Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

"DISEÑO Y SECURIZACIÓN DE UN RACK DESPLEGABLE EN ZONA DE OPERACIONES"

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: D. DANIEL COSTA FORTEA

DIRECTORES: D. FERNANDO SUÁREZ LORENZO

D. NORBERTO FERNÁNDEZ GARCÍA

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

"DISEÑO Y SECURIZACIÓN DE UN RACK DESPLEGABLE EN ZONA DE OPERACIONES"

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Debido a la inestabilidad política que ha tenido lugar en Europa en los últimos años, la OTAN se ha visto obligada a desplegar múltiples equipos de seguridad y observación en el continente. Para que dichos equipos puedan cumplir la misión encomendada, se necesita disponer de una serie de servicios como son, Directorio Activo, impresión, aplicaciones, ficheros, DNS, DHCP, antivirus y correo, así como conexión a Internet y telefonía IP a través de satélite, aunque estos dos últimos no son objetivo de este proyecto.

La Jefatura CIS responsable de los despliegues españoles en la OTAN, ha determinado lo siguiente: para el correcto desempeño de la misión en zona de operaciones, una Comisión de Seguridad necesita disponer de todos estos servicios mediante satélite, para 20 usuarios en el momento inicial del despliegue, y para un máximo de 40 a posteriori si el destacamento lo solicita.

El presente trabajo trata de desarrollar un planeamiento previo de forma generalizada de los requisitos, arquitectura y montaje necesarios para ofrecer la conectividad requerida en los diferentes destacamentos. Como resultado, permitirá que en futuros despliegues, sólo se necesite la realización de modificaciones de pequeña índole, acorde con las especificaciones particulares de cada nuevo destacamento.

En definitiva, con la estandarización plasmada por escrito de los requisitos, arquitectura y montaje de un Módulo Desplegable con la acreditación del Centro Criptológico Nacional, la velocidad de despliegue de las redes de comunicaciones necesarias en los destacamentos se incrementa en gran medida. Además, también permite mejorar la calidad del servicio prestado, debido a las ventajas que proporciona la estandarización de la totalidad de redes telemáticas a desplegar en el futuro.

PALABRAS CLAVE

Conectividad, Virtualización, Estandarización, Escalabilidad.

Contenido

1 Introducción y objetivos 1
1.1 Justificación 1
1.2 Objetivos 2
1.3 Organización del documento 3
2 TRABAJOS RELACIONADOS 4
3 Desarrollo del TFM 6
3.1 Análisis de tecnologías y propuestas finales 7
3.2 Arquitectura 9
3.3 Desarrollo de la solución técnica 11
3.3.1 Componentes hardware 11
3.3.2 Configuración de los elementos físicos 12
3.3.3 Licenciamiento 13
3.3.4 Configuración lógica propuesta segun plantillas CCN-STIC 14
3.3.5 Plantillas CCN-STIC a aplicar 19
3.3.6 Software de las estaciones de trabajo (clientes) 21
3.4 Pruebas y validación 21
3.5 Normativa aplicable y calidad 23
3.5.1 El sistema de gestión de calidad y sus procesos 24
4 Securización de un rack desplegable 27
4.1 Descripción del sistema 27
4.1.1 Mision del sistema 27
4.1.2 Información manejada 27
4.1.3 Usuarios 28
4.1.4 Arquitectura del sistema 28
4.2 Definición de los requisitos de seguridad 28
4.2.1 Criticidad de la información manejada 29
4.2.2 Analisis y gestión de riesgos 29
4.3 Definición del entorno de seguridad 30
4.3.1 Control de Acceso 30
4.3.2 Identificación y autenticación 31
4.3.3 Registro 32
4.3.4 Auditoría 32
4.3.5 Reutilización de objetos 33

4.3.6 Integridad 33
4.3.7 Disponibilidad 34
4.3.8 Comunicaciones 35
4.3.9 Requisitos legales 37
4.3.10 Riesgos 38
5 ADMINISTRACIÓN DE LA SEGURIDAD 40
5.1 Gestión de la Seguridad 40
5.2 Gestión de la Seguridad 40
5.3 Procedimientos operativos de seguridad 40
5.4 Formación y concienciación 41
5.5 Gestión de incidentes 41
5.6 Acreditación / Re-acreditación 42
5.7 Baja de servicio 43
6 Validación 44
7 Conclusiones y líneas futuras 45
8 Bibliografía 48
Anexo I: PRESUPUESTO 50
Anexo II: Configuración del sistema 52

Índice de figuras

Figura 1 - Arquitectura diseñada para dar soporte a los diferentes servicios, Fuente: Elaboración propia 9
Figura 2 - Vista Física y vista lógica de los Servidores Anfitriones. Fuente: Elaboración propia...13
Figura 3 - Backup Servidor 2. Fuente: Elaboración Propia.....13
Figura 4 - Máquinas Virtuales alojadas en Host 1 y 2.Fuente Elaboración propia 15
Figura 5 - Distribución de las diferentes particiones en Disco 0. Fuente Elaboración propia 16
Figura 6 - Distribución de las diferentes particiones en Disco 1. Fuente Elaboración propia 17
Figura 7 - Distribución de las diferentes particiones en Disco 0. Fuente Elaboración propia 18
Figura 8 - Distribución de las diferentes particiones en Disco 1. Fuente Elaboración propia 19
Figura 9 - Zonning Fuente: Elaboración propia 37

Índice de tablas

Tabla 1 - Licencias Adquiridas.Fuente Ministerio de Defensa 14

Tabla 2 - Software instalado en los terminales de trabajo.Fuente.Elaboración propia 21

Tabla 3 - Documento de Validación de los diferentes procesos de pruebas del Módulo Desplegable.Fuente Elaboración propia 22

Tabla 4 - Matriz actividades vs responsables – Fuente: Elaboración propia 40

Tabla 5 - Comparación de los objetivos definidos y niveles alcanzados.Fuente.Elaboración propia 46

1 INTRODUCCIÓN Y OBJETIVOS

Este trabajo fin de máster tiene como objetivo fundamental el poder profundizar en el diseño y securización de la arquitectura de un módulo desplegable acreditable por el Centro Criptológico Nacional (CCN). Es así como este documento se caracteriza por ser más argumentativo y conceptual que práctico, aunque también involucra como elemento nuevo en el marco referencial la acreditación de seguridad. A continuación se describen cada uno de los diversos apartados fundamentales que se deben tener en cuenta para su elaboración.

En cuanto a la planificación y desarrollo de este trabajo comprende las siguientes fases:

1. Recopilación y estudio de la bibliografía básica necesaria para la realización del proyecto.
2. Diseño lógico de la arquitectura.
3. Implementación física de todos los componentes hardware, según lo determinado en el diseño lógico.
4. Instalación, configuración, securización y validación de los elementos que componen el módulo desplegable.
5. Elaboración de la memoria correspondiente justificando la realización del trabajo, detallando sus diferentes fases, proponiendo posibles mejoras e incluyendo las conclusiones obtenidas del trabajo realizado.

1.1 Justificación

La relevancia del presente trabajo se puede justificar atendiendo a la trascendencia que tienen las misiones de la OTAN en el continente europeo. Esto hace que dar una serie de servicios básicos a los usuarios finales en un tiempo mínimo, así como ofrecer conectividad a Internet y telefonía IP en zona

de operaciones, sea una de las prioridades fundamentales en cualquier despliegue que se realice dentro del marco de la OTAN, siendo indispensable para el correcto desempeño de la misión encomendada a cada destacamento.

Actualmente, la forma en la que se ejecutan los montajes de las redes telemáticas en los destacamentos, se realiza de un modo casi automatizado por el personal CIS perteneciente a la OTAN, en colaboración con el personal externo del ISP por satélite.

Esto tiene la ventaja de que dicho personal experimentado conoce las vicisitudes que tienen lugar, así como las necesidades existentes en los destacamentos. Por otro lado, tiene la gran desventaja de que en caso de que dicho personal abandone la organización, no se dispone de documentación al respecto, relativa a las instalaciones realizadas en los destacamentos. La experiencia en misiones de Afganistán, Mali, Irak, etc. indica que cada una de ellas ha sido diferente en el número de personas, pero sin embargo todas han sido muy semejantes en los servicios solicitados, lo que hace que los servidores se configuren siempre de la misma manera, cambiando sólo el ancho de banda para dar cobertura a más usuarios.

Esta forma de trabajar, implica la falta de documentación técnica, entre otros aspectos, sobre las necesidades de material y transporte para el despliegue de nuevas redes telemáticas.

1.2 Objetivos

El objetivo principal es diseñar, configurar y securizar un módulo desplegable completo (*rack*) utilizado por el Ejército Español tanto en misiones nacionales como en misiones internacionales, y cuya configuración cumple con las normas del CCN para la securización de redes.

Lo que se pretende implementar con este trabajo es:

a. Plasmar por escrito las necesidades genéricas que pueda requerir un módulo de despliegue de una red en una determinada misión.

b. Diseñar un módulo desplegable para posterior conexión a Internet a través de Satélite.

c. Dotar a la infraestructura de los elementos de red necesarios para poder dar servicio a cada destacamento.

d. Securizar el módulo desplegable.

Para poder conseguir todo esto es necesario acometer los siguientes pasos:

a. Investigar y desarrollar las necesidades genéricas de infraestructura de red, así como la logística necesaria para prestar los diversos servicios del destacamento.

b. Contratar un ISP por satélite en el continente donde se lleve a cabo el despliegue, así como realizar la búsqueda de proveedores para adquirir el material necesario en la instalación y montaje de la red.

c. Contratar el transporte logístico del material desde el territorio nacional, hasta el destino donde se va a desplegar.

d. Una vez contratado el ISP para obtener conexión a Internet por satélite, y tras la instalación de la antena receptora por parte del personal externo, se enlaza dicha señal al rúter de entrada del destacamento. Éste sirve la conexión al conmutador (*switch*), encargado de realizar la distribución de la señal al módulo desplegable y a las rosetas finales a su vez mediante el *patch panel*.

e. Configurar la securización del módulo desplegable.

1.3 Organización del documento

La descripción de los recursos necesarios para realizar el trabajo es el que se detalla a continuación.

1. Microsoft Word 2016

   Se utiliza para redactar los diferentes documentos que componen el presente proyecto.

2. Microsoft Excel 2016

   Se utiliza para realizar el presupuesto necesario para acometer el presente proyecto.

3. Aplicación Recortes de Microsoft Windows 2010

   Se utiliza para capturar las figuras que se incluyen en el presente proyecto.

4. Microsoft Project 2013

   Se utiliza para generar el diagrama de Gantt utilizado en la planificación.

5. Cisco Packet Tracer

   Se utiliza para desarrollar y reflejar gráficamente el mapa lógico de la infraestructura de red utilizada en el proyecto.

6. LibreCAD

   Necesario para el diseño del plano de planta del destacamento base a desarrollar en la fase de planeamiento, conforme a los requisitos facilitados por la Jefatura CIS de la OTAN.

2 TRABAJOS RELACIONADOS

El marco de trabajo que se describe, va a ser aplicado dentro del Ministerio de Defensa y concretamente en todas las misiones tanto nacionales como internacionales en las que el Ejército Español se encuentre implicado. Este mismo, provee la posibilidad de la puesta en práctica paulatina de un marco de referencia frente a un proceso indefinido e improvisado, en el que confluyen una metodología, un modelo de proceso, una colección de técnicas y herramientas recomendables para el despliegue de todos los elementos necesarios para dar diferentes servicios al destacamento, así como facilitar el camino para la implementación de un modelo de proceso integral, de mejora continua.

El Centro de Informática de Gestión (CIGES) va a ser el organismo encargado de gestionar todos los elementos necesarios para poder desplegar un *rack* modular en cualquier parte del mundo, junto a su personal altamente cualificado que se encuentran siempre con una disponibilidad de 24 horas. Ellos van a ser los responsables de equipar una superficie en "tierra de nadie" de una infraestructura básica para poder dar un servicio telemático a todos los usuarios del destacamento. Para ello es necesario conocer una serie de parámetros como puede ser el número de usuarios, situación geográfica etc., para poder hacer un análisis pormenorizado de todos los elementos hardware y software necesarios para poder levantar los diferentes servicios para poder cumplir con la misión.

Existen tres trabajos que hacen referencia a todo este tema. El primero de ellos lleva como título "*Hiperconvergencia: papel en la evolución de los centros de datos. Aplicación a los nodos de misión desplegables FMN-ESP",* el segundo de ellos titulado *"Presente y Futuro de los Nodos Desplegables. Estudio de la viabilidad de la tecnología HCI para albergar servicios clasificados/no clasificados de la OTAN a los nodos de misión desplegables"* y el último trabajo lleva de título "*Internet como canal de comunicaciones para redes clasificadas, posible solución versátil y segura para despliegues militares"* pero son mucho más específicos en sus contenidos. En todos estos temas en donde se exponen una

solución específica y segura a través de Internet para este tipo de despliegues o la viabilidad de la tecnología HCI para albergar servicios clasificados o no clasificados de la OTAN o bien aplicar hiperconvergencia en este tipo de nodos de misión, son respuestas muy específicas a este tipo de despliegue. Sin embargo, lo que se quiere exponer aquí es la base en que se fundamenta todas estas soluciones específicas como son el montaje y securización de un nodo desplegable a nivel conceptual.

3 DESARROLLO DEL TFM

A lo largo de la historia, las Fuerzas Armadas han realizado sus funciones en el exterior del territorio nacional. Actualmente este tipo de funciones fuera del territorio nacional están siendo claves en el desarrollo de pacificación y estabilización en países que necesitan algún tipo de colaboración armada.

Dentro del ámbito CIS/TIC la respuesta ante cualquier salida al exterior debe ser inmediata dando una serie de servicios en el mínimo tiempo posible. Esto motiva la necesidad de que el personal esté debidamente formado en su especialidad y tenga un documento por escrito en donde seguir las instrucciones básicas a la hora de realizar el primer montaje en cualquier parte del mundo con un número de personal bajo para poder hacer un primer reconocimiento “in situ”. Posteriormente aumentaríamos los servicios según las necesidades de la misión encomendada, así como el aumento de hardware y software ajustándolo al número de usuarios.

Las tareas a realizar son las siguientes:

1. Toma de requisitos.

Recogida de información necesaria para estimar la totalidad del material a utilizar, así como localizar y solventar las incidencias técnicas.

2. Requisitos de la red local.

Esta parte, incluye toda la infraestructura de red existente desde el rúter de entrada hasta las rosetas finales.

