



Universidad
Zaragoza

Trabajo Fin de Grado

Nuevo concepto para el despliegue de un Centro de Transmisiones de un Puesto de Mando táctico de Gran Unidad, permanentemente acreditable dentro de un entorno OTAN

Autor

Jesús López Aguado

Director/es

Director académico: Dra. Dña. M^a Teresa Sánchez Rúa

Director militar: Cap. D. Edgar Forner Cotillas

Centro Universitario de la Defensa-Academia General Militar

2018

Agradecimientos

En este punto, me gustaría agradecer a todo el personal de la Academia General Militar y el Centro Universitario de la Defensa por la formación recibida durante estos años, sin la cual no habría sido posible la realización de este Trabajo Fin de Grado.

En particular, me gustaría agradecerle a la profesora Dña. María Teresa Sánchez Rúa por su constante asesoramiento en el desarrollo de este Trabajo Fin de Grado.

Además, me gustaría agradecerle a todo el personal del Regimiento de Transmisiones nº 21, y en especial a la 22 Compañía por todo el apoyo mostrado durante la realización de las Prácticas Externas. En especial, agradecerle a su Capitán D. Edgar Forner Cotillas por su dedicación, sin la cual no habría sido posible la realización de este Trabajo de Fin de Grado.

Resumen

Se entiende por información todo el conocimiento que puede ser comunicado o guardado de cualquier forma. Es un recurso de gran valor militar, tanto técnica como tácticamente, es por ello por lo que las medidas establecidas para su protección siempre deben de ser de obligado cumplimiento. Más aún cuando se trabaja en colaboración con otros países.

Con la realización del presente Trabajo Fin de Grado (TFG) se pretende transmitir y proponer mejoras sobre el Nuevo Concepto, el cual está en su fase inicial siendo planificado y dirigido por el Mando de Transmisiones (MATRANS), sobre el despliegue táctico de los Centros de Transmisiones de Puesto de Mando de Gran Unidad (CTPCGU), siendo la rapidez y la eficiencia las principales características. Por tanto, no sólo se describen las nuevas medidas adoptadas actualmente, sino que tras establecer una comparativa entre el sistema anterior y el presente, se detallan las propuestas de mejora como parte de las conclusiones halladas tras la fase práctica.

Para ello se ha realizado un estudio del estado del arte de las tecnologías actuales y la forma actual de proceder a la hora de desplegar un Centro de Transmisiones (CT), comprobando el resultado de dicha tecnología en el ejercicio DEPLOYEX18. Este estudio se ha basado en la experiencia del personal con un determinado nivel de perfil técnico destinado en la Unidad, empleando encuestas y entrevistas que permiten valorar y justificar los resultados obtenidos.

Abstract

“Information” is defined as any kind of knowledge that could be either, preserved or stored in different states. Being a highly valuable military asset, both from a technical and from a tactical point of view, measures aimed at protecting this information should be implemented.

In order to grant or restrict the access to the information, one of such protective measures is the “classification” of the information. The more sensitive or important the information is, the higher the level of classification will be.

Thus, information is classified as Restricted, Confidential, Secret, Top Secret or even Cosmic Top Secret. In order to have access to the different levels of classified information the correct security clearance is required for the individual who handles it. Not only those security measures are required for individuals, but also for the material with which this information is accessed through or stored in.

Clearance is a long and complex process in which individuals and facilities are evaluated in order to determine if the required security requisites are fulfilled. This process becomes even more important when working in collaboration with other countries within the North Atlantic Treaty Organization (NATO) structure. In order to achieve this level of collaboration, a series of minimum common requirements are established to be able to share/communicate this sensitive information, known as Federated Mission Network (FMN).

The aim of this end-of-degree-project is to introduce a New Concept for the deployment of an Army Corps Headquarters’ Signals Center, permanently certified within the NATO environment. The initial phase of this New Concept is being planned and directed by the Signals Command (MATRANS) over the basis of the tactical deployment of an HQ Signals Center (CTPCGU), being speed and effectiveness its main characteristics.

The New Concept is based on the creation of a permanent structure in the Signals Unit, called Permanent Node. This new Permanent Node will be managed by a group of administrators with high technical training and provided with some SIMACET V5 nodes. This nodes will be dedicated to the virtualization of all the services required by NATO users in the different deployments (Virtualized Nodes, up to a maximum of 8 nodes). In this way, both the facilities of administration, centralized in the Permanent Node, and the deployable resources, can be permanently certified. As a consequence, the administrators of the Permanent Node performs the planning and remote administration of the deployable means, while the Signal Center are dedicated to the deployment of the Command Post Signal Center (CTPC).

The New Concept will be based on the former procedure in the aspects related to the configuration, deployment and CIS structure, divided in CORE, COMMS and Functional Services. The main difference will be the fact that, contrary to the former model of deployment, in which the accreditation process had to be done for every exercise, in this new model the main node will be permanently certified and will remain operative and ready to be deployed. Not only the new accreditation measures but also the deployment process will be described in order to establish a comparison between

the present and future models. Thus, detailing the existing differences between the two models will lead to discover why adopting this New Concept is more convenient.

For this purpose, a brief overview of the state-of-the-art of the new communication technologies as long as some of the present procedures to deploy a Signals Center will be presented. This study is based on the personal experience of qualified personnel with a technical profile belonging to the Signals Regiment No. 21 (RT21), gathered by using surveys and interviews that let assess and justify the results collected in the manuscript.

Within the framework of the external practices phase carried out in the RT21, during the first half of September, the DEPLOYEX18 exercise was developed in the NRDC-ESP HQ (NATO Rapid Deployable Corps Spain Headquarters) in Bétera (Valencia). In this exercise, a first test of this New Concept consisting of the deployment of one of the Virtualized Nodes, controlled by the Permanent Node, was carried out. On this occasion, the correct security clearance, mandatory in other exercises, was not taking into account, since the purpose of this exercise was to test the management of a Deployable Node by the administrators of the Permanent Node. With this exercise, the first conclusions about the New Concept were obtained.

Finally, with the study carried out during the seven weeks in the RT21 and thanks to the knowledge of its crew together with the execution of the DEPLOYEX18 maneuvers, it was possible to obtain the correct understanding of the New Concept for the realization of this end-of-degree-project. Due to this, some conclusions have been prepared and possible action guide for future maneuvers in which the RT21 should work to be able to act in a more efficient way and with a better qualified crew has been proposed.

Índice

Índice	1
Índice de ilustraciones	3
Índice de tablas	4
Lista de acrónimos	5
1. Introducción	8
1.1. Objetivos y alcance del proyecto.....	8
1.2. Estructura de la memoria.....	8
2. Conceptos teóricos básicos	9
2.1. Información clasificada.....	9
2.2. Seguridad de la información.....	10
2.3. Seguridad de las comunicaciones.....	12
2.4. La seguridad física y del personal.....	12
2.5. Acreditación de sistemas.....	14
2.6. Procedimiento para solicitar una acreditación.....	16
3. Modelo de despliegue anterior	17
3.1. Los Centros de Transmisiones.....	17
3.2. Áreas de un Centro de Transmisiones.....	17
3.3. Procedimiento de configuración y despliegue.....	18
3.3.1. Conexión de los equipos.....	18
3.3.2. Creación de máquinas virtuales e instalación de clientes.....	19
3.3.3. Aplicación de políticas de seguridad.....	19
3.3.4. Aplicación de políticas incrementales.....	19
3.3.5. Auto-auditorías.....	20
3.3.6. Borrado de servidores.....	20
3.4. Federated Mission Network.....	20
3.5. Órganos de trabajo de los CIS.....	22
3.5.1. CORE.....	22
3.5.2. COMMS.....	24
3.5.3. FUNCTIONAL SERVICES (FS).....	25
4. Desarrollo del Nuevo Concepto de despliegue de un Centro de Transmisiones en un entorno OTAN	27
4.1. Comparativa entre el sistema anterior y el actual.....	30
5. Práctica	31
5.1. Antecedentes.....	31
5.2. Ejercicio DEPLOYEX 18.....	32

6. Conclusiones	35
6.1. Líneas futuras	36
Bibliografía	37
Anexos	39
Anexo A. Solicitud de Habilitación Personal de Seguridad	40
Anexo B. Declaración Personal de Seguridad	42
Anexo C. Aplicación políticas incrementales	50
Anexo D. Entrevista de administradores de nodo	51
Anexo E. Encuesta administradores	53

Índice de ilustraciones

Ilustración 1. Proceso completo para obtener una acreditación de seguridad.....	16
Ilustración 2. Esquema de una Mission Network.	21
Ilustración 3. Servidor de Backup nodo SIMACET v5.	23
Ilustración 4. Terminal CISCO CP 7821 y Firewall ASA 5520.	24
Ilustración 5. Clasificación nodos SIMACET	26
Ilustración 6. Posible estructura del Nuevo Concepto de despliegue.....	28
Ilustración 7. Ejemplo de posible ejercicio de Nodos Desplegables	30
Ilustración 8. Nuevo concepto Nodos Permanentes	33
Ilustración 9. Nuevo concepto Nodo Desplegable	33
Ilustración 10. Ejemplo de despliegue en ejercicio multinacional sistema continuo	34
Ilustración 11. Ejemplo de despliegue en ejercicio nacional sistema discontinuo	35

Índice de tablas

Tabla 1. Guía de equivalencias entre grados de información.....	10
Tabla 2. Documentación de seguridad en los sistemas.....	15

Lista de acrónimos

AAS	Administrador de Seguridad de Sistemas
ADA	Autoridad Delegada de Acreditación
ANS	Autoridad Nacional de Seguridad
AOSTIC	Autoridad Operacional del Sistema de las TIC
APO	Autorización para Operar
AR	Análisis de Riesgos
ASTIC	Autoridad de Seguridad de las TIC
ATPO	Autorización Temporal para Operar
BDT	Base de Datos Táctica
BIOS	Basic Input-Output System o sistema básico de entrada/salida
BOD	Boletín Oficial de Defensa
CCN	Centro Criptográfico Nacional
CIS	Communications and Information Systems o sistemas de comunicación e información
CISCC	Centro de Control y Coordinación de los Sistemas CIS
CN	Centros Nodales
CNI	Centro Nacional Inteligencia
COMSEC	Communication Security o seguridad de las telecomunicaciones
COS	Concepto de Operación de Sistema
CPU	Central Processing Unit o unidad central de procesamiento
CRIPTOSEC	Cryptography Security o seguridad criptográfica
CT	Centro de Transmisiones
CTAR	Centro Transmisiones Acceso Radio
CTD	Centro de Transmisiones Destacado
CTPC	Centro de Transmisiones de Puesto de Mando
CTPCGU	Centros de Transmisiones de Puesto de Mando de Gran Unidad
DC	Domain Controller o controlador de dominio
DLP	Data Loss Prevention o prevención de pérdidas de datos
DNS	Domain Name Server o Sistema de Nombres de Dominio
DPS	Declaración Personal de Seguridad
DRS	Declaración de Requisitos de Seguridad
EEFF	Endpoint Encryption for Files and Folders
EM	Estado Mayor
EPO	Epolicy Orchestrator
ESA	Agencia Espacial Europea o European Space Agency
ET	Ejército de Tierra
EXCON	Control Exercise o controlador del ejercicio
FMN	Federated Mission Network o red federada para misiones
GU	Gran Unidad
HPS	Habilitación Personal de Seguridad
IGEOSIT	Interin Geospatial Intelligence Tool

INFOSEC	Information Security o seguridad de la información
JCHAT	NATO Joint Tactical Chat
JCISAT	Jefatura de los Sistemas de Información y Telecomunicaciones y Apoyo Técnico
JOIIS	Joint Ops/Intel Information System
LOGFAS	Logistic Functional Area Services o área de servicios de función logística
MATRANS	Mando de Transmisiones
MCU	Multipoint Control Unit o unidad de control multipunto
MN	Mission Network o red de misión
MNX	Mission Network Extension o red de misión extendida
NRDC-ESP HQ	NATO Rapid Deployable Corps Spain Headquarters o Cuartel General Terrestre de Alta Disponibilidad España
NTP	Network Time Protocol o protocolo servidor de tiempos
OTAN/NATO	Organización del Tratado Atlántico Norte/North Atlantic Treaty Organization
PAR	Punto Acceso Radio
POS	Procedimientos Operativos de Seguridad
RT21	Regimiento de Transmisiones nº21
SEGINFO	Seguridad de la Información
SEGINFODOC	Seguridad de la información en los documentos
SEGINFOEMP	Seguridad de la información en poder de las empresas
SEGINFOINS	Seguridad de la información en las instalaciones
SEGINFOPER	Seguridad de la información en las personas
SEGINFOSIT	Seguridad de la información en los sistemas de información y telecomunicaciones
SHPS	Solicitud de Habilitación Personal de Seguridad
SIMACET	Sistema para el Mando y Control del Ejército de Tierra
SMA	Services Management Authority o autoridad del servicio de gestión
SQL	Structured Query Language
STIC	Seguridad de Tecnologías de la Información y las Comunicaciones
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions o material electrónico de telecomunicaciones protegido frente a las emisiones de emanaciones espurias
TFG	Trabajo de Fin de Grado
TIC	Tecnologías para la información y las telecomunicaciones
TOPFAS	Tool for Operational Planning Force Activation and Simulation
TRANSEC	Transmission Security o seguridad de la transmisión
UCO	Unidad, Centro y Organismo
UE	Unión Europea
USB	Universal Serial Bus o bus universal en serie
UT	Unidad de Transmisiones
VL18	Valiant Lynx 18

