceso no autorizado, en base al daño o perjuicio que su divulgación puede causar a la seguridad e intereses de España o sus aliados. Dicho grado de clasificación irá marcado sobre la propia información o material.

2. Los grados de clasificación de la información clasificada, de mayor a menor, son:

   - SECRETO (son equivalentes COSMIC TOP SECRET, EU TOP SECRET, etc.).
   - RESERVADO (equivalentes NATO SECRET, SECRET UE, etc.).
   - CONFIDENCIAL (equivalentes NATO CONFIDENTIAL, CONFIDENTIEL UE, etc.).
   - DIFUSIÓN LIMITADA (equivalentes NATO RESTRICTED, RESTREINT UE, etc.).

3. Toda persona que tenga conocimiento de cualquier información clasificada, voluntaria o involuntariamente, deberá mantener la oportuna reserva sobre la misma. Dicho deber de reserva no expira mientras la información afectada no sea desclasificada.

4. La divulgación no autorizada de información clasificada tendrá la consideración de delito o falta, y llevará pareja unas responsabilidades penales o disciplinarias para la persona que la cometa, conforme al código penal o disciplinario que le afecte.

5. El acceso por un individuo a información clasificada con grado de CONFIDENCIAL o superior, requiere:

   - Tener concedida una Habilitación Personal de Seguridad del grado adecuado.
   - Tener la "necesidad de conocer".
   - Haber recibido la instrucción de seguridad preceptiva, antes de dicho acceso.

6. La información CONFIDENCIAL o superior debe circular por los Servicios de Protección de Información Clasificada u Órganos de Control, que son los responsables de su registro y custodia, siendo los únicos que pueden autorizar su transmisión.

7. La información DIFUSIÓN LIMITADA sólo puede ser manejada por individuos que han sido instruidos en materia de protección de la información clasificada.

8. La clasificación de información es un acto formal, y no puede ser realizada por los usuarios. Sólo pueden proponerla, y elevarla para aprobación, según el procedimiento por el que se regula.

9. La información clasificada sólo podrá ser manejada en zonas específicamente autorizadas para dicho fin. Se prohíbe su manejo fuera de las mismas, salvo en los casos de transporte autorizado, o autorización expresa.

10. En todas las instalaciones y órganos en que se maneje información clasificada existirá la figura del Responsable de Seguridad, que podrá ser el Jefe de Seguridad de un Servicio de Protección u Órgano de Control, y que se responsabilizará del correcto manejo de la información clasificada en su ámbito de responsabilidad.

Firma completa interesado o huella electrónica)

Anexo II
Leyes que amparan la disciplina del secreto

CÓDIGO PENAL (Ley Orgánica 10/1995, de 23 de noviembre, modificada por L.O. 1/2015, de 30 de marzo)

Artículo 277. - "Será castigado con las penas de prisión de seis meses a dos años y multa de seis a veinticuatro meses, el que intencionadamente haya divulgado la invención objeto de una solicitud de patente secreta, en contravención con lo dispuesto en la legislación de patentes, siempre que ello sea en perjuicio de la defensa nacional".

Artículo 417

1. - "La Autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados, incurrirá en la pena de multa de doce a dieciocho meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años. Si de la revelación a que se refiere el párrafo anterior resultare grave daño para la causa pública o para tercero, la pena será de prisión de uno a tres años, e inhabilitación especial para el empleo o cargo público por tiempo de tres a cinco años.

2. - Si se tratara de secretos de un particular, las penas serán las de prisión de dos a cuatro años, multa de doce a dieciocho meses, y suspensión de empleo o cargo público por tiempo de uno a tres años".

Artículo 418. - "El particular que aprovechare para sí o para un tercero el secreto o la información privilegiada que obtuviere de un funcionario público o autoridad, será castigado con multa del tanto al triplo del beneficio obtenido o facilitado y la pérdida de la posibilidad de obtener subvenciones o ayudas públicas y del derecho a gozar de los beneficios o incentivos fiscales o de la Seguridad Social durante el período de uno a tres años. Si resultara grave daño para la causa pública o para tercero, la pena será de prisión de uno a seis años y la pérdida de la posibilidad de obtener subvenciones o ayudas públicas y del derecho a gozar de los beneficios o incentivos fiscales o de la Seguridad Social durante el período de seis a diez años".

Artículo 442. - "La autoridad o funcionario público que haga uso de un secreto del que tenga conocimiento por razón de su oficio o cargo, o de una información privilegiada, con ánimo de obtener un beneficio económico para sí o para un tercero, incurrirá en las penas de multa del tanto al triplo del beneficio perseguido, obtenido o facilitado e inhabilitación especial para empleo o cargo público y para el ejercicio del derecho de sufragio pasivo por tiempo de dos a cuatro años. Si obtuviere el beneficio perseguido se impondrán las penas de prisión de uno a tres años, multa del tanto al séxtuplo del beneficio perseguido, obtenido o facilitado e inhabilitación especial para empleo o cargo público y para el ejercicio del derecho de sufragio pasivo por tiempo de cuatro a seis años.

Si resultara grave daño para la causa pública o para tercero, la pena será de prisión de uno a seis años, e inhabilitación especial para empleo o cargo público y para el ejercicio del derecho de sufragio pasivo por tiempo de nueve a doce años. A los efectos de este artículo se entiende por información privilegiada toda información de carácter concreto que se tenga exclusivamente por razón del oficio o cargo público y que no haya sido notificada, publicada o divulgada".

Artículo 584. - "El español que, con el propósito de favorecer a una potencia extranjera, asociación u organización internacional, se procure, falsee, inutilice o revele información clasificada como reservada o secreta, susceptible de perjudicar la seguridad nacional o la defensa nacional, será castigado, como traidor, con la pena de prisión de seis a doce años".

Artículo 598. - "El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con la pena de prisión de uno a cuatro años".

Artículo 599. - "La pena establecida en el artículo anterior se aplicará en su mitad superior cuando concurra alguna de las circunstancias siguientes:

1º. Que el sujeto activo sea depositario o conocedor del secreto o información por razón de su cargo o destino.

2º. Que la revelación consistiera en dar publicidad al secreto o información en algún medio de comunicación social o de forma que asegure su difusión".

Artículo 600

1- "El que sin autorización expresa reprodujere planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido y cuyo conocimiento esté protegido y reservado por una información legalmente calificada como reservada o secreta, será castigado con la pena de prisión de seis meses a tres años.

2- Con la misma pena será castigado el que tenga en su poder objetos o información legalmente calificada como reservada o secreta, relativos a la seguridad o a la defensa nacional, sin cumplir las disposiciones establecidas en la legislación vigente".

Artículo 601. - "El que por razón de su cargo, comisión o servicio, tenga en su poder o conozca oficialmente objetos o información legalmente calificada como reservada o secreta o de interés militar, relativos a la seguridad nacional o la defensa nacional, y por imprudencia grave dé lugar a que sean conocidos por persona no autorizada o divulgados, publicados o inutilizados, será castigado con la pena de prisión de seis meses a un año".

Artículo 602. - "El que descubriere, violare, sustrajere o utilizare información legalmente calificada como reservada o secreta relacionada con la energía nuclear, será castigado con la pena de prisión de seis meses a tres años, salvo que el hecho tenga señalada pena más grave en otra Ley."

Artículo 603. - "El que destruyere, inutilizare, falseare o abriere sin autorización la correspondencia o documentación legalmente clasificada como reservada o secreta, relacionadas con la defensa nacional y que tenga en su poder por razones de su cargo o destino, será castigado con la pena de prisión de dos a cinco años e inhabilitación especial de empleo o cargo público por tiempo de tres a seis años".

CÓDIGO PENAL MILITAR (Ley Orgánica 14/2015, de 14 de octubre)

Artículo 25. - "El extranjero que, en situación de conflicto armado, se procurare, difundiera, falseare o inutilizare información clasificada como reservada o secreta o de interés militar susceptible de perjudicar a la seguridad o a la defensa nacionales, o de los medios técnicos o sistemas empleados por las Fuerzas armadas o la Guardia Civil o las industrias de interés militar, o la revelase a potencia extranjera, asociación u organismo internacional, será castigado, como espía, a la pena de diez a veinte años de prisión.

El militar español que cometiere este delito será considerado autor de un delito de traición militar y castigado con la pena prevista en el artículo anterior". (*Nota: el citado artículo 24 del Código Penal Militar indica pena de prisión de quince a veinticinco años.*)

Artículo 26. - "El militar que cometiere cualquiera de los delitos previstos en los artículos 277 ó 598 a 603 del Código Penal será castigado con la pena establecida en el mismo incrementada en un quinto de su límite máximo. En situación de conflicto armado o estado de sitio se impondrá la pena superior en uno o dos grados".

Formulario ONS/DPS-101/2018.01-Pg.8

(Firma completa interesado o huella electrónica)

ANEXO B. Focus Group

"El *Focus Group* (grupo focal) es una técnica que centra su atención en la pluralidad de respuestas obtenidas de un grupo de personas, y es definida como una técnica de la investigación cualitativa cuyo objetivo es la obtención de datos por medio de la percepción, los sentimientos, las actitudes y opiniones de un grupo de personas." [35]

El método de trabajo consiste en reunir a un grupo de entre 6 a 12 expertos en el producto a analizar, además de un moderador. Este último será el encargado de realizar las preguntas necesarias y evitar que en el transcurso de la reunión se desvíe el tema a tratar. Una vez planteado el tema, el grupo dialoga sobre el asunto en cuestión, en este caso la mejora del Mando y Control de una UDAA. Se exponen una serie de cuestiones al grupo, a las que cada miembro ofrece su opinión. De esta primera ronda de preguntas, surgen otras nuevas, que se resolverán mediante la interacción de todos los miembros del grupo. Una de las claves del éxito en el método, es la libertad de expresión de cada uno de los componentes del grupo a la hora de ofrecer su opinión personal, y para ello, el moderador ha de lograr la creación de un clima de confianza entre los asistentes.

Para la realización del *Focus Group*, se han llevado a cabo los siguientes pasos [18]:

- Plantear o definir los objetivos de la investigación. Lo primero de todo fue detectar el objeto de estudio, para posteriormente determinar los objetivos que se querían desarrollar en esta metodología.
- Elaboración de una guía (se encuentra en la página siguiente). Con ella se estructuró como fue la reunión desde su comienzo hasta su finalización. Además, aparece un guion ordenado de lo general a lo particular, en el que se trata el tema a discutir.
- Seleccionar a los participantes de la reunión. Por un lado, el moderador fue el redactor de este Trabajo de Fin de Grado, el presente alumno. Por otro lado, los participantes seleccionados fueron especialistas en ambos sistemas de Mando de Control, así como los operadores del CIO y del CPL de una UDAA.
- Selección del lugar. El lugar seleccionado fue la sala de juntas del Grupo I/73 del RAAA 73, situada en el edificio de mandos, y en horario laboral. De esta manera, se aseguró la posibilidad de asistencia de todos los especialistas necesarios a la reunión.
- Realización del informe final. Una vez finalizada la reunión, se analizó la información obtenida, para así redactar un informe final con la finalidad de analizar las conclusiones en su conjunto.