2.1. *Rack*

Armario de comunicaciones en el que se ubica la infraestructura de red.

2.2. *Rúter*

En este caso, sólo se utiliza un *rúter* en la entrada de la señal. Enlaza la señal proveniente de la antena receptora y la distribuye al conmutador.

2.3. *Conmutador*

Se utiliza un conmutador de 48 puertos, más que suficiente para recibir la señal proveniente del *rúter*, distribuir la señal al servidor y al *patch panel*.

2.4. *Patch panel*

Panel de cableado que da conectividad a las 20 rosetas iniciales.

2.5. Cableado

Elemento clave que interconecta toda la infraestructura de red y proporciona Internet a las rosetas, y a los terminales de usuario.

2.6. Canaletas exteriores

Elementos de protección por los que se despliega el cableado a instalar en el destacamento.

2.7. Rosetas

Elemento final de la red local, que permite conectar los terminales de usuario y dar conectividad a Internet.

3.1 Análisis de tecnologías y propuestas finales

En cuanto al análisis de la tecnología se va a dar una breve explicación del porqué se han elegido los diferentes productos en este módulo de despliegue y cuáles han sido las propuestas de las que se han partido.

En el mercado existen multitud de servidores en cuanto a marcas y características de cada uno de ellos. En principio, el Ministerio de Defensa en el año 2005 redujo el estudio a tres marcas de servidores que fueron HPE, Dell y FUJITSU. Obviamente las características más importantes que tenían que tener los servidores eran las extensiones de capacidad, tanto en discos duros, memorias, etc., que fueran una empresa líder a nivel mundial por varios motivos, uno de ellos sería para tener la posibilidad de encontrar elementos que se pudieran deteriorar dentro de un servidor, como son discos duros tipo Serial Attached SCSI (SAS), memorias, fuentes de alimentación etc., otro de los motivos sería tener un buen mantenimiento de todos y cada uno de los servidores a nivel nacional y también internacional donde estuvieran ubicados los mismos. Hay que tener en cuenta que estos servidores desplegables deben estar alojados en unos armazones reforzados, ya que donde se suelen ubicar son en zonas donde las

condiciones tanto físicas como de acondicionamiento no son las más propicias para un servidor y para la función tan importante que desempeña en los diferentes despliegues que hacen las FF.AA. en todo el mundo.

Por todo ello se eligió un servidor de la marca HPE, ya que Dell y FUJITSU no cubrían el mantenimiento en misiones internacionales y además eran menos estables en condiciones extremas. La primera de ellas era sensible a temperaturas elevadas en sus discos duros, y la segunda era sensible en la fuente de alimentación ya que con picos más o menos aceptables de tensión la fuente de alimentación se quemaba.

En cuanto al almacenamiento, podemos decir que existen dos grandes empresas que compiten por este sector: uno es HPE y el otro Dell. En el caso de módulos desplegables, tuvo mucha importancia la elección del servidor descrito anteriormente. En este caso, había una cierta predilección porque la marca del servidor fuera la misma que la del almacenamiento y, en condiciones de igualdad, como era el caso entre una empresa y otra, se eligió por HPE, simplemente por motivos de costes y mantenimiento.

Por otro lado las comunicaciones desde el punto de vista de los despliegues que se realizan tienen que tener una cualidad fundamental y es que tienen que ser seguras y lo más unificadas posibles. Existían en el mercado tres empresas que ofrecían sus servicios dentro del ámbito del Ministerio de Defensa que eran: Cisco, Enterasys y Unitronics. Esta última quedó descartada en un primer momento debido a los costes más elevados de sus productos de comunicaciones. Entre Cisco y Enterasys se ha decantado en módulos desplegables por la segunda principalmente porque las soluciones técnicas y de configuración son más simples, intuitivas y mejor documentadas que las de Cisco.

Por otra parte, la seguridad está compuesta por diferentes capas como pueden ser un cortafuegos (*firewall*), el antivirus, etc. que debe ser implementada para cualquier aplicación dentro del Ministerio de Defensa con unas garantías muy altas y esta condición sólo nos la podía administrar la empresa Enterasys con un contrato de confiabilidad entre las partes afectadas.

Por último, en cuanto análisis de tecnología tenemos la virtualización, pero aquí la elección está mucho más limitada ya que todas las licencias que compra el Ministerio de Defensa son de Microsoft y por tanto el software utilizado actualmente en cualquier módulo de despliegue es Windows Server 2016 R2. Por tanto, dentro la virtualización teníamos HyperV (Microsoft), VMWare y Citrix, obviamente se eligió el primero por las razones que expongo a continuación.

- HyperV es una plataforma de virtualización que puede funcionar bien como producto autónomo o bien como parte integrada de Windows Server.
- El coste total para la administración de HyperV es más bajo que el de las otras dos compañías.

- Con HyperV, el ahorro de los costes de virtualización es mayor que con VMWare y Citrix, además se puede hacer un uso óptimo de las inversiones de hardware del servidor mediante la configuración de varios roles del servidor por separado.
- Actualmente, esta plataforma es una de las que más capacidad tiene de ejecutar máquinas virtuales en una sola máquina física. Además, se pueden ejecutar eficientemente múltiples sistemas operativos, Windows, Linux y otros, en paralelo, en un solo servidor de Windows Server 2012 R2.

En resumen, debido a la escalabilidad, rendimiento y portabilidad de HyperV (Microsoft) fue la elección óptima como herramienta de virtualización en los módulos desplegables dentro de las FF.AA.

3.2 Arquitectura

La arquitectura sugerida es la que se muestra en la Figura 1 y que se describe a continuación.

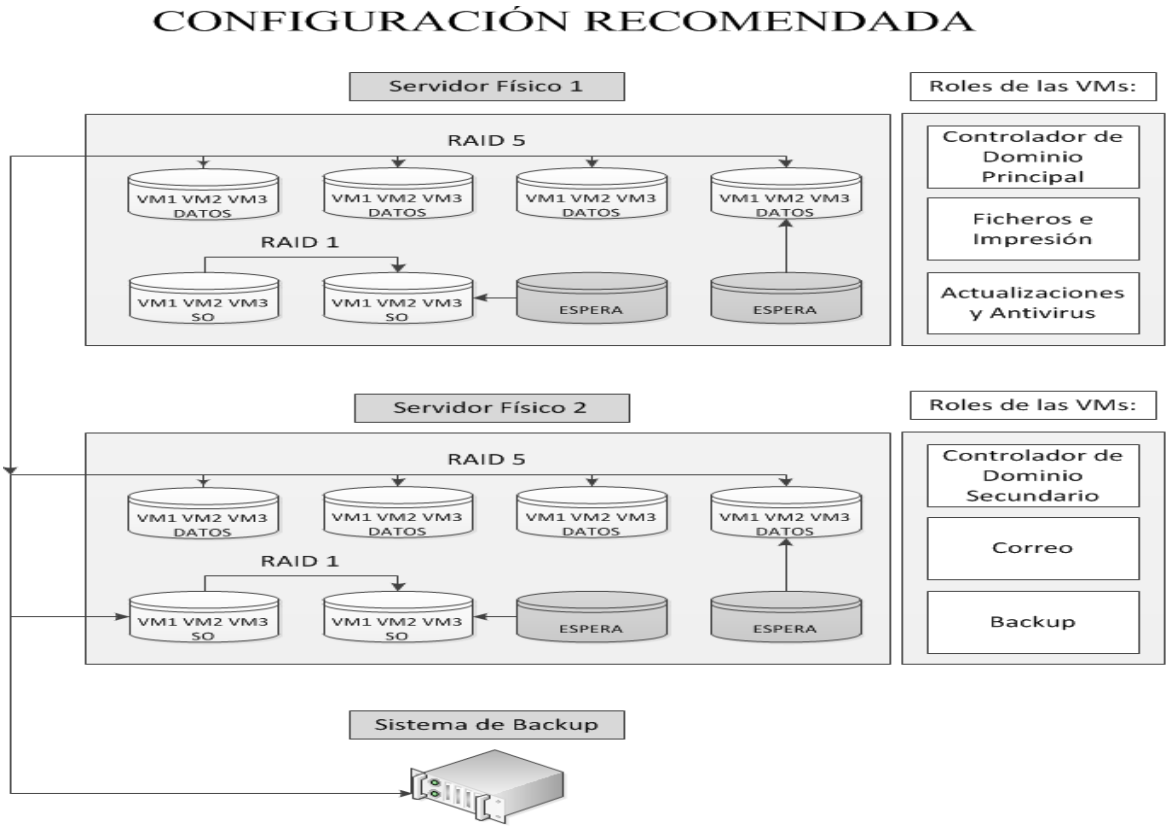

Figura 1 - Arquitectura diseñada para dar soporte a los diferentes servicios, Fuente: Elaboración propia

La arquitectura diseñada, se ha realizado teniendo en cuenta la necesidad de adquisición de la infraestructura mediante un procedimiento abierto, que requiere establecer unas condiciones técnicas en un Pliego de Prescripciones Técnicas (PPT), para poder crear una arquitectura eficiente que soporte los servicios que se quieren prestar.

Se compone de dos servidores físicos configurados como sigue:

Configuración física de los servidores:

- Cada servidor físico constará de 8 discos duros. Estos serán los encargados de alojar los servidores virtuales y la información manejada por cada uno de ellos.
- La disposición de los discos duros se realizará de la siguiente manera:
    - ✓ 3 discos duros configurados en RAID 1, con un disco de repuesto ante fallos. Estos discos deberán ser de altas prestaciones y velocidad de acceso.
    - ✓ 5 discos duros configurados en RAID 5, con un disco de repuesto ante fallos, destinados a alojar la información que manejarán todas las máquinas virtuales alojadas en el servidor físico.

Configuración lógica de los servidores:

- Cada servidor físico tendrá instalado localmente un Sistema Operativo (SO) anfitrión, que será el encargado de gestionar el funcionamiento de los servidores virtuales que se ejecuten sobre ese hardware.
- Cada SO anfitrión tendrá el rol de HyperV configurado.
- Cada servidor físico ejecutará 3 servidores virtuales que serán los encargados de dar servicio al despliegue.
- La disposición de los servidores virtuales será la siguiente:
    - En el servidor físico 1:
        - Controlador de dominio principal.
        - Servidor de ficheros e impresión.
        - Servidor de actualizaciones y antivirus.
    - En el servidor físico 2:
        - Controlador de Dominio secundario.
        - Servidor de correo.
        - Servidor de *backup*.
- La información que contendrán cada uno de los sistemas RAID de discos, existentes en cada uno de los servidores físicos, será la siguiente:
    - RAID 1: está destinado a alojar el sistema operativo anfitrión de los servidores físicos y todas las particiones de sistema de las máquinas virtuales que corran en ese servidor.
    - RAID 5: dedicado a alojar la información que manejarán todas las máquinas virtuales alojadas en el servidor físico.
- Se generarán distintas particiones de los RAID, con el fin de segregar la información que se contenga en su inferior. Quedando de la siguiente manera:

- En el RAID 1:
  - Partición 1: SO anfitrión.
  - Partición 2: Partición del SO de la VM que va a ser el servidor Controlador de Dominio principal.
  - Partición 3: Partición del SO de la VM que va a ser el servidor de ficheros e impresión.
  - Partición 4: Partición del SO de la VM que va a ser el servidor de actualizaciones y antivirus.
- En el RAID 5:
  - Partición 1: SO anfitrión.
  - Partición 2: Particiones de datos de la VM que va a ser el servidor Controlador de Dominio secundario.
  - Partición 3: Particiones de datos de la VM que va a ser el servidor de correo.
  - Partición 4: Particiones de datos de la VM que va a ser el servidor de *backup*.

3.3 Desarrollo de la solución técnica

3.3.1 Componentes hardware

El material, destinado a dar soporte a la red, se compone de lo siguiente:

- Servidores:
  - Marca y modelo: HP Proliant DL 380P G8.
    - Cantidad: 2.
  - Procesadores
    - Cantidad: 4 (2 por servidor).
    - Características: Intel Xeon E5-2640 a 2.50 Ghz, 15 MB L3 cache.
- BIOS
  - Características: HP Bios P70.
- Controladora de Discos
  - Características: HP Smart Array P420i Controller.
- Discos Duros
  - Cantidad: 16 (8 por servidor).
  - Características:
    - 6 unidades HP 600GB 6G SAS 15K rpm LFF (3.5 inch), de las cuales hay dispuestas 3 por servidor.
    - 10 unidades HP 3 TB 6G SATA 7.2K rpm LFF (3.5 inch), de las cuales hay dispuestas 5 por servidor.
- RAM

  - Cantidad: 128 GB (64 GB por servidor).
  - Características: 8 módulos HP 16 GB 2Rx4 PC3L-10600R-9 kit, de los cuales hay dispuestos 4 módulos por servidor.
- Vídeo
  - Cantidad: 1 tarjeta de vídeo de 16 Ghz.
  - Marca y modelo: Matrox G200eH.
- NICs (al margen del puerto de iLo 4)
  - Marca y modelo: HP Ethernet 1 Gb 4-port 331 FLR.
  - Cantidad: 2 (1 tarjeta por servidor – 4 puertos –).
- Tarjeta de conexión con la unidad de *backup*
  - Marca y modelo: HP H222 Host Bus Adapter.
  - Cantidad: 1 (en un único servidor).
- Tarjeta de fibra (HBA)
  - Marca y modelo: HP StorageWorks 82Q 8 Gb PCI-e Dual Port HBA.
  - Cantidad: 2 (1 por servidor – 2 puertos –).
- Unidad de b*ackup*:
  - Marca y modelo: HP StorageWorks MSL LTO-6 Ultrium 6250 FC.
    - Cantidad: 1.
    - Drives: 1

3.3.2 Configuración de los elementos físicos

3.3.2.1 Discos duros

La configuración de los discos, que se ha realizado en ambos servidores es la siguiente:

- Se han agrupado los discos duros SAS en una configuración RAID 1 con un disco de repuesto ante fallos. Las características de estos discos proporcionan una alta velocidad de acceso, pero tienen una capacidad de almacenamiento menor.

  El almacenamiento disponible con esta configuración es de 600 GB.

- Se han agrupado los discos duros SATA en una configuración RAID 5. Las características de estos discos proporcionan una velocidad de acceso menor, pero una capacidad de almacenamiento mucho mayor.

  El almacenamiento disponible con esta configuración es de 12 TB.