Vlan	Virtual Local Area Network o red virtual de área local
VoIP	Voice on Internet Protocol o protocolo de voz sobre internet
VTC	Video Teleconference o video teleconferencia
VTS	Verificación Técnica de Seguridad
WSUS	Windows Server Update Services
ZAR	Zonas de Acceso Restringido

1. Introducción

El Regimiento de Transmisiones Nº21 (RT21) es la más antigua de todas las Unidades de Transmisiones (UT) de España y uno de los Regimientos de Transmisiones más antiguos del mundo (ver [1]). Su misión principal es apoyar al Cuartel General Terrestre de Alta Disponibilidad (NRDC-ESP) de Bétera (Valencia) y por tanto, se somete a las particularidades que marca el entorno OTAN (Organización del Tratado Atlántico Norte). Por ello siempre está a la vanguardia en cuanto a innovaciones y desarrollo y su prestigio se basa en el alto nivel de instrucción técnica de su personal. Gracias a esta alta cualificación del componente humano ha sido posible plantear un nuevo sistema a la hora de desplegar los Centros de Transmisiones de Puesto de Mando de Gran Unidad (CTPCGU).

Para el desarrollo de este TFG se han realizado las prácticas pertinentes para demostrar que un Nuevo Concepto para el despliegue de un CTPCGU, permanentemente acreditable en entorno OTAN es un hecho factible y con una gran cantidad de mejoras con respecto al actual.

1.1. Objetivos y alcance del proyecto

El objetivo fundamental del presente trabajo es el desarrollo del Nuevo Concepto de despliegue de un CT en un entorno OTAN y la búsqueda de las mejores soluciones para el diseño de una nueva estructura de Sistemas de Comunicación e Información o Communications and Information Systems (CIS).

Este Nuevo Concepto se basa fundamentalmente en la creación de una nueva infraestructura permanente en la UT que se basará en la virtualización de todos los servicios requeridos por el usuario OTAN en los distintos despliegues, denominada Nodo Permanente. Este nuevo Nodo Permanente estará gestionado por un grupo de administradores con alta preparación técnica y provista de varios Nodos SIMACET V5¹.

De este modo evitamos los largos periodos de tiempo previos a la maniobra, en los que el personal de la Unidad se dedica a la correcta preparación de los Nodos y acreditaciones necesarias para cada ejercicio.

Con este trabajo se pretende alcanzar la sustitución del actual sistema de despliegue de CTPC por el nuevo, consiguiendo una mayor eficiencia en el despliegue de los CTPC en un menor tiempo de preparación.

1.2. Estructura de la memoria

Esta memoria se estructura en 6 capítulos diferenciados. Comenzamos con la *Introducción*, es la primera toma de contacto con la temática del proyecto. En este capítulo se recogen los objetivos y el alcance del proyecto. El segundo capítulo, *Conceptos teóricos básicos*, habla de los conocimientos y definiciones básicas que se han

¹ Sofisticados equipos virtualizados con gran capacidad para procesar información.

de conocer a la hora de hablar de información clasificada, y de los medios y procedimientos para poder trabajar con ella. Gracias a esta información se entrará en contexto para la posterior comprensión del trabajo. El tercer capítulo, *Modelo de despliegue anterior*, da a conocer el método de despliegue que se seguía hasta el momento y que se pretende sustituir por el Nuevo Concepto. El cuarto capítulo, *Desarrollo del Nuevo Concepto de despliegue de un centro de transmisiones en un entorno OTAN*, es la base fundamental de este TFG donde se describe en detalle la propuesta realizada para mejorar los procedimientos de despliegue, incluyendo una comparativa con el modelo anterior. En el quinto capítulo, *Práctica*, se evaluarán las diferentes pruebas que se han llevado a cabo durante la realización de las maniobras realizadas en la unidad para valorar el Nuevo Concepto y las mejoras que conlleva. Por último, en el sexto capítulo, *Conclusiones*, se exponen las conclusiones alcanzadas después de la realización del TFG.

2. Conceptos teóricos básicos

En los siguientes apartados se va a tratar la información básica para entender los motivos del desarrollo de este TFG. En primer lugar, se explicará el concepto de información clasificada y qué tipo de personal puede acceder a ella. Después se hará un resumen de los diferentes tipos de seguridad que habrá que tener en cuenta a la hora de conseguir una acreditación de seguridad para trabajar con material clasificado, algo necesario al trabajar en un entorno OTAN, con otras naciones, en el cual la información transmitida será clasificada. Por último, se indicará el procedimiento requerido para conseguir las diferentes acreditaciones de los CIS.

2.1. Información clasificada

Se entiende por información clasificada cualquier material o documento que no puede ser divulgado libremente, y lleve asignado un grado de seguridad (ver [2]).

- Información clasificada nacional: Es la generada por los órganos del Estado y clasificada por el Centro Nacional de Inteligencia (CNI), órgano competente para ello.
- Información clasificada internacional: Es la generada por organismos u organizaciones internacionales en los que España participa como país miembro como por ejemplo la OTAN, la Unión Europea (UE) y la Agencia Espacial Europea (ESA), debido a esto se establecen acuerdos de seguridad para cada una de ellas. Por ello, se establece la existencia de una institución en cada país miembro, denominada Autoridad Nacional de Seguridad (ANS), que será la responsable del cumplimiento de las medidas de protección y seguridad en cada país.

La Tabla 1 recoge las distintas nomenclaturas dadas a los diferentes niveles de información según el ámbito: Nacional, europeo u OTAN.

Nacional	Unión Europea	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

Tabla 1. Guía de equivalencias entre grados de información².

El apartado 2.4 recoge más información sobre el proceso de acceso a información clasificada del personal.

2.2. Seguridad de la información

La definición de Seguridad de la Información (SEGINFO) regida por la Norma Técnica 04/11 es la siguiente: “El conjunto de procedimientos, recursos y actividades encaminadas a la protección adecuada, proporcionada y razonable de la información contra actos hostiles, así como contra pérdidas o revelaciones no autorizadas mediante la preservación de sus requisitos básicos de seguridad” (ver [3]). Estos requisitos básicos de seguridad son:

- **Confidencialidad:** Se entiende como el requisito mínimo de seguridad para garantizar que solo las personas o entidades autorizadas accedan a la información.
- **Integridad:** Sirve para verificar la autenticidad de la información, garantizando que no ha sido modificada por personal no autorizado.
- **Disponibilidad:** Permite el acceso a la información y a los recursos que la manejan.
- **Autenticación:** Se utiliza para validar una transmisión, un mensaje o a una persona, para acceder a un servicio con alguna categoría de información.
- **Negativa al repudio:** Entendida como la garantía de que el receptor de la información la ha recibido y no puede negar dicho hecho.
- **Trazabilidad:** Garantiza conocer en todo momento quien ha realizado algún cambio.

La SEGINFO se alcanza al estipular un conjunto de medidas y procedimientos para el adecuado uso de la información, así como para identificar las posibles incidencias que puedan afectar para su correcta confidencialidad, integridad o disponibilidad.

La información que maneja el Ejército de Tierra (ET) se protege de manera proporcional al nivel de clasificación y criticidad de dicha información. La autorización para el acceso a la información clasificada del ET se proporciona según el concepto de “necesidad de conocer”, entendiéndose como: “la determinación de forma positiva de que una entidad o individuo necesita acceder, conocer o poseer información en orden

² Fuente de la Tabla: Elaboración propia.

a realizar una tarea o servicio oficial”³, y siempre que el personal disponga de la Habilitación Personal de Seguridad (HPS) correspondiente. La SEGINFO se puede dividir en (ver [3] [4]):

- Seguridad de la información en las personas (SEGINFOPER): Su finalidad es garantizar que las personas que acceden a determinada información cumplen con los requisitos para ello.
- Seguridad de la información en los documentos (SEGINFODOC): Tiene la finalidad de garantizar la seguridad de la información de los documentos, para permitir su confidencialidad e integridad.
- Seguridad de la información en los sistemas de información y telecomunicaciones (SEGINFOSIT): Tiene por finalidad establecer los protocolos de seguridad y las normas que faciliten la integridad y confidencialidad de la información.
- Seguridad de la información en las instalaciones (SEGINFOINS): Tiene como función el garantizar la seguridad, integridad y disponibilidad de la información en las instalaciones.
- Seguridad de la información en poder de las empresas (SEGINFOEMP): Todas las empresas ya sean nacionales o internacionales que manejen información clasificada deberán tener un acuerdo de seguridad.

Debido al constante crecimiento de la información en la sociedad, esta se convierte en un factor muy importante para cualquier tipo de organización. Por desgracia este avance en los CIS también está acompañado por un incremento en los riesgos. Los posibles riesgos a los cuales se puede enfrentar la información pueden ser de diferente índole, desde posibles averías en los componentes o uso incorrecto de los usuarios, hasta medidas de seguridad inapropiadas o acciones intencionadas de sabotaje o terrorismo.

El mayor aumento de estas vulnerabilidades también se debe en gran medida a que (ver [3] [4]):

- Cada vez hay un mayor número de usuarios y por ello aumentan los posibles enemigos.
- Los medios para atacar los CIS están al alcance de cualquiera.
- La dependencia de la sociedad cada vez mayor en los medios CIS.

Es por todo ello que la seguridad en los CIS es fundamental para lograr los objetivos de cualquier unidad del Ejército de Tierra. Puesto que la total seguridad es inalcanzable, las medidas SEGINFO se mejoran hasta alcanzar niveles óptimos de seguridad.

³ Instrucción Técnica 04/03 “Protección de la información clasificada OTAN en el Ejército de Tierra. Funcionamiento de un órgano de control OTAN”.

2.3. Seguridad de las comunicaciones

Se entiende por Seguridad de las Telecomunicaciones (COMSEC), a aquella que se ocupa específicamente de la información referente a las comunicaciones que emplean la transmisión por medio de señales.

Para alcanzar el mayor nivel de seguridad en las telecomunicaciones, se diferencian dos tipos de medidas a adoptar (ver [4]):

- Seguridad de la Transmisión (TRANSEC): Son las medidas que se ocupan de impedir una posible interceptación enemiga.
- Seguridad Criptológica (CRIPTOSEC): Son un conjunto de medidas físicas colocadas en los equipos y material por el cual circula la información, con el objetivo de codificar la información.

2.4. La seguridad física y del personal

Se establece una seguridad en las instalaciones y en el personal que maneja la información clasificada para proteger la documentación y equipos clasificados ante posibles pérdidas o accesos de personal no autorizado.

La seguridad en las instalaciones implica la implantación de medidas de seguridad en los edificios donde se maneje dicha información como pueden ser cámaras de vigilancia o una alambrada perimetral. Es decir, se requieren unas instalaciones con un perímetro definido en las que exista un control y unas condiciones específicas de seguridad. Dependiendo del tipo de protección podemos distinguir entre Zonas de Acceso Restringido (ZAR) o Zonas Administrativas de Protección.

Todos los locales donde exista hardware o software normalmente con grado superior a confidencial han de ser definidos como ZAR. Estas instalaciones deben de ser formalmente acreditadas, y según niveles OTAN se pueden clasificar en (ver [2] [4]):

- CLASE I: Zonas donde se instalan los cifradores, enrutadores y servicios de sistemas clasificados. Se tomarán las medidas adecuadas para que el acceso a este material esté cerrado y con vigilancia, permitiendo el acceso únicamente al personal autorizado, el cual estará indicado en una lista visible. El personal, aún teniendo concedida la HPS, no podrá acceder si no tiene la “necesidad de conocer”. El oficial de SEGINFOSIT será el encargado de permitir el acceso a personal que no esté reflejado en la lista como autorizado. El Nodo Permanente del Nuevo Concepto de despliegue sería una instalación Clase I.
- CLASE II: Lugares donde los administradores hacen uso de sus terminales y donde se encuentran los centros de transmisiones, con acceso vigilado y restringido, siendo posible acceder solo si se dispone de la HPS y se tiene la “necesidad de conocer”; en caso de no disponer de alguna de las anteriores condiciones se le proporcionará escolta, para de esta manera evitar el acceso no autorizado a la información. Quedará prohibido el uso de teléfonos móviles en el interior de los centros de transmisiones, solo siendo posible mediante previa autorización el uso de móviles oficiales, cuyo modelo y software está controlado.

