PREMIOS EJÉRCITO DEL AIRE Y DEL ESPACIO 2024

XLV Edición

Disciplina: Promoción de la cultura aeroespacial.

Modalidad: Promoción de la cultura aeroespacial en el ámbito de la Transformación Digital del EA, categoría individual.

“CREACIÓN Y OPERACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN EN EL ALA 31, BASE AÉREA DE ZARAGOZA”

RESUMEN

A lo largo de las siguientes páginas, se detalla el proceso completo de creación de un sistema de gestión de información en el entorno del Ala 31, Zaragoza, considerando como puntos clave la eficiencia, la optimización de procesos y la accesibilidad de los servicios a proporcionar así como la disponibilidad, trazabilidad, autenticidad, integridad y confidencialidad consideradas como dimensiones de seguridad, partiendo de una situación inicial y real que requiere cambios para su evolución y desarrollo tecnológico frente a una sociedad cada vez más interconectada y desafiante.

En dicho documento, se tratan también aspectos de ciberseguridad, tecnología de la información y comunicación, redes, defensa y aeronáutica, describiendo sistemas aeronáuticos cuya comprensión es relevante dentro de este contexto debido a la información que generan y procesan.

Se debe tener en cuenta que toda la evaluación de este proyecto se realiza de acuerdo con el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS).

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

GLASARIO DE TÉRMINOS

AES (Advanced Encryption Standard): Estándar de Cifrado Avanzado

Autenticidad: verificar la identidad de alguien o algo.

CCN: Centro Criptológico Nacional

CPD: Centro de Procesamiento de Datos

Confidencialidad: Garantizar el nivel necesario de secreto de la información y su tratamiento.

Disponibilidad: Capacidad de un servicio, sistema o datos a ser accesible y utilizable

EA: Ejército del Aire

EFB (Electronic Flight Bag): Dispositivo portátil utilizados por los pilotos de las aeronaves.

ENS: Esquema Nacional de Seguridad

FLIGHTOPS (Flight Operations System): Sistema de Planificación de Misión.

GPO (Group Policy Object): Política de Grupos de Objetos.

HTTPS (Hypertext Transfer Protocol Secure): Protocolo seguro de Transferencia de Hipertexto.

IETP-X (Integrated Electronic Technical Publications): Sistema de Integración de Publicaciones Electrónicas.

Integridad: Garantía de exactitud y fiabilidad de la información.

IPSec: Protocolo de seguridad de la capa de Internet.

ISS (Initial Support Service): Soporte de Servicio Inicial de las aeronaves.

LTMS (Lifetime Monitoring System) Sistema de Monitorización a Largo plazo.

LPC-NG (Less Paper in Cockpit - New Generation): Sistema Aeronáutico.

MDS (Maintenance Data System): Sistema de Mantenimiento de Datos.

MPRS (Mission Planning and Resources System): Sistema de Planificación de Misión

NAS (Network Attached Storage): Sistema de Almacenamiento.

OpenVPN (Open Virtual Private Network): Red Privada Virtual.

PHM (Power Plant Health Monitoring): Enfoque proactivo para monitorear la capacidad de estructuras, sistemas y componentes.

PMAT (Portable Multipurpose Aircraft Terminal): Terminal portable.

RSA (Rivest-Shamir-Adleman): Sistema criptográfico de clave pública.

SHA-256 (Secure Hash Algorithm): Algoritmo de hash seguro de 256 bits.

SMBv3 (Server Message Block versión 3): Protocolo del Bloque de mensajes del servidor.

SSL(Secure Sockets Layer) Protocolo de seguridad a través de Internet.

TIC: Tecnología de la Información y Comunicación

TCP/IP: Transmission Control Protocol/Internet Protocol

TLS: Transport Layer Security

Trazabilidad: Propiedad de un conjunto de daos que gartiza la posibilidad de conocer su origen, uso, recorrido y localización.

WebDAV: Web-based Distributed Authoring and Versioning

1. INTRODUCCIÓN

En la era actual, la información se ha convertido en un recurso invaluable que impulsa el funcionamiento de la sociedad y las organizaciones. Su adecuada gestión no solo previene errores que podrían generar repercusiones significativas, sino que también permite tomar decisiones informadas y eficientes.

La Tecnología de la Información y Comunicación (en adelante TIC) se caracteriza por ser la aplicación de ordenadores y equipos de telecomunicaciones y desempeña un papel fundamental en la recopilación, transmisión y manipulación de datos en diversos sectores. Dentro de este contexto, el ámbito militar es un terreno donde la información adquiere una dimensión crítica.

El presente trabajo se enfoca en abordar un desafío específico dentro del Ejército del Aire y del Espacio (EA), centrándose en el Ala 31 ubicada en la Base Aérea de Zaragoza a fecha de enero del 2024. Esta unidad desempeña un papel esencial en las operaciones del EA, utilizando aeronaves A400M para una variedad de misiones estratégicas y operativas.

Los aviones A400M representan una avanzada tecnología de transporte militar, cuya eficacia depende no solo de la aeronave en sí, sino también de los sistemas en tierra que la respaldan como se indica más adelante. El edificio de Soporte de Sistemas del Ala 31, por ende, se convierte en un elemento crucial para el éxito operativo de estas aeronaves al gestionar y almacenar la información necesaria para sus operaciones.

El presente trabajo, no solo analiza la situación actual de la gestión de información en este contexto, sino que también propone e implementa una solución para mejorarla. Al examinar las prácticas existentes y deseadas, se pretende identificar áreas de mejora y establecer prácticas recomendadas que optimicen la gestión de la información en el contexto específico del Ala 31 y sus operaciones con el A400M. Además, se hace un análisis exhaustivo de las regulaciones y normativas a tener en cuenta desde el punto de vista de la seguridad de la información.

Por ello, para abordar las deficiencias identificadas en la gestión de la información, se propone la creación de un sistema de gestión de información que se implementará desde cero para optimizar la recopilación, almacenamiento, transmisión y manipulación de datos, permitiendo una toma de decisiones más informada y eficiente.

En resumen, las siguientes páginas explorarán la importancia crucial de la gestión de la información en el ámbito militar, enfocándose en el papel fundamental que desempeñan el Ejército del Aire, el Ala 31 y los sistemas de soporte en el éxito operativo de las misiones aéreas. Además, se analizará la creciente importancia de aprovechar eficazmente la información en un entorno en constante cambio, donde el cumplimiento de los objetivos estratégicos y operativos de las Fuerzas Armadas depende en gran medida de una gestión de datos efectiva y segura.

2. SEGURIDAD Y CIBERESPACIO

La creciente dependencia tecnológica de la sociedad es un hecho innegable, y resulta esencial para el funcionamiento eficaz de los Estados, así como de sus fuerzas de seguridad y sus infraestructuras.

Esta dependencia está en constante aumento y se prevé que siga en aumento en los años venideros. Además, las tecnologías de la información han posibilitado muchas de las funciones de las Fuerzas Armadas a nivel global: como pueden ser el respaldo logístico, el mando y control de sus unidades, y la obtención de información en tiempo real, entre otras muchas. Cada una de estas funciones se encuentra interconectada y depende directamente de las redes de comunicación e informáticas.

Este panorama plantea tanto oportunidades como desafíos. Si bien las TIC han mejorado la eficiencia y efectividad en la planificación y ejecución de operaciones militares, también han introducido nuevos riesgos en términos de seguridad y protección de datos sensibles.

Como ya se sabe, el ciberespacio es la nueva dimensión de confrontación que se añade a los dominios tradicionales de tierra, mar y aire. Los actores estatales y no estatales pueden buscar ventajas estratégicas a través de operaciones cibernéticas y por ello esta evolución ha llevado a que los conflictos y las tensiones entre naciones se manifiesten no solo en el mundo físico, sino también en el mundo digital.

Por consiguiente, los ataques cibernéticos ya no solamente tienen motivación intelectual o económica, sino también política. Por esta razón, en este proyecto se hace especial hincapié en la seguridad de los datos ya que es fundamental mantener los sistemas de gestión de información correctamente protegidos frente a posibles ataques o filtraciones y comprender la importancia de la ciberseguridad, especialmente en el ámbito militar debido al carácter confidencial de la información.

3. EJÉRCITO DEL AIRE Y DEL ESPACIO

El Ejército del Aire y del Espacio de España, también conocido como Fuerza Aérea Española corresponde a uno de los tres ejércitos que forman las Fuerzas Armadas Españolas y tiene asignada la misión de garantizar la soberanía e independencia de España, el ordenamiento constitucional, la defensa de su integridad territorial con cuidado especial del espacio aéreo y mantener la seguridad de las operaciones, según dicta el Artículo octavo de la Constitución Española.

En el presente documento se tienen en cuenta los valores positivos de la Fuerza Aérea garantizando el profesionalismo y compromiso de las personas implicadas, la adherencia estricta a los procedimientos y normativas establecidas y tratadas en el proyecto, el compromiso con la ética, la integridad y el respeto, el ajuste a la institución y sus objetivos, la vocación al servicio público, el compromiso con la protección y defensa de los intereses nacionales, la seguridad de los ciudadanos y de la información, la promoción del desarrollo tecnológico mejorando las capacidades operativas y el cumplimiento estricto de las responsabilidades asegurando una gestión de recursos eficiente y transparente.

4. AERONAVE A400M

En diciembre de 2016, el EA recibió el primer A400M, que fue entregado en la Base Aérea de Zaragoza al Ala 31, unidad que se encarga del mantenimiento y operación de los aviones de la flota de T.23 (nombre que recibe el A400M en nomenclatura del Ejército del Aire).

Figura 1: Aeronave A40M. Google Imágenes

Actualmente, en el Ala 31 trabajan alrededor de esta nave un grupo extenso de personas que se ha encargado de dar apoyo inicial a la entrada en servicio de la aeronave (ISS, Initial Support Service).

El Airbus A400M es un avión militar de transporte diseñado con tecnologías avanzadas que le otorgan un rendimiento excepcional. Además, cuenta con avanzados sistemas de aviónica, que incluyen pantallas electrónicas multifuncionales, un sistema de navegación por satélite, sistemas de comunicaciones avanzados y sistemas de alerta temprana y de evitación de colisiones. También cuenta con un sistema de protección contra amenazas enemigas, incluyendo un sistema de autodefensa y un sistema de contramedidas electrónicas, que pueden proteger al avión contra misiles y otros ataques enemigos.

Otras tecnologías avanzadas que se incluyen en el A400M son su sistema de tren de aterrizaje avanzado, que permite aterrizar en pistas no preparadas, y su sistema de navegación por terreno, que proporciona una mayor seguridad en vuelos a baja altitud.