En la Figura 2 se muestra gráficamente la composición de los servidores.

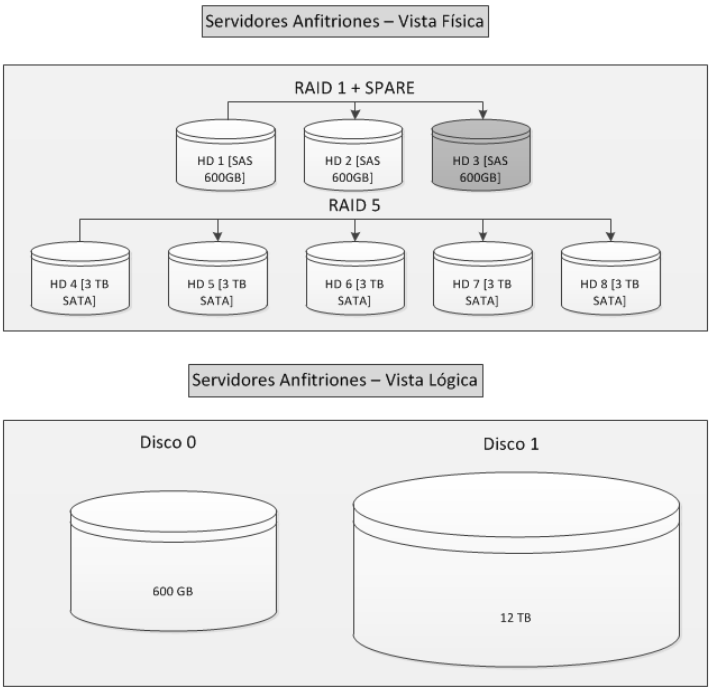

Figura 2 - Vista Física y vista lógica de los Servidores Anfitriones. Fuente: Elaboración propia

3.3.2.2 Unidad de *Backup*

Se ha conectado la unidad de backup, HP StorageWorks MSL LTO-6, con el servidor 2, dejando al servidor 1 sin conexión alguna. En la figura 3 se puede ver un esquema de las conexiones.

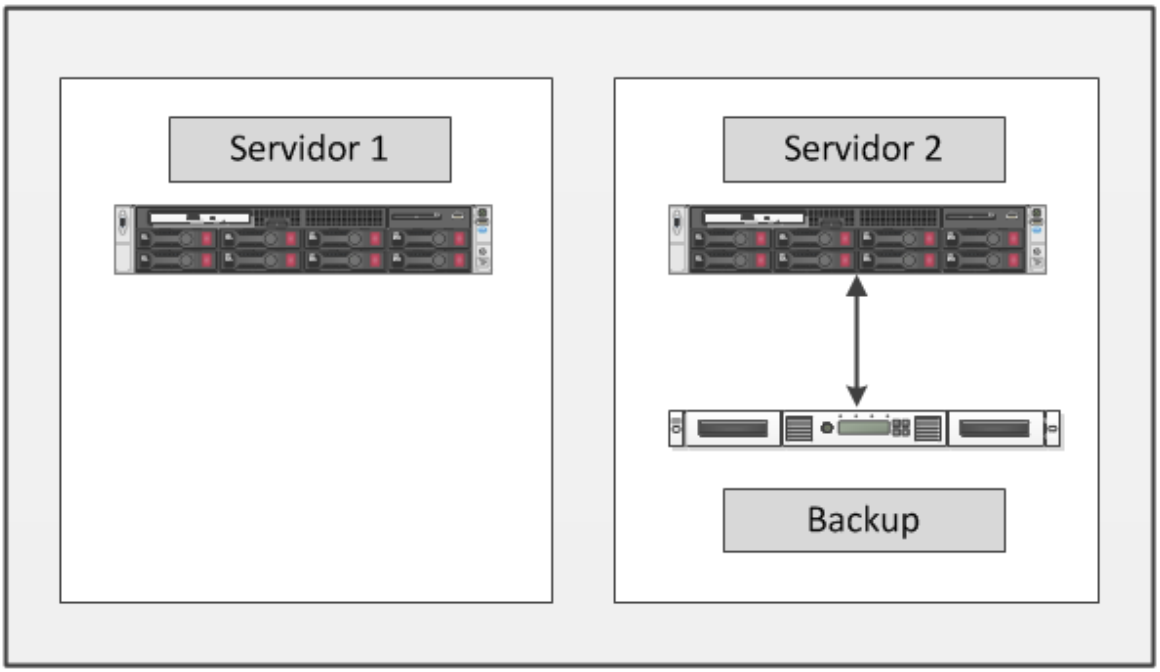

Figura 3 - *Backup* Servidor 2. Fuente: Elaboración Propia.

3.3.3 Licenciamiento

Se ha adquirido las siguientes licencias para albergar los servidores: Windows Server 2012 R2 y 2016R2.En la tabla 1 se muestran las licencias adquiridas.

Tabla 1 - Licencias Adquiridas. Fuente Ministerio de Defensa

Grupo de licencias	Familia de productos	Versión	Cantidad real	Cantidad de SA activo
Servers	Windows Server - Standard	2012 R2	3	3
Grupo de licencias	Familia de productos	Versión	Cantidad real	Cantidad de SA activo
Servers	Windows Server - Standard	2016R2	1	1

3.3.4 Configuración lógica propuesta segun plantillas CCN-STIC

Se propone instalar en los servidores físicos (en adelante *hosts* anfitriones), el siguiente software como sistema operativo: Microsoft Windows Server 2016 R2.

La instalación del sistema operativo se hará completa en cada *host* anfitrión, de manera "*no core*". La diferencia entre un sistema operativo "*core*" y uno "*no core*" es que el primero es un sistema operativo más ligero y más rápido debido a que carece de capa de presentación. Este tipo de sistema operativo no posee entorno gráfico y esto hace que todos los comandos de ejecución se hagan a través de *power shell*.Sin embargo, el sistema operativo "no core" es un sistema operativo completo, mucho más pesado y más lento que el anterior. Se habilitará en cada uno de los hosts anfitriones los roles de HyperV y, sobre ellos, se generarán las máquinas virtuales necesarias para dar soporte a la red de la NATO Secret WAN (NSWAN).

Asimismo, el *hos*t anfitrión 2, también tendrá habilitadas las características de *backup*, ya que está conectado físicamente con dicha unidad.

Las máquinas virtuales que están previstas que se alojen en cada uno de los *hosts* anfitriones se pueden ver en la Figura 4.

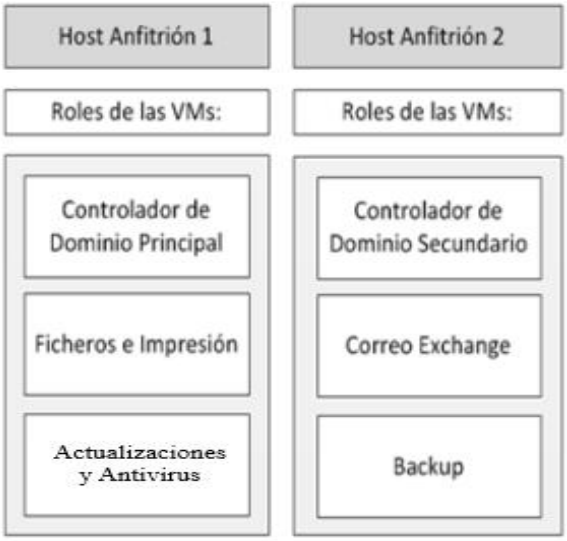

Figura 4 - Máquinas Virtuales alojadas en Host 1 y 2.Fuente Elaboración propia

3.3.4.1 *Host* Anfitrion 1

El RAID 1 (disco lógico 0) estará destinado a alojar el sistema operativo anfitrión del servidor físico y todas las particiones de sistema de las máquinas virtuales que corran en ese servidor, excepto del controlador de dominio principal que solo va a tener una partición del sistema.Hay que dejar claro que el controlador de dominio no lleva partición de datos porque la base de datos del Directorio Activo es muy pequeña, no más de 100 personas, que es el dominio de un desplegable en este tipo de misiones.Por lo tanto dicho controlador de dominio solo va a disponer de una partición de sistema.

La distribución propuesta es la siguiente:

- Partición 1: Sistema Operativo del *host* anfitrión.
- Partición 2: Particiones correspondientes a la VM con rol de servidor Controlador de Dominio principal.
- Partición 3: Sistema Operativo de la VM correspondiente al servidor de ficheros e impresión.
- Partición 4: Sistema Operativo de la VM correspondiente al servidor de actualizaciones y antivirus.

A continuación se muestra gráficamente lo anteriormente expuesto en la figura 5.

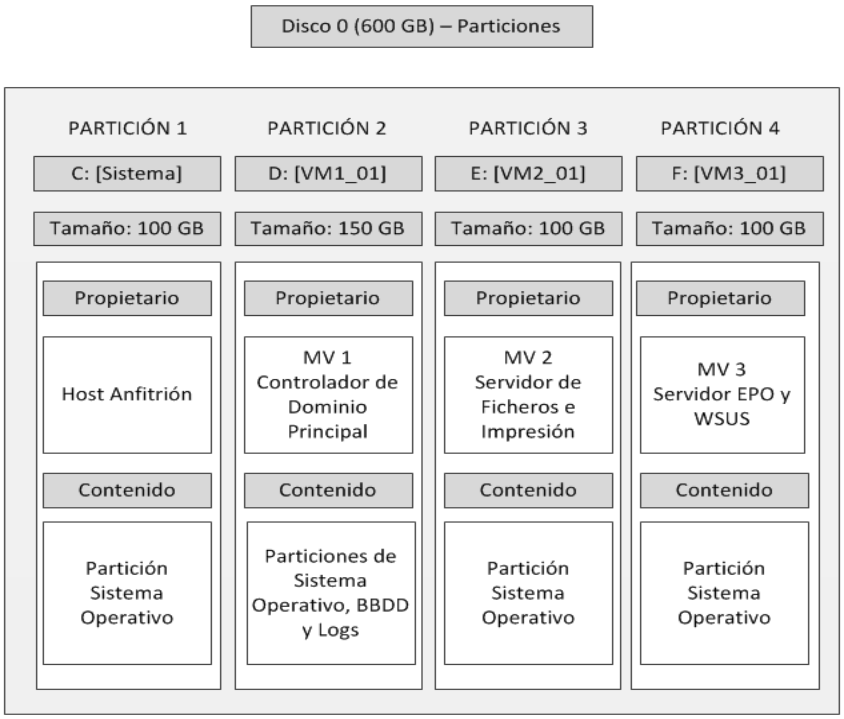

Figura 5 - Distribución de las diferentes particiones en Disco 0. Fuente Elaboración propia

Por otro lado, el RAID 5 (disco lógico 1) estará destinado a alojar las particiones de datos del sistema operativo anfitrión y de las máquinas virtuales que se ejecutan en ese servidor.

La distribución propuesta es la siguiente:

- Partición 1: Datos del *host* anfitrión.
- Partición 2: Datos de la VM que va a ser el servidor de ficheros e impresión.
- Partición 3: Datos de la VM que va a ser el servidor de EPO y WSUS.

Se muestra gráficamente lo anteriormente expuesto, en la Figura 6.

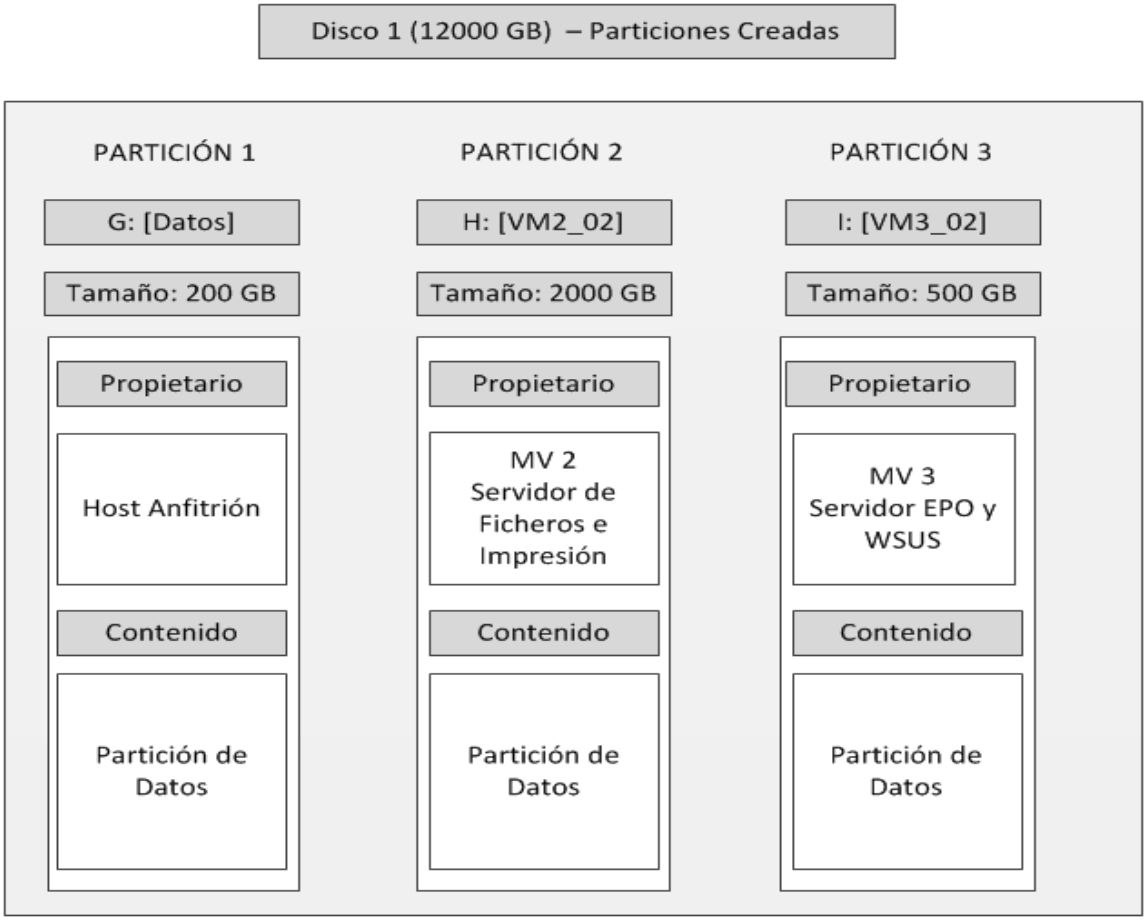

Figura 6 - Distribución de las diferentes particiones en Disco 1. Fuente Elaboración propia

3.3.4.2 *Host* Anfitrión 2

El RAID 1 (disco lógico 0) estará destinado a alojar el sistema operativo anfitrión del servidor físico y todas las particiones de sistema de las máquinas virtuales que corran en ese servidor, excepto del controlador de dominio secundario que solo llevará una partición del sistema

La distribución propuesta es la siguiente:

- Partición 1: Sistema Operativo del *host* anfitrión.
- Partición 2: Particiones correspondientes a la VM con rol de servidor Controlador de Dominio secundario.
- Partición 3: Sistema Operativo de la VM correspondiente al servidor de correo Exchange.
- Partición 4: Sistema Operativo de la VM correspondiente al servidor de *backup.*

La nomenclatura utilizada para la implementación de lo anteriormente expuesto es la siguiente:

VM→ Máquina Virtual

1→ número de host físico nº 1

01→ Número de Máquina Virtual en ese *host* anfitrión.