Un ejemplo de instalaciones Clase II en el Nuevo Concepto serían los CT de los Nodos Desplegables.

No existe una expresa relación entre ambas clasificaciones y el grado de protección de información que aportan. Simplemente se diferencian en las condiciones de accesibilidad a dicha información clasificada dentro de cada zona.

En las Zonas Administrativas de Protección sólo se manejará información difusión limitada. Estas zonas no necesitan ser oficialmente acreditadas, pero sí que se tendrá un control sobre ellas. Por ejemplo se deberá tener un control en la puerta de acceso, deberá contar con alarmas en el perímetro y deberán poseer mobiliario adecuado para guardar la información (ver [2]).

Las zonas Clase I y II han de superar las medidas Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) o material electrónico de telecomunicaciones protegido frente a las emisiones de emanaciones espurias, es decir, la prevención de las emisiones no deseadas. Entendemos por emisiones no deseadas las radiaciones eléctricas y magnéticas que producen de forma involuntaria los equipos CIS y otros componentes que pueden no parecer un riesgo, como los monitores, microprocesadores e impresoras. Estas señales generadas pueden ser origen de información en caso de ser interceptadas por personal no autorizado. Las medidas TEMPEST tienen por finalidad eliminar estas emisiones generadas involuntariamente, o por lo menos, controlar los posibles efectos perjudiciales. Para ello estas medidas se centran en el aislamiento o apantallamiento electromagnético de los elementos radiantes o a la ubicación en la que se encuentran (ver [5]).

La seguridad del personal está enfocada en controlar las personas que tengan acceso a la información clasificada; para ello en primer lugar se deberá comprobar que todo el personal tenga la HPS en vigor.

Con esta habilitación de seguridad la Autoridad Nacional de Seguridad (ANS), en nombre del Gobierno de España, autoriza a una persona al acceso a información clasificada. Los diferentes niveles de habilitación son (ver [2] [6]):

- Cosmic top secret: Para niveles de información cosmic top secret e inferior.
- NATO secret: Para niveles de información NATO secret e inferior.
- NATO confidential: Para niveles de información NATO confidential e inferior.

La posesión de una de estas habilitaciones no es la única condición que debe cumplir el personal para acceder a este tipo de información. Debe darse además la “necesidad de conocer”. Será el jefe de la UCO (Unidad, Centro y Organismo) o el jefe del Estado Mayor (EM) de una Gran Unidad (GU) quien acredite la necesidad de conocer mediante el documento de Solicitud de Habilitación Personal de Seguridad (SHPS) (ver [6]).

Para solicitar la HPS para el uso de información clasificada se deben cumplir los siguientes requisitos (ver [6]):

- Complimentar SHPS, incluyendo la firma del superior jerárquico que acredita la necesidad de dicha acreditación. El Anexo A muestra el formulario a rellenar.
- Rellenar la Declaración Personal de Seguridad (DPS) del formulario DPS-101, recogido en el Anexo B. Se compone de varias páginas de información personal

del solicitante, que posteriormente estudiará y analizará el órgano autorizado, en este caso el CNI.

- Una vez recibidos los documentos anteriores se seguirán las siguientes fases:
 - Investigación de antecedentes e idoneidad del solicitante.
 - Remisión del expediente a la ANS.
 - Resolución de la ANS.
 - Comunicación de la denegación o concesión de la HPS, con fecha de inicio y de caducidad.

Además de estar en posesión de la HPS, el personal debe cumplir unos requisitos en cuanto a confiabilidad y discreción. Estas medidas concretas se recogen en la norma correspondiente a SEGINFOPER (ver [7]).

Algunas de las medidas de seguridad a tener en cuenta son (ver [2] [4]):

- Los usuarios CIS deberán tener la HPS correspondiente al mayor grado de clasificación de la información que vaya a manejar.
- Se establecerán controles de acceso de personal no perteneciente al sistema (personal de mantenimiento o limpieza).
- Se realizará un control y registro de todo el personal que entre en los locales con los sistemas CIS.

Tanto la seguridad física como la del personal son indispensables para que la SEGINFO pueda desarrollarse de manera adecuada (ver [4]).

2.5. Acreditación de sistemas

Se entiende por acreditación de seguridad a la autorización dada a un CIS para manejar información clasificada hasta un cierto grado. Dado que todo lo que maneje información clasificada debe de ser acreditado, hace de este un proceso complejo y caro. Además, todos los ejercicios o despliegues de la UT han de ser acreditados, lo que supone un esfuerzo en la planificación temporal de los mismos.

Según las diferentes necesidades de las unidades y de los requerimientos del ejercicio se podrá optar por un tipo de acreditación de seguridad o por otro (ver [4]):

- Autorización Temporal para Operar (ATPO): Es la forma más usual para la realización de ejercicios, debido a que no pueden someterse al proceso completo.
- Autorización para Operar (APO): Se concede para sistemas en proceso de acreditación pero que aún no lo hayan superado entero.
- Acreditación: Situación final, una vez superado todo el proceso.

Para conseguir la acreditación son necesarios los siguientes documentos (ver [4] [8]):

- Concepto de Operación del Sistema (COS): Documento en el que se establece cual será la función del sistema, el tipo de información que manejará y las

posibles incidencias que tenga. Dicho documento se encuentra regulado en el CCN-STIC 207⁴.

- Análisis de Riesgos (AR): Proceso en el cual se estima el riesgo que puede sufrir dicho sistema. Se regula con el CCN-STIC 206⁵.
- Declaración de Requisitos de Seguridad (DRS): Basado en el AR, se establecen las medidas de seguridad a tomar para prevenir dichos riesgos. Este procedimiento está regulado por el CCN-STIC 202⁶.
- Procedimientos Operativos de Seguridad (POS): Determina las medidas de seguridad que se estipulan en el sistema y los procedimientos para llegar hasta ellas. Regulado por el CNN-STIC 203⁷.

Siguiendo las instrucciones que muestra la guía CCN-STIC 101, la Tabla 2 muestra la documentación que es necesaria para realizar la petición de acreditación, dependiendo del nivel de seguridad que necesitemos.

	SECRETO/RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Concepto de Operación (COS)	SI	SI	SI
Análisis de Riesgos (AR)	FORMAL	FORMAL	NO FORMAL
Declaración de Requisitos de Seguridad (DRS)	SI	SI	OPCIONAL
Procedimientos Operativos de Seguridad (POS)	SI	SI	SI
Declaración de Acreditación de Seguridad	SI	SI	SI

Tabla 2. Documentación de seguridad en los sistemas⁸.

Dependiendo del nivel de información que tenga la documentación, existen diferentes periodos de validez de la acreditación (ver [4]):

- Para sistemas con clasificación reservado o secreto un máximo de 3 años.
- Para sistemas con clasificación confidencial un máximo de 5 años.
- Para sistemas con clasificación de difusión limitada un máximo de 7 años.

Durante este periodo los sistemas podrán ser inspeccionados para comprobar el mantenimiento de las condiciones de seguridad establecidas. El periodo máximo entre inspecciones será (ver [4]):

- Para sistemas clasificados como reservados o superior un máximo de 18 meses.
- Para sistemas clasificados como confidencial máximo de 3 años.

⁴ No se muestra en la bibliografía por ser de acceso restringido.

⁵ No se muestra en la bibliografía por ser de acceso restringido.

⁶ No se muestra en la bibliografía por ser de acceso restringido.

⁷ No se muestra en la bibliografía por ser de acceso restringido.

⁸ Fuente de la Tabla: Elaboración propia.

- Para sistemas clasificados hasta difusión limitada máximo de 4 años.

Según el resultado de la inspección, se podrá proponer la implantación de medidas correctivas y el plazo para solucionarlas, en caso de no cumplirlas ocasionará la pérdida de la acreditación y con ello la prohibición para el uso de información clasificada. Además, puede ser necesaria una reacreditación en caso de cambio de hardware/software, o al verse afectada la seguridad del sistema.

2.6. Procedimiento para solicitar una acreditación

La Ilustración 2 muestra el proceso de acreditación de un sistema. Este proceso es complicado y requiere de bastante tiempo para ser concedido. Previo a la concesión será necesario pasar una Verificación Técnica de Seguridad (VTS) (ver [4][5]).

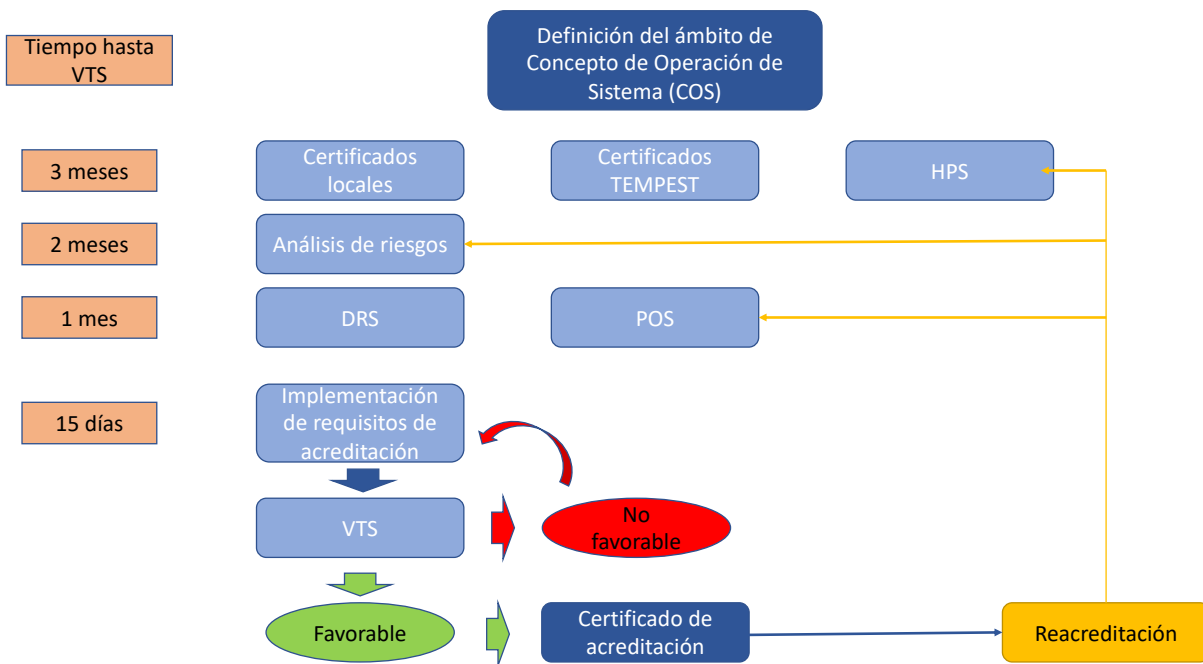


Ilustración 1. Proceso completo para obtener una acreditación de seguridad.⁹

A continuación se detalla el proceso completo (ver [9]):

- 1ª fase: Redacción del COS. Aceptación de la Jefatura de los Sistemas de Información y Telecomunicaciones y Apoyo Técnico (JCISAT) e inicio del proceso de acreditación.
- 2ª fase (3 meses): Envío de la documentación relativa a los certificados del local y de TEMPEST junto a los relativos al personal que trabajaría con dicha acreditación. Para ello, todo el personal deberá tener la HPS en regla. JCISAT lo revisará.

⁹ Fuente de la Ilustración: Elaboración propia.

- 3ª fase (1-2 meses): Envío del AR, DRS y POS. JCISAT revisará toda la documentación.
- 4ª fase (1 semana): JCISAT podrá realizar una VTS que, en caso de ser favorable, conllevará la propuesta de la concesión de acreditación; de no ser favorable se deberán corregir los errores y repetir el proceso.
- Cuando se precise la reacreditación, se deberán revisar todos los documentos tanto de personal como de local, así como elaborar un nuevo DRS y POS.

3. Modelo de despliegue anterior

Para mostrar la problemática de los procedimientos de despliegue y acreditación usados actualmente, en esta sección se describe el modelo que el RT21 está utilizando basado en la doctrina en vigor.