GUIÓN FOCUS GROUP

Sistema de información para el Mando y Control del Ejército de Tierra (SIMACET) y sistema de Mando y Control del Ejército del Aire (SC2N-EA)

i. Introducción de los participantes.

Antes de comenzar la reunión, cada participante realizará una breve presentación incluyendo empleo, unidades en las que ha estado, así como funciones que ha desempeñado, y su cometido en el puesto de mando de una UDAA. A continuación, se expondrá el motivo de la reunión, una breve introducción de lo que ya se conoce hasta el momento, y los objetivos a alcanzar.

ii. Explicación del método.

Explicación sobre la finalidad del método, así como los diferentes puntos a tratar y los objetivos a lograr en cada uno de ellos.

iii. Guion.

Con respecto a ambos sistemas de Mando y Control:

1. Valoración personal del Mando y Control del ET de una UDAA.
2. Limitaciones a la hora de llevar a cabo el Mando y Control de una UDAA en el PC UDAA.
3. Explicación de los diferentes puestos del PC UDAA (jefe UDAA, S-1, S-2, S-3, S-4), para discutir a continuación cómo se podría aumentar la eficiencia de cada uno.
4. Discusión sobre las labores de los dos operadores del CIO, y si fuera conveniente que hubiera un único operador.
5. Valoración personal del Mando y Control del ET desde el terminal con acceso a la red del SC2N-EA en el PC UDAA.
6. Discusión sobre si se puede conectar la red del SC2N-EA al nodo SIMACET.
7. Reflexión sobre qué aportaría esta unión.

Con respecto al software y hardware de los terminales desde los que se lleva a cabo el Mando y Control:

1. Limitaciones existentes (debidas a los modelos de software y hardware).
2. Propuestas de mejora.

Con respecto a las aplicaciones de ambos sistemas de Mando y Control.

1. ANTARES de SIMACET.
2. ICC-NATO de SC2N-EA.
3. JCHAT de SIMACET.
4. JCHAT de SC2N-EA.
5. Outlook de SIMACET.
6. Outlook de SC2N-EA.
7. XoMail de SIMACET.
8. XoMail de SC2N-EA.

9. Sharepoint de SIMACET.
10. Sharepoint de SC2N-EA.
11. JEMM de SIMACET.
12. JEMM de SC2N-EA.

iv. Resumen de la reunión y agradecimientos

Se informa y comentan los puntos más importantes de la reunión, así como las ideas clave que se han extraído. Por último, se agradece al personal la asistencia y ayuda prestada. Se realiza un informe final de la reunión.

ANEXO C. Brainstorming

Es un método de trabajo en grupo que se utiliza para facilitar la búsqueda de ideas para resolver problemas determinados. Para ello se elige a un grupo de especialistas en el tema a tratar, hasta conseguir un total de entre 3 y 9 participantes. Además, debe de haber presente un moderador, el cual será el presente alumno redactor de este TFG. [42]

Para la realización del *Brainstorming*, se han llevado a cabo los mismos pasos redactados en el *Focus Group*. La única diferencia radica en que éste es para crear un nuevo sistema de mando y control, y el *Focus Group* para buscar limitaciones y fortalezas de los actuales. El guion que se siguió en esta metodología se encuentra a continuación de esta pequeña introducción al método.

La reunión comenzó con una explicación exacta del problema a desarrollar. Una vez todos los miembros tenían conocimiento de todos los puntos a tratar, dio comienzo la primera lluvia de ideas, las cuales se anotaron. A continuación, se realizó una discusión sobre la vialidad de las ideas planteadas, para así dar paso a una segunda lluvia de ideas. Finalmente, con todas las ideas finales recogidas, se realizó un informe final con todas las conclusiones.

GUIÓN BRAINSTORMING

SISTEMA DE INFORMACIÓN PARA EL MANDO Y CONTROL TIERRA AIRE (SIMACTA)

i. Introducción de los participantes.

Antes de comenzar la reunión, cada participante realizará una breve presentación incluyendo empleo, unidades en las que ha estado, así como funciones que ha desempeñado, y su función en el puesto de mando de una UDAA. A continuación, se expondrá el motivo de la reunión, una breve introducción de lo que ya se conoce hasta el momento, y los objetivos a alcanzar.

ii. Explicación del método.

Explicación de en qué consiste el método, así como los diferentes puntos a tratar y los objetivos a lograr en cada uno de ellos.

iii. Guion.

Para llevar a cabo el mando y control de una UDAA:

1. ¿Qué software requerirían los terminales?
2. ¿Qué hardware considera necesarios?
3. ¿Qué aplicaciones considera imprescindibles y por qué?
4. ¿Qué usuarios debería tener el sistema para ejercer el Mando y Control?

iv. Resumen de la reunión y agradecimientos

Se informa y comentan los puntos más importantes de la reunión, así como las ideas clave que se han extraído. Por último, se agradece al personal la asistencia y ayuda prestada.

ANEXO D. Preguntas Encuesta

Mando y Control de una UDAA del Ejército de Tierra

1. ¿Cuál es su empleo?

_____

2. ¿En qué unidad está actualmente destinado?

_____

3. ¿Cuál es su puesto a la hora de llevar a cabo el mando y control de una UDAA?

_____

Adhesión de la red del SC2N-EA al nodo SIMACET

En esta sección se hace referencia a la unión de ambos sistemas de mando y control (SIMACET ySC2N-EA)

4. ¿Considera un problema que llegue a terminales diferentes la información de mando y control de la red del SC2N-EA y del SIMACET?

Marca solo un óvalo.

	1	2	3	4	5	
En absoluto	◯	◯	◯	◯	◯	Por supuesto

5. ¿Considera que la red del SC2N-EA debe adherirse al SIMACET para mejorar el mando y control del ET de la UDAA?

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

6. ¿Considera que sería conveniente que aparte de S-2, otros usuarios pudieran tener visible la información del espacio aéreo, proveniente de la red del SC2N-EA, en sus terminales?

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

7. ¿Qué usuarios sería conveniente que tuvieran visión de la información de la red del SC2N-EA en sus terminales?

Selecciona todos los que correspondan.

- [ ] Jefe de operaciones
- [ ] S-1
- [ ] S-2
- [ ] S-3
- [ ] S-4

8. ¿Cómo de apto considera ANTARES para reunir la información del campo de batalla relativa al ET y la del espacio aéreo?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

9. ¿Sustituiría ANTARES por otra aplicación geográfica que pudiera reunir toda la información del campo de batalla relativa al ET y del espacio aéreo del EA?

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

10. De las siguientes aplicaciones geográficas, ¿por cuál sustituiría ANTARES para visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA?

Marca solo un óvalo.

- ◯ Carta Digital
- ◯ TALOS Táctico

11. A la hora de visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA, ¿cómo calificaría Carta Digital como sustituto de ANTARES?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

12. A la hora de visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA, ¿cómo calificaría TALOS Táctico como sustituto de ANTARES?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

Hardware y Software de los terminales

En esta sección, se va a realizar una valoración de los actuales hardware y software que presentan los terminales utilizados en el SIMACET y el SC2N-EA. Respondan únicamente a las preguntas que le conciernen según el sistema de mando y control que operen.

13. ¿Cómo calificaría el procesador que incorporan los terminales?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

14. ¿Cómo calificaría la memoria RAM que incorporan los terminales?

Marca solo un óvalo.

	1	2	3	4	5	
Pésima	◯	◯	◯	◯	◯	Excelente

15. ¿Cómo calificaría la memoria interna que incorporan los terminales?

Marca solo un óvalo.

	1	2	3	4	5	
Pésima	◯	◯	◯	◯	◯	Excelente

16. Con respecto al sistema operativo, ¿cómo calificaría el software instalado en los terminales?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

17. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría ANTARES?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

18. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría JCHAT?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

19. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría Outlook?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

20. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría XoMail?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

21. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría SHAREPOINT?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

22. Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría JEMM?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

23. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría ICC-NATO?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

24. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría JCHAT?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

25. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría Outlook?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

26. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría XoMail?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

27. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría SHAREPOINT?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

28. Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría JEMM?

Marca solo un óvalo.

	1	2	3	4	5	
Pésimo	◯	◯	◯	◯	◯	Excelente

Nuevo SIMACTA (Sistema de Información para el Mando y Control Tierra Aire)

En esta sección, se hace referencia a la posibilidad de crear un nuevo sistema mando y control.

29. ¿Considera beneficiosa la creación de un nuevo sistema de mando y control que ya tenga integrados ambos C-2?

Marca solo un óvalo.

- Sí
- No
- Tal vez

30. En relación con la posibilidad de unión de JCHAT y Outlook, ¿Considera necesaria la incorporación de una aplicación que integre una opción para la mensajería informal de JCHAT, y otra opción para la mensajería formal de Outlook?

Marca solo un óvalo.

- Sí
- No
- Tal vez

31. ¿Considera necesario añadir una aplicación de mensajería común al ET y al EA?

Marca solo un óvalo.

- Sí
- No
- Tal vez

32. ¿Considera necesario crear una nueva aplicación geográfica, con la que visualizar y modificar la información relativa al espacio de batalla del ET y visualizar la del espacio aéreo del EA de forma eficiente, diferente a las existentes?

Marca solo un óvalo.

- ◯ Sí
- ◯ No
- ◯ Tal vez

33. ¿Consideraría útil que los vehículos y sistemas de armas llevaran incluido un sensor GPS que los posicionara automáticamente en la aplicación geográfica?

Marca solo un óvalo.

	1	2	3	4	5	
Nada útil	◯	◯	◯	◯	◯	Muy útil

34. De los siguientes aspectos, ¿Cuáles considera imprescindibles a la hora de desarrollar una nueva aplicación geográfica común a ambos sistemas de mando y control?

Selecciona todos los que correspondan.

- ☐ Capacidad de posicionar las unidades del ET.
- ☐ Capacidad de recibir señal GPS de cada vehículo para su posicionamiento automático en el terreno.
- ☐ Capacidad para el tratamiento geográfico (SIG).Capacidad de
- ☐ visualización en 3D del terreno.
- ☐ Capacidad de carga del ACO.
- ☐ Capacidad de carga del ATO.
- ☐ Capacidad de visualizar únicamente la capa relativa al ET.
- ☐ Capacidad de visualizar únicamente la capa relativa al EA.
- ☐ Capacidad de visualizar ambas capas a la vez, tanto al del ET como la del EA.
- ☐ Capacidad de dar órdenes de fuego, únicamente en el caso en el que el ARS sea incapaz.
- ☐ Capacidad de intercambio de mensajería.
- ☐ Capacidad de recepción de la información del radar RAC-3D del espacio aéreo.

35. ¿Considera necesario añadir alguna aplicación extra a las ya mencionadas?

Marca solo un óvalo.