Se muestra gráficamente lo anteriormente expuesto en la Figura 7.

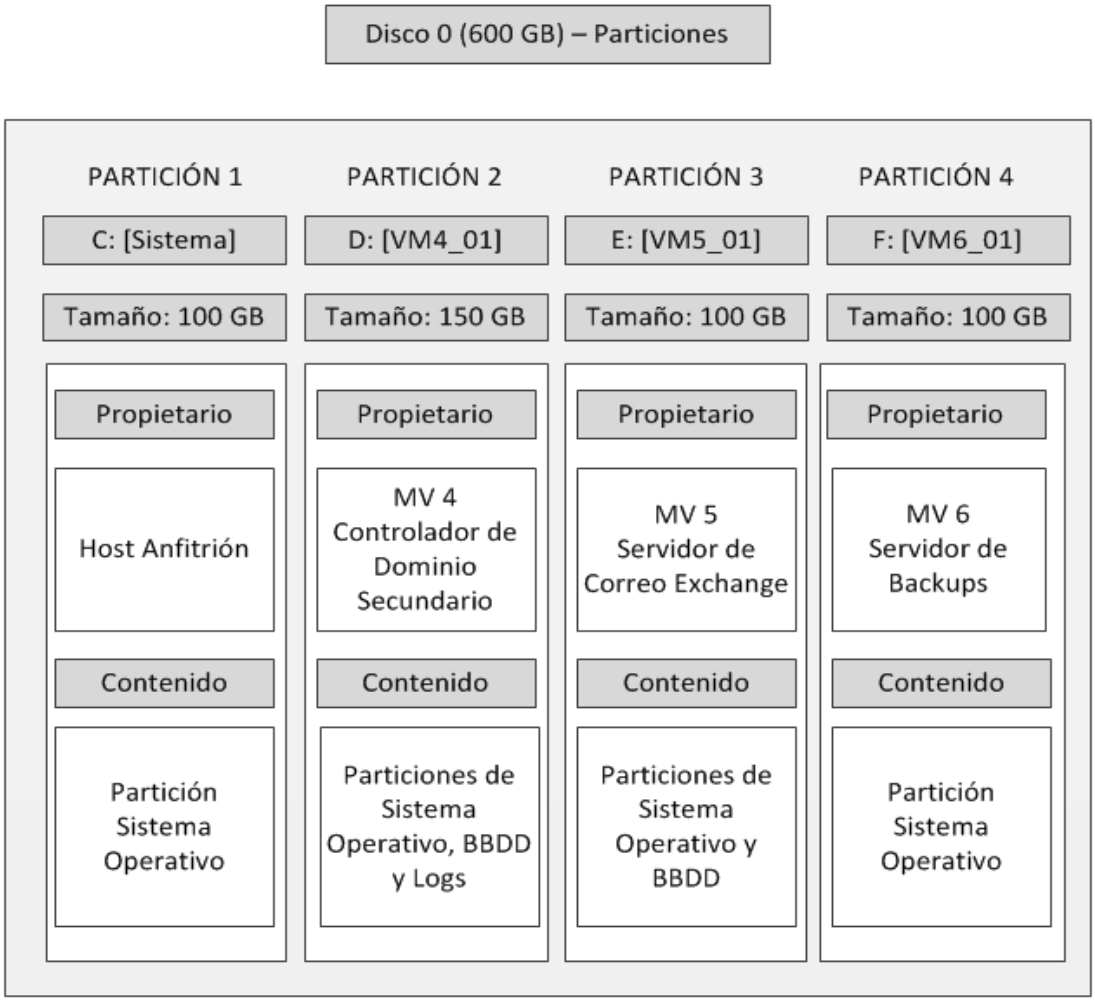

Figura 7 - Distribución de las diferentes particiones en Disco 0. Fuente Elaboración propia

Por otro lado, el RAID 5 (disco lógico 1) estará destinado a alojar las particiones de datos del sistema operativo anfitrión y de las máquinas virtuales que se ejecutan en ese servidor.

La distribución propuesta es la siguiente:

- Partición 1: Datos del *host* anfitrión.
- Partición 2: Datos de la VM que va a ser el servidor de correo Exchange.
- Partición 3: Datos de la VM que va a ser el servidor de *backup.*

En la figura 8 se muestra gráficamente lo anteriormente expuesto.

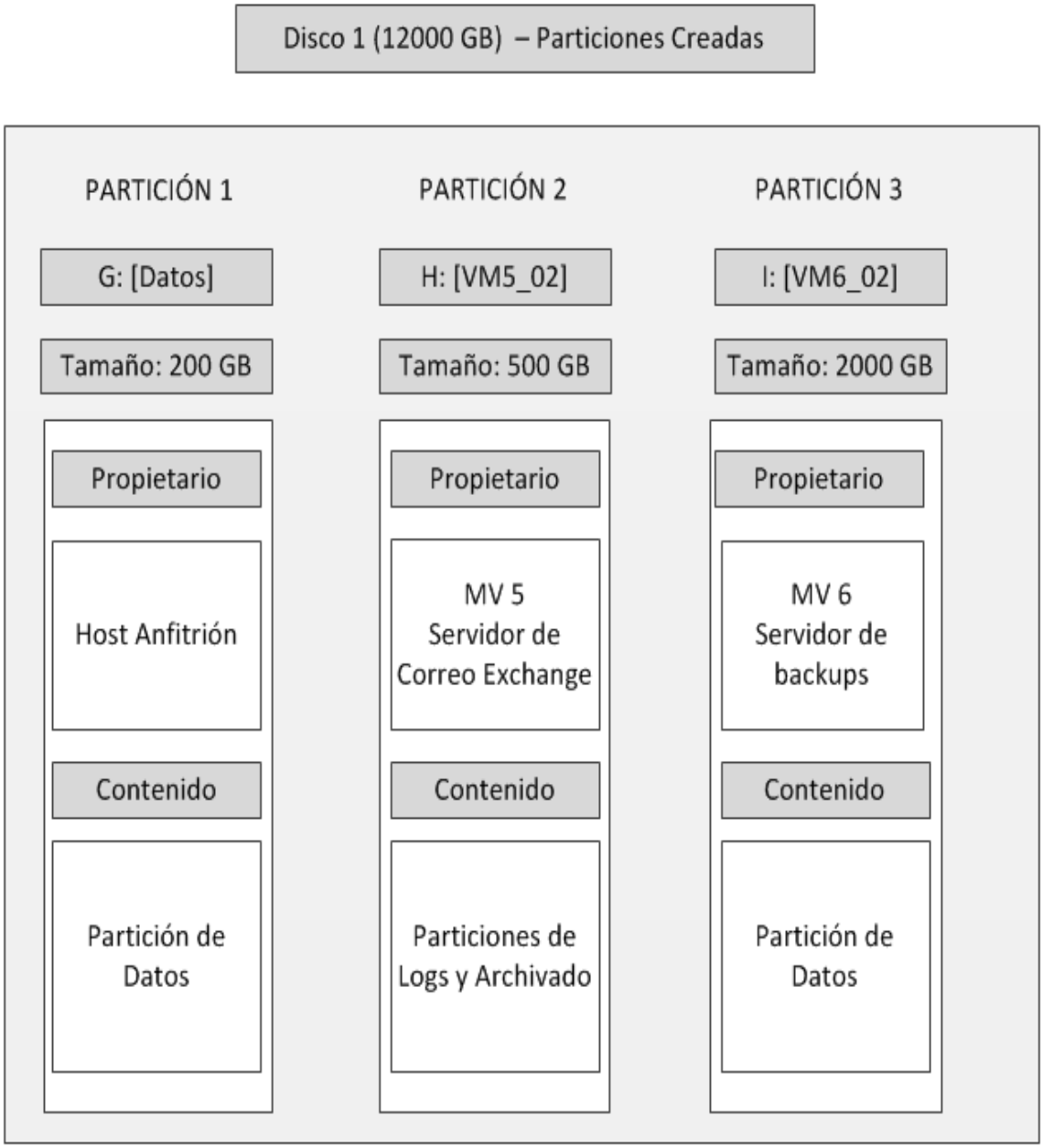

Figura 8 - Distribución de las diferentes particiones en Disco 1. Fuente Elaboración propia

3.3.5 Plantillas CCN-STIC a aplicar

Las plantillas STIC que se proponen aplicar son las siguientes:

3.3.5.1 *Host* Anfitrión 1

Para el host anfitrión aplicaría lo siguiente:

- CCN-STIC-560B: Windows Server 2012 R2: Instalación Completa, servidor independiente (No Core).

Para las VMs que aloja, aplicarían las siguientes plantillas:

- Controlador de Dominio Principal, servidor de Ficheros e Impresión y servidor de actualizaciones y antivirus

- CCN-STIC-560A: Windows Server 2012 R2: Instalación Completa, Controlador de Dominio o servidor miembro (No Core).

3.3.5.2 *Host* Anfitrión 2

Para el *host* anfitrión aplicaría lo siguiente:

- CCN-STIC-560B: Windows Server 2012 R2: Instalación Completa, servidor independiente (no core).

Para las VMs que aloja, aplicarían las siguientes plantillas:

- Controlador de Dominio Principal y Secundario
  - CCN-STIC-560A: Windows Server 2012 R2: Instalación Completa, Controlador de Dominio o servidor miembro (No Core).
- Servidor de Correo Exchange
  - CCN-STIC-521A: Configuración Segura de Windows Server 2016 R2: Instalación Completa, Servidor Miembro (No Core, No Independiente).
  - CCN-STIC-524: Seguridad en Internet Information Server (IIS) 7.5 sobre Windows Server 2016 R2 en Servidor Miembro del Dominio.
  - CCN-STIC-550: Microsoft Exchange Server 2016 en Windows Server 2016 R2.
- Servidor de *Backup*
  - CCN-STIC-560A: Windows Server 2012 R2: Instalación Completa, Controlador de Dominio o servidor miembro (No Core).

3.3.5.3 Estaciones de trabajo

Las estaciones de trabajo, también conocidas como *workstations*, consisten en una serie de equipos que son empleados por los Ejércitos en cualquier misión en el exterior, y cuya funcionalidad es dar los servicios necesarios y estipulados en el SLA para finalizar con éxito la misión encomendada.Estas estaciones son utilizadas por los usuarios finales.

Forman parte de una red donde se almacenan y comparten un sinfín de archivos y carpetas con información relacionada con el trabajo a realizar en la misión encomendada.

Este tipo de estaciones o *workstations* son exactamente iguales a las que tenemos en territorio nacional, excepto en dos cosas que son muy importantes. La primera es que todas las estaciones son portátiles, para facilitar la huella logística de todo el proceso y la segunda diferencia importante es que todos los clientes son clientes ligeros, es decir a través de la virtualización de escritorios (VDI,s) los clientes finales acceden a sus aplicaciones a través de un servidor central que proporciona todos los servicios. Este sistema proporciona una mayor seguridad en todas las estaciones de trabajo que estén en una

determinada misión, y además centraliza todos los servicios, dando una mayor rapidez a la gestión de todas las aplicaciones instaladas.

Las plantillas a aplicar en este tipo de estaciones serían:

- CCN-STIC-522A: Configuración Segura Windows 10 LTSC Enterprise (Cliente Miembro de Dominio).
- CCN-STIC-530: Seguridad en Microsoft Office.

3.3.6 Software de las estaciones de trabajo (clientes)

En general, el inventario de programas a instalar en estos equipos serían los que se muestran en la Tabla 2.

Tabla 2 - Software instalado en los terminales de trabajo.Fuente.Elaboración propia

CONFIGURACIÓN SOFTWARE DE LAS TERMINALES DE TRABAJO	
Sistema Operativo (incluyendo versión):	Windows Enterprise
ANTIVIRUS	Mcafee VirusScan Enterprise 8.8.0.02004
	Mcafee Agent 4.6.0.3122
BORRADO SEGURO	Eraser 6.0.10.2620
VISOR DE FICHEROS PDF	Adobe Acrobat Reader XI Español (11.0.02)
HERRAMIENTA DE CIFRADO	TRUECRYPT 7.1a
COMPRESIÓN DE DATOS	Winzip v11.0 (7313)
NAVEGADOR WEB	Internet Explorer 11
MOTOR WEB	Java (TM) 7 Update 55 (64-bits)
OFIMÁTICA	MS Office Professional Plus 2010
CLASIFICADOR CATEGORÍAS MENSAJES	Classify for Outlook 2010 (64-bits)

3.4 Pruebas y validación

Una vez realizado todo el análisis, montaje y configuración del módulo desplegable tenemos que hacer las pruebas y validaciones pertinentes. Para ello, es necesaria la auditoría de una sección independiente como es la sección de ciberdefensa que va a ser la responsable de realizar todas las pruebas y validaciones necesarias para que el módulo desplegable pueda trabajar tanto a nivel nacional como internacional. En este caso concreto existe un formulario que no es más que una lista de comprobación donde se van verificando punto por punto todos los apartados realizados en el trabajo y si cumplen con la normativa vigente de seguridad.