3.1. Los Centros de Transmisiones

Los Centros de Transmisiones se pueden clasificar según su funcionabilidad o el apoyo CIS que prestan (ver [5]):

- De Puesto de Mando (CTPC): Aquellos que aportan unos servicios a los usuarios finales de un puesto de mando.
- Destacados (CTD): Asignados a ciertos grupos de usuarios para permitir el acceso a la red táctica principal cuando se requieren de medios de los que no se dispone en dotación. De carácter fijo o temporal.
- Nodales (CN): Son los que constituyen la base de la arquitectura de la red táctica principal.
- De Acceso Radio (CTAR): Aquellos en los que se dan los Puntos de Acceso Radio (PAR) por los cuales, se proporciona a los usuarios radio móviles autorización para el acceso a los servicios de la red táctica principal.

3.2. Áreas de un Centro de Transmisiones

Por razones de trabajo y seguridad, se establece la creación de diferentes zonas en los centros de transmisiones, las cuales son (ver [5]):

- Área de explotación: Donde se encuentran los medios principales para el mando y control, así como los medios CIS no radiantes.
- Área hertziana: Formada fundamentalmente por los elementos radiantes del CT (estaciones radio, terminales satélites, radioenlaces, etc.) cuyo funcionamiento puede suponer la localización del centro, con el riesgo que ello supone para la seguridad física.
- Área de vida: Donde se despliegan los elementos de vida y servicios del CT.

3.3. Procedimiento de configuración y despliegue

El proceso de despliegue y configuración requerido para establecer un nodo acreditable se divide en varias partes, en esta sección se detallará la forma de proceder del RT21 (ver [10]).

En primer lugar, hay que tener en cuenta que el despliegue de un CT debe realizarse según 3 áreas bien diferenciadas: Área Hertziana, área de explotación y área de vida (definidas en el apartado 3.2). Además de dichas áreas también se debe establecer un aparcamiento en las inmediaciones del centro para colocar los vehículos.

Se empieza estableciendo la configuración del área Hertziana, radio y satélite, con los servicios de voz que de ella dependen. En caso de que tenga lugar una maniobra OTAN debe acreditarse la red, siguiendo los requisitos establecidos por la Federated Mission Network (FMN), que se describe en el apartado 3.4. Esta acreditación la realiza el Centro Criptológico Nacional (CCN). Para obtener dicha acreditación, es necesario una maqueta de la red con 3 meses de antelación. Una vez se consigue la acreditación, el sistema ya está en disposición de desplegar en el ejercicio OTAN que corresponda.

También se tiene que tener en cuenta a la hora de desplegar, que cada CT debe contar con personal autosuficiente para resolver cualquier incidencia de administración de los CIS, dado que nadie ajeno al CT tiene la posibilidad de gestionar remotamente dicho centro.

Cuando se despliega más de un CTPC se debe establecer un Centro de Control y Coordinación de los Sistemas CIS (CISCC), cuyas funciones se limitan a controlar y coordinar a estos CT de forma exclusiva.

Por otro lado, cada nodo trabaja en un dominio diferente lo que hace que la administración de estos sea compleja, debido al nivel de maniobras que se realizan en el Regimiento. Además, cada nodo SIMACET tiene su propia capa virtual, lo que conlleva que entre nodos no se comuniquen estas capas. Esto hace inviable una administración realmente centralizada y remota.

3.3.1. Conexión de los equipos

En primer lugar, se realizan las conexiones de los servidores, clientes y equipos de electrónica de red como por ejemplo los switches o routers. También es necesario el marcado de todos los cables de interconexión y reflejarlos en el apéndice de trazabilidad, necesario para la acreditación.

En esta fase también es necesario realizar el Tampering, es decir, la colocación de etiquetas anti-manipulación, en todos los equipos que puedan ser susceptibles de ser manipulados por personal ajeno (ver [10]).

3.3.2. Creación de máquinas virtuales e instalación de clientes

Una vez conectados todos los equipos, se configura la capa virtual con la creación de las máquinas virtuales del vCenter¹⁰ y Domain Controller¹¹ o Controlador de Dominio (DC) de capa virtual, que proporcionará el entorno del resto de máquinas y servicios, junto con los switches virtuales para la gestión de Vlan¹² (Virtual Local Area Network).

Una vez finalizado, se procede a crear el resto de las máquinas virtuales que alojan los servidores necesarios para la maniobra en función de los servicios que hay que ofrecer para el ejercicio. A su vez, paralelamente se pueden crear tantos clientes como sean necesarios (ver [10]).

3.3.3. Aplicación de políticas de seguridad

Con todos los equipos de electrónica de red desplegados y configurados y una vez instalados los servidores y clientes, hay que proceder a aplicar las políticas de seguridad necesarias para estar en disposición de obtener la acreditación. Para ello son de obligado cumplimiento las STIC (Seguridad de Tecnologías de la Información y las Comunicaciones) que se pueden consultar en la pagina web del CCN¹³. Dichas STIC están ordenadas por familias según el ámbito de aplicación; en este caso se consultan las STIC de la familia 500, pertenecientes a sistemas Windows, y hacen referencia a casi todos los elementos del sistema (servidores, clientes, switches, routers, etc.). Estas guías de seguridad son de obligada aplicación para poder manejar información clasificada, ya que establecen las configuraciones mínimas de seguridad de los elementos que se basan en tecnología Windows. Es por ello que deben aplicarse antes de solicitar la acreditación correspondiente.

En lo referente a la electrónica de red, la aplicación de estas políticas se traduce en segurización de los puertos switch, listas de acceso, puertos cerrados en firewall, etc.

Para terminar, es necesario comprobar que se dispone de la última versión de los sistemas operativos de todos los dispositivos de la red, así como, todas las actualizaciones de Windows en los equipos de usuarios y administradores (ver [10]).

3.3.4. Aplicación de políticas incrementales

Una vez aplicadas las STIC es necesario comprobar que todos los servicios que se ofrecen funcionan correctamente. En caso de que se presente alguna dificultad será necesario crear políticas incrementales de seguridad para asegurar la funcionalidad del sistema de información. Para que el sistema siga siendo acreditable hay que

¹⁰ Es la utilidad de administración centralizada para VMware y se usa para administrar máquinas virtuales y todos los componentes dependientes desde una ubicación centralizada.

¹¹ Su responsabilidad es la de garantizar o denegar el acceso de un usuario a recursos compartidos o a otra máquina de la red, para ello se suelen utilizar contraseñas.

¹² Método que permite crear redes independientes, dentro de una mis red física.

¹³ www.ccn-cert.cni.es/gl/.

documentar qué políticas incrementales se han aplicado junto con una justificación. Un ejemplo de aplicación de políticas incrementales se recoge en el Anexo C (ver [10]).

3.3.5. Auto-auditorías

Una vez que el sistema está completamente configurado y desplegado es conveniente utilizar alguna herramienta para evaluar la seguridad de este. Para ello, se hace uso de las herramientas Clara¹⁴ y Nessus¹⁵, que evaluarán al completo todos los equipos y máquinas virtuales en busca de posibles errores de configuración, ausencia de aplicación de medidas de seguridad o presencia de software y sistemas operativos desactualizados. Dichas herramientas son las usadas por la autoridad acreditadora. De esta manera se podrán solventar dichos problemas, de cara a la auditoria oficial, o al menos poder justificar el error (si este no es subsanable).

Además, se revisará toda la documentación necesaria que se remitirá a dicha autoridad en busca de posibles errores con la configuración presentada y se documentarán los diferentes procedimientos que se llevarán a cabo en materia de actualizaciones, control de dispositivos USB o renovación de licencias (ver [10]).

3.3.6. Borrado de servidores

Una vez finalizado el ejercicio, los administradores de los Nodos Desplegables serán los encargados de borrar todo el contenido de estos. De esta manera, los nodos se guardan completamente vacíos de información.

3.4. Federated Mission Network

La Federated Mission Network (FMN) son una serie de requisitos¹⁶ que establece la OTAN y firman los países pertenecientes al tratado, con los cuales se pretende apoyar al mando y control, facilitando la toma de decisiones mediante un intercambio de información mucho más fluido entre los países que pertenecen a la coalición. Sin el establecimiento de estos requisitos un sistema no se puede conectar a la red OTAN; por lo tanto, no podría participar en Ejercicios de ámbito internacional (ver [11] [12]).

El concepto principal de la FMN es la interoperabilidad entre naciones, ya que intenta mejorar las comunicaciones entre Puestos de Mando, obteniendo de esta manera una mayor eficiencia a la hora de tomar decisiones.

Se entiende por Mission Network (MN) la red que se crea en cada misión y que proporciona las capacidades necesarias para un ejercicio. Consta de 3 elementos distintos (ver [13]):

¹⁴ Herramienta para hacer auditorias de seguridad acordes al esquema nacional de seguridad. No se adjuntan ejemplos dado que son de acceso restringido.

¹⁵ Programa que escanea vulnerabilidades de los diferentes sistemas operativos, ya sean por falta de actualización o por fallos de software, además es capaz de encontrar errores de configuración. No se adjuntan ejemplos dado que son de acceso restringido.

¹⁶ Recogido en los manuales FMN Spiral 1.

- Mission Network Element (MNE): Se basa en un sistema CIS perfectamente compatible con OTAN, que contiene una infraestructura de información y redes capaces de mantenerse en funcionamiento de forma autónoma, sin necesidad de apoyo de otro centro. Dicho sistema debe de ser capaz de proporcionar servicios OTAN a unidades subordinadas.
- Mission Network Extension (MNX): Se basa en un sistema CIS subordinado a un MNE. Es capaz de autoabastecerse, pero no puede ofrecer los mismos servicios que un MNE. Dicho MNX no requiere el mismo nivel de cumplimiento de FMN que un MNE. Se suele utilizar como elemento destacado para cubrir unos servicios menores.
- Hosted Users: Elemento adicional que se utiliza para labores específicas con unos servicios limitados, tanto para MNE como MNX.

La Ilustración 3 muestra un posible esquema de despliegue de una red FMN. En la que se pueden observar los distintos elementos que la conforman.

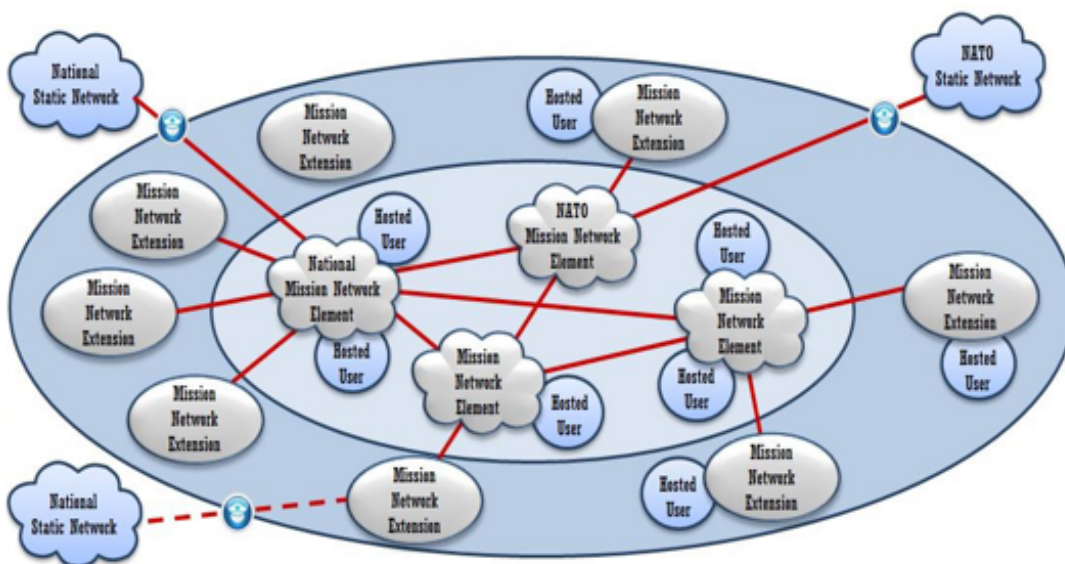


Ilustración 2. Esquema de una Mission Network¹⁷.

Para la supervisión de la Mission Network y para evitar conflictos entre participantes en la red, la FMN marca imprescindible poseer un Service Management Authority (SMA) en cada centro. En caso de cualquier tipo de error en la red se avisará inmediatamente al SMA. En un despliegue del ET esta figura equivaldría a un jefe de centro, por ejemplo un teniente.

La ventaja de estar en una red FMN es el establecimiento de una red plana, es decir, todos los centros de transmisiones se encuentran en el mismo nivel. Esto es una variación importante ya que anteriormente en cada ejercicio OTAN se establecía una organización jerárquica, donde todos los servicios de todos los países dependían lógicamente y físicamente de un organismo central. Con FMN, todos los centros CIS, incluido el de

¹⁷ Fuente de la Ilustración: Manual FMN Spiral 1.