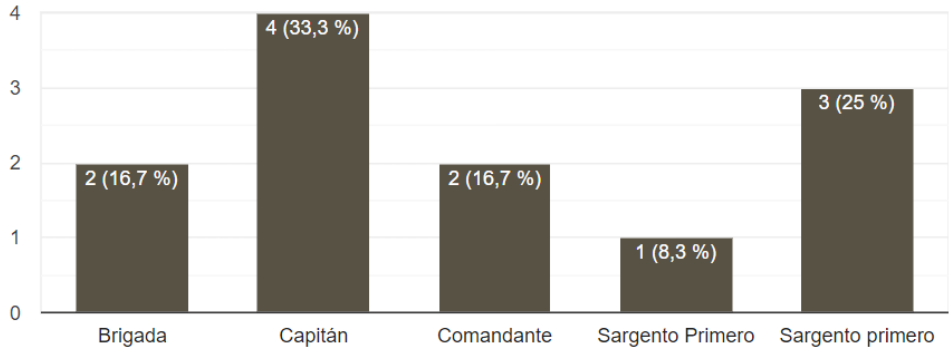
- Sí
- No

36. En el caso de que en la pregunta anterior haya marcado ""Sí"", ¿Qué aplicación sería y qué funciones desempeñaría?

ANEXO E. Respuestas Encuesta

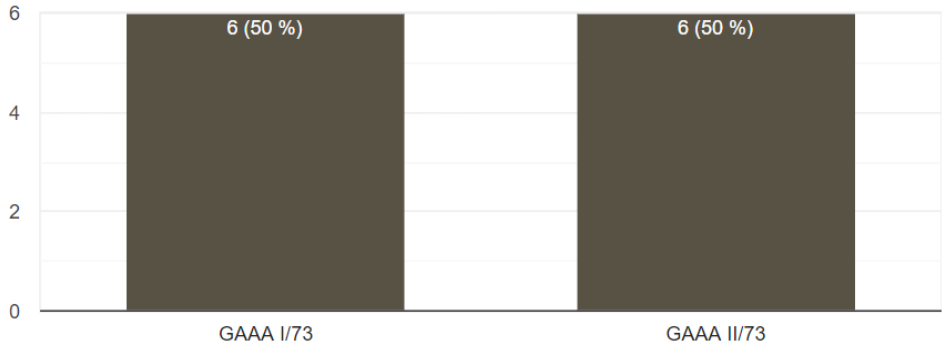
¿Cuál es su empleo?

12 respuestas



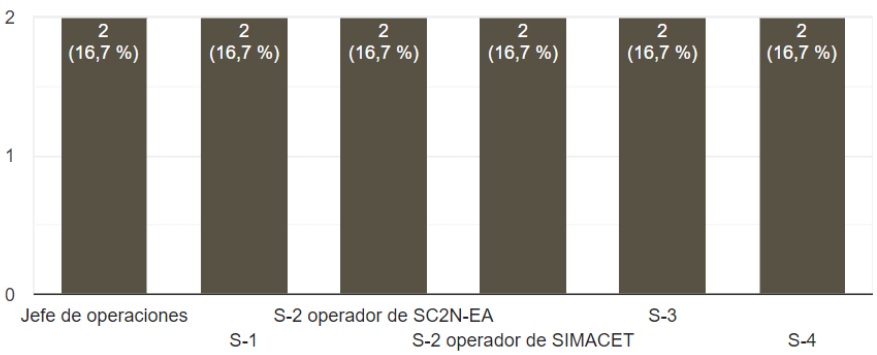
¿En qué unidad está actualmente destinado?

12 respuestas



¿Cuál es su puesto a la hora de llevar a cabo el mando y control de una UDAA?

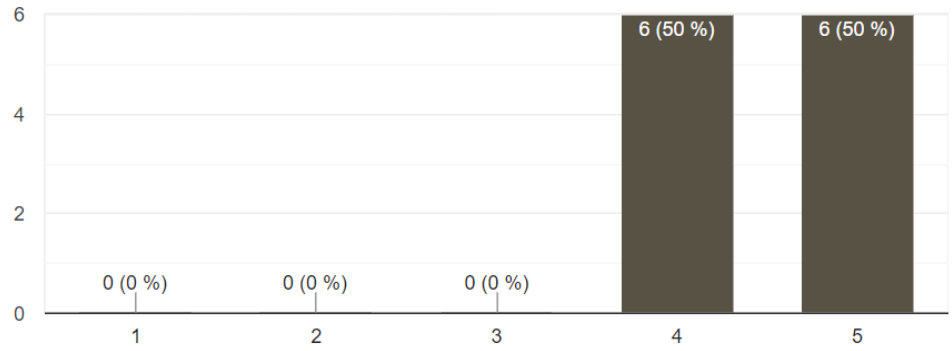
12 respuestas



Adhesión de la red del SC2N-EA al nodo SIMACET

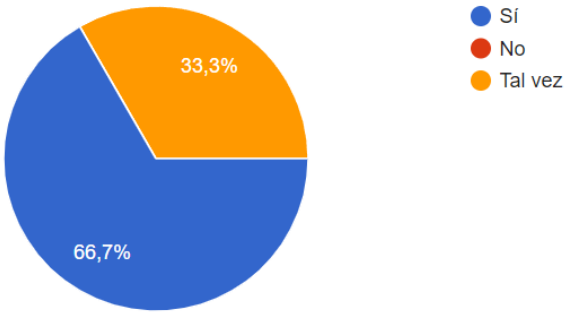
¿Considera un problema que llegue a terminales diferentes la información de mando y control de la red del SC2N-EA y del SIMACET?

12 respuestas



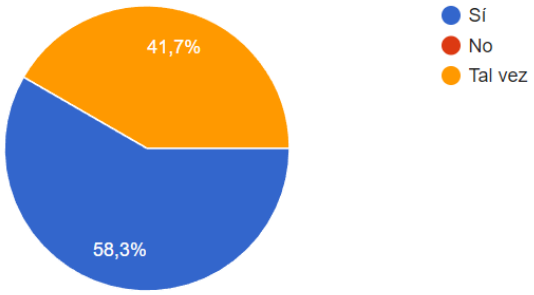
¿Considera que la red del SC2N-EA debe adherirse al SIMACET para mejorar el mando y control del ET de la UDAA?

12 respuestas



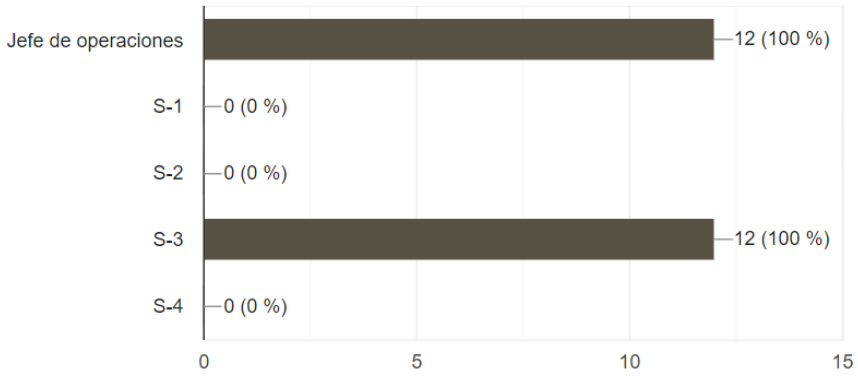
¿Considera que sería conveniente que aparte de S-2, otros usuarios pudieran tener visible la información del espacio aéreo, proveniente de la red del SC2N-EA, en sus terminales?

12 respuestas



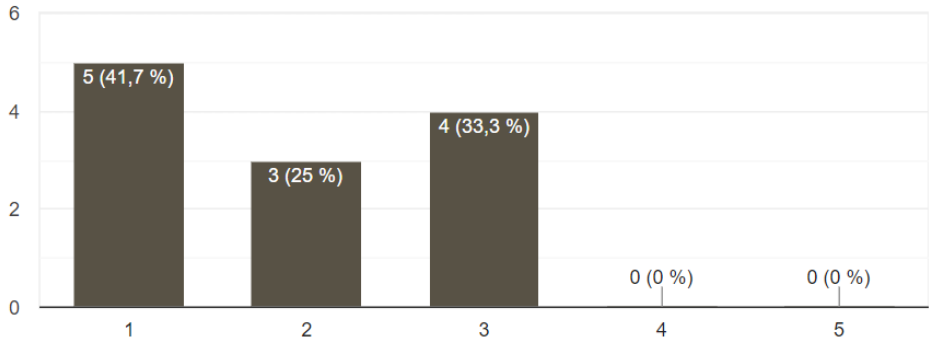
¿Qué usuarios sería conveniente que tuvieran visión de la información de la red del SC2N-EA en sus terminales?

12 respuestas



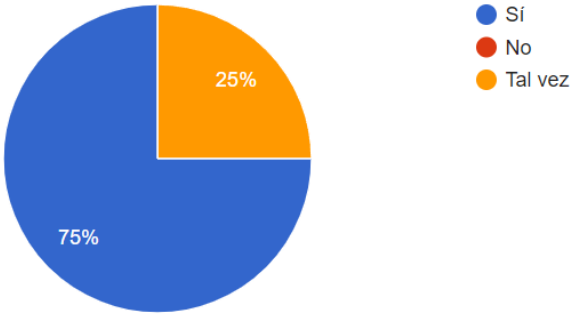
¿Cómo de apto considera ANTARES para reunir la información del campo de batalla relativa al ET y la del espacio aéreo?

12 respuestas



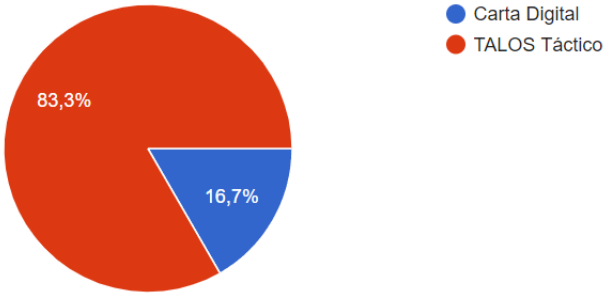
¿Sustituiría ANTARES por otra aplicación geográfica que pudiera reunir toda la información del campo de batalla relativa al ET y del espacio aéreo del EA?

12 respuestas



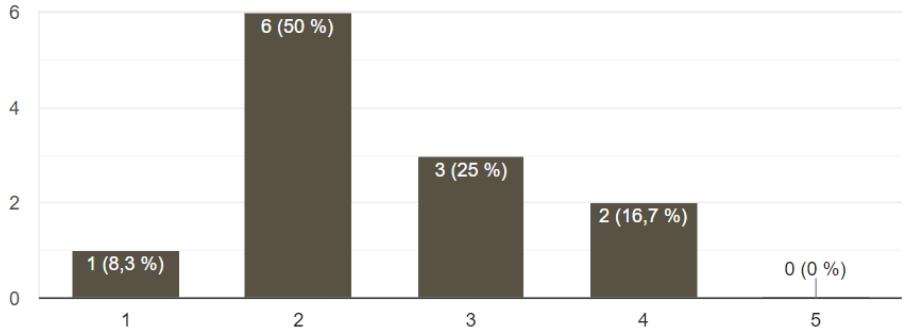
De los siguientes aplicaciones geográficas, ¿por cuál sustituiría ANTARES para visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA?