DESCRIPCIÓN DE LAS PRUEBAS Y VALIDACIONES

1. Despliegue de la MV (desde una plantilla)
2. Personalizar MV:
    a. Nombre final de la MV
    b. Pasar WSUS si es necesario
    c. Activar Windows
    d. Configurar la IP y la red
    e. Compartir redes

f. Instalar el software específico

g. Configurar el hardware

3. Realizar SNAPSHOT
    a. Indicar ubicación en disco del SNAPSHOT
4. Meter la MV en dominio piloto
5. Realizar SNAPSHOT
    a. Indicar ubicación en disco del SNAPSHOT
6. Pasar plantillas CCN-STIC o aquellas que sean requeridas
7. Realizar SNAPSHOT
    a. Indicar ubicación en disco del SNAPSHOT
8. Realizar pruebas de campo en el piloto final
9. Validación final de la Arquitectura del módulo desplegable
    a. Documentación del proceso seguido (anotando en una lista de comprobación las novedades/modificaciones)
    b. Decidir si se consolida la arquitectura final obtenida.

Tabla 3 - Documento de Validación de los diferentes procesos de pruebas del Módulo Desplegable.Fuente Elaboración propia

PROCESO DE PRUEBAS Y VALIDACIÓN DE LA ARQUITECTURA DE UN MODULO DESPLEGABLE			
PROCESO	**SUBPROCESO**	**OBSERVACIONES**	**REALIZADO**
Despliegue MV desde plantilla		Determinado según normativa vigente.	SI
Personalizar MV	**Nombre MV**	El nombre de la máquina viene impuesto por el Ministerio de Defensa	SI
	WSUS	Se han realizado todas las actualizaciones	SI
	Activar Windows	Activación de Windows con nº de licencia dado	SI
	Configurar IP/red	Viene determinado por departamento de redes	SI
	Compartir redes	La única red auditada es la VLAN	SI
	Instalar SW	Instalación de todo el software para el despliegue	SI
	Configurar HW	Configuración correcta del hardware para el despliegue.	SI
SNAPSHOT	**Ubicación HD**	Se aloja donde se encuentre la máquina virtual	SI

Meter MV en dominio piloto		Comprobación de funcionamiento en dominio prueba.es	SI
SNAPSHOT	**Ubicación HD**	Se aloja donde se encuentre la máquina virtual	SI
Pasar plantillas seguridad		Se han pasado y comprobado todas las plantillas de seguridad necesarias para este tipo de módulo	SI
SNAPSHOT	**Ubicación HD**	Se aloja donde se encuentre la máquina virtual	SI
Realizar pruebas		Se han realizado todas la pruebas tanto en laboratorio como una prueba en exterior para verificar todos los puntos establecidos por normativa.	SI
Validación final	**Documentar proceso seguido**	Todos los documentos quedarán registrados en el órgano de ciberdefensa con copia al interesado	SI
	Decidir etapa consolidación MV	Se decidirá en siguientes salidas o despliegues	SI

Trabajo desarrollado por	Jefe del Departamento de Sistemas	Auditor por parte de Ciberdefensa

3.5 Normativa aplicable y calidad

La normativa aplicable, en este caso, para el despliegue de una arquitectura de un módulo tanto a nivel nacional como internacional se define a partir de los requisitos generales del Sistema de Gestión de Calidad (SGC), según se establece la aplicabilidad de los requisitos de la norma UNE-EN ISO 9001:2015, UNE-EN ISO/IEC 27001 así como los requisitos Específicos OTAN para los Sistemas de Gestión de Calidad (SGC).

Referencias normativas:

1. UNE-EN ISO 9001:2015 Sistemas de Gestión de la Calidad. Requisitos.

2. UNE-EN ISO 9000:2015 Sistemas de Gestión de la Calidad. Fundamentos y vocabulario.

3. PECON-2100 Requisitos Contractuales de Gestión de la Configuración.

4. UNE-EN ISO 10012:2003 Sistemas de Gestión de las Mediciones. Requisitos para los procesos de medición y los equipos de medición.

5. UNE-EN ISO 31000:2010 Gestión del Riesgo. Principios y directrices.

Referencias informativas:

1. PECAL-2000 Política OTAN de calidad enfocada a sistemas integrados durante su ciclo de vida.

2. PECAL-2009 Guía OTAN para el uso de las PECAL Serie2000.

3. PECAL-2105 Requisitos OTAN para planes de calidad entregables.

4. PECAL-2070 Aseguramiento Oficial de la Calidad (AOC) mutuo en la OTAN.

5. UNE-EN ISO 10007:2003 Sistemas de Gestión de la Calidad. Directrices para la Gestión de la Configuración.

6. ADMP Allied Dependability Management Publications

Los requisitos generales del Sistema de Gestión de Calidad son los siguientes:

- Aplicabilidad de los requisitos de la norma UNE-EN ISO 9001:2015
- El suministrador debe establecer, documentar, implementar, evaluar y mejorar un Sistema de Gestión de Calidad económico y eficaz, de acuerdo con lo establecido en esta publicación, que incluya los requisitos de la norma UNE-EN ISO 9001:2015 que sean necesarios para satisfacer los requisitos del contrato.

3.5.1 El sistema de gestión de calidad y sus procesos

El comprador y/o el representante para el Aseguramiento Oficial de la Calidad se reservan el derecho de rechazar el Sistema de Gestión de Calidad del suministrador cuando aplique al contrato. Debe ponerse a disposición del Responsable del Aseguramiento de la Calidad y/o comprador la información documentada sobre el alcance del sistema del suministrador, los registros de las auditorías y evaluaciones internas, y cualquier otra evidencia objetiva que muestre que el sistema es conforme con el pliego de prescripciones técnicas realizado anteriormente.

En los casos en los que el comprador y/o Responsable del Aseguramiento de la Calidad rechacen el Sistema de Gestión de Calidad, el suministrador debe presentar propuestas de acciones correctivas y de sus respectivas revisiones en el plazo acordado. Se aplicarán las penalizaciones que se hayan establecido en el contrato establecido entre el Ministerio de Defensa y el proeevedor.

Acceso a las instalaciones del suministrador y de los proveedores externos, y apoyo a las actividades de Aseguramiento Oficial de la Calidad.

El suministrador y/o los proveedores externos deben proporcionar al Responsable del Aseguramiento de la Calidad y/o comprador:

1. El derecho de acceso a las instalaciones en las que se estén realizando las actividades contratadas.

2. La información relativa al cumplimiento de los requisitos del contrato.

3. La posibilidad de evaluar sin restricciones el cumplimiento de los requisitos de esta publicación por parte del suministrador.

4. La posibilidad de evaluar sin restricciones el cumplimiento de los requisitos de esta publicación por parte de los proveedores externos. El suministrador será informado antes de realizar dicha evaluación.

5. La posibilidad de verificar la conformidad del producto con los requisitos del contracto, sin ninguna restricción.

6. La ayuda que se precise para la evaluación, verificación, validación, pruebas, inspección o liberación del producto, a fin de realizar el Aseguramiento Oficial de la Calidad según los requisitos del contrato.

7. Los locales y medios necesarios para llevar a cabo el Aseguramiento Oficial de la Calidad.

8. Los equipos disponibles que sean necesarios para llevar a cabo el Aseguramiento Oficial de la Calidad, mediante un uso razonable de los mismos.

9. El personal del suministrador o de los proveedores externos que se precise para operar tales equipos, cuando se requiera.

10. Acceso a la información y sistemas de comunicación.

11. La documentación del suministrador necesaria para evidenciar la conformidad del producto con las especificaciones.

12. Copias de los documentos necesarios, incluyendo aquellos almacenados en medios electrónicos.

El suministrador debe presentar al Responsable del Aseguramiento de la Calidad y/o comprador un Plan de Calidad aceptable basado en los requisitos contractuales, en un plazo mutuamente acordado pero siempre antes del comienzo de las actividades (lo cual puede definirse como una reunión de lanzamiento del proyecto o contrato, o como se haya determinado en el contrato o pedido). El Plan de Calidad puede ser un documento independiente y claramente identificado, o parte de cualquier otro documento que se haya preparado para el contrato.

El Plan de Calidad debe:

a. Describir y documentar los requisitos del Sistema de Gestión de Calidad que sean «específicos para el contrato» y se necesiten para satisfacer los requisitos contractuales (haciendo referencia, cuando sea aplicable, al Sistema de Gestión de Calidad «global de la empresa»).

b. Describir y documentar la planificación de la realización del producto en términos de requisitos de calidad para el producto, recursos necesarios, actividades de control requeridas (verificación, validación,

seguimiento, inspección, pruebas), y criterios de aceptación. También deben incluirse los acuerdos específicos y los requisitos de comunicación cuando el trabajo deba realizarse en localizaciones externas a las instalaciones de los suministradores.

c. Documentar y mantener la trazabilidad de los requisitos desde el proceso de planificación, incluyendo una matriz de cumplimiento de requisitos y soluciones que justifique el cumplimiento de todos los requisitos contractuales (a los que se hará referencia cuando sea aplicable).

3. El comprador y/o Responsable del Aseguramiento de la Calidad se reservan el derecho de rechazar los Planes de Calidad y sus revisiones.

Nota: Los requisitos contractuales relativos al contenido del Plan de Calidad se han incluido en la PECAL-2105 «Requisitos OTAN para planes de calidad entregables».

La matriz de cumplimiento de requisitos y soluciones puede ser parte del Plan de Calidad o un documento anexo al mismo. Esta matriz puede ser preparada y añadida al Plan de Calidad después de que se haya elaborado la versión inicial de dicho plan, en un plazo mutuamente acordado con el Responsable del Aseguramiento de la Calidad y/o comprador, teniendo en cuenta el contenido del contrato o pedido.

4 SECURIZACIÓN DE UN RACK DESPLEGABLE

4.1 Descripción del sistema

4.1.1 Misión del sistema

La red del *rack* desplegable tiene por objetivo proporcionar a los usuarios, los medios fiables para almacenar, procesar e intercambiar la información sobre la operación del mismo.

El siguiente listado refleja los servicios proporcionados por el sistema:

• Servicio de directorio activo y Controlador de Dominio.

• Servicio de ficheros.

• Servicio de impresión

• Servicio de *backup*.

• Servicio de actualizaciones de Microsoft.

• Servicio de implementación de imágenes con sistema de distribución inalámbrica (WDS).

4.1.2 Información manejada

En el sistema se maneja información clasificada nacional CONFIDENCIAL. El Modo Seguro de Operación utilizado es UNIFICADO A NIVEL SUPERIOR, es decir, el personal con acceso al Sistema está autorizado para acceder al grado más elevado de clasificación de la información manejada en el sistema, pero por otra parte, no todos tienen la misma necesidad de conocer "*Need to Know*". La "necesidad de conocer" se garantiza gracias a procesos informales, los cuales, promueven la discriminación de datos por parte del sistema de forma fiable, disponiendo de un control de accesos selectivo a la información, atendiendo a dicha necesidad de conocer y cumpliendo tanto con lo establecido en la normativa de seguridad vigente como en las propias políticas del sistema que se sustentan gracias a los procedimientos de seguridad elaborados para tal fin.

4.1.3 Usuarios

Todos los usuarios del sistema estarán acreditados hasta el nivel más alto para la información procesada por el sistema (CONFIDENCIAL), y deberán contar con la "Necesidad de Conocer" para acceder a dicha información.

Los tipos o clases de usuario vendrán definidos por las plantillas de seguridad TIC del Centro Criptológico Nacional (CCN).Los privilegios y los requisitos para las autorizaciones de acceso al Sistema vendrán reflejados en el apartado de control de accesos.

Los usuarios de la red serán el personal militar relacionado con el Sistema.

Los usuarios estarán autorizados a acceder únicamente a la información de acuerdo con su función y necesidad de conocer, y además, todos dispondrán de la correspondiente autorización de acuerdo a lo que establece la normativa para acceder a información clasificada.

Dentro de cada tipo de usuario se definirán diferentes perfiles y derechos de acuerdo con las tareas específicas a desempeñar y la necesidad de conocer de cada uno de ellos.

Los usuarios se agruparán de acuerdo con la función que desempeñen en el Sistema y de forma que se garantice una adecuada segregación de funciones.

En primera instancia los usuarios se clasificarán en usuarios operativos, autorizados a acceder al mismo, y usuarios administradores, dedicados a las tareas de administración del sistema.

4.1.4 Arquitectura del sistema

La configuración de los equipos que forman el sistema viene reflejada en el Anexo II.

Se incluyen datos de:

- Configuración Hardware/Firmware.
- Configuración Software.
- Direccionamiento IP.
- Dispositivos de almacenamiento extraibles autorizados.
- Etiquetas anti manipulación.
- Diagrama de red.

4.2 Definición de los requisitos de seguridad

Los estándares de seguridad mínimos a implementar en el sistema, son los establecidos por la normativa nacional, así como por la Autoridad Delegada de Acreditación.

El Análisis de Riesgos ha sido realizado con la herramienta PILAR. En el análisis de riesgos se indican los valores sobre el impacto y el riesgo (repercutido y acumulado) de los activos del sistema.

En este análisis de riesgos se han tenido en cuenta los riesgos específicos para el sistema CIS desplegable.

Según la guía CCN-STIC-301 los servidores físicos que hacen de *host* para las máquinas virtuales se tratan con el mismo grado de clasificación que las máquinas virtuales, tanto las máquinas físicas como las virtuales se encuentran bastionados y securizados de un modo seguro. La gestión de parcheado, cuentas de usuarios, software antivirus, etc. en ambos entornos tanto físico como virtual es idéntico.

Esta sección describe los motivos por los que el sistema debe ser seguro en cuanto a los siguientes aspectos:

4.2.1 Criticidad de la información manejada

El acceso a la información puede considerarse crítico en cualquier organización y, especialmente, en el ámbito del Ministerio de Defensa y de la Fuerzas Armadas. Por este motivo, el impacto que podría suponer la pérdida de confidencialidad, integridad o disponibilidad en el sistema y, por tanto en la organización, puede ser muy importante dependiendo del tipo y cantidad de información puesta en riesgo.

La pérdida de confidencialidad, integridad y, en su caso, la modificación no autorizada de la información, podría dañar la seguridad del Ministerio de Defensa, dificultar el cumplimiento de su misión y perjudicar sus intereses.

4.2.2 Analisis y gestión de riesgos

En el análisis de riesgos se indican los valores sobre el impacto y el riesgo (repercutido y acumulado) de los activos del Sistema, no obstante lo anterior es preceptivo definir los siguientes conceptos:

- Amenaza: como un evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- Activos: son los recursos del sistema de información o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- Vulnerabilidad: es la estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.
- Impacto: es la consecuencia que sobre un activo tiene la materialización de una amenaza.
- Riesgo: es la estimación del grado de exposición de un sistema de información frente a amenazas que pudieran causar daños o perjuicios a la Organización.