OTAN, están al mismo nivel desde un punto de vista lógico lo cual facilita la gestión de las comunicaciones (ver [13]).

3.5. Órganos de trabajo de los CIS

Para remarcar la complejidad relativa a la instalación de un servidor para un despliegue de CT se detalla a continuación los distintos elementos CIS requeridos para que sea operativo y acreditable.

Se pueden dividir los elementos CIS en 3 áreas muy diferenciadas, según su uso y capacidades CORE, COMMS y Functional Services. Cada uno de estos elementos requiere de administradores con experiencia para su instalación (ver [14] [15]) .

3.5.1. CORE

- DOMINIOS

Todo sistema de telecomunicaciones e información esa formado por un conjunto de elementos que se agrupan en:

- Dominio de usuario, el cual comprenden todos los recursos de los CIS desplegados en las zonas de los usuarios y controladas por ellos mismos, lo cual les permite manejar la información según ellos la necesiten.
- Dominio de red, es el que comprende todos los recursos en lo referente a las telecomunicaciones, que mediante una gestión centralizada proporciona los servicios necesarios a los usuarios.

- DNS

El diseño, planificación y configuración de la arquitectura Domain Name Server o Sistema de Nombres de Dominio (DNS) es un elemento fundamental para que las aplicaciones funcionen correctamente. Se configuran zonas para su optimización y los DNS raíz son los de OTAN.

- MAIL

El correo interpersonal se basa en topologías de servidores Exchange Server, y es un medio de mensajería informal.

- LYNC

Es una aplicación de mensajería instantánea y videoconferencia. Utiliza el mismo usuario de Windows. Esta aplicación también nos permite conectarnos con la Unidad de Control Multipunto o Multipoint Control Unit (MCU)¹⁸ de videoconferencia agregando en el propio cliente la dirección de la sala MCU.

¹⁸ Es un dispositivo de red al que se conectan los usuarios que quieren participar en la video conferencia.

- WSUS

Los servidores de actualizaciones WSUS (Windows Server Update Services) se utilizan para las actualizaciones de seguridad de Windows. Se distribuyen de manera jerárquica y requiere de una conexión a internet ya que existen actualizaciones diarias.

- KMS

Permite las licencias de los diferentes sistemas de información (aplicaciones) en una red local sin la necesidad de conectarse a Microsoft.

- MCAFEE EPO

El servidor McAfee EPO (Epolicy Orchestrator) es el encargado de gestionar la seguridad informática de los clientes y servidores de la red. Los servidores EPO al igual que pasa con los servidores WSUS reciben actualizaciones según una topología jerárquica.

- POLITICA BACKUP

Procedimiento basado en el clonaje de las máquinas virtuales gestionado por el VCenter de la plataforma de VMWare. El servidor de backup no esta redundado, por lo que en caso de fallo el nodo no dispondría del servicio de backup, aunque podría seguir trabajando sin él.



Ilustración 3. Servidor de Backup nodo SIMACET v5.

- DIRECTIVA DE SEGURIDAD

La configuración de seguridad del sistema se ha realizado conforme a la serie 500 de las guías STIC del CCN. La aplicación efectiva de las STIC, sobre todo la aplicación de las directivas de grupo debe ser planificada, coordinada y controlada a alto nivel. Se debe evitar en la medida de lo posible la administración de directivas por personal inexperto en la materia.

- AIMS

Es una aplicación para la mensajería oficial y pre formateada. Se configura los clientes por medio del Outlook. Para utilizar AIMS en los clientes desplegados, los servidores de correo tienen que tener conexión con la red de OTAN. La configuración de AIMS se suele localizar centralizada en su servidor de ficheros o servidores Exchange.

- SINCRONIZACIÓN DE TIEMPOS

El servidor de tiempos NTP¹⁹ (Network Time Protocol) sincroniza con el servidor de tiempos OTAN de forma jerárquica. Deben aislarse el tiempo de los servidores virtuales ya que, en caso contrario, sincronizan la hora de la BIOS²⁰ (Basic Input-Output System o sistema básico de entrada/salida) de los servidores físicos.

- NAMING CONVENTION

El naming convention son las directrices que se deben seguir a la hora de crear los usuarios y de los atributos que tiene que tener cada uno.

3.5.2. COMMS

- SOPORTES

Los soportes de transmisión dan la continuidad a los terminales. Con ello, se permite la recepción de la información mediante la propagación de energía. En un soporte se pueden encontrar uno o varios canales dependiendo de las transmisiones que necesite.

- RED

Las redes son el componente material fundamental para el funcionamiento de un sistema de telecomunicaciones, ya que proporciona los servicios de telecomunicación e información entre diferentes posiciones. Las redes las podemos clasificar según su topología, según el servicio que prestan y según su finalidad.

- VOIP

El desarrollo de la tecnología de voz con protocolos de internet, VoIP (Voice on Internet Protocol), permite que la calidad de las señales de audio digitales sea superior y accesible desde cualquier cliente de una red.



Ilustración 4. Terminal CISCO CP 7821²¹ y Firewall ASA 5520²².

¹⁹ Protocolo de internet que se utiliza para sincronizar los relojes de los sistemas CIS a través del enrutamiento de paquetes en redes.

²⁰ Es un chip localizado en la placa base encargado de guardar la configuración inicial del ordenador.

²¹ Fuente de la Ilustración: <https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7821/model.html> (consultado 14/10/2018).

²² Fuente de la Ilustración: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-24-switch/model.html> (consultado 14/10/2018).

- QOS

La calidad de servicio o Quality of Service (QoS), es el promedio en cuanto al rendimiento de una red visto desde el punto de vista de los usuarios de dicha red. Comprende los requisitos en todos los aspectos de una conexión, como por ejemplo el tiempo de respuesta de los servicios, las pérdidas o el ruido en la señal.

Con la calidad del servicio lo que obtenemos es la capacidad de proveer diferentes prioridades a cada aplicación, usuario o dato, para garantizar un correcto nivel de flujo de información.

- FIREWALL

Un firewall o cortafuegos es un sistema de seguridad de la red, desde donde se controla la información entrante y saliente y decide si esa información puede ser dañina para la red y debe ser bloqueado, es una política de seguridad entre varios dominios. Es por esto por lo que debe de ser el único punto físico común entre los distintos dominios de seguridad.

- VTC

La videoconferencia o video teleconferencia (VTC), es un sistema interactivo entre varios puntos capaces de transferirse simultáneamente en ambos sentidos señales de video y audio. Mediante la utilización de videocámaras o cámaras web y micrófonos.

3.5.3. FUNCTIONAL SERVICES (FS)

Existen innumerables funciones, pero en este apartado solo se hará referencia a las principales (ver [15]).

- ANTARES (SIMACET)

La definición recogida en el manual del ET es la siguiente "El Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) permite a los Cuarteles Generales, Estados Mayores de las Divisiones y Brigadas (Grandes Unidades) y a las Planas Mayores de Mando de los escalones de Regimiento, Grupo Táctico, Batallón o Grupo (Pequeñas Unidades), planear, gestionar, controlar y dirigir las operaciones, así como obtener una visión coherente y homogénea del campo de batalla de todos los Puestos de Mando en tiempo operativo."²³

Entendemos como nodo al conjunto de medios hardware y software, capacidades, personal y procedimientos. Los nodos se caracterizan por disponer de una Base de Datos Táctica (BDT) que facilita la interacción con los otros nodos. Al conjunto de varios nodos con los procedimientos de intercambio de información entre ellos, es lo que llamamos la red SIMACET.

Los objetivos que se pretende obtener con SIMACET son entre otros: La alta supervivencia del sistema, una visión común del campo de batalla, mensajería fiable y alta movilidad para los usuarios (ver [15] [4] [5])

²³ Mando de adiestramiento y doctrina: "Empleo de la unidad de transmisiones de la brigada".

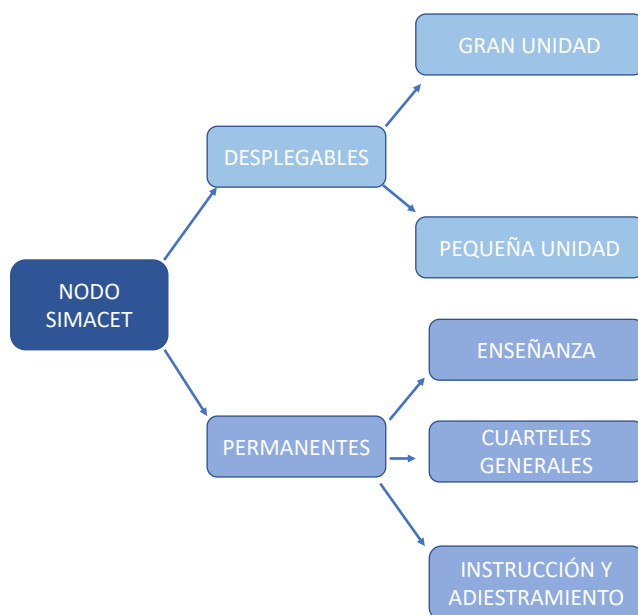


Ilustración 5. Clasificación nodos SIMACET²⁴.

- IGEOSIT

El sistema IGEOSIT (Interin Geospatial Intelligence Tool) es una herramienta web con acceso a un sistema geográfico de información, del que se pueden obtener mapas topográficos, imágenes satélite, etc.
- SQL

Los gestores de bases de datos SQL²⁵ (Structured Query Language), tienen una gran importancia en el despliegue del sistema ya que son la base de otras aplicaciones que se sirven de las bases de datos que son generador en los servidores de bases de datos.
- SHAREPOINT

Es una de las herramientas más empleadas por los usuarios, es una pagina web donde los usuarios pueden colgar y descargar contenidos, con el propósito de eliminar la utilización de las carpetas compartidas. Funciona sobre SQL.
- JCHAT

La aplicación JCHAT (NATO Join Tactical Chat) es una herramienta ampliamente utilizada por el usuario, es un tipo de mensajería instantánea entre usuarios. Se gestiona mediante la creación de salas y el login²⁶ coincide con el de Windows.

²⁴ Fuente de la Ilustración: Elaboración propia.

²⁵ Lenguaje de programación, diseñado para la administración de los sistemas de gestión de bases de datos, permite ordenar, agregar y eliminar nuevos registros.

²⁶ Es el proceso utilizado para controlar el acceso a un sistema informático mediante la identificación de usuario y contraseña.

- LOGFAS

La aplicación LOGFAS (Logistic Functional Area Services) se basa en la réplica de bases de datos logísticas. Al manejar un gran volumen de información puede provocar que en ocasiones la carga deba de hacerse local.

- TOPFAS

La aplicación TOPFAS (Tool for Operational Planning, Force Activation and Simulation) es una herramienta OTAN para el apoyo al planeamiento, desarrollo y evaluación de operaciones.

- JOCWATCH

Es una aplicación que se utiliza para obtener una visión global de los diferentes tipos de eventos e incidentes que ocurren en una operación. Algunas de sus informaciones funcionan a través de las salas de Jchat.

- ARCGIS

Es un servidor cartográfico que proporciona cartografía de manera centralizada a una gran variedad de aplicaciones. La topología consiste en un servidor ArcGis localizado en cada emplazamiento que da servicio de cartografía a las aplicaciones de manera local, esto es muy recomendable debido al tamaño de los mapas.

La carga de la cartografía se puede hacer tanto vía web como por un script²⁷. Una vez que se termina la carga la cartografía aparece publicada como servicio web.

- JOIIS

Aplicación donde el usuario añade información sobre unidades, posicionamiento, etc. La información generada en JOIIS (Joint Ops/Intel Information System) es mostrada en las capas solicitadas en IGEOISIT.

4. Desarrollo del Nuevo Concepto de despliegue de un Centro de Transmisiones en un entorno OTAN

La idea básica del Nuevo Concepto desarrollado en este TFG es establecer un procedimiento que permita disponer de varios nodos permanentemente acreditables y preparados para desplegar rápidamente y en cualquier momento. El objetivo es reducir el periodo actual necesario para configurar los CIS (fundamentalmente los sistemas basados en los nodos SIMACET v5). La composición del sistema se basa en la configuración de distintas máquinas virtuales cuya misión es proporcionar todos los servicios que requiere el usuario OTAN. La virtualización de los servicios implica una rápida configuración, evitando los largos procesos de instalación. En un entorno de desastre permite la fácil recuperación de los datos en poco tiempo y tiene la ventaja de establecer un único dispositivo físico para varios recursos lógicos.