12 respuestas



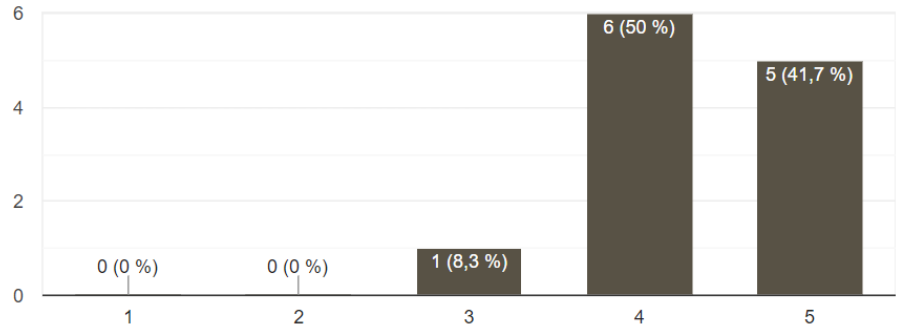
A la hora de visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA, ¿cómo calificaría Carta Digital como sustituto de ANTARES?

12 respuestas



A la hora de visualizar y modificar toda la información del campo de batalla relativa al ET y visualizar la del espacio aéreo del EA, ¿cómo calificaría TALOS Táctico como sustituto de ANTARES?

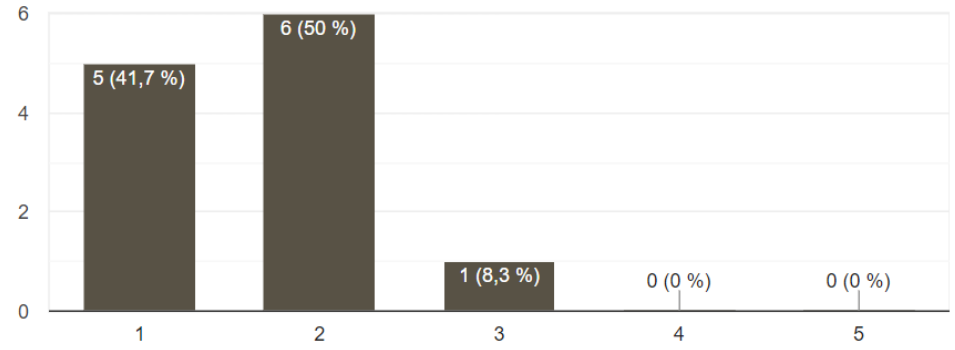
12 respuestas



Hardware y Software de los terminales

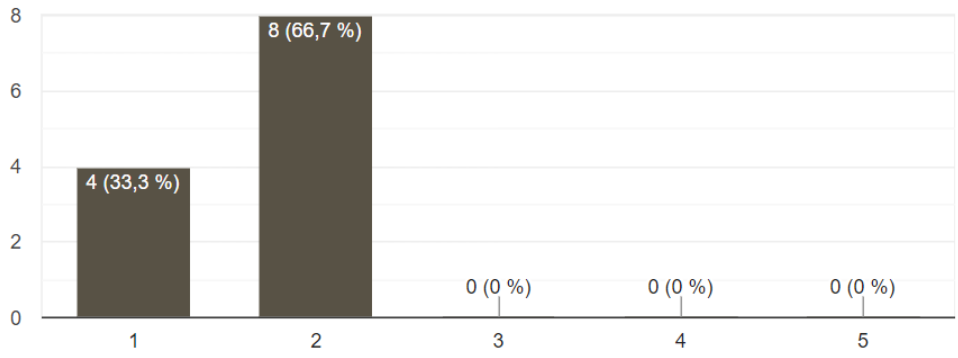
¿Cómo calificaría el procesador que incorporan los terminales?

12 respuestas



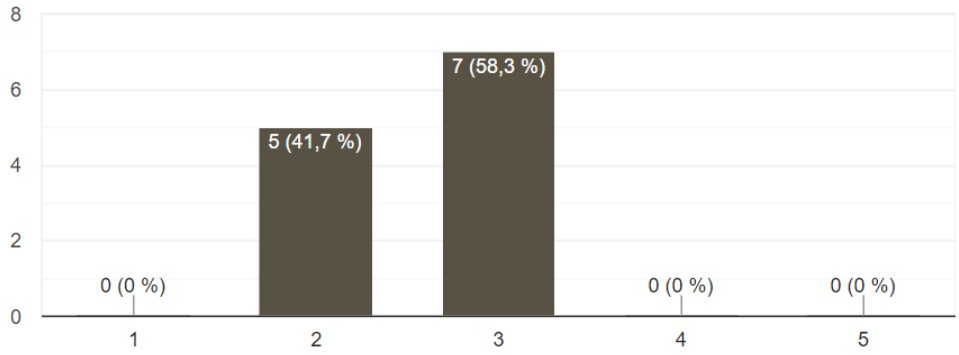
¿Cómo calificaría la memoria RAM que incorporan los terminales?

12 respuestas



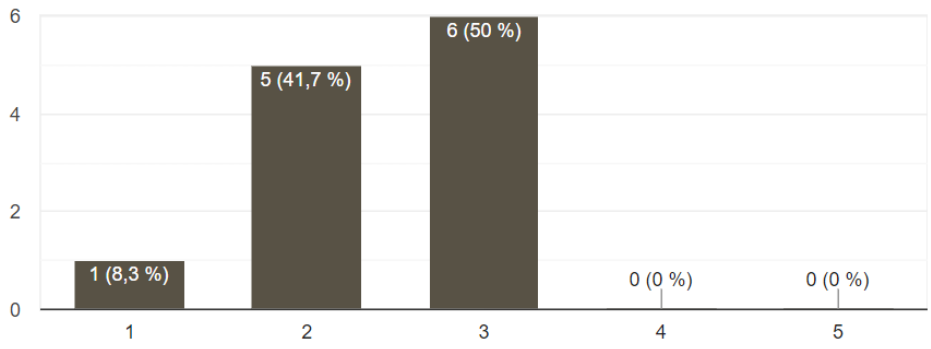
¿Cómo calificaría la memoria interna que incorporan los terminales?

12 respuestas



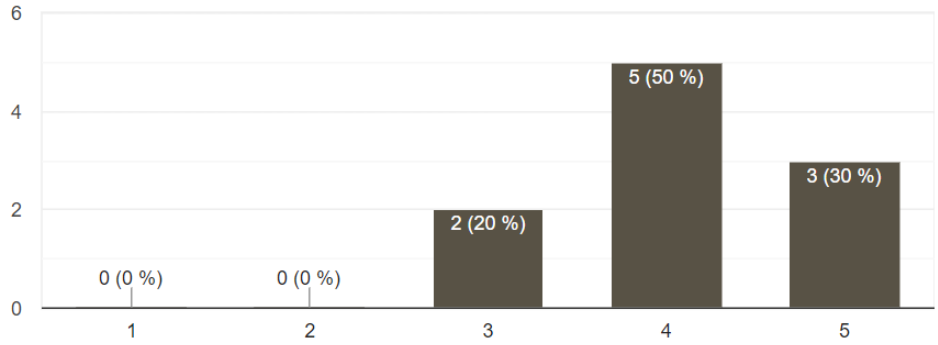
Con respecto al sistema operativo, ¿cómo calificaría el software instalado en los terminales?

12 respuestas



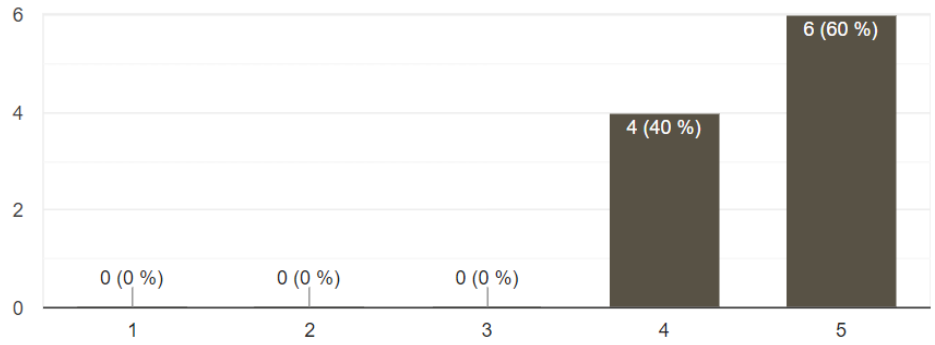
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría ANTARES?

10 respuestas



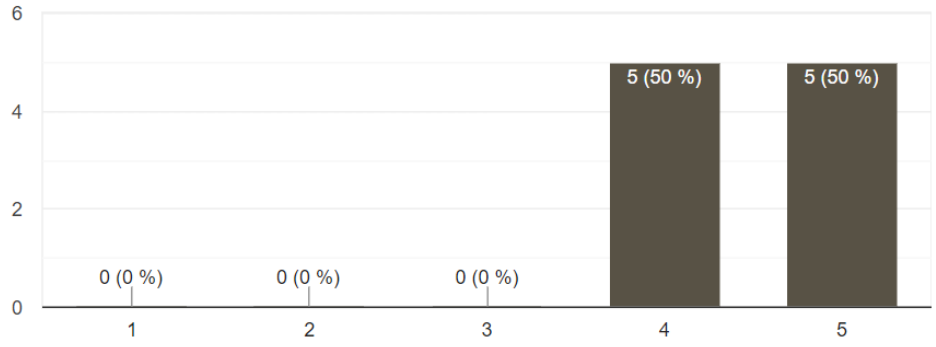
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría JCHAT?

10 respuestas



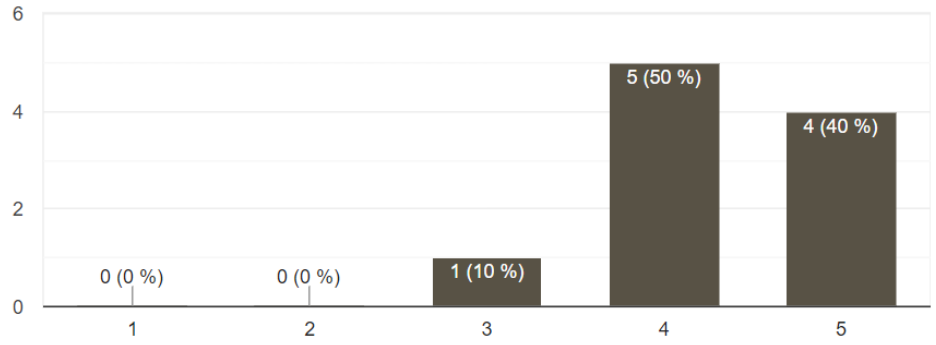
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría Outlook?