La metodología empleada en el análisis de riesgos del sistema es MAGERIT v.3 mediante la herramienta PILAR.

Todos los cambios que se produzcan tanto en la configuración como en el uso del Sistema deberán ser actualizados en dicho análisis.

4.3 Definición del entorno de seguridad

En primer lugar se realiza una descripción del (Entorno Global de Seguridad). Este único entorno que se va a definir es el entorno global de seguridad que se corresponde con el emplazamiento en el que reside la red aislada, en este caso se delimita por su perímetro externo de la Base donde se vaya a desplegar. Este establecimiento militar debe tener la suficiente capacidad de reacción ante cualquier intento de acceso ilícito, estando la seguridad física del entorno monitorizada 24 horas al día. Por otra parte también existen otros entornos de seguridad como pueden ser el entorno local de seguridad o el entorno de seguridad electrónica pero que quedan fuera del estudio en este trabajo.

A continuación se definen las medidas de seguridad que se aplican al objeto de proteger el Sistema y la información clasificada dentro de los límites del entorno del Sistema. Se establecen las medidas de seguridad (físicas, ligadas al personal, documental y STIC) que se han de tomar en cada uno de los entornos de seguridad, y para cada uno de los aspectos que a continuación se irán detallando. Dichas medidas nacen fruto del Análisis de riesgos y han sido verificadas por parte del administrador de seguridad del sistema (ASS).

La Normativa aplicable a la presente Declaración de Requisitos Específicos de Seguridad del Sistema está en concordancia con lo expresado por la Instrucción técnica CCN-STIC-301, donde se establecen los requisitos STIC. Asimismo se contempla también lo expresado en las normas de la autoridad nacional para la protección de la información clasificada (ANPIC).

Además, hay que tener en cuenta que la evaluación de riesgos se ha elaborado teniendo en cuenta las amenazas, vulnerabilidades y riesgos factibles utilizando como herramienta de análisis PILAR, basada en la metodología MAGERIT.

4.3.1 Control de Acceso

El acceso es una interacción entre un sujeto (usuario) y un objeto (recurso) que da como resultado un flujo de información de uno a otro. El control de acceso es el ejercicio de control sobre esa interacción.

Los controles en el EGS proporcionan un control de acceso adecuado tanto para el personal militar destinado como para las visitas que se produzcan.

El acceso al módulo desplegable se limitará a los usuarios autorizados que ostenten la preceptiva habilitación personal de seguridad (HPS) (CONFIDENCIAL o superior) y que tengan Necesidad de Conocer o "*Need to Know*" derivada del puesto asignado dentro del "*job description*" definido para el destacamento (DAT).

El principal riesgo al que se puede enfrentar el sistema en este ámbito es que personal sin la preceptiva HPS o que teniendo la misma no tenga necesidad de conocer acceda de forma intencionada o accidental a la información almacenada en el sistema o a recursos del mismo.

Los riesgos identificados son:

- Destrucción de la información.
- Fuga de información.
- Abuso de privilegios de acceso.
- Alteración deliberada de la información.
- Revelación de información.

Todos los usuarios deben poseer la habilitación personal de seguridad para poder acceder a la información manejada en el Sistema asimismo son responsables de la gestión adecuada de la misma.

Los Administradores del Sistema tendrán una habilitación personal de seguridad CONFIDENCIAL o superior y deberán estar reconocidos como personal autorizado dentro de la estructura del Sistema.

Existe un Procedimiento Operativo de Seguridad para el acceso, control e identificación del personal estableciéndose un estricto control tanto sobre personal como cualquier entrada o salida de material que pudiera tener lugar.

La habilitación de seguridad del personal con acceso a información clasificada se realizará de acuerdo al procedimiento establecido en la norma NS/02 de la ANPIC sobre seguridad en el personal, y con los criterios y particularidades que allí se marcan.

La relación detallada de personas autorizadas a acceder al sistema y/o a la información en él contenida, así como sus derechos y permisos de acceso, deberá figurar, y mantenerse actualizada, como anexo a las pruebas de diagnóstico que el ordenador realiza después de encenderse *Power On Self Test* (POST) del sistema.

4.3.2 Identificación y autenticación

Definición.

Identificación y Autenticación (I&A), es el proceso para establecer la validez de una identidad declarada.

Medidas de seguridad en el EGS.

Las medidas de seguridad del EGS vienen indicadas en el plan de seguridad de la Base donde se vaya a desplegar el modulo, además del plan de protección del destacamento y recaen sobre el personal de seguridad de dicha Base y la *Force Protection* española.

Deberá tenerse en cuenta que:

- El personal que necesite acceder al EGS deberá pasar un control de identificación para proteger los componentes del sistema.
- Todo el personal que acceda al EGS deberá disponer de una tarjeta de identificación. La tarjeta deberán portarla visible en todo momento.
- Todas las visitas al EGS deberán presentar su DNI o pasaporte, y recibir confirmación por parte de la persona que recibe la visita.
- En los POS se establecerán los procedimientos para la generación, el empleo y la modificación de las tarjetas y etiquetas de identificación y de sus códigos de acceso al EGS.

4.3.3 Registro

Es necesario registrar la creación, transmisión, modificación o borrado de la información del módulo desplegable.

Como parte de las medidas de Seguridad en el EGS deberá tenerse en cuenta que:

- Las medidas de seguridad física en el EGS contarán con controles aleatorios de salida y supervisión de los objetos trasportados por los usuarios y se prevendrán la salida no autorizada de copias impresas o de soportes informáticos.
- Se registrarán las acciones de los usuarios (entradas, salidas).
- La entrada y la salida de visitas al EGS se registrarán de acuerdo con el plan de seguridad de Base donde se vaya a desplegar el módulo.

4.3.4 Auditoría

La auditoria consiste en la monitorización de sucesos relacionados con la seguridad para detectar y advertir las actividades llevadas a cabo en el sistema que pudieran amenazar la seguridad de éste.

La función de auditoría se encargará principalmente de monitorizar el sistema, al objeto de detectar posibles incidentes o eventos que pudieran comprometer la seguridad del Sistema, así como prevenir posibles ataques o violaciones de la seguridad CIS.

Como parte de las medidas de Seguridad en el EGS deberá tenerse en cuenta que:

- Se establecerán procedimientos en el plan de seguridad del EGS para auditar los registros que tengan implicación en el sistema, por ejemplo, el registro de personal ajeno al sistema o movimiento de material.
- Cualquier fisura en la seguridad física o electrónica será comunicada al AOSTIC.

4.3.5 Reutilización de objetos

Para la reutilización de objetos del sistema, se seguirá la CCN-STIC-305.En relación a los medios de almacenamiento:

- Todos los medios que almacenen información (discos duros, discos externos, cintas magnéticas, pendrives, CD, DVD, tarjetas de memoria, memorias principales, etc.) deberán estar inventariados y clasificados de acuerdo con el nivel de clasificación de la información almacenada y etiquetados según se indique en los POS.
- Todos los discos duros de las estaciones de trabajo, discos externos (HDD) y pendrives que almacenen información clasificada deberán estar cifrados con productos autorizados.
- Los medios de almacenamiento removibles deberán ser autorizados por la AOSTIC, identificados y controlados por los AS, registrando su conexión y desconexión a estaciones aduana/frontera y la información transferida.
- Los medios de almacenamiento informáticos deberán protegerse en contenedores de seguridad (armarios de seguridad, cajas fuertes, cámaras acorazadas o armarios ignífugos) para evitar su manipulación o destrucción.
- La destrucción y sanitización de soportes se hará de acuerdo a la normativa CCN-STIC en vigor.

En relación a la información clasificada:

- Las directrices a seguir en materia de SEGINFODOC para el tratamiento de información clasificada vienen reflejadas en un documento interno (Plan de Protección) de la propia Unidad donde se despliegue el módulo.

4.3.6 Integridad

Deberá tenerse en cuenta que:

- Los procedimientos para la identificación, autenticación y control de acceso, deben asegurar que la información no puede ser modificada por personal no autorizado.
- Las herramientas de seguridad del sistema, deben asegurar que se controlan los flujos de información.
- El sistema utilizará software de detección de virus y código dañino, en todos los servidores y estaciones de trabajo. Este software será actualizado periódicamente de acuerdo con lo establecido en los POS.
- Toda la información de entrada y de salida a la red será escaneada contra virus.
- Todos los datos anexados (ficheros) a los mensajes de correo electrónico serán escaneados antes de ser abiertos.

- La utilización de código activo (software) adicional o diferente al existente en el sistema requerirá verificar el origen del código, su integridad y la posibilidad de que contenga código malicioso, así como un control de cambios y de configuración para su autorización por la AOSTIC, antes de su puesta en producción.

4.3.7 Disponibilidad

Deberá tenerse en cuenta que:

- Para proteger la disponibilidad de los servicios que prestan la información manejada por el sistema, existirá un plan de protección que incluirá planes de contingencia, de seguridad y de emergencia.
- Cuando se produzca la interrupción de algún servicio del sistema, este deberá poderse restaurar de forma segura.
- Asimismo, en un documento interno se establecerá la frecuencia de las copias de respaldo (*backup*) y su almacenamiento en contenedores de seguridad (armarios de seguridad, cajas fuertes, cámaras acorazadas o armarios ignífugos) para evitar su manipulación o destrucción.
- Los procedimientos de mantenimiento del hardware y el software del sistema estarán definidos en un documento interno de la Unidad.
- Los equipos, los soportes informáticos, el equipamiento auxiliar y el cableado del sistema dispondrán del hardware y del apoyo de mantenimiento suficientes para garantizar su restablecimiento, en caso de fallo, en un tiempo limitado.
- El personal de mantenimiento dispondrá de la cualificación necesaria para restaurar el sistema en un tiempo limitado.
- Los fallos del sistema debidos al hardware deberán ser solucionados por personal de mantenimiento in situ debidamente acreditado y formado.
- El personal de mantenimiento perteneciente a un contratista debe estar acreditado.
- Los administradores de seguridad (AS) mantendrán un stock de repuestos esenciales.
- El control de configuración del software será responsabilidad de los AS y supervisado por el administrador de seguridad del Sistema (ASS) y el administrador de seguridad del sistema delegado (ASS-D).
- Los AS dispondrán de copias de seguridad y de procedimientos de recuperación para garantizar el restablecimiento del sistema en el menor tiempo posible.

- Las medidas electrónicas establecidas para la recuperación de la información serán probadas periódicamente por los AS. Los AS realizarán copias de seguridad periódicas de la configuración del sistema.
- Los AS realizarán copias de seguridad periódicas de la información.
- Los ASS-D realizarán copias de seguridad de los *logs* del sistema según lo establecido en documento interno de la Unidad donde se vaya a desplegar.
- Los ASS-D establecerán planes de contingencia que indicarán los procedimientos a seguir en casos de fallos de hardware, software o equipamiento auxiliar.
- Los responsables de seguridad del área (RSA) mantendrán un inventario del equipamiento auxiliar.
- Los AS implantarán redundancia de los equipos críticos del sistema.
- Se implantarán fuentes de alimentación redundantes en los servidores de producción del sistema.
- Se instalarán sistemas de protección física contra causas naturales: fuego, agua, etc.
- Se instalarán sistemas de alimentación ininterrumpida (SAI) para evitar fallos de suministro eléctrico y climatización.
- Se controlarán y protegerán las condiciones de temperatura y humedad de los locales por resultar críticas para la disponibilidad del sistema.
- Cualquier denegación de servicio del sistema será tratada como incidente de seguridad.

4.3.8 Comunicaciones

Deberá tenerse en cuenta que:

- Todos los equipos estarán integrados dentro de la red privada aislada a excepción del equipo frontera, que estará aislado de la red.
- Se permite la conexión con territorio nacional para la administración remota de los servidores a través del ILO (*Integrated Light Out*) de HP mediante la red IPC2.
- Solamente se podrán instalar o conectar a la red de comunicaciones equipos autorizados.
- Los equipos de comunicaciones y servidores, deben estar ubicados en un entorno local de seguridad (CORIMEC –*shelter o* contenedor de puerto-) salvo que se implanten medidas de seguridad adicionales.
- Todas las comunicaciones dentro del EGS estarán protegidas de acuerdo a la política de seguridad.
- Los protocolos de comunicaciones proporcionarán mecanismos de recuperación para preservar la integridad de los datos.

- No deberán mantenerse conversaciones, vídeos o presentaciones confidenciales en lugares públicos o sin medidas de protección a personas sin HPS o sin necesidad de conocer.

Las normas de la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), en su norma NS/03 -Seguridad Física- establece:

1. Si el local donde se van a instalar los terminales se encuentra a más de 1000 metros del perímetro de acuartelamiento, se considerará que éste está ubicado en una zona 3 TEMPEST.

2. Se debe establecer una adecuada separación física entre los equipos rojos y negros, y todo aquel elemento susceptible de ser inducido electromagnéticamente y que salga del área segura. Se define:

- Equipo rojo: todo elemento del sistema que maneje información clasificada sin cifrar, o simultáneamente información clasificada sin cifrar y otro tipo de información (información no clasificada, información clasificada cifrada, etc., como pueden ser los equipos cifradores).

- Equipo negro: todo elemento del sistema que maneja información no clasificada o clasificada cifrada, y cualquier otro elemento ajeno al sistema que sea susceptible de ser inducido electromagnéticamente por equipos rojos. Solo se tendrán en cuenta, y presentan un riesgo en cuanto a la emisiones TEMPEST, aquellos equipos negros que formen parte de un sistema que tenga líneas o elementos que salgan del área segura.

3. De manera específica, la normativa establece:

- Se establece una separación mínima de 50 cm, recomendable 1m, entre los equipos rojos y los equipos negros.
- Se establece separación de, al menos, 50 cm, recomendable 1m, entre equipos rojos y conductores fortuitos (tuberías de agua, cables, estructuras metálicas, etc.), incluyendo las líneas de corriente, que salgan del área segura.

- Se establece una separación mínima de 15 cm entre las líneas de alimentación rojas y cualquier línea o equipo negro que salga del área segura. Además, no se puede emplear un mismo conducto de distribución. En el caso de que las líneas rojas sean de fibra, la separación no es necesaria, y podrían ir por el mismo conducto.

- Se debe establecer una separación mínima de 15 cm entre las líneas de alimentación rojas y cualquier línea o equipo negro que salga del área segura.

- Si no se puede establecer una separación mínima entre los equipos rojos y negros, las líneas negras se deben filtrar antes de salir del área segura y aislar los conductores fortuitos en el punto en el que salen del área.