Sin embargo, este proyecto centra el foco de atención en los sistemas en tierra que contribuyen y actúan como soporte para el buen funcionamiento y operatividad de la aeronave A400M y en la seguridad de la información que utilizan, ya que estos sistemas generan y procesan gran cantidad de datos e información que será almacenada en el sistema de gestión de información que se propone.

4.1. SISTEMAS EN TIERRA

Cada una de las tareas realizadas por la aeronave conlleva la administración de una extensa cantidad de recursos y siempre implica el uso de uno o varios equipos terrestres destinados a esta función. Además, para asegurar la disponibilidad de los sistemas en tierra, se requiere llevar a cabo un proceso de calibración de equipos y herramientas.

Cada vez que la aeronave realiza una operación, ya sea en vuelo o un arranque de motor, se genera una gran cantidad de datos que deben ser registrados y analizados con el fin de anticipar diversas situaciones o fallos. Por ello, los sistemas informáticos de aviación militar en tierra desempeñan un papel crucial en el almacenamiento y la creación de información a la hora de respaldar las operaciones aéreas. Estos sistemas varían en su función y alcance, pero en general, están diseñados para recopilar, gestionar y distribuir información que es esencial para la planificación, ejecución y análisis de misiones y tareas militares.

A continuación, se mencionan brevemente tres de los sistemas en tierra más relevantes en el escenario del Ala 31.

4.1.1. SISTEMA DE MANTENIMIENTO (MDS)

El Sistema de Mantenimiento, conocido como MDS (Maintenance Data System), corresponde a uno de los pilares esenciales para el funcionamiento eficiente y seguro de la aeronave A400M.

Este sistema web integra diversos perfiles y realiza, en función de la responsabilidad, la gestión de la flota, la gestión de misión, y tareas de ingeniería, mantenimiento y documentación.

El sistema MDS despliega un enfoque proactivo para el mantenimiento de la aeronave al almacenar y registrar datos cruciales relacionados con su funcionamiento y estado, incluyendo información sobre el rendimiento de los sistemas, registros de mantenimiento previo, historiales de reparaciones y reemplazos de componentes, entre otros. Por ello, este sistema se convierte en una herramienta estratégica para garantizar la aeronavegabilidad, prevenir fallos y optimizar los procesos de mantenimiento.

De esta forma, los sensores y sistemas integrados en la aeronave transmiten datos constantemente al MDS, permitiendo una evaluación continua del rendimiento y la detección temprana de cualquier anomalía. Por consiguiente, se habilita una respuesta proactiva a posibles problemas y ayuda a prevenir fallos inesperados.

Por otro lado, se pueden planificar las misiones simulando sus posibles consumos de potenciales y cambios de configuración de misión (rol) antes de asignar definitivamente una aeronave gracias a los módulos dedicados a la gestión de flota y misión. Una vez preparada la misión, se puede acceder a datos concretos del estado de la aeronave, al libro de avión y al certificado de aptitud para el servicio (CSR, Certificate of Release to Service), que se emite una vez finalizado el mantenimiento sobre la aeronave y que engloba todas las tareas realizadas sobre el avión entre misiones.

Tras el vuelo, los distintos sistemas del avión generan una serie de archivos que se cargan en el MDS para introducir los parámetros de envejecimiento del avión y para reportar los códigos de fallo y así automatizar, en función de estos, el proceso de seguimiento y detección de averías. Por ello, una característica distintiva del MDS es su capacidad para monitorear el estado de la aeronave en tiempo real.

Así, el MDS tiene la capacidad de predecir y planificar tareas de mantenimiento utilizando los datos almacenados y el análisis en tiempo real. Al evaluar patrones de rendimiento y desgaste, el sistema puede sugerir cuándo es el momento óptimo para llevar a cabo inspecciones, reemplazos de componentes o ajustes. Esto no solo minimiza el tiempo de inactividad de la aeronave, sino que también optimiza la eficiencia de los recursos.

Los reportes generados por este sistema son valiosos para el equipo de mantenimiento y para la toma de decisiones operativas. Además, el análisis de los datos históricos puede ayudar a identificar patrones de problemas recurrentes y guiar mejoras continuas en la aeronave.

Al concluir este punto, queda patente la vital importancia de una gestión eficiente de toda la información generada y manejada por el sistema MDS. La efectividad operativa y la toma de decisiones estratégicas respectivas a las aeronaves A400M del Ala 31 dependen en gran medida de la disponibilidad, integridad y seguridad de la información que fluye a través del MDS.

4.1.2. SISTEMA DE PLANIFICACIÓN DE MISIÓN (MPRS)

El Sistema de Planificación de Misión, conocido como MPRS (Mission Planning and Resources System), es otro de los sistemas que juegan un papel esencial en la planificación y ejecución eficiente de las misiones aéreas de la aeronave A400M.

Este sistema abarca desde la organización de recursos y datos hasta la creación de rutas y horarios, desempeñando un rol crucial en la garantía de operaciones exitosas y seguras. Además, permite la gestión integral de recursos necesarios para cada misión incluyendo la asignación de tripulaciones, equipos, cargas útiles y combustible. El MPRS integra información relevante como datos meteorológicos, regulaciones de tráfico aéreo y consideraciones logísticas y también facilita la creación y optimización de rutas de vuelo.

Teniendo en cuenta factores como la distancia, el tiempo, el consumo de combustible y las restricciones del espacio aéreo, el sistema genera rutas eficientes y seguras generando planes de vuelo resultantes que cumplen con las regulaciones y optimizan el tiempo y los recursos.

Gracias a este sistema, los usuarios pueden compartir datos, intercambiar comentarios y ajustar planes en tiempo real. Esta funcionalidad fomenta la toma de decisiones informada y la adaptación ágil a los cambios en condiciones operativas. Por otro lado, el sistema permite la simulación y análisis de diferentes escenarios antes de la ejecución de la misión. Esto ayuda a evaluar la viabilidad y los posibles desafíos de cada enfoque, permitiendo ajustes previos y una mejor preparación para contingencias

4.1.3. SISTEMA DE OPERACIONES DE VUELO (FLIGHTOPS)

El Sistema FLIGHTOPS, conocido como Flight Operations System, juega un rol central en la operación y gestión eficiente de las misiones aéreas de la aeronave A400M.

Dicho sistema abarca desde la planificación inicial de vuelos hasta la ejecución y el análisis post-misión e integra datos críticos y herramientas para garantizar la toma de decisiones informadas y la optimización de las operaciones aéreas. Además, permite la planificación detallada de vuelos, esto incluye la creación de rutas, la asignación de tripulaciones y recursos, la programación de horarios, la integración de datos meteorológicos, regulaciones aéreas y parámetros de la aeronave para garantizar que los vuelos se planifiquen con precisión y seguridad.

Además, FLIGHTOPS ofrece un monitoreo continuo de los vuelos en tiempo real. Al igual que en el caso del sistema MDS, los sistemas integrados en la aeronave transmiten y proporcionan datos de navegación, rendimiento y condiciones de vuelo a FLIGHTOPS. Esto permite a los operadores y equipos de control en tierra supervisar el progreso y tomar decisiones basadas en datos en cualquier momento.

El sistema facilita la comunicación entre tripulaciones y equipos de soporte en tierra ya que los cambios en la planificación o las condiciones pueden comunicarse rápidamente, lo que garantiza una colaboración efectiva y una adaptación ágil a situaciones cambiantes.

Una vez finalizada la misión, FLIGHTOPS permite el análisis exhaustivo de los datos generados incluyendo la revisión de parámetros de vuelo, el rendimiento de la aeronave y las decisiones tomadas. El análisis post-misión proporciona información valiosa para mejorar futuras operaciones.

Gracias a este sistema, se garantizan operaciones seguras y eficientes en un entorno operativo dinámico y la integración de datos y toma de decisiones basadas en los mismos son los pilares que permiten una operación efectiva y una continua mejora en la aviación militar de transporte del Ala 31.

4.1.4. OTROS SISTEMAS

La documentación técnica se encuentra integrada en un sistema informático mediante el IETP-X (Integrated Electronic Technical Publications) que aúna toda la documentación aplicable a cada aeronave en particular, tanto de mantenimiento como de operación y que es renovada cada 3 meses. También, el sistema incorpora sistemas de seguimiento de la vida en servicio de la aeronave.

Por otro lado, el sistema LTMS (Life Time Monitoring System) tanto para la estructura del avión como para su planta de potencia (PHM, Power Plant Health Monitoring) es la base del programa de fiabilidad para control de envejecimiento y partes críticas de la flota.

Por último, el sistema posee la capacidad de realización de despliegues, mediante el uso del PMAT (Portable Multipurpose Aircraft Terminal), que realiza, con la misma estructura del servidor en base, todas las operaciones mencionadas anteriormente sin necesidad de estar conectado a la red.

En conclusión, la gestión del mantenimiento y de la aeronavegabilidad ha ido evolucionando de la mano del progreso tecnológico, y en un sector que se encuentra en vanguardia, es de vital importancia que los procesos asociados a la gestión de la aeronavegabilidad empleen tecnología de última generación.

4.2. ELECTRONC FLIGHT BAG (EFB)

Aunque no sean sistemas en tierra de soporte a la aeronave, se debe tener en cuenta la presencia de los dispositivos EFB (Electronic Flight Bag) ya que con flotas modernas como es el A400M, quedan atrás las cartas, procedimientos y manuales de miles de páginas impresos en papel para ser sustituidas por estos dispositivos.

Estas EFB son un portátil/Tablet en las que viene instalado software propio del fabricante de la aeronave, Airbus en este caso, para el manejo de la documentación del avión en cabina y se trata de un componente fundamental en este contexto ya que es el dispositivos través del cual accederán los pilotos y el personal autorizado a los datos almacenados en el sistema de gestión de información objetivo de este proyecto.

En el caso del A400M, este software denominado LPC-NG (Less Paper in Cockpit - New Generation), permite al tripulante la consulta rápida y sencilla de los procedimientos y manuales del avión, además de integrar un módulo de cálculo de performance del avión para despegue, crucero y aterrizaje.

En el Ala 31 es la subsección de sistemas de apoyo, perteneciente a la sección de Información Aeronáutica, la encargada de que toda EFB esté siempre actualizada y puesta a punto para su despacho a cualquier misión. Para ello es necesario su preparación con equipos en tierra de gestión de la documentación y preparación de EFB.

Conviene resaltar en este punto la importancia que la seguridad informática tiene en esta sección como paso previo indispensable a cualquier actuación dado que es imprescindible asegurar que todo el material que es introducido en las EFB, cualquier otro sistema de apoyo o el avión mismo está libre de software corrupto o malicioso.