²⁷ También llamado archivo de órdenes o guion, es un programa cuyo uso habitual es realizar diversas funciones como combinar componentes y trabajar con el sistema operativo o con el usuario.

Por tanto, el Nuevo Concepto se basa en la creación de una infraestructura permanente en la UT, denominada Nodo Permanente. Este Nodo Permanente estará gestionado por un grupo de administradores con alta preparación técnica y provista de varios nodos SIMACET v5 y se dedicará a la administración de un Nodo de Referencia donde se virtualizarán todos los servicios requeridos por los usuarios OTAN en los distintos despliegues. Estos nodos virtualizados se denominan Nodos Desplegables. Así, tanto los medios de administración, centralizados en el Nodo Permanente, como los medios desplegados, podrán ser acreditables en todo momento. El personal del Nodo Permanente realiza la planificación y administración remota de los medios desplegados, mientras que los Centros de Transmisiones (CT) se limitarán al despliegue del Centro de Transmisiones de Puesto de Mando (CTPC). Dicho de otra manera, un CTPC debe acudir con su Nodo Desplegable al Nodo Permanente para volcar la configuración de su Nodo en cuanto a securización y actualizaciones y de esta manera estar en condiciones de desplegar. La Ilustración 6 recoge una maqueta de un Nodo Permanente.

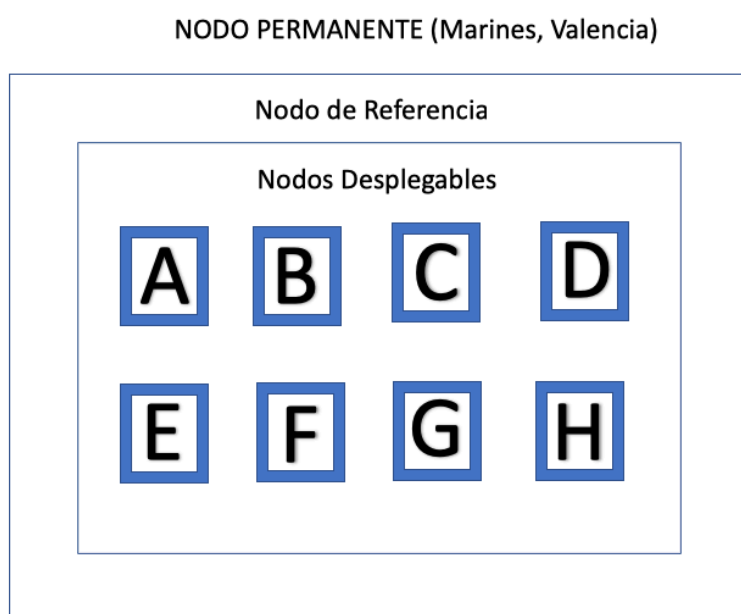


Ilustración 6. Posible estructura del Nuevo Concepto de despliegue.²⁸

El Nodo de Referencia, deberá cumplir los requisitos que se enumeran a continuación (ver [2]):

- Estar virtualizado. No es técnicamente un requisito, pero el ahorro económico que supone el evitar la adquisición de servidores físicos y el mantenimiento es sustancial.
- Tener conexión a internet.
- Ser acreditable en todo momento.
- Ser capaz de proporcionar la configuración para extender los servicios necesarios a los CTPC desplegados.

²⁸ Fuente de la Ilustración: Elaboración propia.

- Tener administradores con un alto nivel de preparación técnica, dado el alto nivel de complejidad que requiere el correcto conocimiento y manejo del nuevo Nodo de Referencia.
- Instalaciones adecuadas (refrigeración, seguridad de accesos, sistemas de alimentación, etc.).
- Los Nodos Desplegables deben poder desplegarse eficientemente (rapidez y seguridad).
- Establecer un único dominio, que facilite la administración y configuración.

Mediante el uso de la virtualización el Nodo de Referencia tiene capacidad para dar servicio a 8 Nodos Desplegables. A nivel software los servicios que ofrecen están virtualizados, de esta manera si falla uno de los servicios no afecta al resto, pudiendo ser restaurado en un tiempo menor.

Con la virtualización se obtienen grandes ventajas como son (ver [16]):

- Ahorro en costes de servidores físicos.
- Aislamiento: Cada máquina es independiente por lo que el fallo de una de ellas no afecta al resto.
- Flexibilidad: Se puede crear máquinas virtuales con las características del CPU, memoria, etc. que necesitemos, sin tener que comprar.
- Agilidad: La creación de una máquina virtual es muy rápido.
- Seguridad: Cada máquina tiene un acceso independiente por lo que el ataque a una de ellas no afecta al resto.

Se describe a continuación el concepto de máquina virtual y el de hipervisor, fundamentales para entender las técnicas utilizadas en el despliegue del Nuevo Concepto (ver [17] [18]).

▪ **Máquina virtual**

Se pueden dividir según las funcionalidades y características de la máquina entre máquinas virtuales de hardware (de sistemas) o máquinas virtuales de proceso (de aplicación).

Las máquinas virtuales de hardware son las que funcionan paralelamente sobre un ordenador físico llamado "host" o anfitrión, de esta manera se utilizan los recursos físicos del ordenador. Son máquinas muy útiles ya que permite que coexistan varios sistemas operativos en un mismo ordenador.

Las máquinas virtuales de proceso tienen la misión de conseguir la portabilidad del código mediante la separación del código fuente de un programa del código máquina que depende del hardware.

El Ejército puede utilizar cualquiera tipo de máquina virtual, pero en estos momentos en el RT21 se utiliza Windows server 2012, al disponer de licencias comerciales del mismo.

▪ **Hipervisor**

Es un visor de máquinas virtuales que automáticamente se pone en funcionamiento durante el arranque. En el Ejército se utiliza VMware esxi 6.5. Con el

hipervisor se consigue identificar, captar y manejar las operaciones de la CPU (Central Processing Unit o unidad central de procesamiento) e instrucciones dadas por las máquinas virtuales.

El procedimiento de configuración y despliegue del nuevo Nodo de Referencia es análogo al descrito en el Apartado 3.3, pero con la salvedad de que con el Nuevo Concepto solo se necesitará realizar todo el proceso una sola vez: Una vez configurado el Nodo de Referencia se mantendrá activo, sin tener que borrarlo al finalizar cada ejercicio como se hace actualmente. Esto supone un ahorro de tiempo y trabajo sustancial en la preparación de una maniobra.

Además, el Nodo de Referencia debe seguir los requisitos FMN, vistos en el Apartado 3.4, para poder conectarse y participar en una red OTAN.

El procedimiento para realizar el despliegue de un CTPC con el Nuevo Concepto es el siguiente (ver Ilustración 7): Para proceder al despliegue de un CT, los administradores del Nodo Desplegable acudirán al Nodo Permanente. Allí los administradores del Nodo de Referencia, a través de un disco duro entregarán las máquinas virtuales ya preparadas para el ejercicio. Al finalizar la maniobra, devuelven el disco duro al Nodo de Referencia. Puede suceder que durante un despliegue de larga duración, salga una actualización de Windows y se necesite actualizar para seguir acreditado. En este caso, a través de otro disco duro se introducirá el WSUS actualizado en el Nodo Desplegable para de esta manera no perder la acreditación.

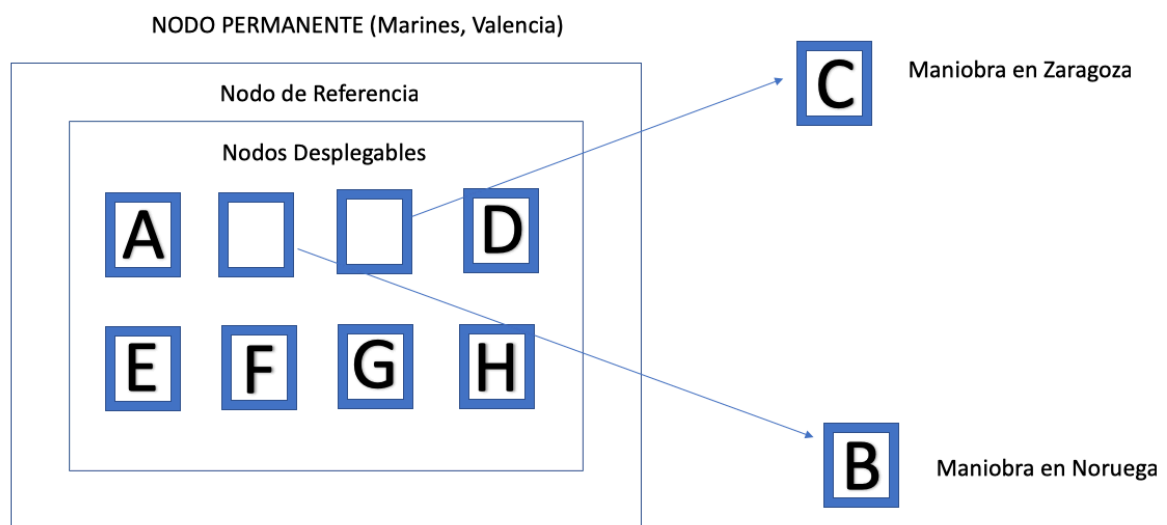


Ilustración 7. Ejemplo de posible ejercicio de Nodos Desplegables²⁹

4.1. Comparativa entre el sistema anterior y el actual

Con el estudio realizado durante el presente TFG se han podido identificar una serie de diferencias entre el modelo de despliegue anterior y el nuevo que se quiere implantar. Las diferencias encontradas son las que a continuación se mencionan:

²⁹ Fuente de la Ilustración: Elaboración propia.

- La principal diferencia radica en el tiempo empleado para acreditar la red. Anteriormente cada Nodo Desplegable preparaba su maniobra y para ello necesitaba 3 meses de antelación a su inicio para conseguir la acreditación. Con el nuevo Nodo de Referencia se consigue que en una instalación, el Nodo Permanente, se centralicen todos los Nodos Desplegables, continuamente acreditados. De esta manera se logra ahorrar meses de trabajo en la preparación de ejercicios.
- Con respecto al personal, la mayor diferencia radica en que en el anterior método de despliegue cada nodo debía contar con personal preparado técnicamente para solucionar cualquier tipo de incidencia. Esto era inviable puesto que no se dispone de tanto personal con esas características. Con el nuevo sistema el personal especializado se encontrará en el Nodo Permanente, desde donde podrán gestionar los problemas de los Nodos Desplegables remotamente, limitando de esta manera las funciones de los administradores de dichos nodos.
- El Nuevo Concepto también establece el uso de un mismo dominio para toda la red. Gracias a ello la administración de todos los sistemas se hace mucho más sencilla.
- Por último, gracias a la implantación del nuevo concepto, la gestión de cada nodo sigue el mismo procedimiento, evitando así que los administradores de los Nodos Desplegables trabajen de maneras diferentes.

En resumen, con la implantación del nuevo concepto, se conseguirá desplegar los CT de una manera más fluida, reduciendo el tiempo y el trabajo. Además, al estar todo el proceso centralizado el despliegue será más eficiente.

5. Práctica

Durante el ejercicio DEPLOYEX 18 desarrollado durante la primera quincena de septiembre en el NRDC-ESP HQ (NATO Rapid Deployable Corps Spain Headquarters/ Cuartel General Terrestre de Alta Disponibilidad) en Bétera (Valencia), se han podido realizar pruebas sobre el Nuevo Concepto de despliegue de CTPC acreditado permanentemente en una red OTAN. Se han obtenido unas conclusiones y unas propuestas de mejora que se evaluarán a continuación.

5.1. Antecedentes

Durante el pasado mes de mayo se realizaron las maniobras Valiant Lynx 18 (VL18), lideradas por el NRDC-ESP HQ, con la misión de adoptar una estructura de mando y control del ET desde el nivel de Cuerpo de Ejército o Brigada. Estas maniobras de ambiente multinacional permitieron medir y verificar el nivel de preparación para el combate de las unidades participantes.

El RT21 desplegó sus medios repartidos por toda la geografía española: San Gregorio (Zaragoza), Marines (Valencia), Chinchilla (Albacete) y Bétera (Valencia). Su

función era dar enlace tanto al Control Exercise o controlador del ejercicio (EXCON), como al CT de cuerpo de ejército y a los puestos de mando táctico, principal y móvil.

Durante el ejercicio VL18 las capacidades CIS fueron evaluadas y certificadas. Gracias a ello, se desarrollaron unas lecciones aprendidas que junto con la recomendación de optimizar la estructura de los puestos de mando del NRDC-ESP realizadas por el Mando del NRDC-ESP HQ, ha significado una reducción en el despliegue de los CTPC, es decir, una administración más centralizada y un menor número de personal desplegado. Para ello el G6³⁰ del NRDC-ESP HQ con el apoyo del RT21 desarrollaron un Nuevo Concepto de empleo del mando y control CIS.