10 respuestas



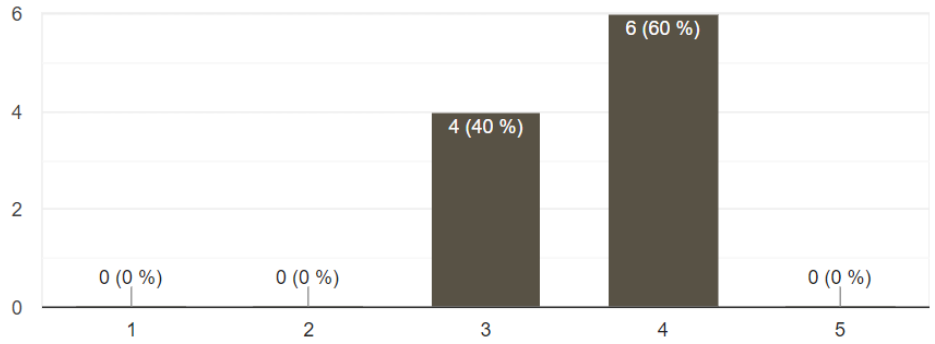
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría XoMail?

10 respuestas



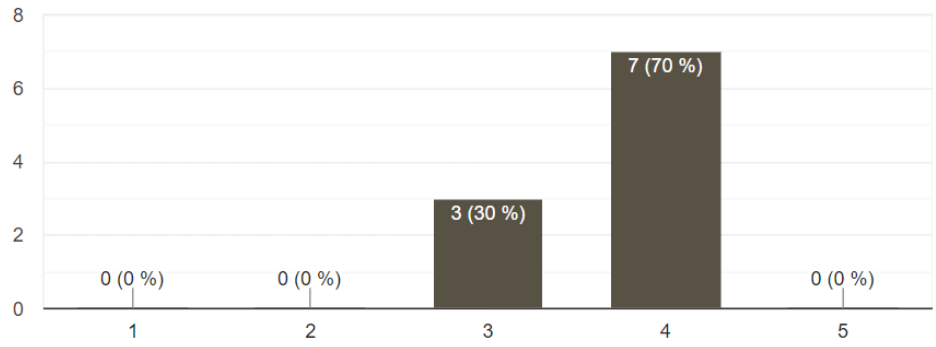
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría SHAREPOINT?

10 respuestas



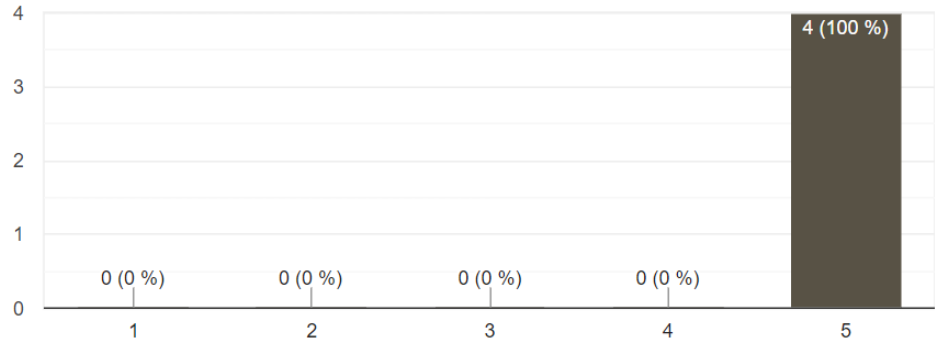
Con respecto a las aplicaciones existentes en el SIMACET, ¿cómo calificaría JEMM?

10 respuestas



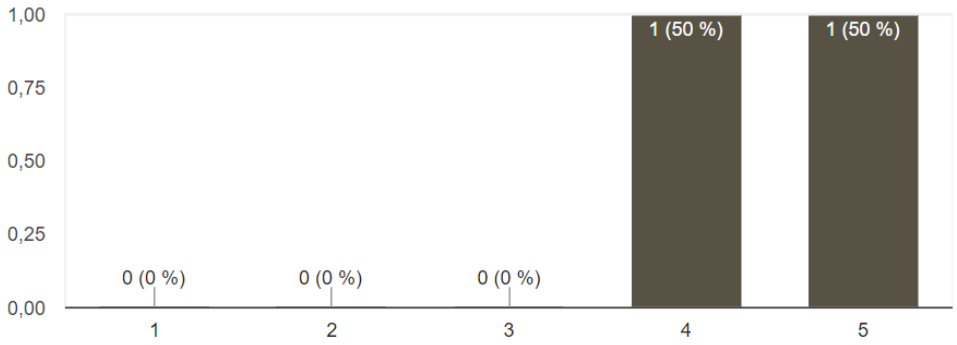
Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría ICC-NATO?

4 respuestas



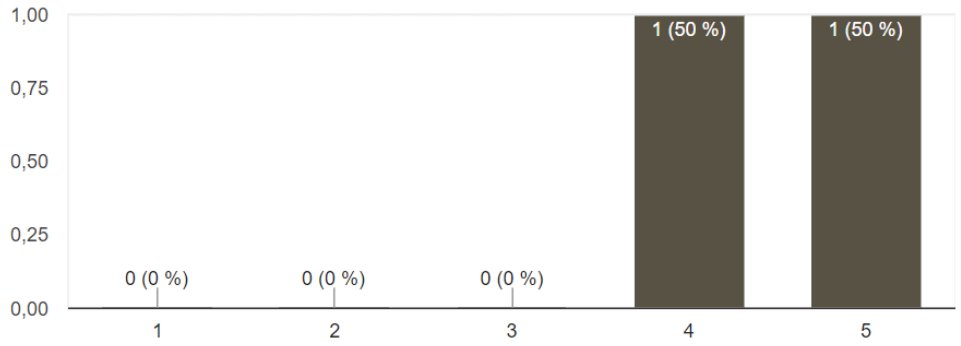
Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría JCHAT?

2 respuestas



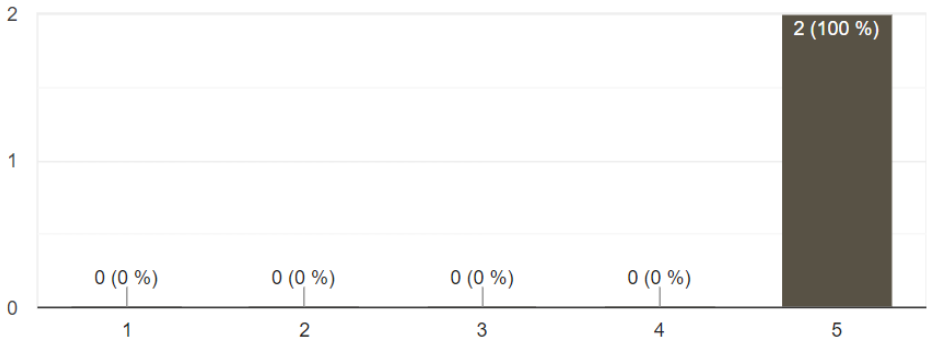
Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría Outlook?

2 respuestas



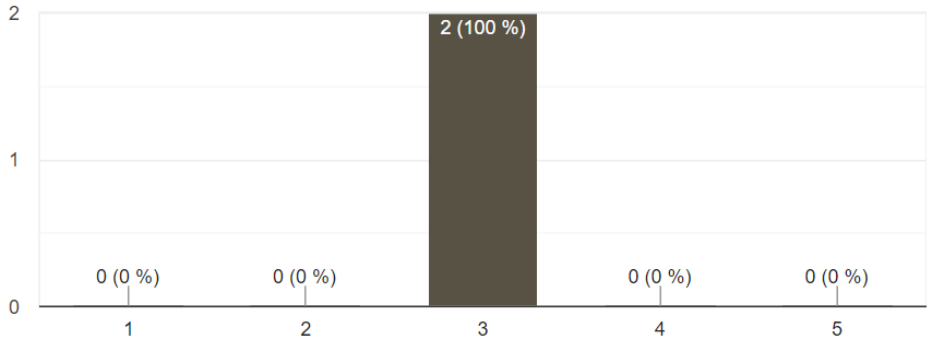
Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría XoMail?

2 respuestas



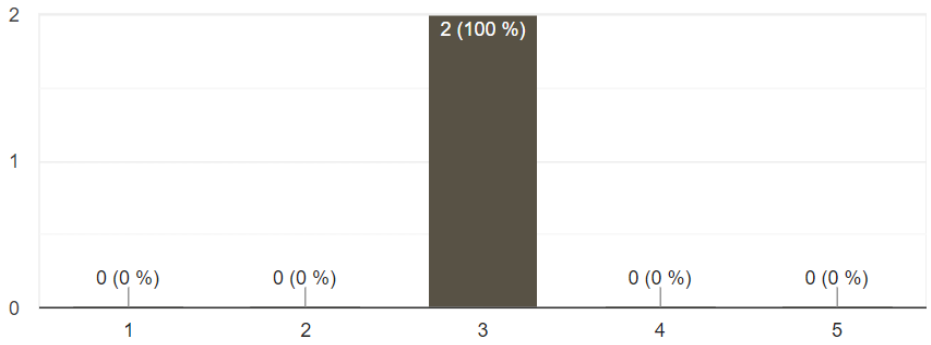
Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría SHAREPOINT?

2 respuestas



Con respecto a las aplicaciones existentes en el SC2N-EA, ¿cómo calificaría JEMM?

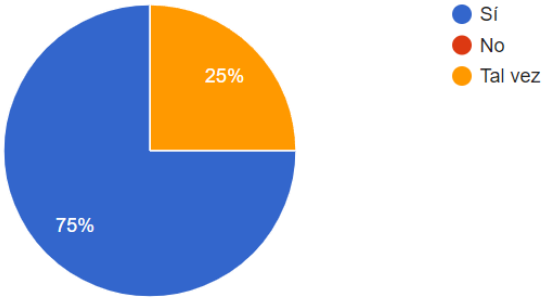
2 respuestas



Nuevo SIMACTA (Sistema de Información para el Mando y Control Tierra Aire)

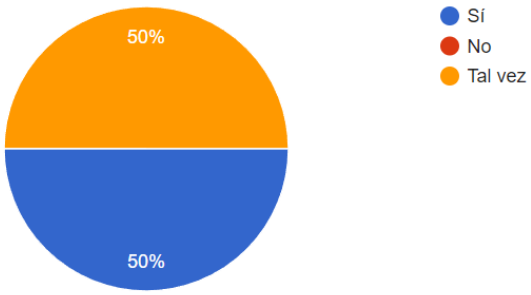
¿Considera beneficiosa la creación de un nuevo sistema de mando y control que ya tenga integrados ambos C-2?

12 respuestas



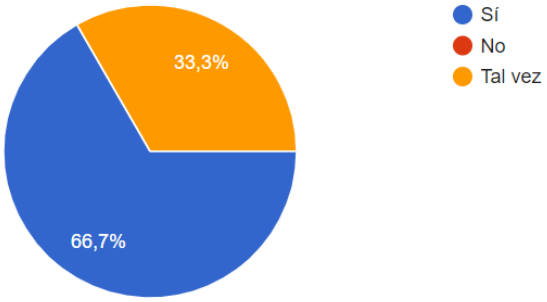
En relación a la posibilidad de unión de JCHAT y Outlook, ¿Considera necesaria la incorporación de una aplicación que integre una opción para la mensajería informal de JCHAT, y otra opción para la mensajería formal de Outlook?