Para terminar este capítulo, es importante destacar la gran cantidad de datos y de información que se genera y fluye a través de estos sistemas que a su vez interactúan con otros. Dicha información en la mayoría de los casos dentro de este contexto tiene carácter estrictamente confidencial, por ello, el correcto y seguro almacenamiento es de vital importancia.

5. CONTEXTO DEL PROBLEMA

Como ya se ha mencionado en varias ocasiones, el principal objetivo es la optimización de procesos y la eficiencia operativa para garantizar el éxito de las misiones y la seguridad de las operaciones desde el punto de vista de gestión de información confidencial. Sin embargo, existen desafíos que demandan soluciones innovadoras y adaptadas a las demandas tecnológicas de la era actual. En este contexto, surge la necesidad apremiante de abordar un problema que afecta tanto a la gestión interna de las operaciones como a la interacción entre pilotos y sistemas en tierra.

En el escenario sobre el que se parte, existen tres componentes o actores principales. Por un lado, se encuentran los sensores y sistemas integrados dentro de la aeronave, por otro lado, los dispositivos EFB que utilizan los pilotos y en tercer lugar, el personal de la sección de Soporte de Sistemas, que es el lugar donde se encontrará físicamente el sistema de gestión y almacenamiento de información. Estos tres componentes principales se ven inmersos en una red de intercambio de información que, si bien es crucial para la eficiencia, presenta obstáculos.

Tanto la información generada y manejada por los sistemas integrados de la aeronave, como la información utilizada desde los EFB que se comparte en algunas ocasiones con los sistemas en tierra, así como la información proporcionada por estos últimos, se encuentra almacenada en un servidor NAS ubicado en el edificio donde se encuentra la unidad de Soporte de Sistemas.

Además, toda la información independiente a los vuelos o a las funciones de las aeronaves, relativa a las tareas diarias del personal de Soporte de Sistemas también se encuentra almacenada en esta misma unidad de almacenamiento.

De esta forma, los pilotos y los trabajadores de Soporte de Sistemas tienen acceso a la misma información, esté dentro de sus competencias o no, lo que provoca problemas de eficiencia a la hora de acceder a la información de forma rápida, problemas de centralización y orden de la información y también problemas de

seguridad, ya que los accesos a los archivos deben estar filtrados y controlados en función del tipo de usuario que accede a los mismos.

A continuación, se muestra un esquema que detalla la situación de partida.

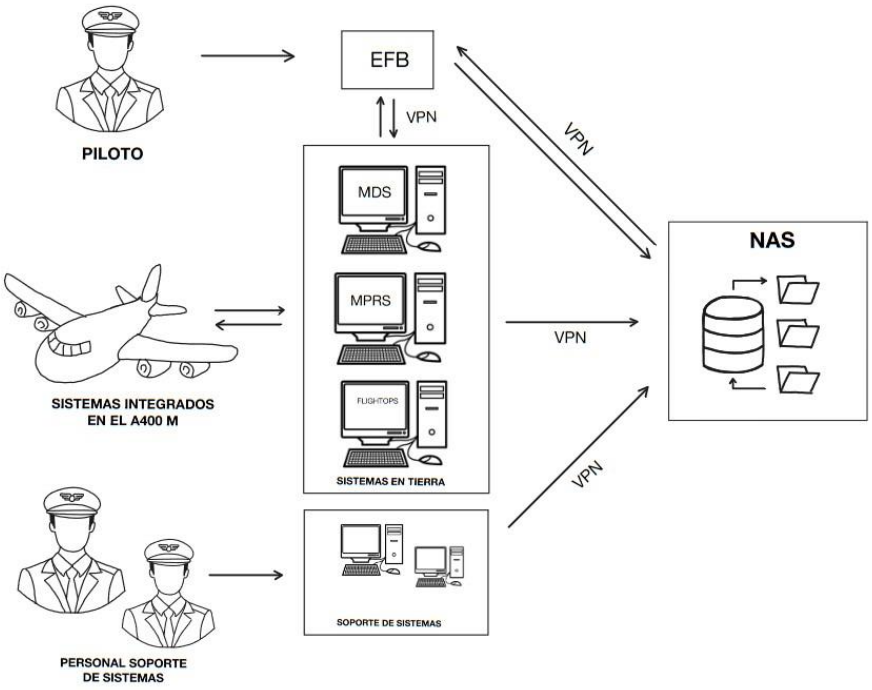


Tabla 1: Esquema de Situación Inicial. Elaboración propia.

Por otro lado, el acceso y gestión están limitados por la estructura de directorios y la necesidad de utilizar una VPN para establecer la conexión. Este proceso, aunque esencial, plantea desafíos en términos de accesibilidad, actualización en tiempo real y eficiencia en la transferencia de datos.

En respuesta a estos desafíos, el enfoque de este proyecto se orienta hacia una transformación digital integral que abarca más allá de la simple sustitución de papel por medios electrónicos. Se busca gestionar y almacenar todos los datos e información necesarios para los procedimientos operativos y la toma de decisiones.

6. LEGISLACIÓN Y NORMATIVA

Crear e instalar una unidad de almacenamiento implica cumplir con diversas normativas y legislaciones, especialmente en lo que respecta a la protección de datos y la seguridad de la información, que son aspectos clave en este proyecto. A lo largo del mismo, se consideran los requisitos que debe cumplir el sistema según el Esquema Nacional de Seguridad (en adelante ENS) establecido en el Real Decreto 311/2022, de 3 de mayo, y los artículos a considerar son explicados en este capítulo. Además, en el Anexo A. se explican aquellos artículos excluidos en este contexto.

Por otro lado, también se realiza un análisis de las medidas de seguridad establecidas por el Centro Criptológico Nacional (CCN) que se tienen en cuenta, aplicando la Gobernanza de Ciberseguridad Nacional.

NORMATIVA NACIONAL

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

A continuación, se mencionan aquellos artículos que aplican en este proyecto en términos de política de seguridad y requisitos mínimos de seguridad.

Artículo 2. Este real decreto se aplica a los sistemas que tratan información clasificada, como es el caso, pudiendo adoptar medidas complementarias de seguridad específicas para estos sistemas.

Artículo 5. Principios básicos del ENS. Garantiza que la organización cumple los objetivos, desarrolla sus funciones y ejerce sus competencias. Se consideran

aspectos como: seguridad como proceso integral, seguridad basada en riesgos, prevención, detección, respuesta, vigilancia continua, evaluación periódica y diferenciación de responsabilidades.

Artículo 6. Seguridad como proceso integral: todos los elementos humanos, materiales, técnicos y jurídicos relacionados con el sistema deben estar controlados.

Artículo 7 y 14. Seguridad y gestión basada en riesgos: Analizar los riesgos es una práctica esencial para la seguridad del sistema y debe ser continua y actualizada. Permite el mantenimiento controlado del sistema.

Artículo 8. Prevención, detección, respuesta y conservación: Minimizar vulnerabilidades y lograr que no se materialicen las amenazas o que afecten lo mínimo posible al sistema.

Artículo 9. Existencia de líneas de defensa: Estrategia de protección constituida por varias capas de seguridad.

Artículo 10. Vigilancia continua y reevaluación periódica. El sistema debe estar vigilado para permitir detectar actividades o comportamientos anómalos. La evaluación permanente del estado del sistema permite su evolución y detectar deficiencias en la configuración.

Artículo 11 y 15. Diferenciación de responsabilidades y Gestión de personal. Se debe diferenciar y reconocer al responsable de la información o del servicio que se presta. Además, la actuación del personal deberá estar justificada y supervisada cumpliendo los procedimientos.

Artículo 17. Autorización y control de acceso: el acceso controlado al sistema debe estar limitado a los usuarios, procesos, dispositivos o sistemas debidamente autorizados y exclusivamente a las funciones permitidas.

Artículo 18. Protección de las instalaciones. El sistema debe permanecer en un área controlada que disponga de mecanismos de acceso restringidos sin perjudicar a lo establecido en el Reglamento de protección de las Infraestructuras Críticas.

Artículo 2. Mínimo privilegio. El sistema proporciona la funcionalidad imprescindible para que la organización alcance los objetivos y las funciones serán las mínimas necesarias, asegurando que sean desarrolladas por personal autorizado.

Artículo 21. Integridad y actualización del sistema. La inclusión de cualquier elemento en el catálogo de activos del sistema requerirá autorización previa.

Artículo 22. Protección de información almacenada y en tránsito. Se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles, soportes de información y comunicaciones.

Artículo 24. Registro de actividad y detección de código dañino. Con garantía del derecho del honor, la intimidad personal y la imagen de los afectados, se registran las actividades de los usuarios reteniendo solo la información estrictamente necesaria.
En este caso, nombre de usuario y contraseña.

Artículo 26. Continuidad de la actividad. El sistema dispone de copias de seguridad y se establecen los mecanismos necesarios para garantizar la continuidad de las operaciones.

NORMATIVA EUROPEA

Teniendo en cuenta que el sistema pertenece a un entorno militar, existen una serie de estándares que se deben tener en cuenta.

Estándares de seguridad de la OTAN (NCSS): son aplicables en el caso de la creación y gestión de unidades de almacenamiento para funciones militares.

- **AJP-6 (Allied Joint Doctrine for Command and Control)**: Establece los principios y procedimientos para el comando y control militar en operaciones

conjuntas y multinacionales. Incluye directrices sobre la gestión de la información y la ciberseguridad en entornos militares.

- **STANAGs (Standardization Agreements)**: Son acuerdos de estandarización adoptados por los países miembros de la OTAN para garantizar la interoperabilidad y la seguridad en áreas específicas. En el caso de la seguridad de la información, incluyen STANAGs relacionados con la protección de sistemas de tecnología de la información y comunicaciones militares.
- **NCIA (NATO Communications and Information Agency) Security Policies and Guidelines:** La Agencia de Comunicaciones e Información de la OTAN emite políticas y directrices de seguridad para proteger la información clasificada y los sistemas de información de la OTAN y sus países miembros. Estas políticas pueden abordar aspectos como la gestión de contraseñas, el cifrado de datos, la autenticación de usuarios y la protección contra amenazas cibernéticas que se mencionan y utilizan en el presente proyecto.

SEGURIDAD DE INFRAESTRUCTURAS CRÍTICAS:

Es importante tener en cuenta en todo momento que el sistema está doblemente considerado en el Catálogo Nacional de Infraestructuras críticas debido a que, por un lado, pertenece al sector estratégico del Ministerio de Defensa y por otro lado pertenece al sector estratégico de Servicios Digitales. Es por ello que es fundamental cumplir con las disposiciones del **Catálogo Nacional de Infraestructuras Estratégicas (CNIE)**, especialmente en lo que respecta a la protección de la información y la ciberseguridad.