5.2. Ejercicio DEPLOYEX 18

Durante la estancia que realizó el autor de este TFG en el RT21 se llevó a cabo el ejercicio DEPLOYEX18. Los objetivos establecidos para este ejercicio han sido:

- Desplegar un CTPC ICE con el Nuevo Concepto en el menor tiempo posible, como parte de la arquitectura CIS diseñada junto con el resto de las fuerzas propias.
- Establecer los servicios CIS requeridos por el NRDC-ESP HQ, basados en la arquitectura SIMACET V5.
- Adiestrar al personal del CTPC ICE para una activación rápida y eficiente, así como para testear permanentemente su activación.
- Comprobar las capacidades de mando y control de los sistemas CIS del CTPC ICE.
- Comprobar y certificar el Nuevo Concepto del Nodo de Referencia.

Con este ejercicio se ha conseguido que la administración principal se lleve desde el CTPC donde se encuentra el Nodo Permanente del RT21, teniendo el resto de CTPC capacidades más limitadas en cuanto a administración. En la centralización de la administración se incluye tanto la gestión de los servicios (Functional Services), como los servicios core (mensajería Exchange, SharePoint y los controladores de dominio). El ejercicio no necesitaba acreditación real ya que se trataba de un despliegue meramente táctico.

³⁰ Puesto que ocupa el encargado de los medios CIS del Ejercicio.

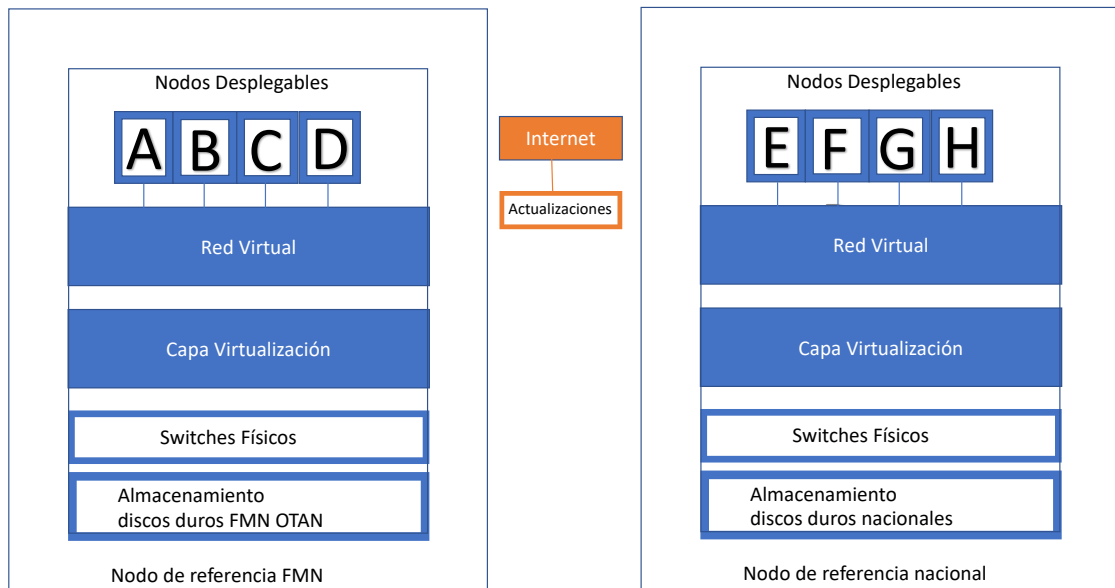


Ilustración 8. Nuevo concepto Nodos Permanentes ³¹.

En la Ilustración 8 se muestra la creación de dos Nodos de Referencia en el acuartelamiento General Almirante en Marines (Valencia), uno de ellos estará permanente disponible para ser utilizado en una red FMN para ejercicios internacionales y el otro estará preparado para ejercicios nacionales, ambos capacitados para dar servicio con 4 Nodos Desplegables (nodos A,B,C,D y E,F,G,H). Estos nodos tendrán conexión a internet lo que les asegurará tener siempre actualizados todos los servicios.



Ilustración 9. Nuevo concepto Nodo Desplegable ³².

³¹ Fuente de la Ilustración: Elaboración propia.

³² Fuente de la Ilustración: Elaboración propia.

Independientemente del tipo de ejercicio a realizar, ya sea nacional o internacional, el nodo que se despliega es un nodo virtualizado, como el mostrado en la Ilustración 9, que se encontraba en el Nodo Permanente. Como se puede observar este nodo tiene limitaciones con respecto a los Nodos de Referencia en cuanto a la administración de los usuarios, ya que lo que se pretende es que la gestión se realice desde el Nodo Permanente.

Durante el ejercicio DEPLOYEX18 se llevó a cabo el despliegue de dos ejercicios diferentes:

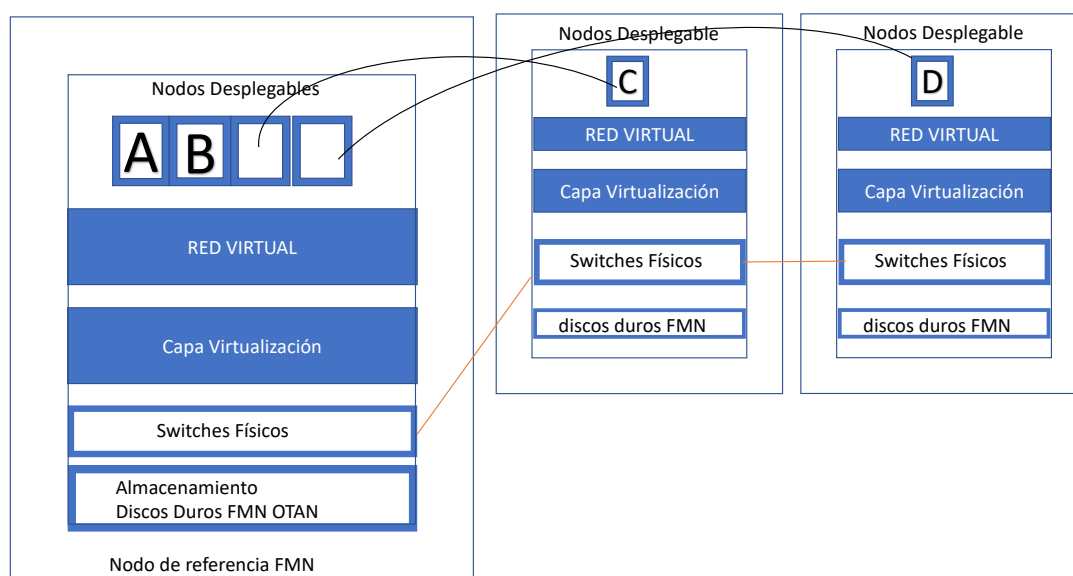


Ilustración 10. Ejemplo de despliegue en ejercicio multinacional sistema continuo ³³.

1. Con el primer despliegue mostrado en la Ilustración 10 se consigue una administración remota desde el Nodo Permanente, ya que se crea una red de comunicación a través de los switches, gracias a la cual los administradores del Nodo de Referencia gestionan todos los servicios. Únicamente se permiten unas mínimas opciones de gestión a los Nodos Desplegables. En este caso se trata de un ejercicio OTAN ya que cumple los requisitos de FMN.

³³ Fuente de la Ilustración: Elaboración propia.

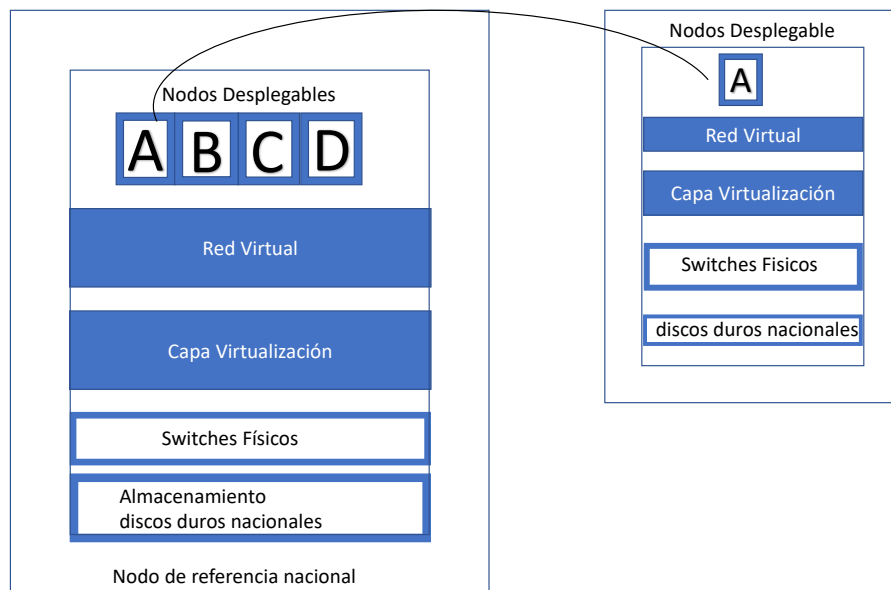


Ilustración 11. Ejemplo de despliegue en ejercicio nacional sistema discontinuo ³⁴.

2. El segundo despliegue mostrado en la Ilustración 11, se corresponde con una administración autónoma dentro de un ejercicio nacional con sistema discontinuo, es decir, no existe conexión con el Nodo de Referencia. Debido a esto, los administradores del Nodo Desplegable deben tener mayores privilegios de gestión.

Las pruebas realizadas durante este ejercicio han sido satisfactorias puesto que se han conseguido suministrar los servicios requeridos a los usuarios en un plazo de 1 semana y no con 3 meses de antelación como antes ocurría con el despliegue antiguo.

6. Conclusiones

Con este Nuevo Concepto de despliegue de los CT llevado a cabo por el RT21 se pretende una mayor rapidez y eficiencia a la hora de desplegar los CTPCGU, ya que todos los nodos se encontrarán centralizados en el Nodo Permanente, estando acreditados en todo momento.

La llegada de este nuevo modelo de despliegue no implica grandes cambios en cuanto a material (el necesario ya está a disposición del ET). Sin embargo, sí supone una completa reestructuración de la estructura orgánica y de los cometidos que hasta ahora estaban desarrollando los administradores de los nodos.

Como consecuencia de haber realizado el estudio del Nuevo Concepto de despliegue, de las maniobras DEPLOYEX18 y de las entrevistas realizadas a administradores de los diferentes nodos (recogidas en el Anexo D), se ha constatado que el sistema propuesto es viable y cumple con los objetivos marcados ya que ha conseguido dar servicios a los Nodos Desplegables remotamente.

³⁴ Fuente de la Ilustración: Elaboración propia.

La primera desventaja o limitación es la necesidad de dar una mayor protección de seguridad al Nodo de Referencia, debido a estar todo el sistema en el mismo dominio: Este podría verse afectado por un error de un administrador del dominio en uno de los Nodos Desplegables. Esto puede solventarse mediante la inclusión en la red de más dispositivos de seguridad (por ejemplo, firewalls), con la misión de proteger los diferentes sistemas de información del Nodo de Referencia. Su configuración sería específica para cubrir este fin.

Otra de las desventajas que se debe abordar es la organización y los nuevos cometidos que se asignarán a los administradores de los Nodos Desplegables, ya que sus privilegios a la hora de gestionar el nodo se verán reducidos con el Nuevo Concepto, siendo ahora el Nodo de Referencia quien se encarga de la mayor parte de la gestión.

Finalmente, se debe tener en cuenta que actualmente el personal del Regimiento es escaso, y para la correcta entrada en funcionamiento del Nodo de Referencia, cada Batallón deberá ceder al nodo a sus administradores más expertos. De esta forma se quedarán los Batallones con administradores delegados, pero en proceso de formación para adquirir mayores capacidades técnicas.

6.1. Líneas futuras

Para seguir con la evolución del Nuevo Concepto de despliegue, se establecerán nuevas maniobras con las mismas características que el ejercicio DEPLOYEX18, en las que se irá aumentando la complejidad de los servicios a desplegar. De esta manera, se podrá observar la evolución del personal para desenvolverse en dichos despliegues.