12 respuestas



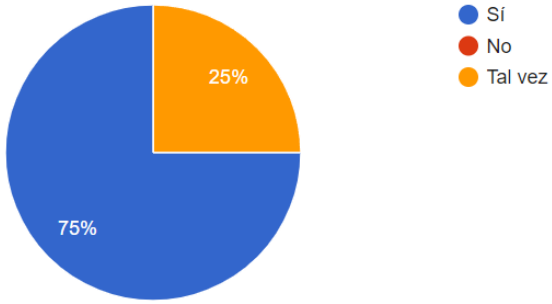
¿Considera necesario añadir una aplicación de mensajería común al ET y al EA?

12 respuestas



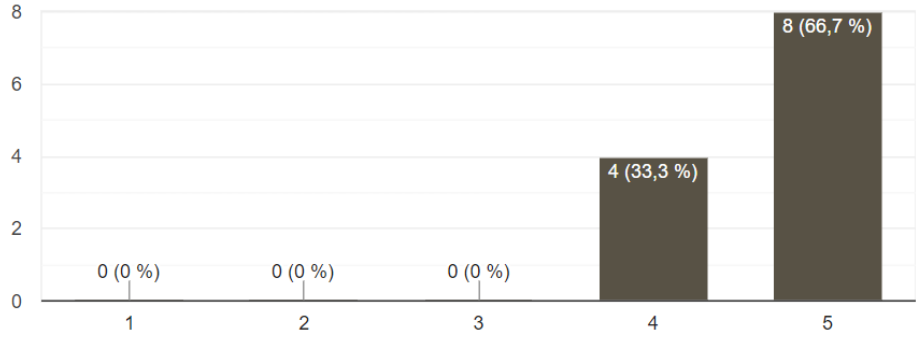
¿Considera necesario crear una nueva aplicación geográfica, con la que visualizar y modificar la información relativa al espacio de batalla del ET y visualizar la del espacio aéreo del EA de forma eficiente, diferente a las existentes?

12 respuestas



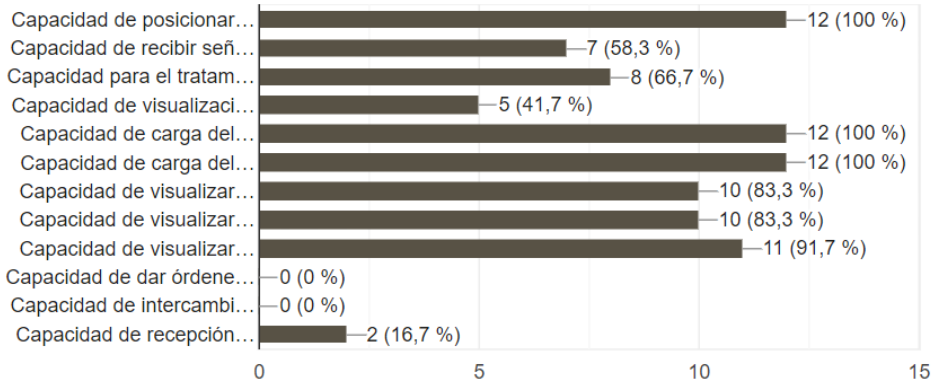
¿Consideraría útil que los vehículos y sistemas de armas llevaran incluido un sensor GPS que los posicionara automáticamente en en la aplicación geográfica?

12 respuestas



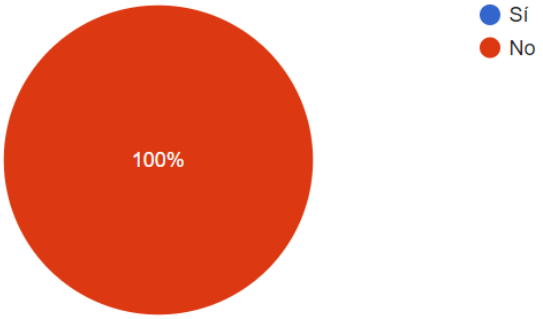
De los siguientes aspectos, ¿Cuáles considera imprescindibles a la hora de desarrollar una nueva aplicación geográfica común a ambos sistemas de mando y control?

12 respuestas



¿Considera necesario añadir alguna aplicación extra a las ya mencionadas?

12 respuestas



En el caso de que en la pregunta anterior haya marcado ``Sí´´, ¿Qué aplicación sería y qué funciones desempeñaría?

0 respuestas

Aún no hay respuestas para esta pregunta.

ANEXO F. Coste Primera Solución

Tabla 10 Costes desglosados de la primera solución. Fuente: elaboración propia.

PRODUCTO	ENLACE	CANTIDAD	COSTE	TOTAL
Router TC MGUARD RS4000	TC MGUARD RS4000 3G VPN 2903440 PHOENIX CONTACT Enrutador (electricautomationnetwork.com)	1	2.018,39 €	2.018,39 €
Switch Allied Tellesis x530L-28GPX	Comprar Switch Allied Telesis AT-x530L-28GPX PoE (AT-X530L-28GPX-50) (bechtle.com)	1	2.700€	2.700€
SAI EATON 9SX6KiRT	Eaton 9SX 6000i RT3U 9SX6KIRT EATON ELECTRIC SAI On Line 6.. (electricautomationnetwork.com)	1	4114,05€	4114,05€
Duplicador conector de red RJ-45 macho a 2xRJ-45 hembra	Duplicador Conector De Red RJ45 Macho A 2xRJ45 Hembra Cat 5e | PcComponentes.com	3	3x6,30€	18,90
Windows 10 Pro	https://www.microsoft.com/es-es/d/windows-10-pro/df77x4d43rkt/0002?rtc=1&activetab=pivot%3aoverviewtab	6	6x259,00€	1554,00€
TOTAL				10.405,34€

ANEXO G. Coste Segunda Solución

Tabla 11 Costes desglosados de la segunda solución. Fuente: elaboración propia.

PRODUCTO	ENLACE	CANTIDAD	COSTE	TOTAL
Router TC MGUARD RS4000	TC MGUARD RS4000 3G VPN 2903440 PHOENIX CONTACT Enrutador (electricautomationnetwork.com)	1	2.018,39 €	2.018,39 €
Switch Allied Tellesis x530L-28GPX	Comprar Switch Allied Telesis AT-x530L-28GPX PoE (AT-X530L-28GPX-50) (bechtle.com)	1	2.700€	2.700€
SAI EATON 9SX6KiRT	Eaton 9SX 6000i RT3U 9SX6KIRT EATON ELECTRIC SAI On Line 6.. (electricautomationnetwork.com)	1	4114,05€	4114,05€
Duplicador conector de red RJ-45 macho a 2xRJ-45 hembra	Duplicador Conector de red RJ45 Cat 5e | PcComponentes.com	3	3x6,30€	18,90
Pantalla integrada CyberView N119	N119 - 1U 19 pulgadas LED rack mount monitor teclado cajón w / Touchpad o Trackball (kvm-switches-online.com)	1	1.085,00€	1.085,00€
Servidor modelo Dell PowerEdge R 350	https://www.dell.com/es-es/work/shop/cty/pdp/spd/poweredge-r350/emea_r350	3	3x4.640,67€	13.922,01
Terminal HPEliteBook 840 G-8	Portátil HP EliteBook 840 G8 - HP Store España	6	6x1.820,38€	10.922,28
Software JADTAGES		1	100.000,00€	100.000,00€
Software MIXCHAT		1	100.000,00€	100.000,00€
TOTAL				234.780,00€

ANEXO H. AHP

1. Cómo obtener el resultado final de todas las encuestas.

Una vez contestadas las encuestas por parte de los operadores, y recibidas, se ha realizado un método cualitativo para conseguir un resultado final en base a valores cuantitativos. Con este método se han comparado los puntos de vista de los operadores para así llegar a un valor intermedio, de este modo, se tendrían en cuenta los puntos de vista de todos. Los pasos a seguir en el método han sido los siguientes:

1) Si los dos operadores han puesto la "X" en la misma casilla:

   a) Si los valores asignados son los mismos, se ha mantenido el valor.

   b) Si los valores asignados no han coincidido, se ha hecho la media entre todos los valores asignados y se ha seleccionado el valor de la escala de Saaty que le continúa. Por ejemplo: Si el operador 1 da un valor de 5, el operador 2 un valor de 7, y el operador 3 un valor de 7, la media resultante de los tres valores es 6,33, y el valor que le continua es 7, que será el valor asignado.

2) Si los operadores no han puesto la "X" en la misma casilla:

   c) Si los valores asignados son iguales, el resultado de la comparativa se cambia al valor de 1.

   d) Si los valores asignados son diferentes, se ha realizado la media de los valores de cada "X", y la "X" se ha dejado en la casilla que tenía la media más elevada. Por ejemplo: Si el criterio Técnico tiene un valor medio de 5,66 y el criterio Táctico tiene un valor de 6,34, al ser el Táctico mayor que el Técnico, la "X" se quedará en el criterio Táctico, y el valor asignado será de 7 [44].

2. Resto de matrices de la comparación entre los subcriterios de cada criterio.

Criterio Táctico

Tabla 12 Matriz de resultados de la comparación entre los subcriterios del criterio Táctico.

TÉCNICO	INTEGRACIÓN	C2	VELOCIDAD	PESO(W)	RI
INTEGRACIÓN	1	1	1	0,33	
C2	1	1	1	0,33	0,0000
VELOCIDAD	1	1	1	0,33	

Criterio Mantenimiento

Tabla 13 Matriz de resultados de la comparación entre los subcriterios del criterio Mantenimiento.

MANTENIMIENTO	COMPLEJIDAD	COSTE	PESO(W)	RI
COMPLEJIDAD	1	1/3	0,25	0,0000
COSTE	3	1	0,75	

Criterio Coste

Tabla 14 Matriz de resultados de la comparación entre los subcriterios del criterio Coste.

COSTE	HARDWARE	SOFTWARE	PESO(W)	RI
HARDWARE	1	5	0,83	0,0000
SOFTWARE	1/5	1	0,17	

3. Definición criterios y subcriterios en función de las propuestas.

- Criterio Técnico. Este criterio está relacionado con la capacidad de las propuestas de mantener la seguridad de ambos sistemas de C-2.

- Hardware. Este subcriterio hace referencia a la capacidad de los elementos hardware presentes en las propuestas de conseguir los objetivos técnicos.

- Software. Este subcriterio hace referencia a la capacidad de las aplicaciones presentes en las propuestas de conseguir los objetivos técnicos.

➢ Criterio Táctico. Este criterio está relacionado con la capacidad de las propuestas de tener los aspectos tácticos necesarios en el sistema para llevar a cabo el mando y control de la UDAA de forma eficiente.

- Integración. Este subcriterio hace referencia a la capacidad de las propuestas de visualizar la información del ET y del EA en un mismo terminal.

- C-2. Este subcriterio hace referencia a la capacidad de las propuestas de realizar el mando y control de manera satisfactoria.