Además, teniendo en cuenta el grado de criticidad asociado al sistema en caso de fallos o ausencia de funcionalidades, se considera como infraestructura crítica y por ello, se debe tener en cuenta el Real Decreto 704/2011, del 20 de mayo, por el que se aprueba el **Reglamento de Protección de las Infraestructuras Críticas y la Directiva 2022/2557,** del 14 de diciembre, “Resiliencia de entidades críticas”.

NORMATIVA INTERNACIONAL

Norma de seguridad de la información, ISO 27001: Establece estándares internacionales para la gestión de la seguridad de la información.

7. GESTIÓN DEL PROYECTO

7.1. ALCANCE DEL PROYECTO

7.1.1. OBJETIVOS DEL PROYECTO

El objetivo principal de este proyecto es abordar los desafíos identificados en la gestión de la información en el Ala 31 relativa a las operaciones de las aeronaves y mejorarla mediante la implementación de soluciones innovadoras y adaptadas a las demandas tecnológicas actuales.

De forma más específica, los objetivos se centran en los siguientes aspectos generales:

- **Optimizar la eficiencia en el acceso a la información:** se busca agilizar el proceso de acceso a la información para que los usuarios puedan obtener los datos necesarios de manera rápida y sin obstáculos.
- **Mejorar la centralización y el orden de la información:** organizar y centralizar la información de manera que sea fácilmente accesible y comprensible para los usuarios autorizados.
- **Reforzar la seguridad y el control de accesos a archivos:** Se pretende implementar medidas de seguridad robustas para controlar quién puede acceder a la información, asegurando que solo los usuarios autorizados puedan acceder a los archivos pertinentes.
- **Facilitar la actualización en tiempo real y la transferencia eficiente de datos:** establecer un sistema que permita la actualización instantánea de la información y una transferencia eficiente de datos entre los diferentes sistemas y usuarios, garantizando la disponibilidad de información actualizada en todo momento.
- **Asegurar que el sistema funciona en conjunto con los recursos ya creados con este fin.** El sistema debe funcionar en conjunto con un software ya creado que se explica en los capítulos posteriores.

Estos objetivos específicos se alinean con el objetivo de contribuir al desarrollo y evolución tecnológica del Ejército del Aire.

7.1.2. RESTRICCIONES

La efectividad y el alcance de cualquier proyecto están influenciados por una serie de restricciones que definen los límites y las condiciones dentro de las cuales se puede trabajar. En el caso específico de este proyecto destinado, es crucial identificar y comprender estas restricciones para garantizar la viabilidad y el éxito de este. Dichas restricciones son las siguientes:

- **Contexto Específico del Ala 31:** El proyecto se desarrollará exclusivamente en el contexto del Ala 31 y su infraestructura tecnológica asociada. No se considerarán soluciones que estén fuera de este ámbito.
- **Cumplimiento de Regulaciones y Políticas de Seguridad:** Se deben respetar todas las regulaciones y políticas de seguridad establecidas por las autoridades competentes, indicadas en el punto 6. Cualquier solución propuesta debe ajustarse a estos requisitos regulatorios y de seguridad.
- **Restricciones de Acceso a Información Confidencial:** Se deben establecer medidas de seguridad adecuadas para proteger la información confidencial del Ala 31. El acceso a ciertos datos o recursos estará restringido a personal autorizado, siguiendo los protocolos de seguridad establecidos.

7.1.3. LIMITACIONES

El desarrollo del proyecto puede verse influenciado por diversas limitaciones y que deben ser consideradas durante su planificación y ejecución. Estas limitaciones pueden abarcar aspectos temporales, recursos disponibles y restricciones tecnológicas que podrían impactar tanto en la implementación como en los resultados obtenidos.

- **Restricciones Tecnológicas:** La infraestructura tecnológica existente en el Ala 31 puede imponer ciertas restricciones en términos de compatibilidad,

capacidad y funcionalidades. La integración de nuevas soluciones tecnológicas podría enfrentarse a desafíos técnicos que requieran abordarse de manera adecuada para garantizar su efectiva implementación y operatividad. Además, los componentes que se utilizan son reutilizados de otras tareas.

- **Disponibilidad del personal militar del Ala 31:** en este contexto, el personal implicado tiene asignadas múltiples responsabilidades y tareas además de las relacionadas con este proyecto. Esta restricción implica que el personal puede enfrentarse a limitaciones de tiempo y recursos para dedicar exclusivamente a las actividades y requerimientos del proyecto.

7.1.4. EVALUACIÓN DEL ÉXITO

La evaluación del éxito del proyecto se llevará a cabo mediante varios criterios que abarcan diferentes aspectos clave. Estos criterios incluyen:

- **Logro de Objetivos Establecidos:** Se evaluará en qué medida el proyecto cumple con los objetivos específicos definidos en el punto 7.1.1.
- **Mejora de los Procesos Operativos:** Se analizará cómo el proyecto contribuye a la mejora de los procesos operativos dentro del Ala 31. Esto puede implicar la reducción de tiempos de acceso a la información, la optimización de los flujos de trabajo, la disminución de errores en la gestión de información y la mejora general de la eficiencia y productividad en las operaciones cotidianas.
- **Cumplimiento de Restricciones y Limitaciones:** Se evaluará si el proyecto logra cumplir con las restricciones y limitaciones establecidas. El grado de cumplimiento de estas restricciones influirá en la percepción global del éxito del proyecto.
- **Operatividad del Producto:** Se evaluará la efectividad y la estabilidad del sistema implementado en el entorno operativo del Ala 31 después de su creación.

7.2. PLAN DE TRABAJO

En el contexto de este proyecto, la identificación de tareas cobra una importancia significativa ya que existe un compromiso con los objetivos y para alcanzarlos, es esencial una estructura coherente y sistemática de las actividades que llevarán a cabo esta visión.

La ejecución del proyecto se ha dividido de la siguiente manera:

- **Definición del proyecto:** establecimiento de objetivos, capacidades, limitaciones y criterios necesarios para ejecutar la solución.
- **Desarrollo del proyecto:** implementación de los requisitos en base a diferentes necesidades. Se divide en dos fases:
  - Configuración de BIOS/UEFI
  - Configuración post-instalación
- **Evaluación de los resultados y definición de conclusiones:** documentación del producto desarrollado, revisión, evaluación de resultados, comprobación de cumplimiento de objetivos y requisitos y definición de conclusiones.

7.2.1. CRONOGRAMA DE TAREAS

A continuación, se muestra el cronograma de los procedimientos más relevantes que se llevan a cabo a lo largo del proceso de desarrollo cronológicamente ordenados.

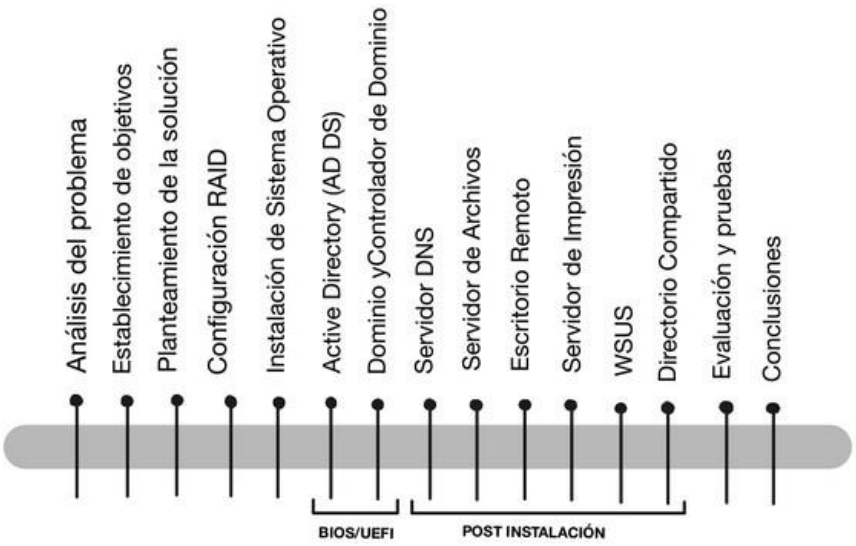


Tabla 2. Cronograma de procedimientos. Elaboración propia.

7.3. GESTÓN DE RECURSOS

7.3.1. RECURSOS HARDWARE

Para la creación y operación del sistema de gestión de información en cuestión, se cuenta con el hardware específico FUJITSU Primergy RX2540 M4, servidor de alto rendimiento diseñado para entornos empresariales y de centros de datos y cuyas características se indican a continuación.

- Dos procesadores Intel Xeon Silver 4112, cada uno con 4 núcleos
- Velocidad de reloj de 2.60 GHz, ofrece un equilibrio eficiente entre rendimiento y consumo energético.
- 256 GB de RAM DDR4, es capaz de manejar aplicaciones intensivas en recursos.
- Factor de forma en rack para montaje en bastidores estándar
- Amplia conectividad
- Puertos Ethernet Gigabit
- Puertos USB
- Opciones de conexión remota

- Fuente de alimentación y ventiladores redundantes
- Alta disponibilidad
- 8 discos de almacenamiento de 300 GB

Este servidor está diseñado para ofrecer una alta fiabilidad y disponibilidad ya que incorpora características como la redundancia de componentes y la capacidad de intercambio en caliente, lo que minimiza el tiempo de inactividad y asegura la continuidad operativa.

Además, el Primergy RX2540 M4 cuenta con características de seguridad avanzadas, incluyendo funciones de encriptación de datos, autenticación de usuarios y protección contra amenazas cibernéticas. Esto garantiza la integridad y confidencialidad de la información almacenada en el servidor, que como se ha dicho, es uno de los principales objetivos. Además, es altamente escalable, lo que significa que puede adaptarse fácilmente a las necesidades cambiantes de tu proyecto.

Cabe resaltar que dicho hardware ha sido utilizado anteriormente para otros fines o tareas dentro del Ala 31 y será reutilizado para este nuevo fin, lo que reduce significativamente los costes asociados a la implementación de dicho sistema.

7.3.2. RECURSOS SOFTWARE

Dentro de este contexto, destaca la presencia de un software que ha sido desarrollado por personal especializado con el fin de trabajar en conjunto con el sistema de gestión de información que se va a crear. Dicho software sirve como enlace entre el usuario y el sistema permitiendo subir y descargar archivos.

Concretamente, la aplicación utiliza la funcionalidad de *Robocopy* y está destinada a la gestión, sincronización, actualización y almacenamiento de documentos y datos relevantes para las operaciones de vuelo, siendo especialmente útil durante la planificación y el acceso a información crítica.