- Dentro del área segura las líneas de señal pueden ir bajo falso suelo o techo, pero siempre que sean fácilmente inspeccionables. Si es necesario que líneas rojas salgan del área, éstas deben ser protegidas por un tubo metálico que esté situado al menos a 1m de distancia del suelo. En ningún caso pueden salir líneas rojas del EGS.
- Los tubos dentro de los cuales se protegen los cables pueden ser metálicos, de plástico o fibra de vidrio, y deben:
  - Proporcionar un grado adecuado de atenuación y protección.
  - Soportar el peso de los cables que hay en su interior.
- Los tubos conteniendo líneas rojas deben ser sellados en toda su longitud, de modo que cualquier manipulación sea fácilmente detectable.
- Si se utilizan tubos metálicos:
  - En los puntos de entrada y salida del área segura el tubo debe ser protegido con material aislante.
  - El tubo debe ser puesto a tierra dentro y fuera del área segura.
- Los equipos rojos y negros no pueden tener el mismo cable de alimentación, a no ser que éste se filtre, que los equipos rojos estén tempestizados o que los equipos y/o líneas negras no salgan del área segura.
- A no ser que los equipos rojos estén tempestizados, su toma de tierra tendrá que tener las siguientes características:
  - La piqueta debe estar dentro del acuartelamiento.
  - El cable que une los equipos rojos con la piqueta no deben de salir del acuartelamiento.
  - La resistencia debe ser inferior a 5 ohmios.

ZONING

INSTALACIÓN EVALUADA ZONING		CLASIFICACIÓN ZONING DE LOCAL			
		ZONA 0	ZONA 1	ZONA 2	ZONA 3
CLASIFICACIÓN DE LA INFORMACIÓN	RESERVADO/SECRETO	Equipo CAT A	Equipo CAT A B	Equipo CAT A B C	Equipo CAT A B C D
	CONFIDENCIAL	Equipo CAT A B	Equipo CAT A B C	Equipo CAT A B C D	Equipo CAT A B C D
INSTALACIÓN NO EVALUADA ZONING		MENOR 20 m	ENTRE 20 Y 100 m	ENTRE 100 Y 1000 m	MAYOR QUE 1000 m
		ESPACIO INSPECCIONABLE DE SEGURIDAD			

Figura 9 - Zonning Fuente: Elaboración propia

4.3.9 Requisitos legales

Cualquier usuario que acceda al sistema debe conocer las responsabilidades legales aplicables:

- La Ley de Secretos Oficiales (9/1968) establece que podrán ser declaradas “materias clasificadas” los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento

por parte de personas no autorizadas puede causar daños o poner en riesgo la seguridad y defensa del Estado.

- Las conductas más graves contra la seguridad de las materias clasificadas de acuerdo con la Ley de Secretos Oficiales, encuentran su tipificación penal en el Código Penal (Ley Orgánica, 10/1995) y, para el caso de que dichas conductas se lleven a cabo por militares o por españoles en tiempo de guerra, en el Código Penal Militar (Ley Orgánica, 14/2015).
- El Código Penal contempla y penaliza diversas conductas relativas a la obtención, revelación, falseamiento e inutilización de materias clasificadas. El artículo 584 castiga como traidor, con la pena de prisión de seis a doce años, al español que con el propósito de favorecer a una potencia extranjera, procure, falsee, inutilice o revele información clasificada como secreta o reservada. A su vez los artículos 598 a 603, contemplan similares conductas, llevadas a cabo sin propósito de favorecer a potencia extranjera, castigándolas con penas que van desde los seis meses a los cinco años de prisión.
- Similares conductas, pero con penas en general más graves, son contempladas en el Código Penal Militar, para el caso de que los autores de las mismas sean militares o personal civil en tiempo de guerra.
- Aunque la Ley de Secretos Oficiales no contempla las materias clasificadas por otras naciones, sin embargo la Constitución Española, promulgada en el año 1978, otorga validez en el ordenamiento legal interno a cuantas disposiciones se contengan en tratados y acuerdos internacionales suscritos por España, al establecer en el artículo 96.1 que "los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno…". En coherencia con dicho artículo, la legislación española sobre materias clasificadas es directamente aplicable a las materias clasificadas según tratados o acuerdos firmados por España y otras naciones.
- Deberán respetarse los derechos de propiedad intelectual de las aplicaciones software (licencias, código) y de la información utilizadas por el sistema.

4.3.10 Riesgos

El análisis de riesgos (AR) permite valorar los riesgos existentes en el sistema teniendo en cuenta que, todos los activos del sistema (información, servicios, equipos, instalaciones, personal, etc.) pueden estar expuestos a diferentes amenazas.

Las amenazas al materializarse, degradan el activo produciendo un impacto que podemos estimar a partir del valor del activo en cada dimensión de seguridad CIDAT (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad).

Las estimaciones de las frecuencias con que se producen las amenazas y del impacto de las mismas, nos permiten estimar el riesgo. La adopción de acciones mitigadoras o salvaguardas nos permiten mitigar el riesgo, limitar el impacto o reducir la frecuencia con la que pueden ocurrir las amenazas.

El tratamiento de los riesgos, permite estimar el riesgo residual en cada fase del ciclo de vida del sistema dependiendo del nivel de madurez o grado de implantación de las salvaguardas.

El AR incluye:

- Evaluación de las salvaguardas con expresión del nivel de madurez actual y de las fases planificadas para alcanzar el objetivo final (alto nivel de implantación que permita un mínimo riesgo residual).
- Valoración de los riesgos acumulados y repercutidos por cada activo y para cada dimensión (CIDAT) a partir de la evaluación de las salvaguardas mencionada anteriormente.

5 ADMINISTRACIÓN DE LA SEGURIDAD

5.1 Gestión de la Seguridad

De acuerdo con las responsabilidades y la organización de seguridad del sistema, las actividades relacionadas con la gestión de seguridad les corresponden a:

Tabla 4 - Matriz actividades vs responsables – Fuente: Elaboración propia

Actividad	Responsables
Supervisión de la seguridad del sistema	ASS
Validación de documentos	AAS y ASS-D
Acreditación del sistema	AAS y ASS-D
Administradores del sistema	Administrador de Sistemas
Responsables de Seguridad de Áreas	RSA

5.2 Gestión de la Seguridad

La gestión de riesgos es el proceso de identificar, controlar y minimizar aquellos incidentes que pudieran afectar a los recursos del sistema. La gestión de riesgos trata las opciones para manejar el riesgo, incluyendo la reducción, transferencia, eliminación, posibilidad de ser evitado y la aceptación del riesgo. Tras el proceso inicial de gestión de riesgo, la base de información resultante será mantenida por la AOSTIC y utilizada como base para las actualizaciones futuras.

5.3 Procedimientos operativos de seguridad

Los Procedimientos Operativos de Seguridad (POS) de cada módulo o nodo, proporcionarán las instrucciones necesarias para procesar, almacenar y transmitir la información en el sistema. Para ello:

- Todos los POS serán actualizados en cada relevo.
- Las últimas versiones de los POS estarán disponibles digitalmente.

- Todos los usuarios deberán acusar recibo de la última versión de los POS haciendo constar su conformidad con los requisitos, su conocimiento y comprensión.

5.4 Formación y concienciación

A todos los usuarios se les impartirá formación por parte del ASS en el IN-PROCESING CIS que se lleva a cabo en todos los relevos del DAT, en lo referente a sus responsabilidades sobre:

- Protección de la seguridad de la información contra la pérdida de integridad, disponibilidad y confidencialidad.
- Protección de los servicios y de los recursos del Sistema, contra la pérdida de integridad y de disponibilidad.
- Gestión de soportes informáticos y conexión de dispositivos extraibles autorizados.
- Detección, reporte y gestión de incidentes.

Como parte de un programa de formación continuo, se realizarán comunicaciones periódicas sobre seguridad a todos los usuarios del sistema, de acuerdo al perfil de cada usuario, los procedimientos de uso de los distintos elementos del sistema (incluyendo hardware, software y comunicaciones) y la documentación técnica necesaria.

5.5 Gestión de incidentes

Para la gestión de incidentes de seguridad, se seguirá la CCN-STIC-403.

Se destaca que:

- De acuerdo con las actividades que describan los POS, cualquier usuario del sistema podrá comunicar al ASS, cualquier tipo de incidente de seguridad. En particular:
  - Incumplimiento de los POS que pueda afectar a la seguridad del sistema.
  - Detección de intrusiones, códigos maliciosos, *phishing* o robo de información.
  - Accesos físicos o lógicos no autorizados.
  - Manipulaciones no autorizadas de la información o material de cifra.
  - Personal que haya sido amenazado o coaccionado.
- Cualquier incidente será tratado como incidente de seguridad y se comunicará al ASS.
- Todos los usuarios conocerán los procedimientos de gestión de incidentes.
- Todos los procedimientos de gestión de incidentes estarán detallados en el POS.
- Los ASS comunicarán estos incidentes de seguridad a la autoridad correspondiente en materia de ciberdefensa para su investigación, análisis, solución y reparación. Por su parte, el ASS mantendrán informada a la AOSTIC y a la autoridad correspondiente en materia de ciberdefensa de los incidentes de seguridad graves detectados y de su estado.

- De acuerdo con las actividades que describan los POS, cualquier usuario del sistema podrá comunicar al AS cualquier otro tipo de incidente:
- Fallo de hardware, software, comunicaciones, aplicaciones, etc.
- Fallos de autenticación, impresión, alimentación, etc.
- Indisponibilidad de personal que afecte a la disponibilidad del sistema.

Los ASS, ASS-D/AS mantendrán un registro de incidentes y darán apoyo a los usuarios afectados por cualquier tipo de incidente, adoptando las acciones correctivas y preventivas necesarias para corregir el incidente y evitar su repetición.

5.6 Acreditación / Re-acreditación

El proceso para acreditar el sistema seguirá el procedimiento y los criterios establecidos por la Autoridad de Acreditación. En la página de intranet de la Dirección de Ciberdefensa del Ejército del Aire y del Espacio se puede encontrar documentación de apoyo a la acreditación.

La correcta operación de las características y controles de seguridad estará sujeta a auditoría y revisión continuas. Cualquier cambio en el entorno del sistema o fallos en la operación segura pueden determinar que deban implementarse nuevas contramedidas, y que el sistema deba ser reacreditado.

A continuación se muestra una lista de los cambios que pueden dar lugar a una re-acreditación:

- Cambios en el grado de clasificación de la información, que cause un cambio en las medidas de seguridad.
- Cambios en los requisitos de seguridad como resultado de cambios en la Política de Seguridad o la normativa aplicable.
- Cambios en las amenazas a, o vulnerabilidades del sistema.
- Modificaciones del sistema operativo o del software de seguridad relevante.
- Modificaciones del hardware que requieran un cambio en las medidas de seguridad aprobadas.
- Un fallo de seguridad, un fallo de la integridad, o de una situación inusual que invalide la acreditación indicando un defecto en el diseño de la seguridad.
- Un cambio significativo en la estructura física o en los POS.
- Un cambio significativo en la configuración del sistema.
- En referencia a la red, la inclusión de un sistema acreditado por separado, o la modificación o reemplazo del sistema.
- El resultado de una evaluación llevada a cabo por la AOSTIC.
- Un cambio significativo en el estado de seguridad del software de seguridad.

5.7 Baja de servicio

Cuando se produzca la baja del sistema o de algún equipo (hardware, software, comunicaciones, etc.) o servicio, la AOSTIC es responsable de asegurar que se llevan a cabo las siguientes actividades:

En materia de SEGINFODOC:

- Destrucción de información clasificada.
- Asegurar que se cumple todo lo referente a la Estructura Nacional de Protección de la información clasificada.
- Asegurar el cumplimiento referente a la seguridad de la información.

En materia de SEGINFOSIT:

- Para la destrucción y sanitización de soportes informáticos, se seguirá la CCN-STIC-305.

6 VALIDACIÓN

Este proyecto que es la base del diseño de un nodo desplegable en cualquier sitio del mundo, es un trabajo teórico, abierto, con implicaciones prácticas que se verán en un futuro no muy lejano.

Las pruebas y la posterior validación de todos los datos expuestos en este trabajo vendrán dados en las distintas misiones que los Ejércitos realicen tanto a nivel nacional como a nivel internacional.

Con el paso del tiempo y las diferentes evoluciones que vayan adquiriendo las misiones, tanto a nivel nacional, como a nivel internacional se podrá ir adaptando este trabajo a las futuras necesidades informáticas que puedan surgir.

El Centro de Informatica de Gestión (CIGES) es el centro de referencia dentro del Ejército del Aire y del Espacio en cuanto a informática en misiones en el exterior y es allí donde se ha puesto en marcha todo lo relativo a este proyecto, desde la compra de material hasta la configuración de todos los elementos hardware. Obviamente, esto es un proceso lento donde la compra tanto del software como del hardware se hace a través de un expediente de contratación con su pliego de prescripciones técnicas correspondiente, que se gestiona a través de una plataforma de contratación del Estado, lo que conlleva una serie de trámites con unos plazos preestablecidos.

7 CONCLUSIONES Y LÍNEAS FUTURAS

Se puede observar, que en la realización de un proyecto con semejantes singularidades, que además incluye diversas variables abiertas (país destino, detalles específicos de la ubicación, etc), el proceso de estandarizar los procedimientos de trabajo adquiere una complejidad aún mayor.

Con la finalidad de realizar la ejecución del presente proyecto con las garantías suficientes, se han concretado las citadas variables. Para ello, se ha seleccionado un conjunto de parámetros y especificaciones técnicas, para solventar las vicisitudes técnicas que plantea el proyecto.

Seguidamente, se especifican las citadas variables abiertas:

1. Selección del medio de transporte para el transporte logístico.
2. Cálculo del tiempo necesario para trasladar el material al país destino.
3. Soluciones técnicas de cableado y configuración para realizar la instalación.

En definitiva, la solución propuesta puede ser implementada en un gran número de escenarios. Aun así, existe la posibilidad de que, en algunas situaciones, el despliegue de módulos desplegables acreditados por el CCN en condiciones muy singulares, no pueda ser llevado a cabo con la información presente en el proyecto. En estas situaciones, se deberán realizar las modificaciones oportunas, para solucionar la posible problemática y contratiempos técnicos que no se hayan contemplado.

A continuación, se relacionan los objetivos del trabajo:

1. Plasmar por escrito las necesidades genéricas que pueda requerir un despliegue de módulos acreditados por el CCN en cualquier país del mundo.