- Velocidad de decisión. Este subcriterio hace referencia a la capacidad de las propuestas de proporcionar velocidad a la toma de decisiones.

➢ Criterio Mantenimiento. Este criterio está relacionado con la importancia que tiene el mantenimiento a la hora de desarrollar las propuestas. Hay que tener en cuenta que, para valorar ambos subcriterios, asignar un valor alto significa que es mejor opción, es decir, que la propuesta importante será menos compleja, o que conllevará menos coste su mantenimiento.

- Complejidad. Este subcriterio hace referencia a la importancia de la complejidad para llevar a cabo las tareas de mantenimiento.

- Coste. Este subcriterio hace referencia a la importancia del coste del mantenimiento.

➢ Criterio Coste. Este criterio está relacionado con el coste que conllevaría la adquisición de los elementos hardware y software presentes en las propuestas. Hay que tener en cuenta que, para valorar ambos subcriterios, asignar un valor alto significa que es mejor opción, es decir, que la propuesta importante será más económica que la otra.

- Hardware. Este subcriterio hace referencia al coste que conllevaría la adquisición de los elementos hardware de las propuestas.

- Software. Este subcriterio hace referencia al coste que conllevaría la adquisición de nuevas aplicaciones software.

4. Resto de matrices de la comparación de los subcriterios con cada propuesta.

Criterio Técnico

Tabla 15 Matriz final con los resultados de la comparación del subcriterio integración, del criterio Táctico, con ambas propuestas. Fuente: elaboración propia.

INTEGRACIÓN	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1/3	0,25	0,0000
SIMACTA	3	1	0,75	

Tabla 16 Matriz final con los resultados de la comparación del subcriterio C2, del criterio Táctico, con ambas propuestas. Fuente: elaboración propia.

C2	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1	0,5	0,0000
SIMACTA	1	1	0,5	

Tabla 17 Matriz final con los resultados de la comparación del subcriterio Velocidad, del criterio Táctico, con ambas propuestas. Fuente: elaboración propia.

VELOCIDAD	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1/7	0,13	0,0000
SIMACTA	7	1	0,87	

Criterio Mantenimiento

Tabla 18 Matriz final con los resultados de la comparación del subcriterio Complejidad, del criterio Mantenimiento, con ambas propuestas. Fuente: elaboración propia.

COMPLEJIDAD	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1/3	0,25	0,0000
SIMACTA	3	1	0,75	

Tabla 19 Matriz final con los resultados de la comparación del subcriterio Coste, del criterio Mantenimiento, con ambas propuestas. Fuente: elaboración propia.

COSTE	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	1/3	0,25	0,0000
SIMACTA	3	1	0,75	

Criterio Coste

Tabla 20 Matriz final con los resultados de la comparación del subcriterio Hardware, del criterio Coste, con ambas propuestas. Fuente: elaboración propia.

HARDWARE	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	7	0,87	0,0000
SIMACTA	1/7	1	0,13	

Tabla 21 Matriz final con los resultados de la comparación del subcriterio Software, del criterio Coste, con ambas propuestas. Fuente: elaboración propia.

SOFTWARE	UNIÓN SISTEMAS	SIMACTA	PESO(W)	RI
UNIÓN SISTEMAS	1	9	0,9	0,0000
SIMACTA	1/9	1	0,1	

ANEXO I. Cuestionario Criterios/ Subcriterios AHP

CUESTIONARIO PARA LA VALORACIÓN DE LOS CRITERIOS Y LOS SUBCRITERIOS PARA LA METODOLOGÍA AHP

Para la realización de este cuestionario, en primer lugar, habrá que familiarizarse con la escala de Saaty (véase Figura1), en base a la cual se llevará a cabo una comparación entre criterios y subcriterios, acerca de los sistemas de mando y control.

La siguiente tabla recoge la escala de Saaty, junto con unos comentarios, que resultarán de ayuda a la comprensión, en la que deberá apoyarse para la ejecución de la encuesta.

VALOR	DEFINICIÓN	COMENTARIO
1	Igual importancia	A y B tienen la misma importancia
3	Importancia moderada	A es ligeramente más importante que B
5	Importancia grande	A es más importante que B
7	Importancia muy grande	A es mucho más importante que B
9	Importancia extrema	A es extremadamente más importante que B

Tabla 1 Escala de Saaty.

A continuación, se muestra una explicación tanto de los criterios como de los subcriterios a valorar en la siguiente encuesta.

CRITERIOS A VALORAR

Criterio Técnico. Este criterio está relacionado con los aspectos técnicos necesarios en el sistema, así como la viabilidad de materializar las propuestas de interoperabilidad entre sistemas. Hace referencia a la importancia que tienen los elementos tanto hardware como software para mantener los niveles de seguridad de cada red de C-2, a la hora de llevar a cabo las propuestas.

- **Hardware**. Este subcriterio hace referencia a la importancia o necesidad de renovar los elementos hardware para mantener los niveles de seguridad de ambas redes de C-2.
- **Software**. Este subcriterio hace referencia a la importancia o necesidad de renovar los elementos software para mantener los niveles de seguridad de ambas redes de C-2.

Criterio Táctico. Este criterio está relacionado con la importancia que tienen los aspectos tácticos, necesarios en el sistema para llevar a cabo el mando y control de la UDAA de forma eficiente, a la hora de desarrollar las propuestas.

- **Integración.** Este subcriterio hace referencia a la importancia que tiene la integración de la información proveniente del C-2 de ET como del C-2 del EA en un único sistema.
- **C-2.** Este subcriterio hace referencia a la importancia que tiene que el mando y control de la operación de la UDAA se pueda hacer de la manera más eficiente posible.
- **Velocidad de decisión.** Este subcriterio hace referencia a la importancia que tiene que el sistema provea de una velocidad suficiente para que la toma de decisiones sea veloz.

Criterio Mantenimiento. Este criterio está relacionado con la importancia que tiene el mantenimiento a la hora de desarrollar las propuestas.

- **Complejidad.** Este subcriterio hace referencia a la importancia de la complejidad para llevar a cabo las tareas de mantenimiento.
- **Coste.** Este subcriterio hace referencia a la importancia del coste del mantenimiento.

Criterio Coste. Este criterio está relacionado con la importancia que se le da al coste a la hora de desarrollar las propuestas.

- **Hardware.** Este subcriterio hace referencia a la importancia que se le asigna al coste de los elementos hardware.
- **Software.** Este subcriterio hace referencia a la importancia que se le asigna al coste del desarrollo de aplicaciones nuevas.

A continuación, deberá responder las siguientes preguntas. En primer lugar, deberá indicar que criterio/subcriterio tiene más importancia de los dos comparados, poniendo una "X" en el hueco establecido para el efecto, a la derecha del criterio en cuestión. Por último, tendrá que asignar un valor, de los preestablecidos según la escala de Saaty (véase Tabla 1), en la casilla establecida para el efecto, situada debajo de "VALOR" (véase el ejemplo 1). En el caso de considerar que son igual de importantes las comparaciones poner el valor de 1, sin necesidad de poner una "X" (véase el ejemplo 2).

Ejemplo 1.

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el criterio Técnico con Táctico:	Técnico	X	Táctico		3

Tabla 2. Ejemplo de la valoración 1. Fuente: elaboración propia.

Significado: El criterio Técnico es más importante que el criterio Táctico con un valor de 3 (ligeramente más importante)

Ejemplo 2.

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el criterio Técnico con Táctico:	Técnico		Táctico		1

Tabla 3. Ejemplo de la valoración 2. Fuente: elaboración propia.

Para comenzar con el desarrollo de la encuesta, en primer lugar, escriba en el siguiente campo que función desempeña en el puesto de mando de una UDAA.

COMPARACIÓN ENTRE CRITERIOS

En esta primera tabla se realiza una comparación entre los diferentes criterios.

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el criterio Técnico con Táctico:	Técnico		Táctico		
Compare el criterio Técnico con Mantenimiento:	Técnico		Mantenimiento		
Compare el criterio Técnico con Coste:	Técnico		Coste		
Compare el criterio Táctico con Mantenimiento:	Táctico		Mantenimiento		
Compare el criterio Táctico con Coste:	Táctico		Coste		
Compare el criterio Mantenimiento con Coste:	Mantenimiento		Coste		

COMPARACIÓN ENTRE SUBCRITERIOS

En las sucesivas tablas se realizará una comparación entre subcriterios de los diferentes criterios.

CRITERIO TÉCNICO

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el subcriterio Hardware con Software:	Hardware		Software		

CRITERIO TÁCTICO

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el subcriterio Integración con C-2:	Integración		C-2		
Compare el subcriterio Integración con Velocidad:	Integración		Velocidad		
Compare el subcriterio C-2 con Velocidad:	C-2		Velocidad		

CRITERIO MANTENIMIENTO

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el subcriterio Complejidad con Coste:	Complejidad		Coste		

CRITERIO COSTE

COMPARACIÓN	CRITERIO		CRITERIO		VALOR
Compare el subcriterio Hardware con Software:	Hardware		Software		

MUCHAS GRACIAS POR SU COLABORACIÓN, TIEMPO Y DEDICACIÓN

ANEXO J. Cuestionario Propuestas AHP

CUESTIONARIO PARA LA VALORACIÓN DE LOS CRITERIOS Y LOS SUBCRITERIOS DE LAS DOS PROPUESTAS PARA LA METODOLOGÍA AHP

Para la realización de este cuestionario, en primer lugar, habrá que familiarizarse con la escala de Saaty (véase Figura1), en base a la cual se llevará a cabo una comparación propuesta en función del subcriterio a tratar.

La siguiente tabla recoge la escala de Saaty, junto con unos comentarios, que resultarán de ayuda a la comprensión, en la que deberá apoyarse para la ejecución de la encuesta.

VALOR	DEFINICIÓN	COMENTARIO
1	Igual importancia	A y B tienen la misma importancia
3	Importancia moderada	A es ligeramente más importante que B
5	Importancia grande	A es más importante que B
7	Importancia muy grande	A es mucho más importante que B
9	Importancia extrema	A es extremadamente más importante que B

Tabla 4 Escala de Saaty.

En este cuestionario se va a realizar una comparación de dos propuestas (Unión de sistemas y SIMACTA), para la interoperabilidad del SIMACET y de la red del SC2N-EA, en base a los subcriterios que presentan los diferentes criterios.

Antes de comenzar con el cuestionario, es necesario conocer ambas propuestas, así como los criterios y subcriterios. Para ello en primer lugar, se explicará en qué consisten las dos propuestas; en segundo lugar, se dará una pequeña explicación de lo que supone cada criterio/subcriterio a valorar para las propuestas.

UNIÓN DE SISTEMAS

Consiste en la interoperabilidad del SIMACET y de la red del SC2N-EA por medio de la sustitución del router y del *switch*. El SAI también sería renovado, mientras que el resto de los elementos hardware que componen el SIMACET se reutilizarían, al igual que el teléfono del sistema de la red del SC2N-EA que se incorporaría al sistema. En cuanto a los softwares de las aplicaciones, el único cambio es la sustitución de ANTARES (presente en el SIMACET) e ICC-NATO (presente en el SC2N-

EA) por TALOS Táctico, permitiendo así la visualizar en el software tanto la RAP, como la posición geográfica, personal y composición de las unidades del ET desplegadas en la UDAA.