La aplicación está diseñada para interactuar principalmente con pilotos del Ala 31, quienes acceden a través de una VPN al nuevo servidor. Se recuerda que este servidor contiene directorios clasificados con diversos archivos relacionados con las operaciones a realizar en el avión de tal forma que los pilotos utilizan los EFB (Electronic Flight Bag) a bordo del avión para acceder a él, iniciando el ejecutable de la aplicación. El objetivo principal es facilitar el trabajo y las actuaciones de los pilotos, asegurando máxima seguridad en la comunicación entre los EFBs y el servidor.

La aplicación se ejecuta en el sistema operativo Windows y se ha desarrollado en el lenguaje de programación C#. Por otro lado, el mantenimiento y actualizaciones (fundamentales para garantizar la seguridad, estabilidad, compatibilidad y funcionalidad de la aplicación en un entorno operativo dinámico como el del Ala 31) se llevan a cabo en el laboratorio de Soporte de Sistemas por personal especializado.

Bajo términos más técnicos, la aplicación implementa una serie de protocolos que aportan diferentes funcionalidades. Dichos protocolos se describen a continuación.

- **HTTPS:** asegura la seguridad y privacidad de la comunicación cifrando los datos transmitidos entre los pilotos y el servidor, garantizando la autenticación del mismo. Este protocolo se describe con más detalle en el punto 8.2.

- **WebDAV**: es una extensión del protocolo HTTP que permite la creación, modificación y eliminación de archivos almacenados en servidores web de forma colaborativa. Cuando se utiliza sobre HTTPS, WebDAV proporciona un canal seguro para transferir archivos entre el cliente y el servidor.

- **SMB** para compartir archivos en una red local, permite un acceso eficiente a los archivos almacenados en el servidor, favoreciendo así la colaboración entre pilotos para que puedan acceder siempre a información actualizada por otros pilotos o usuarios.

Teniendo en cuenta la importancia de la seguridad en este proyecto, es crucial destacar que tanto HTTPS como WebDAV sobre HTTPS y SMBv3, cuando se

habilita el cifrado, ofrecen cifrado de extremo a extremo para proteger la comunicación entre los clientes (pilotos y EFB) y el servidor. El cifrado extremo a extremo protege los datos mientras se transmiten desde el origen hasta el destino, de manera que solo el remitente y el destinatario puedan acceder a la información y de esta forma, la comunicación del piloto con el software es segura y también lo es la comunicación de este último con el servidor.

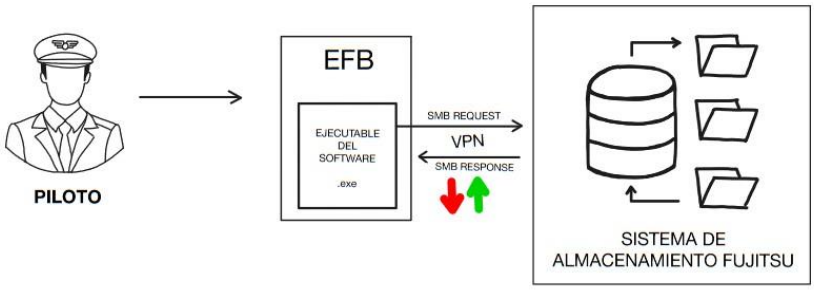


Tabla 3. Conexión Software-Servidor y protocolo SMB. Elaboración propia

7.4. GESTIÓN DE RIESGOS

7.4.1. RIESGOS GENÉRICOS

La anticipación y gestión de los riesgos juegan un papel crucial en el éxito y la viabilidad de cualquier iniciativa. Este capítulo se adentra en el análisis de los riesgos genéricos asociados a este proyecto, buscando identificar las posibles amenazas que podrían surgir a lo largo de su desarrollo y ejecución.

- Riesgos de disponibilidad: surgen debido a los posibles destacamentos o ejercicios a los que acude el personal militar en ocasiones o incluso por demasiada carga de trabajo en una unidad concreta que provoque que todo el personal esté ocupado con asuntos de mayor urgencia o importancia.
- Retrasos en la ejecución o en las actualizaciones
- Riesgos de aumento de la carga de trabajo al personal disponible.
- Riesgos técnicos: pueden surgir imprevistos durante la implementación del servidor.
- Riesgos de tiempo

- Riesgos de seguridad: vulnerabilidades en la seguridad de los datos almacenados y transmitidos por el servidor.
- Riesgos de cumplimiento normativo
- Riesgo de fallos en las comunicaciones entre los componentes

7.4.2. RIESGOS ESPECÍFICOS

A diferencia de los riesgos genéricos, que abarcan una amplia gama de escenarios potenciales, los riesgos específicos se centran en amenazas más concretas y particulares que podrían surgir debido a las características únicas del proyecto, su entorno operativo y las tecnologías involucradas. A continuación, se indican los riesgos específicos más relevantes en este contexto:

- Riesgos de compatibilidad de datos ○ Recopilación de información difícil ○ Aumento de la complejidad del proyecto ○ Mayor necesidad de tiempo
- Mayor necesidad de recursos de desarrollo
- Formatos de los datos generados por los EFBs
- Utilización de estándares y versiones diferentes o demasiado antiguas
- EFBs de diversos fabricantes o pertenecientes a distintas generaciones de hardware y software.

8. SOLUCIÓN

8.1. DESCRPCIÓN DE LA SOLUCIÓN PROPUESTA

El escenario delineado, como ya se ha indicado en varias ocasiones, se enfoca en la materialización de una arquitectura tecnológica avanzada y segura para la gestión y almacenamiento de datos cruciales en el entorno de la aviación militar del Ala 31, centrado en la operatividad de las aeronaves. Este enfoque implica una amalgama de elementos técnicos y protocolos especializados para asegurar la confidencialidad, integridad y disponibilidad de la información, al tiempo que garantiza la eficiencia y la colaboración dentro de este entorno altamente crítico.

Para hacer frente a los desafíos mencionados, la solución seguirá estando formada por los tres actores principales, los sistemas y sensores integrados en el avión, los EFB de los pilotos y los trabajadores del área de Soporte de Sistemas.

En este caso, la información no se centraliza en una misma unidad de almacenamiento, sino que, por un lado se mantiene la unidad NAS para uso exclusivo del personal de soporte de sistemas y por otra parte, se crea una unidad de almacenamiento desde cero, un servidor que realiza funciones de almacenamiento, intercambio y gestión de datos y archivos por parte de los pilotos y del personal autorizado en todo lo respectivo al estado, mantenimiento y funcionamiento de las aeronaves, así como de planificación, ejecución y revisión de los vuelos asociados a cada una de las mismas.

De esta forma, el personal externo al área de Soporte de Sistemas no tiene acceso a la unidad NAS que contiene la información relativa al trabajo de dicha unidad.

Por otro lado, el personal de soporte de sistemas, de mantenimiento y los pilotos, todos bajo autorización, podrán acceder al nuevo servidor y visualizar o modificar archivos según las necesidades.

Al dividir la información en dos unidades de almacenamiento distintas, se mejora la eficiencia y la accesibilidad de los datos, permitiendo encontrar y acceder a la información de manera rápida y sencilla, mejorando a su vez el rendimiento general del sistema ya que, al distribuir la carga de trabajo entre ambos servidores, se reduce la congestión y se facilita un acceso más rápido a los datos, lo que implica tiempos de respuesta más rápidos para los usuarios.

Además, esta práctica aumenta significativamente la seguridad y confidencialidad de la información almacenada en ambos servidores. Se restringe el acceso a la información solo a aquellos usuarios que tienen autorización para ello, en función de sus roles o responsabilidades específicas. Esto reduce las posibilidades de filtraciones de información y garantiza que solo las personas adecuadas puedan acceder a datos confidenciales.

Además, esta estructura permite una mayor escalabilidad del sistema ya que si la cantidad de datos aumenta con el tiempo, es más fácil añadir capacidad de almacenamiento adicional a cada servidor de forma independiente, sin necesidad de afectar al otro servidor. Esto permite adaptarse más fácilmente a las necesidades cambiantes de almacenamiento.

En términos más técnicos, se debe considerar la existencia del software detallado en el punto 7.3.2, desarrollado para este fin. Conectados a la red, los EFBs utilizan dicho software para facilitar la transferencia bidireccional de documentos y archivos, que se ejecuta en sintonía con los requerimientos y las necesidades operativas de los pilotos, es decir, a través del software, los pilotos suben y descargan archivos o documentos actualizados que se encuentran en el servidor.

En este caso, como la seguridad es un requisito importante, una vez que los archivos son cargados desde los EFBs a través del software, la capa adicional de seguridad se establece mediante la implementación de un túnel VPN (Virtual Private Network). Este túnel VPN establece una conexión cifrada y privada entre los EFBs y el servidor

principal. La tecnología VPN garantiza que los datos se transmitan de manera segura, sin comprometer la confidencialidad ni la integridad.

A continuación, se muestra el esquema equivalente a la solución propuesta para mayor claridad.

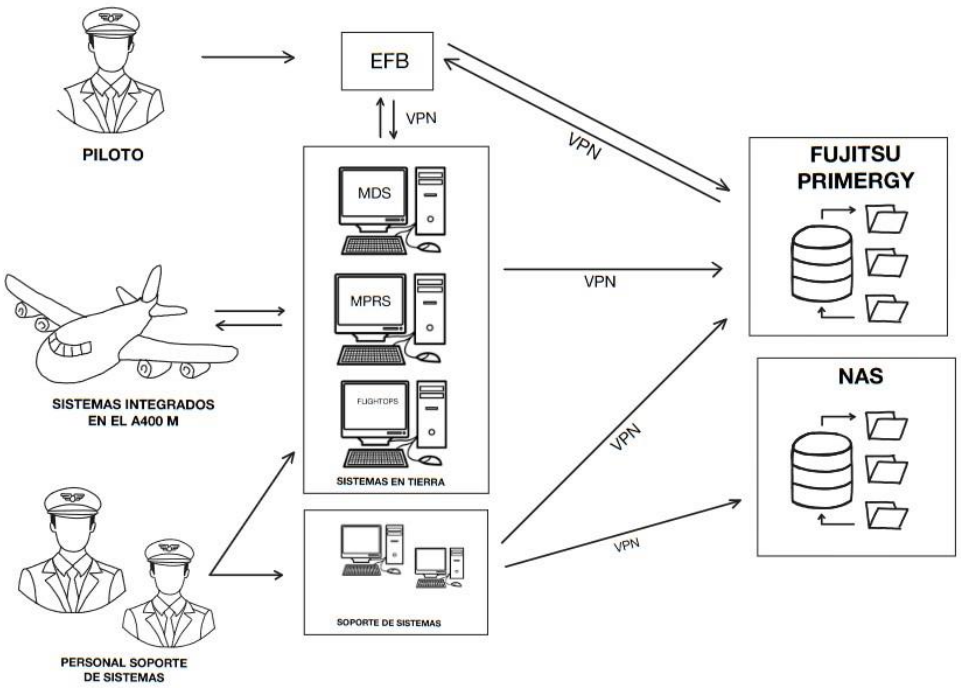


Tabla 4. Solución propuesta Elaboración propia.