También se está estudiando un plan específico de instrucción y adiestramiento, para impedir que el personal del Nodo Desplegable se desmotive, dado que su papel ha perdido cierta importancia en el Nuevo Concepto de despliegue. Dicho plan incluye la formación en cursos específicos que, junto con la experiencia que se adquiere con la realización de maniobras en el RT21, les pueda hacer progresar en el futuro y optar a un puesto en el Nodo de Referencia. Con la realización de una encuesta al personal del RT21, que se puede consultar en el Anexo E, se ha llegado a la conclusión de que los cursos más importantes que deberían impartirse son SIMACET y Windows Server 2008 y 2012.

Además, los actuales administradores del RT21 están de acuerdo en decir que la experiencia en el manejo de los sistemas de información es lo más importante, y para ello son necesarios años de práctica.

Bibliografía

- [1] «Regimiento de Transmisiones 21» 2012. [En línea]. Available: <http://www.ejercito.mde.es/unidades/Valencia/rt21/Historial/index.html>. [Último acceso: 1 Octubre 2018].
- [2] Normas de la autoridad nacional para la protección de la información clasificada, Madrid: Ministerio de la Presidencia. Secretaria General Técnica-Secretariado del Gobierno-Centro de Publicaciones, 2016.
- [3] Norma Técnica 04/11 Seguridad de la información en los sistemas de información y telecomunicaciones (SEGINFOSIT) en el ámbito del Ejército de Tierra, Ministerio de Defensa, 2011.
- [4] PD4-500 Procedimientos operativos CIS, MADOC, 2013.
- [5] OR3-501 Sistemas de telecomunicaciones e información (CIS), MADOC, 2007.
- [6] Instrucción Técnica 04/03 Protección de la información clasificada OTAN en el Ejército de Tierra. Funcionamiento de un órgano de control OTAN., Madrid, 2003.
- [7] Norma Técnica 11/10 Seguridad de la Información de las Personas (SEGINFOPER), 2010.
- [8] CCN-STIC 001 política de seguridad de las TIC, Seguridad de las tecnologías de la información y las comunicaciones que maneja información clasificada en la administración, CCN, 2016.
- [9] CCN-STIC 101 acreditación de sistemas de las TIC que manejan información clasificada, CCN, 2016.
- [10] M. de la Vega, «Informe EXE TRITÓN Prueba Nº12» Valencia , 2018.
- [11] Federated Mission Network Spiral 1 Reference Architecture.
- [12] «Federated Mission Networking,» 26 2 2015. [En línea]. Available: <https://www.act.nato.int/fmn>. [Último acceso: 2018 10 14].
- [13] E. P. Piqué, «Implementación del concepto "Federated Mission Network" en el Ejército de Tierra», Trabajo Fin de Grado, CUD, 2016.
- [14] A. A. Moret, «Infraestructura de alta disponibilidad en redes desplegables», Trabajo Fin de Grado, CUD, 2017.
- [15] E. F. Cotillas, «Planeamiento CIS en ejercicios. Uso de SIMACET,» Valencia, 2018.
- [16] I. Martín, «Ventajas y desventajas de la virtualización» 23 Mayo 2008. [En línea]. Available: <http://www.techweek.es/virtualizacion/tech-labs/1003109005901/ventajas-desventajas-virtualizacion.1.html>. [Último acceso: 2018 Octubre 16].
- [17] «Administración de Sistemas Operativos,» [En línea]. Available: http://www.adminso.es/index.php/Virtualizaci%C3%B3n-Virtualizacion_en_sistemas_GNU/Linux. [Último acceso: 2018 10 14].
- [18] M. de la Vega, «Alternativas de software libre para la consolidación de servidores en unidades tácticas», Trabajo Fin de Grado, CUD, 2017.

[19] «CISCO» [En línea]. Available:
<https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7821/model.html>. [Último acceso: 14 Octubre 2018].

Anexos

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 posee 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 estales que añadan documentos al mismo, deberán anotarlos 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"**.

Anexo B. Declaración Personal de Seguridad

ESTE FORMULARIO DEBE SER CUMPLIMENTADO EXCLUSIVAMENTE POR EL INTERESADO					
 AUTORIDAD NACIONAL PARA PROTECCIÓN IC	 ONS <small>ORGANISMO NACIONAL DE SEGURIDAD</small> <small>ESPASA</small>	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: <input type="checkbox"/>		Segunda nacionalidad:		Tiene o ha tenido Habilitación Personal de Seguridad: <input type="checkbox"/>	
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:	
País:		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		

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: <input type="checkbox"/>	Segunda nacionalidad: <input type="checkbox"/>	Tiene o ha tenido Habilitación Personal de Seguridad <input type="checkbox"/>	Está aún en vigor: <input type="checkbox"/>
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 aproximadas)			
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: <input type="checkbox"/>) (Convive con el interesado en su domicilio habitual: <input type="checkbox"/>)			
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 <input type="checkbox"/>	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

MADRE o PROGENITOR "B" DEL INTERESADO (FALLECIDO: <input type="checkbox"/>) (Convive con el interesado en su domicilio habitual: <input type="checkbox"/>)			
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 <input type="checkbox"/>	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: <input type="checkbox"/>) (Convive con el interesado en su domicilio habitual: <input type="checkbox"/>)			
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 <input type="checkbox"/>	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: <input type="checkbox"/>) (Convive con el interesado en su domicilio habitual: <input type="checkbox"/>)			
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 <input type="checkbox"/>	Domicilio actual:	Lugar:	Provincia:
País:	Fecha desde la que reside en el domicilio actual:	Profesión o empleo:	

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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	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 <input type="checkbox"/>	Profesión, empleo u ocupación:	Estudios:

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.

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 Seguridad¹ 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 aplicación².

- 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

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.

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 aprovechar 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 triple 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 periodo 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 periodo 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 triple 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 procure, revele, falsee o inutilice información legalmente clasificada 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 concorra alguna de las circunstancias siguientes:

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

2ª. 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, falsee 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

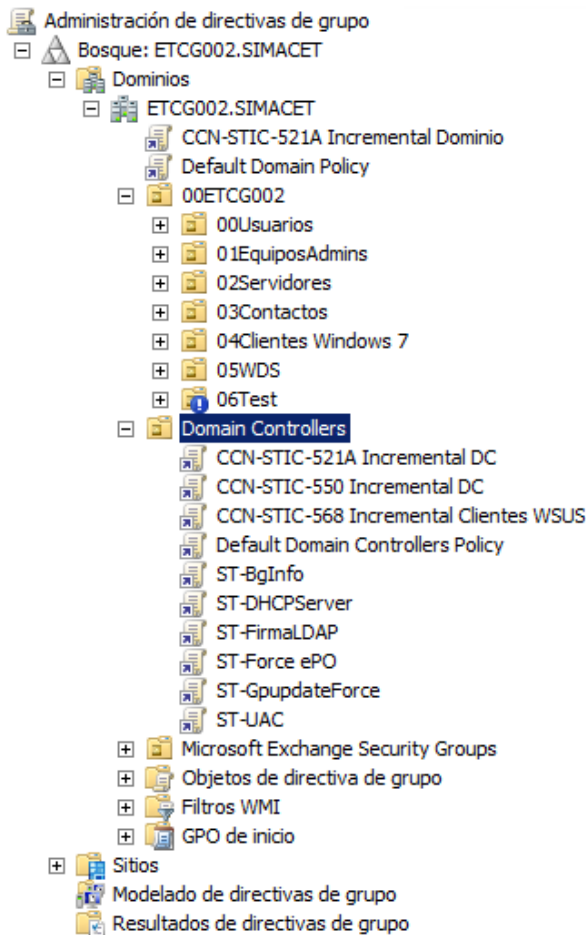
(Ley Orgánica 14/2015, de 14 de octubre)

Artículo 25. - "El extranjero que, en situación de conflicto armado, se procure, difundiera, falsee 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".

Anexo C. Aplicación políticas incrementales



Como podemos ver en esta imagen, para aplicar las políticas de seguridad al DC en primer lugar se han aplicado las políticas más restrictivas, es decir, las diferentes CCN-STIC y posteriormente se han añadido políticas incrementales como la Default Domain Controllers Policy que implica que los usuarios puedan instalar impresoras, o la ST-BgInfo que permite mostrar información sobre el equipo que se ejecuta (por ejemplo, la información que se muestra en el escritorio de los ordenadores).

Anexo D. Entrevista de administradores de nodo

Se ha entrevistado a personal tanto del Nodo de Referencia como del Nodo Desplegable realizando las siguientes preguntas:

Personal del Nodo Desplegable

1. ¿Qué cometidos tiene actualmente en el Nodo Desplegable?
2. ¿Qué cometidos tenía antes del Nodo de Referencia?
3. ¿En su opinión ha mejorado el concepto de despliegue de los CT con el nuevo Nodo de Referencia? ¿de qué manera?
4. ¿Qué se podría mejorar?

Respuesta Sgto. 1º M.O.L.

1. Administración de todos los nodos y sus máquinas tanto de CORE como de FAS.
2. Administrador delegada en maniobras de apoyo a otras unidades más pequeñas, el despliegue de toda la LAN y su configuración.
3. Sí que ha mejorado en el aspecto que vamos con los equipos probados y configurados, gracias a esto en el despliegue tenemos menos fallos y todo funciona más rápido.
Lo único malo es que al no poder tocar mucho en el sentido de no tener permisos, ya no somos los administradores, sino que somos administradores delegados dependientes de otras personas para resolver problemas.
4. La organización y la planificación es muy importante, así como saber cuales son los cometidos de cada uno.

Respuesta Sgto. H.C.R.

1. Administración delegada del dominio y la administración de las aplicaciones que no se pueden administrar de forma centralizada.
2. Administración del dominio y comunicación con los demás dominios a los que tenga que conectarse, además de la instalación y mantenimiento de todos los servidores.
3. Sí, evita los problemas que pueden surgir de que cada administrador tenga unas directivas en el dominio diferentes a las de los demás dominios, y las que se puedan producir por las relaciones de confianza entre dominios.
4. La organización y la definición de los cometidos para los administradores de los nodos desplegables ya que no todos los servicios deben de gestionarse de manera remota. Además solucionar problemas relacionados con directivas de seguridad afectarían a todo el dominio.

Personal del Nodo Referencia

1. ¿Qué cometidos tiene actualmente en el Nodo Referencia?
2. ¿Qué cometidos tenía antes del Nodo de Referencia?
3. ¿En su opinión ha mejorado el concepto de despliegue de los CT con el nuevo Nodo de Referencia? ¿de qué manera?
4. ¿Qué se podría mejorar?

Respuesta Administrador de CORE

1. Administrador CORE.
2. Administrador de sistemas en una Compañía. En ella tocaba todos los campos relacionados con sistemas. Ahora en el nodo te especializas más en un solo área.
3. Sí ha mejorado. Antiguamente cada administrador gestionaba su nodo “a su manera” y ahora se orienta a los administradores para trabajar de una manera más común.
4. Aparte de la falta de personal, haría falta una visión más global del Regimiento en el área de sistemas para que todos los administradores supieran cómo y de qué manera se gestionan los distintos nodos.

Respuesta Administrador de redes

1. Administrador de área voz IP y video.
2. Antes era administrador de redes y voz IP en la sección de redes de una Compañía.
3. Sí, al centralizar la mayor parte del trabajo más complicado de configuración de los nodos.
4. Intentaría mejorar el proceso de aprendizaje, ya que para llegar a ser especialista en uno de los campos se requiere demasiado tiempo, es por ello que falta personal especializado.

Anexo E. Encuesta administradores

Se ha realizado una encuesta a 6 de los administradores del Nodo de Referencia sobre los cursos que considerarían necesarios y de utilidad para poder trabajar con garantías de solucionar los múltiples errores que surgen en los Nodos Desplegables. Los resultados de dicha encuesta se recogen en la siguiente tabla:

CURSOS	PERSONAL QUE LO CONSIDERA NECESARIO
Windows server 2008 ³⁵	5
Windows server 2012	5
Exchange 2010	4
SQL 2008	4
Virtualización avanzada	4
CCNA ³⁶	4
EPO McAfee	3
SharePoint	2
SIMACET	6
LYNC	2
Power shell ³⁷	2

El personal que ha participado en la encuesta ha sido:

- Sgto. 1º M.O.L.
- Sgto. 1º D.C.T.
- Sgto. H.C.R.
- Sgto. Y.G.V.
- Sgto. L.D.M.
- Administrador redes.

Se ha de tener en cuenta que dependiendo del departamento en que se encuentre cada administrador aconsejarán un curso u otro. Pero los cursos de mayor importancia son los básicos que cualquiera debería tener para estar en el Nodo de Referencia.

³⁵ Son cursos que se desarrollan para obtener conocimientos sobre Windows en materia de virtualización, almacenamiento y redes.

³⁶ Cursos CISCO.

³⁷ Cursos de Scripts.