SIMACTA

El Sistema de Información para el Mando y Control Tierra Aire (SIMACTA) es un nuevo sistema de C-2 propuesto por el presente alumno, para la integración de los sistemas de mando y control del ET y del EA. Es una propuesta en la que se renovarían todos los elementos hardware, menos la DTU, el cifrador, el teléfono del EA y el *switch* de los servidores. Por otro lado, los terminales no sólo serían sustituidos, sino que los sustitutos serían ordenadores HP de última generación que garantizarían la velocidad de decisión y el C-2. En cuanto a los softwares de las aplicaciones: se ha presentado la propuesta de JADTAGES, una aplicación geográfica para el C-2 en la que se pueda recoger tanto la información geográfica de las unidades del ET, como la RAP del EA; otra propuesta de desarrollo es la de MIXCHAT, una aplicación que permitiría el intercambio de mensajería tanto con el ET como con el EA, tanto formal como informal, además de, dar la posibilidad del intercambio de todo tipo de documentos. El resto de las aplicaciones seguirían siendo las mismas.

CRITERIOS/SUBCRITERIOS

Criterio Técnico. Este criterio está relacionado con la capacidad de las propuestas de mantener la seguridad de ambos sistemas de C-2.

- **Hardware**. Este subcriterio hace referencia a la capacidad de los elementos hardware presentes en las propuestas de conseguir los objetivos técnicos.
- **Software**. Este subcriterio hace referencia a la capacidad de las aplicaciones presentes en las propuestas de conseguir los objetivos técnicos.

Criterio Táctico. Este criterio está relacionado con la capacidad de las propuestas de tener los aspectos tácticos necesarios en el sistema para llevar a cabo el mando y control de la UDAA de forma eficiente.

- **Integración.** Este subcriterio hace referencia a la capacidad de las propuestas de visualizar la información del ET y del EA en un mismo terminal.
- **C-2.** Este subcriterio hace referencia a la capacidad de las propuestas de realizar el mando y control de manera satisfactoria.
- **Velocidad de decisión.** Este subcriterio hace referencia a la capacidad de las propuestas de proporcionar velocidad a la toma de decisiones.

Criterio Mantenimiento. Este criterio está relacionado con la importancia que tiene el mantenimiento a la hora de desarrollar las propuestas. Hay que tener en cuenta que, para valorar ambos subcriterios, asignar un valor alto significa que es mejor opción, es decir, que la propuesta importante será menos compleja, o que conllevará menos coste su mantenimiento (véase el ejemplo 3).

- **Complejidad.** Este subcriterio hace referencia a la importancia de la complejidad para llevar a cabo las tareas de mantenimiento.
- **Coste.** Este subcriterio hace referencia a la importancia del coste del mantenimiento.

Criterio Coste. Este criterio está relacionado con el coste que conllevaría la adquisición de los elementos hardware y software presentes en las propuestas. Hay que tener en cuenta que, para

valorar ambos subcriterios, asignar un valor alto significa que es mejor opción, es decir, que la propuesta importante será más económica que la otra (véase el ejemplo 3).

- **Hardware.** Este subcriterio hace referencia al coste que conllevaría la adquisición de los elementos hardware de las propuestas.
- **Software.** Este subcriterio hace referencia al coste que conllevaría la adquisición de nuevas aplicaciones software.

A continuación, deberá responder las siguientes preguntas. En primer lugar, deberá indicar que criterio/subcriterio tiene más importancia de los dos comparados, poniendo una "X" en el hueco establecido para el efecto, a la derecha del criterio en cuestión. Por último, tendrá que asignar un valor, de los preestablecidos según la escala de Saaty (véase Tabla 1), en la casilla establecida para el efecto, situada debajo de "VALOR". En el caso de considerar que son igual de importantes las comparaciones poner el valor de 1, sin necesidad de poner una "X".

Ejemplo 3.

COMPARACIÓN	Unión de sistemas	SIMACTA	VALOR
Compare el subcriterio Hardware.	X		5

Significado: La propuesta "Unión de sistemas" es más importante que la propuesta "SIMACTA" con un valor de 5 (más importante), lo que quiere decir que es mejor esa primera propuesta por ser más económica que la propuesta "SIMACTA".

CRITERIO TÉCNICO

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Hardware.			

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Software.			

CRITERIO TÉCNICO

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Integración.			

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio C-2.			

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Velocidad de decisión.			

CRITERIO MANTENIMIENTO

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Complejidad.			

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Coste.			

CRITERIO COSTE

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Hardware.			

COMPARACIÓN	Unión de ambos sistemas	SIMACTA	VALOR
Compare el subcriterio Software.			

MUCHAS GRACIAS POR SU COLABORACIÓN, TIEMPO Y DEDICACIÓN

pág. 8

ANEXO K. Resultados primer cuestionario AHP

PREGUNTAS CRITERIOS						
Jefe de Operaciones	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico	X				3
	Técnico con Mantenimiento	X				9
	Técnico con Coste	X				3
	Táctico con Mantenimiento		X			7
	Táctico con Coste		X			3
	Mantenimiento con Coste				X	5
S-1	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico					1
	Técnico con Mantenimiento	X				5
	Técnico con Coste				X	3
	Táctico con Mantenimiento		X			5
	Táctico con Coste		X			3
	Mantenimiento con Coste			X		5
S-2 SIMACET	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico	X				3
	Técnico con Mantenimiento	X				5
	Técnico con Coste	X				3
	Táctico con Mantenimiento		X			9
	Táctico con Coste		X			3
	Mantenimiento con Coste				X	3
S-2 SC2N-EA	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico	X				3
	Técnico con Mantenimiento	X				9
	Técnico con Coste	X				3
	Táctico con Mantenimiento		X			7
	Táctico con Coste		X			3
	Mantenimiento con Coste					1
S-3	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico					1
	Técnico con Mantenimiento	X				7
	Técnico con Coste					1
	Táctico con Mantenimiento		X			3
	Táctico con Coste					1
	Mantenimiento con Coste				X	5
S-4	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
	Técnico con Táctico					1
	Técnico con Mantenimiento	X				9
	Técnico con Coste	X				3
	Táctico con Mantenimiento		X			3
	Táctico con Coste					1
	Mantenimiento con Coste			X		3

PREGUNTAS SUBCRITERIOS					
Jefe de Operaciones	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software	X			7
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2		X		3
	Integración con Velocidad				1
	C-2 con Velocidad				1
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste		X		1
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			7
S-1	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software	X			5
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2				1
	Integración con Velocidad				1
	C-2 con Velocidad				1
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste		X		1
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			5
S-2 SIMACET	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software		X		5
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2	X			3
	Integración con Velocidad				1
	C-2 con Velocidad				1
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste		X		3
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			5

S-2 SC2N-EA	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software		X		5
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2				1
	Integración con Velocidad	X			5
	C-2 con Velocidad		X		3
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste		X		3
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			3
S-3	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software	X			9
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2	X			3
	Integración con Velocidad			X	5
	C-2 con Velocidad			X	3
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste				1
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			3
S-4	COMPARACIÓN CRITERIO TÉCNICO	HARDWARE	SOFTWARE	-	VALOR
	Hardware con Software	X			3
	COMPARACIÓN CRITERIO TÁCTICO	INTEGRACIÓN	C-2	VELOCIDAD	VALOR
	Integración con C-2		X		3
	Integración con Velocidad				1
	C-2 con Velocidad				1
	COMPARACIÓN CRITERIO MANTENIMIENTO	COMPLEJIDAD	COSTE	-	VALOR
	Complejidad con Coste				1
	COMPARACIÓN CRITERIO COSTE	HARDWARE	SOFTWARE		VALOR
	Hardware con Software	X			5

RESULTADOS GLOBALES

	COMPARACIÓN	TÉCNICO	TÁCTICO	MANTENIMIENTO	COSTE	VALOR
PREGUNTAS CRITERIOS	Técnico con Táctico	X				3
	Técnico con Mantenimiento	X				9
	Técnico con Coste	X				3
	Táctico con Mantenimiento		X			7
	Táctico con Coste		X			3
	Mantenimiento con Coste				X	5
PREGUNTAS SUBCRITERIOS	**COMPARACIÓN CRITERIO TÉCNICO**	**HARDWARE**	**SOFTWARE**	**-**		**VALOR**
	Hardware con Software	X				7
	COMPARACIÓN CRITERIO TÁCTICO	**INTEGRACIÓN**	**C-2**	**VELOCIDAD**		**VALOR**
	Integración con C-2					1
	Integración con Velocidad					1
	C-2 con Velocidad					1
	COMPARACIÓN CRITERIO MANTENIMIENTO	**COMPLEJIDAD**	**COSTE**	**-**		**VALOR**
	Complejidad con Coste		X			3
	COMPARACIÓN CRITERIO COSTE	**HARDWARE**	**SOFTWARE**			**VALOR**
	Hardware con Software		X			5

ANEXO L. Resultados segundo cuestionario AHP

PREGUNTAS ALTERNATIVAS				
Jefe de Operaciones	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración		X	3
	C-2			1
	Velocidad de decisión		X	9
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad		X	3
	Coste		X	3
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		7
	Software	X		7
S-1	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software			1
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración			1
	C-2			1
	Velocidad de decisión		X	3
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad			1
	Coste			1
	COMPARACIÓN CRITERIO COSTE			
	Hardware		X	3
	Software		X	3
S-2 SIMACET	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración		X	3
	C-2			1
	Velocidad de decisión		X	7
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad		X	3
	Coste		X	3
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		7
	Software	X		9

	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
S-2 SC2N-EA	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración		X	3
	C-2			1
	Velocidad de decisión		X	7
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad			1
	Coste		X	3
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		9
	Software	X		9

	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
S-3	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración		X	3
	C-2			1
	Velocidad de decisión		X	5
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad		X	3
	Coste			1
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		5
	Software	X		7

	COMPARACIONES	UNION DE SISTEMAS	SIMACTA	VALOR
S-4	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración			1
	C-2			1
	Velocidad de decisión		X	7
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad			1
	Coste			1
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		7
	Software	X		7

RESULTADOS GLOBALES				
PREGUNTAS PROPUESTAS	COMPARACIONES	UNIÓN DE SISTEMAS	SIMACTA	VALOR
	COMPARACIÓN CRITERIO TÉCNICO			
	Hardware			1
	Software		X	3
	COMPARACIÓN CRITERIO TÁCTICO			
	Integración		X	3
	C-2			1
	Velocidad de decisión		X	7
	COMPARACIÓN CRITERIO MANTENIMIENTO			
	Complejidad		X	3
	Coste		X	3
	COMPARACIÓN CRITERIO COSTE			
	Hardware	X		7
	Software	X		9