En resumen, este nuevo enfoque proporciona un mayor control sobre quién puede acceder a qué información, y mejora la eficiencia, la optimización y la seguridad del sistema en su conjunto, que son los principales objetivos de este proyecto.

8.2. ARQUITECTURA

La arquitectura que se implementa en el sistema de gestión de información corresponde a la arquitectura Cliente-Servidor. Para visualizar dicha arquitectura se debe considerar que el nuevo servidor es el núcleo de la arquitectura y actúa como la unidad central de almacenamiento, intercambio y gestión de datos para los pilotos, el

personal autorizado y los sistemas en tierra de soporte a la aeronave (que actúan en categoría de clientes).

Como ya se ha mencionado, los pilotos utilizan dispositivos EFB (cliente 1) para acceder al servidor principal y visualizar o modificar archivos según sus necesidades. Estos dispositivos están conectados a la red y utilizan un software desarrollado para este fin, que facilita la transferencia segura de datos entre los EFBs y el servidor. Además, los sistemas en tierra (cliente 2) son responsables de proporcionar soporte operativo y logístico a las operaciones de vuelo e interactúan con el servidor principal para acceder a información relevante sobre el estado de las aeronaves, datos de planificación de vuelos y otras necesidades operativas. Por último, el personal de soporte de sistemas (cliente 3) tiene acceso tanto al servidor principal como al servidor NAS.

La comunicación entre los sistemas en tierra (FlightOps, MDS, MPRS), los EFBs y los equipos únicos de soporte de sistemas con el servidor principal se realiza a través de solicitudes y respuestas HTTPS (Hypertext Transfer Protocol Secure) que es un protocolo de comunicación seguro que utiliza el cifrado SSL/TLS para proteger la integridad y confidencialidad de los datos transmitidos a través de Internet, como se muestra a continuación.

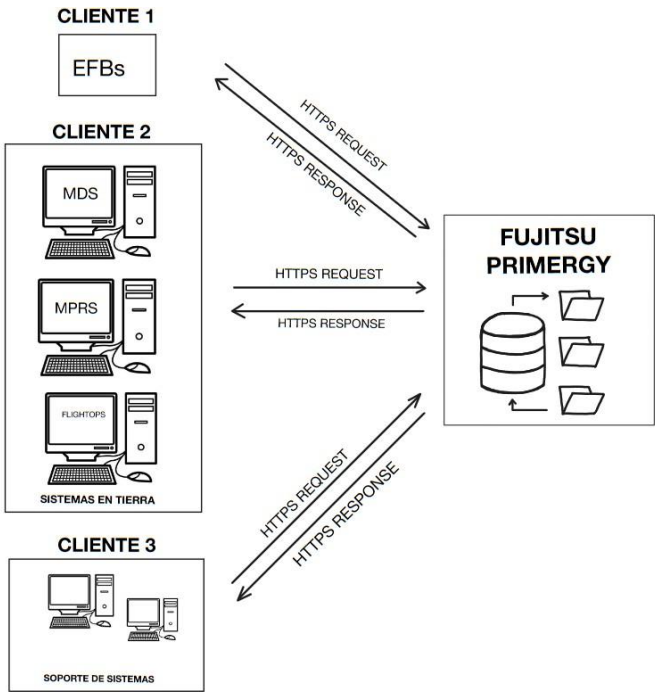


Tabla 5. Representación arquitectura Cliente-Servidor. Elaboración propia.

8.2.1. CONEXIÓN CLIENTES-SERVIDOR

En este caso específico, los clientes se comunican con los servidores a través de una VPN (Red Privada Virtual) y utilizan peticiones y respuestas HTTPS, esto significa que envían solicitudes HTTPS al servidor principal para acceder a información específica sobre el estado de las aeronaves, datos de planificación de vuelos u otras necesidades operativas y el nuevo servidor responde a estas solicitudes con las correspondientes respuestas HTTPS, proporcionando los datos solicitados de manera segura.

El protocolo HTTPS opera sobre el protocolo TCP/IP (Transmisión Control Protocol/Internet Protocol), a través del puerto 443, que corresponde al conjunto de protocolos que permite la comunicación en Internet y en redes locales.

Todo el proceso de conexión entre los tres actores principales y los servidores está formado por varias fases que se indican a continuación.

- **Inicio de la conexión VPN**
    - Los clientes (sistemas en tierra, trabajadores y pilotos) inician una conexión VPN con el servidor utilizando una VPN compatible.
    - Durante este proceso, se negocia una versión del protocolo VPN, como IPSec o OpenVPN, que ambos extremos de la conexión admiten y utilizarán para la comunicación segura.
- **Negociación de parámetros de seguridad VPN**
    - Una vez establecida la versión del protocolo VPN, se negocian otros parámetros de seguridad, como algoritmos de cifrado, modos de operación y parámetros de autenticación.
- **Selección de algoritmos criptográficos**
    - Se seleccionan algoritmos criptográficos para la encriptación de los datos transmitidos a través de la conexión VPN. Esto puede incluir cifrado simétrico (por ejemplo, AES), cifrado asimétrico (como RSA) y funciones hash (por ejemplo, SHA-256).
- **Autenticación del servidor VPN**
    - El servidor VPN presenta su certificado digital al cliente para autenticarse.
    - El cliente verifica la autenticidad del certificado utilizando una cadena de confianza de certificados raíz y comprueba si el nombre de dominio en el certificado del servidor coincide con el nombre de dominio al que está intentando conectarse, dicho dominio se establece en el punto 9.2.3.
- **Generación de secretos compartidos**
    - Durante el proceso de establecimiento de la conexión VPN, se generan secretos compartidos que se utilizan para cifrar y descifrar los datos transmitidos entre el cliente y el servidor a través de la VPN.
- **Establecimiento de la conexión HTTPS**
    - Una vez establecida la conexión VPN, el cliente envía solicitudes HTTPS al servidor principal para acceder a la información deseada.

- El servidor responde a estas solicitudes con las correspondientes respuestas HTTPS, proporcionando los datos solicitados de manera segura.

- **Apretón de manos TLS**
  - Antes de la transmisión de datos reales a través de HTTPS, se realiza un *"apretón de manos TLS (handshake)"* entre el cliente y el servidor para establecer una conexión segura.
  - Durante este apretón de manos TLS, se negocia la versión del protocolo TLS, se intercambian parámetros de seguridad y se autentica el servidor.
  - Esto garantiza una conexión segura y cifrada entre el cliente y el servidor, protegiendo la confidencialidad e integridad de los datos transmitidos a través de HTTPS.

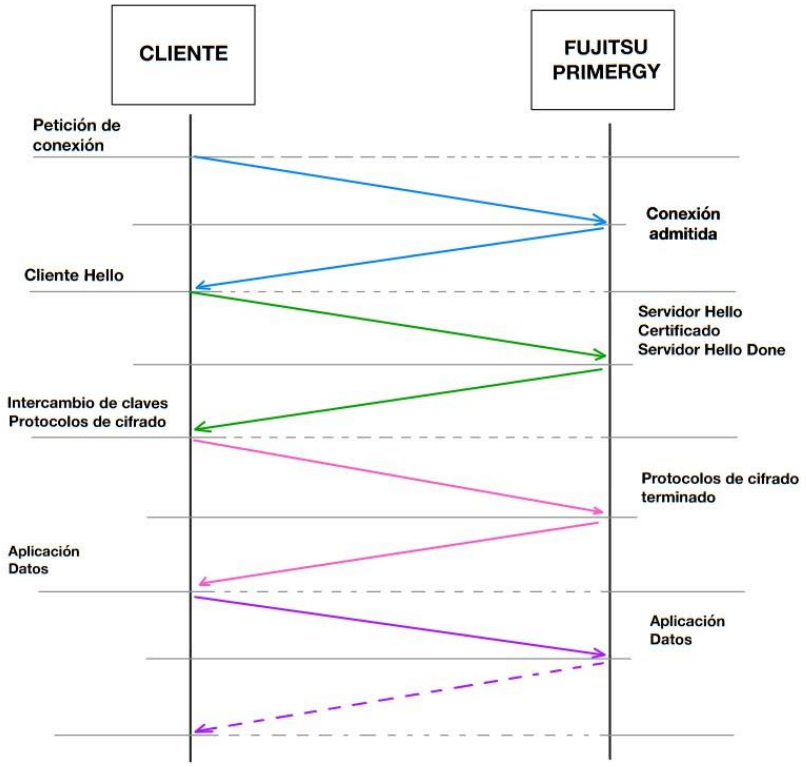


Tabla 6. Apretón de manos TLS. Elaboración propia.

8.3. COMPONENTES DEL PRODUCTO

El sistema de gestión de información en cuestión está formado por varios componentes que contribuyen a su correcta función y que serán instalados e incorporados en las siguientes páginas.

- Distribución de almacenamiento RAID
- Sistema Operativo
- Active Directory
- Servidor DNS
- Controlador de domino
- Dominio
- Servidor de Archivos
- Servidor de Impresión
- Servicio WSUS
- Escritorio Remoto
- Servicio de Directorio Compartido

9. DESARROLLO E IMPLEMENTACIÓN

9.1. CONFIGURACIÓN BIOS/UEFI

9.1.1. CREACIÓN DEL RAID (REDUNDANT ARRAY OF NDEPENDENT DISKS)

Dentro de la complejidad inherente a la configuración del servidor FUJITSU Primergy RX2540 M4, se introduce una faceta que involucra la selección de los componentes de almacenamiento, por ello, surge la necesidad de establecer una estrategia de almacenamiento que sea capaz de optimizar no solo la disponibilidad de la información almacenada, sino también el rendimiento y la resistencia a posibles fallos.

Teniendo en cuenta que se dispone de ocho discos con una capacidad de 300 GB cada uno, se considera como mejor opción la implementación de sistemas RAID (Redundant Array of Independent Disks), cuya misión es la de armonizar estos objetivos en un entorno sinérgico y cohesivo.

Una distribución RAID es una técnica de almacenamiento de datos que combina múltiples unidades de disco en un solo grupo lógico para mejorar la confiabilidad, la velocidad o ambas cosas. Además, hay diferentes niveles de RAID, como RAID 0, RAID 1, RAID 5, RAID 10, entre otros, cada uno con su propia configuración y método de redundancia para proteger los datos en caso de fallo de una unidad.