2. Definir teóricamente un módulo desplegable acreditado por el CNN para dar unos servicios básicos a los usuarios desplegados en un Destacamento del Ejército del Aire y del Espacio, así como la posterior conexión a Internet y telefonía IP a través de satélite.

3. Dotar a la infraestructura de los elementos de red necesarios para poder ampliar el servicio hasta un máximo de 40 personas.

Finalmente, se detalla el cumplimiento real obtenido frente al cumplimiento planificado en la Tabla 4.

Tabla 5 - Comparación de los objetivos definidos y niveles alcanzados. Fuente: Elaboración propia

OBJETIVO	NIVEL DEFINIDO	NIVEL ALCANZADO
1. Estandarización de necesidades por escrito	Documentar las necesidades genéricas y establecer unos parámetros comunes en los despliegues	Se ha conseguido estandarizar y documentar la gran mayoría de procesos presentes en el proyecto. Las únicas situaciones que no se han podido abordar en su totalidad, se han especificado en el apartado
2. Instalar 20 rosetas con Internet y telefonía IP	Instalar las rosetas conforme a los requisitos indicados	Objetivo parcialmente cumplido. Se han cumplido la totalidad de requisitos exigibles a excepción de la velocidad de subida estándar (1000 kbps contratados, por 1620 kbps planeados) necesaria en el destacamento. Para solventar la incidencia, se ha desarrollado un procedimiento para la creación de un listado de usuarios críticos
3. Acondicionar la infraestructura para un máximo de 40 personas	Adaptar la infraestructura de red conforme a los requisitos indicados	Objetivo cumplido

La planificación estipulada, se ha desarrollado teniendo en cuenta los márgenes de tiempo necesarios, para realizar la totalidad de procesos que componen el proyecto.

En lo que respecta a la metodología utilizada para la consecución del proyecto, indicar que se ha tenido en cuenta, la gran cantidad de dificultades y singularidades que conlleva el despliegue de módulos desplegables acreditados por el CCN con estas características (rápida disponibilidad, desconocimiento del lugar y edificación, transporte, etc).

Con el despliegue de futuros módulos desplegables acreditados por el CCN en los destacamentos, y haciendo uso de las líneas maestras determinadas en este proyecto, se podrá obtener el feedback del personal implicado. Todo ello, con la finalidad de solucionar la posible problemática que pueda acaecer en el desarrollo de los trabajos.

Con esta información, se podrán pulir y perfeccionar aquellos detalles técnicos que no hayan sido tenidos en cuenta, o que necesiten modificarse.

Este trabajo continuo de seguimiento y control, tiene como objetivo el realizar una planificación lo más precisa y real posible. Al disponer de una planificación optimizada, se mejora el desarrollo e implementación de los futuros despliegues. Además, sirve de gran ayuda para el planeamiento a gran escala existente en el teatro de operaciones, en el que la OTAN tiene responsabilidad de acción.

8 BIBLIOGRAFÍA

[1] CCN-STIC-522A: Configuración Segura Windows 10 Enterprise (Cliente Miembro de Dominio).

[2] CCN-STIC-530: Seguridad en Microsoft Office 2010.

[3] CCN-STIC-521A: Configuración Segura de Windows Server 2012 R2: Instalación Completa, Servidor Miembro (No Core, No Independiente).

[4] CCN-STIC-524: Seguridad en Internet Information Server (IIS) 7.5 sobre Windows Server 2010 R2 en Servidor Miembro del Dominio

[5] CCN-STIC-550: Microsoft Exchange Server 2010 en Windows Server 2008 R2.

[6] CCN-STIC-590: Recolección y Consolidación de Eventos con Windows Server 2012 R2.

[7] Armelin Asimane; "Windows Server 2012 R2"; 2014.

[8] Willian R. Stanek; "Windows Server 2012: "Guia del Administrador"; 2014

[9] Sebastian Neild; "Windows Server 2012 R2: Administración Avanzada"; 2014.

[10] Características y configuración switch Enterasys. Disponible en:

https://cdn.plixer.com/files/enterasysSflow.pdf

[11] Características y configuración SAI-HP. Disponible en:

http://h10032.www1.hp.com/ctg/Manual/c02948855

[12] Configuración de Exchange

https://sdei.unican.es/paginas/servicios/correo/manual_mapi_casa.aspx

[13] https://www.tiendatr.com/patch-panel-equip-769248-48-puertos-keystone-cat6-19-

[14] http://www.onedirect.es/productos/grandstream/grandstream-gxp1610

[15] http://www.speedtest.net/

[16] http://calderon.cud.uvigo.es/handle/123456789/333

[17] http://calderon.cud.uvigo.es/handle/123456789/498

[18] http://calderon.cud.uvigo.es/handle/123456789/495

[19] La Guía CCN-STIC 305 se reclasifica como Uso Oficial y se ha publicado en la parte privada del portal del CCN-CERT.

[20] "*Hiperconvergencia: papel en la evolución de los centros de datos. Aplicación a los nodos de misión desplegables FMN-ESP"* http://calderon.cud.uvigo.es/handle/123456789/333 (última consulta 10 de enero de 2023)

[21] *"Presente y Futuro de los Nodos Desplegables. Estudio de la viabilidad de la tecnología HCI para albergar servicios clasificados/no clasificados de la OTAN a los nodos de misión desplegables"* http://calderon.cud.uvigo.es/handle/123456789/498 (última consulta 10 de enero de 2023

[22] "*Internet como canal de comunicaciones para redes clasificadas, posible solución versátil y segura para despliegues militares"* http://calderon.cud.uvigo.es/handle/123456789/495 (última consulta 10 de enero de 2023)

[23] HPE https://www.hpe.com/es/es/home.html (última consulta 10 de enero de 2023)

[24] DELL https://www.dell.com/es-es (última consulta 10 de enero de 2023)

[25] FUJITSU https://www.fujitsu.com/es/(última consulta 10 de enero de 2023)

[26] Hyper V Introducción a Hyper-V en Windows 10 | Microsoft Learn (última consulta 10 de enero de 2023)

[27] VMWare VMware España ofrece la base digital para la empresa | ES (última consulta 10 de enero de 2023)

[28] Citrix All in one Workspace Solution for Secure Access to Apps and Data - Citrix (última consulta 10 de enero de 2023)

[29] Herramienta PILAR. https://pilar.ccn-cert.cni.es (última consulta 12 de enero de 2023)

[30] Ley Orgánica 10/1995, de 23 de noviembre https://www.boe.es/eli/es/lo/1995/11/23/10 (última consulta 10 de enero de 2023)

[31] Ley Orgánica 14/2015 de 14 de octubre https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-11070 (última consulta el 10 de enero de 2023)

[32] MAGERIT. https://www.administracionelectronica.gob.es (última consulta 7 de enero de 2023)

[33] Normas NS de la ANPIC -Autoridad Nacional de Protección de la Información Clasificada. https://www.ccn.cni.es/index.php/es/menu-ccn-es/oficina-nacional-de-seguridad-ons (última consulta realizada el 10 de diciembre de 2022)

ANEXO I: PRESUPUESTO

ELEMENTOS HARDWARE QUE COMPONEN EL MODULO DESPLEGLABLE Y COTIZACION	CANT.	PVP	TOTAL
Switch Enterasys A4H124-24FX	2	2.100,00 €	4.200,00 €
APC Smart UPS 450VA USB RM 1U 230V	1	250,00 €	250,00 €
AT-MC 102XL	5	121,67 €	608,35 €
Router CISCO 2901 IOS ADVANCED SECUTITY	1	1.200,00 €	1.200,00 €
Tarjetas CISCO HWIC-2T	1	322,00 €	322,00 €
Cable CISCO p/n CAB-SS_V35 MT (DTE Male)	2	20,00 €	40,00 €
Pc Hp cmt 8300	18	700,00 €	12.600,00 €
Tarjeta de red ethernet pci 100 mbps fibra optica tipo sc	18	100,00 €	1.800,00 €
Servidor HPDl380p Gen8 8-LFF Cto Server (665553-B21)	2	1.192,90 €	2.385,80 €
HP DL380p Gen8E5-2640 FIO kit (662246-L21)	2	727,56 €	1.455,12 €
HP 16 GB 2Rx4 PC3L-10600R-9 kit (647901-B21)	8	162,50 €	1.300,00 €
Factory Integrated (647901-0D1)	8	,00 €	0,00 €
Hp 600Gb 6G SAS 15K 3.1 IN SC ENT HDD (652620-B21)	16	310,23 €	4.963,68 €
HP 12.7 mm SATA DVD RW JB kit (652235-B21)	2	70,17 €	140,34 €
Factory Integrated (652235-0D1)	2	69,00 €	138,00 €
HP Ethernet 1 GBE 4P 331FRL FIO Adapter (684208-B21)	2	7,39 €	14,78 €
HP 2U LFF BB RAIL GEN8 Kit (663480-B21)	2	81,25 €	162,50 €
HP 1 GB FBWC FOR P-SERIES SMART ARRAY (631679-B21)	2	280,68 €	561,36 €
Factory Integrated (631679-0D1)	2	58,00 €	116,00 €
HP 82Q 8GB DUAL PORT PCI-E FC HBA (AJ764A)	2	1.107,95 €	2.215,90 €
Factory Integrated (AJ764A-0D1)	2	70,00 €	140,00 €
HP 460W GS PLAT PL HT PLG PWR SUPPLAY Kit (656362-B21)	4	169,89 €	679,56 €
Factory Integrated (656362-0D1)	4	75,00 €	300,00 €
HP 3Y SUPPORT PLUS 24 SVC (HA110A3)	2	600,00 €	1200,00 €
HP PROLIANT DL 38X (P) HW SUPPORT (HA110A3 7G3)	2	1.046,02 €	2.092,04 €
HP ILO ADV E-LTU INC 1YR TS&U SW (TA850AAE)	2	274,43 €	548,86 €
HP 3Y SUPPORT PLUS 24 SVC (HA110A3)	2	0,00 €	0,00 €
HP ILO ADV Pack NONBL SW SUPPORT (HA110A3 7X4)	2	55,68 €	111,36 €
Impresora CANON LBP 6300dn	2	347,00 €	694,00 €

Latiguillo bifibra MMF MTRJ/SC 50/125 µm 1m	48	25,00 €	1.200,00 €
PigTails de fibra SC 50/125 µm	100	4,00 €	400,00 €
Latiguillo bifibra MMF SC/SC 50/125 µm 2m	90	10,00 €	900,00 €
Latiguillo bifibra MMF SC/SC 50/125 µm 1m	90	9,85 €	886,50 €
Patch Panel 19" 1U de fibra óptica conectores SC	6	171,80 €	1.030,80 €
Panel 19" 1U con 5 anillas de plástico	3	15,10 €	45,30 €
Regleta de alimentación Shucko de 8 enchufes e interruptor	1	56,29 €	56,29 €
Armario de red 19'' 27U, puerta de metacrilato y cerradura de seguridad	1	500,00 €	500,00 €
Fibra Óptica de dos hilos interior 50/125 µm	2000	2,00 €	4.000,00 €
F.O. de dieciséis (16) hilos exterior, con recubrimiento anti-roedores 50/125 µm	600	1,93 €	1.158,00 €
Rosetas de fibra óptica dobles para pigtail SC	50	25,16 €	1.258,00 €
Suspensión clic para Rejiband 400	80	8,81 €	704,80 €
Rejiband 400x60 3m	40	23,97 €	958,80 €
Rejiband ángulo 90º	6	16,50 €	99,00 €
Rejiband semicodo	6	18,00 €	108,00 €
Unión clic rápida	8	4,23 €	33,84 €
Suspensión central clic para M8	200	2,30 €	460,00 €
Soporte universal pared	90	4,97 €	447,30 €
Fijación techo	150	3,28 €	492,00 €
Salida tubos	40	3,85 €	154,00 €
Soporte para bridas	80	1,33 €	106,40 €
Rejifix rollo de 25m	1	80,65 €	80,65 €
Placas de identificación	50	0,95 €	47,50 €
Canaleta	100	2,50 €	250,00 €
Canaleta codos de 90º	80	1,25 €	100,00 €
Canaleta topes	80	1,25 €	100,00 €
Varilla rosacada M8	150	3,71 €	556,00 €
Tacos de expansión M8	100	1,20 €	120,00 €
Arandela plana	400	0,08 €	32,00 €
Bridas UNEX 199x3,6 bolsa 100 ud. (2235)	4	4,72 €	18,88 €
Bridas UNEX 370x4,8 bolsa 100 ud. (2249)	4	10,45 €	41,80 €
Caja Tacos nylon de 6mm	10	6,50 €	65,00 €
Caja Tacos nylon de 8mm	10	7,60 €	76,00 €
Caja tirafondos de 6x40	10	14,00 €	140,00 €
Caja tirafondos de 8x40	10	17,00 €	170,00 €
Tuercas M8	400	0,11 €	44,00 €
Pasamuros SC/SC	60	4,00 €	240,00 €
Tubo corrugado libre de Halogenos M-25 (R-75)	200	1,88 €	376,00 €
Latigullo UTP Cat.6 de 3 mts. Brand Rex	40	6,15 €	246,00 €
Latigullo UTP Cat.6 de 5 mts. Brand Rex	40	7,15 €	286,00 €
	SUMA TOTAL =		**58.228,51 €**

Presupuesto total del Módulo Desplegable

(Todos estos precios son sin IVA y sin descuentos comerciales)

ANEXO II: CONFIGURACIÓN DEL SISTEMA

CONFIGURACIÓN HARDWARE/FIRMWARE

CARACTERÍSTICAS HARDWARE DEL SERVIDOR HP PROLIANT DL 380P G10	
Marca/Modelo:	HP PROLIANT DL380 Gen 10
N/S	CZ2928132S
Microprocesador:	Intel® Xeon® Silver 4214 CPU @ 2.20 Ghz (2 procesadores/12 cores)
Memoria RAM:	96 GB
Discos Duros:	2 Discos 240 GB RAID 1: C: \Disco local 223GB 4 Discos 600GB RAID 5: D:\Hyper-V 2,18TB 4 Discos 600GB RAID 5: E:\Backup 2,18 2 Discos 600GB-Spare Disk
Periféricos:	LCD 8500 N/S: 2C483898F9 KVM N/S: 5CW8282C7E
Monitor:	NO
Teclado / ratón:	NO
Otra información:	Interfaces de red: 4 Ethernet