Teniendo en cuenta lo anterior, en el caso particular de este servidor, se realizan dos configuraciones RAID de tipo RAID 5, cada una compuesta por 4 discos. Estos dos conjuntos RAID, cumplirán dos roles cruciales respectivamente: uno se destinará a gestionar la información inherente a datos y la estructura de directorios, mientras que el otro desempeñará un papel fundamental en el alojamiento del sistema operativo y otros componentes clave.

Se escoge RAID 5 ya que, en este proyecto, se prioriza la seguridad de los datos, la eficiencia operativa y la capacidad de recuperación en situaciones difíciles y esta distribución garantiza la integridad de los datos y permite que el servidor funcione de manera óptima incluso si una unidad de disco falla. Por tanto, se asegura que el

servidor pueda contribuir de manera significativa a la gestión efectiva de la información en el ámbito de la aviación militar, proporcionando un rendimiento excepcional y una mayor confiabilidad.

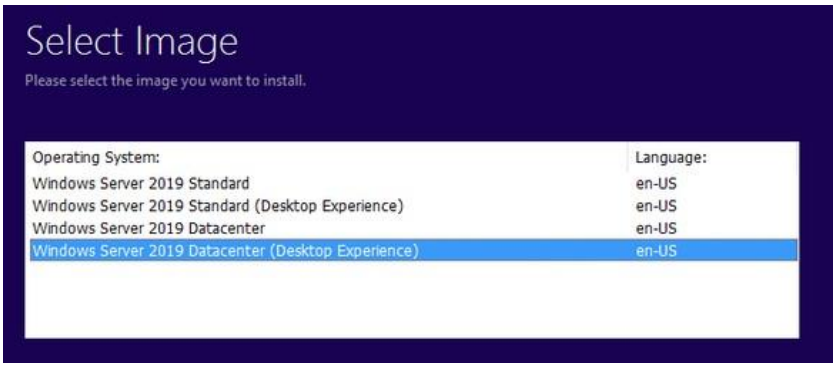
En términos de integridad de datos, RAID 5 se basa en una técnica conocida como “striping” donde los datos se distribuyen en bloques a través de varios discos en la matriz, junto con la paridad calculada para garantizar dicha propiedad. La paridad se calcula a partir de los datos almacenados en los otros discos del conjunto realizando operaciones XOR en los bits correspondientes y se utiliza para regenerar la información perdida en caso de que una unidad falle.

9.1.2. INSTALACIÓN DEL SISTEMA OPERATIVO

El sistema operativo elegido para implementar en este servidor es Windows Server, una solución desarrollada por Microsoft que se encuentra especialmente diseñada para su implementación en entornos de servidores. Su propósito radica en proporcionar una plataforma robusta y versátil para la administración y provisión de servicios y recursos en una infraestructura de red. En el presente contexto, la elección de Windows Server se justifica por su idoneidad para alojar aplicaciones críticas en entornos empresariales y de tecnologías de la información.

En el marco del presente proyecto, se tiene como objetivo establecer un sistema de almacenamiento centralizado que permita la ordenada y accesible disposición de datos relacionados con la aviación militar de transporte. Estos datos abarcan una variedad de tipos, tales como documentos, imágenes, videos y otros formatos de archivo pertinentes, por ello, la infraestructura escogida es Windows Server 2019 ya que proporciona las facilidades necesarias para la eficaz gestión de estos datos, haciendo uso de capacidades tales como la implementación de bases de datos, sistemas de archivos compartidos y funcionalidades avanzadas de búsqueda. Esto, a su vez, permite que los usuarios autorizados puedan llevar a cabo búsquedas efectivas y recuperar la información requerida en tiempos reducidos.

Una vez se haya introducido la licencia pertinente y tras hacer la configuración inicial seleccionando el idioma y la imagen, se instala dicho sistema operativo a partir del cual se añadirán el resto de los componentes.



Figuras 2 y 3. Licencia y selección del Sistema Operativo. Elaboración propia.

La opción Desktop Experience permite que los usuarios puedan utilizar el sistema con facilidad debido a que proporciona entorno gráfico.

El último paso para terminar la instalación es el establecimiento de la contraseña.

Figura 4. Sistema Operativo Windows Server instalado. Elaboración propia.

Al iniciarse el sistema operativo, se abre automáticamente la ventana del Server Manager desde la que se realizan las siguientes configuraciones.

9.2. CONFIGURACIÓN POST-INSTALACIÓN

9.2.1. ACTIVE DIRECTORY (AD DS)

Una de las herramientas utilizadas dentro del Ala 31, y más concretamente, en el área de Soporte de Sistemas es el Active Directory cuya descripción y configuración se detalla a continuación, así como las ventajas de su implementación.

Active Directory (AD DS) es un servicio de directorio desarrollado por Microsoft que actúa como una base centralizada para la administración de identidades, recursos y políticas de seguridad en entornos de red empresariales. Esencialmente, proporciona un conjunto de servicios que permiten a los administradores de red gestionar y organizar usuarios, grupos, sistemas y otros dispositivos en una red.

En términos más simples, Active Directory se puede entender como una especie de *"libreta de direcciones"* y en ella se almacena todo tipo de información importante, como nombres de usuarios, contraseñas, permisos de acceso, configuraciones de seguridad y más. Todo esto se organiza de manera ordenada y jerárquica como se explica en las siguientes líneas.

Además, el sistema de Active Directory se basa en la idea de dominios donde cada dominio es una sección de la red que tiene su propio conjunto de reglas y administración. Dentro de cada dominio, hay servidores llamados "controladores de dominio" que almacenan y gestionan toda esta información. Los controladores de dominio contienen la base de datos para un dominio concreto, incluida la información de seguridad ya que son los que se encargan de la autenticación de objetos.

Cabe destacar que se entiende por objeto cualquier componente que forma parte del directorio (impresoras, carpeta compartida, usuarios, grupos etc.) y cada objeto tiene unas características determinadas y un nombre que permitirá identificarlos y diferenciarlos. Los conceptos de controlador de dominio y objeto serán explicados con mayor detalle en el capítulo 9.2.3 de acuerdo con el contexto de este proyecto.

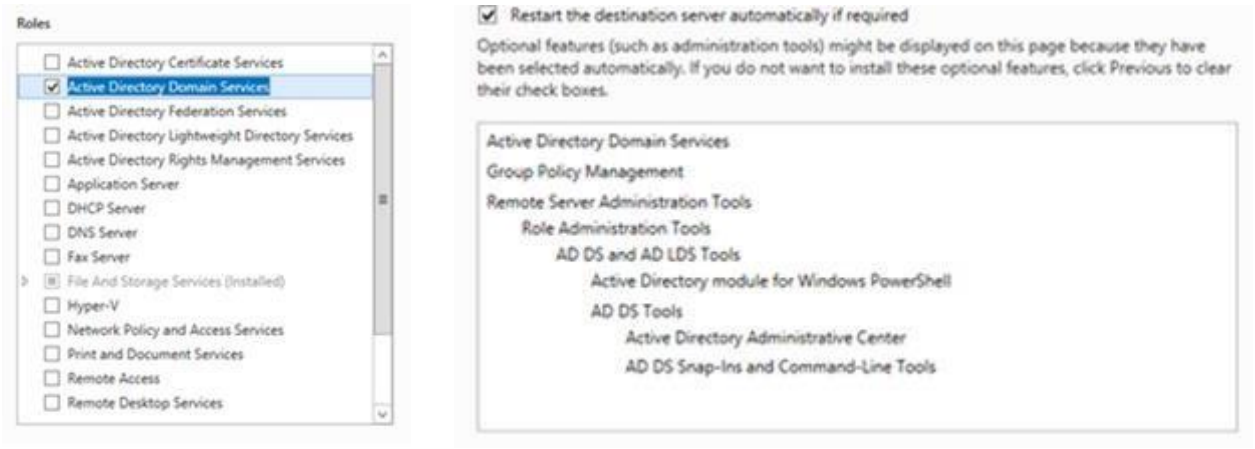
La infraestructura de Active Directory también posibilita la aplicación de políticas de seguridad, lo que implica que los diferentes roles y categorías de usuarios autorizados, como pilotos, personal de mantenimiento y administradores, tengan acceso solo a los recursos que requieran sus funciones.

Para crear el Active Directory se realiza la secuencia de pasos detallada a continuación:

Primeramente, en el panel de navegación del Server Manager se agregan roles y características. El tipo de instalación requerido, en este caso, es aquel basado en roles ya que este tipo de instalación permite seleccionar y activar solo las funciones necesarias para cumplir con los requisitos de la red y los objetivos establecidos.

Figura 5. Selección de tipo de instalación AD DS. Elaboración propia.

Una vez se ha realizado el paso anterior, se selecciona el rol o roles que se quiere instalar, esto abre una ventana emergente que informa sobre las características necesarias del rol.



Figuras 6 y 7. Roles y características instaladas en AD DS. Elaboración propia.

Además, el asistente muestra un resumen de las selecciones y una vez completada la instalación. En el Server Manager, se muestra una notificación que indica "*Promote this server to a domain controller"* que permite promover el servidor a un controlador de dominio dentro de un dominio existente o nuevo.

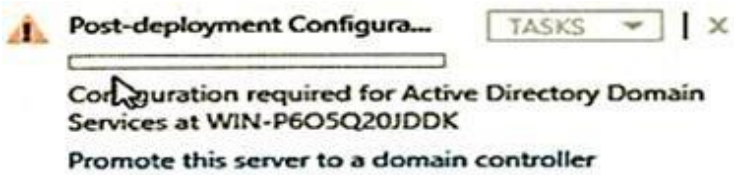


Figura 8. Promoción del servidor. Elaboración propia.

Para una mayor claridad de conceptos y de los siguientes pasos de la configuración, se debe considerar que hay un dominio existente cuyo nombre es “WIN-P6OSQ2QJDDK” que corresponde con el dominio al que se promueve el servidor. Promover el servidor al dominio mencionado significa que el servidor se convierte en un Controlador de Dominio dentro de ese dominio existente.

Este proceso es fundamental para establecer la infraestructura de Active Directory en el sistema, lo que permitirá la gestión centralizada de usuarios, grupos y recursos en la red ya que, promoviendo el servidor, este adquiere una serie de características especiales como autenticación de usuarios, gestión de políticas de grupo, mantenimiento de la coherencia de la base de datos etc.

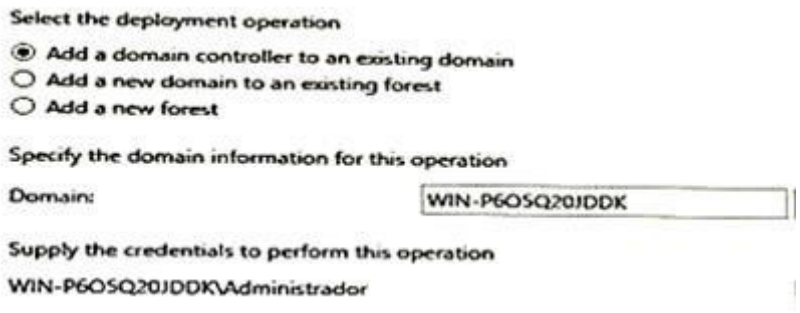


Figura 9. Añadir un controlador de dominio a un dominio. Elaboración propia.

En este caso, el dominio existente ("WIN-P6OSQ2QJDDK") forma parte de una estructura de dominios muy amplia y con esto se está reorganizando la configuración de los dominios para mejorar la administración y la seguridad.

Para terminar este capítulo, es importante considerar que el proceso de promoción de un servidor a un dominio existente implica cierta configuración del servidor DNS ya que es este quien otorga los nombres a los dominios.

9.2.2. SERVIDOR DNS

Los servidores DNS desempeñan un papel crucial en la infraestructura de Internet al traducir los nombres de dominio, fáciles de recordar, en direcciones IP numéricas que las máquinas pueden entender.

En el contexto especializado y riguroso de la Base Aérea de Zaragoza, donde las operaciones de aviación militar imponen requisitos imperativos de conectividad y acceso eficiente a recursos esenciales, la introducción de servidores DNS asume un papel muy relevante.

En síntesis, la adopción del servidor DNS se traduce en una red más confiable, una experiencia del usuario mejorada, una ciberseguridad fortalecida y una optimización de recursos. Configurar el DNS en Windows Server a través del Server Manager es relativamente sencillo, basta con seleccionar el rol e instalarlo.

Figura 11. Configuración servidor DNS. Elaboración propia.

Figura 12. DNS instalado. Elaboración propia.

Una vez completada la instalación, desde el Server Manager. En el panel de navegación izquierdo, aparece una nueva opción llamada DNS para poder administrar dicho servicio.

9.2.3. DOMNIO Y CONTROLADOR DE DOMINIO

Después de haber promovido el servidor al dominio existente "WIN-P6OSQ2QJDDK", se crea un nuevo dominio que se configura como independiente, con su propio conjunto de usuarios, grupos y políticas. Este nuevo dominio se crea en el bosque ya existente y por ello será gestionado por el controlador de dominio anteriormente mencionado (WIN-P6OSQ2QJDDK).

Antes de la creación del nuevo dominio, es importante asegurar la claridad de los conceptos utilizados.

En este contexto, está el dominio existente WIN-P6OSQ2QJDDK al que se ha promovido el servidor y por ello se ha convertido en un Controlador de Dominio. Por

otro lado, es necesaria la creación de uno nuevo que se configura como un dominio independiente a lo largo de este capítulo. Este nuevo dominio está diseñado para el propósito específico de este proyecto, es decir, la gestión de la información que fluye a través de los tres actores principales (EFBs, sistemas en tierra y personal autorizado) y el servidor. Se prefiere tenerlo en un dominio separado para aislar la administración y los recursos

Además, al crear un nuevo dominio, se tiene la oportunidad de implementar políticas de seguridad específicas y ajustadas a las necesidades del entorno. Además, como ya se han configurado correctamente el Active Directory y el servidor DNS, se puede proceder a dicha creación.

En el contexto de Windows Server, un "dominio" (domain) y un "bosque" (forest) son términos que se utilizan para describir diferentes niveles de estructura y jerarquía en una red siendo un dominio una unidad básica de organización con su propia base de datos de Active Directory, mientras que un bosque es una estructura que conecta múltiples dominios y árboles de dominios bajo una base de datos compartida.

En este caso, se selecciona la opción "*Add a new forest*" y a continuación se introduce el nombre del nuevo dominio, como se muestra a continuación.

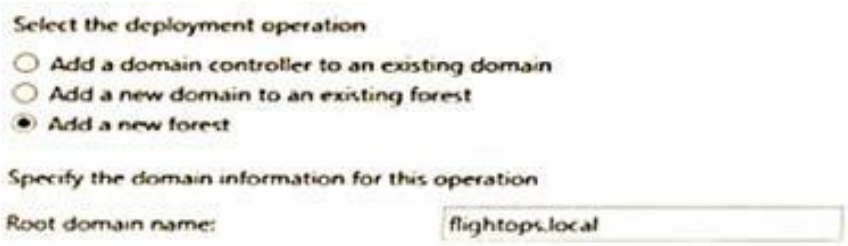


Figura 10. Añadir un nuevo bosque. Elaboración propia.

Como se puede observar en la figura anterior, el nuevo dominio recibe el nombre de "flightops.local".

En el caso de este proyecto en concreto, la situación es la siguiente:

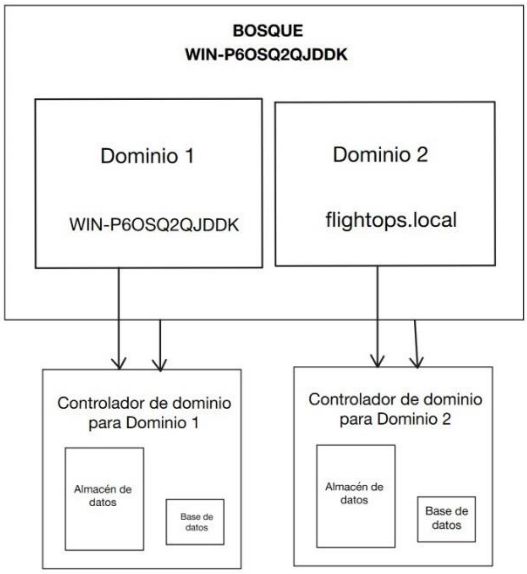


Tabla 7. Arquitectura de dominios. Elaboración propia.

Los dominios, "flightops.local" y "WIN-P6OSQ2QJDDK" son dominios independientes dentro del mismo bosque. Ambos dominios comparten el mismo bosque, lo que significa que comparten una base de datos de Active Directory y comparten la misma infraestructura subyacente.

Todos los usuarios de ambos dominios son gestionados por el mismo servidor, por ello el servidor actúa como un Controlador de Dominio global dentro del bosque, administrando tanto el dominio "WIN-P6OSQ2QJDDK" como el dominio "flightops.local".

En este escenario, el servidor desempeña el papel de autoridad central para la autenticación, la gestión de políticas de grupo y otras funciones relacionadas con la administración de usuarios y recursos en ambos dominios. Esto implica que todos los usuarios, grupos, políticas y demás objetos de Active Directory en los dos dominios están bajo la administración de este único servidor.

Una vez creado el nuevo dominio y teniendo en cuenta la situación, se debe tener en cuenta la existencia de los directorios System Volume (en adelante SYSVOL). Estos

directorios son un recurso especial en los controladores de dominio de Windows que almacena datos de política de grupo, scripts de inicio de sesión y elementos de datos de Active Directory (AD DS). SYSVOL es crucial para el funcionamiento del dominio y garantiza la coherencia de los datos entre todos los controladores de dominio dentro de un dominio o bosque de Active Directory, en este caso, dentro de “flightops.local”.

Estos archivos y directorios son accesibles y replicados en todos los controladores de dominio dentro de ese mismo dominio. Esto asegura que las políticas de grupo sean coherentes en toda la red, permitiendo una gestión unificada de usuarios, equipos y recursos.

En este caso, como "WIN-P6OSQ2QJDDK" es el controlador de dominio para el dominio "flightops.local", los directorios SYSVOL estarán dentro de "flightops.local".

Un aspecto importante a tener en cuenta es que configurar un dominio y un Controlador de Dominio es una tarea crítica que afecta la estructura y seguridad de la red. Se debe asegurar de tener una comprensión sólida de los conceptos y de seguir las mejores prácticas de seguridad.

La elección de un dominio personalizado como "flightops.local" refleja una decisión cuidadosa y coherente con el propósito operativo de la base aérea por lo que este enfoque proporciona una identidad inequívoca a nivel interno y comunica de manera efectiva la naturaleza de las operaciones de vuelo que se gestionan dentro del entorno. Además, la utilización de ".local" como sufijo de dominio contribuye a establecer una clara distinción entre los sistemas internos y los dominios públicos en línea, resguardando la privacidad y la seguridad de la infraestructura.

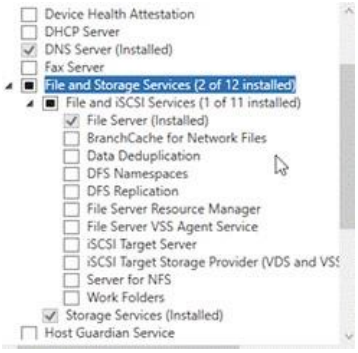
9.2.4. SERVIDOR DE ARCHIVOS

Un Servidor de Archivos en el contexto de Windows Server se refiere a un sistema que se configura específicamente para almacenar, administrar y proporcionar acceso a archivos y carpetas compartidos en una red. Este tipo de servidor es esencial para

organizar y centralizar los recursos digitales en un entorno empresarial, educativo o de cualquier otra organización.

Dado el carácter confidencial de la información en el ámbito militar y concretamente la información que se transmite desde los sistemas en tierra, los EFBs de los pilotos y los trabajadores haca el servidor, un servidor de archivos permite la implementación de estrictos controles de acceso y permisos aumentando así la seguridad. Solo el personal autorizado tendrá acceso a ciertas áreas del servidor, lo que garantiza la seguridad de los datos y evita divulgaciones no autorizadas.

En este caso, para la instalación del servidor de archivos se selecciona el rol “File and Storage Services” y la categoría “File Server”, como se muestra a continuación.



Figuras 13 y 14. Roles del Servidor de Archivos. Elaboración propia.

El servidor de archivos proporciona muchas ventajas al sistema de gestión de información que está en construcción.

Uno de los objetivos descritos en el punto 7.1.1 es la centralización de la información y el servidor de archivos posibilita el cumplimiento de dicho objetivo, lo que facilita una mayor organización y acceso por parte de todos los usuarios autorizados. Un servidor de archivos bien configurado y gestionado puede mejorar el rendimiento general del sistema al optimizar la forma en que se accede y se comparte la información, lo que reduce el tiempo de búsqueda y acceso a los archivos.

Además, un servidor de archivos bien configurado y gestionado puede mejorar el rendimiento general del sistema al optimizar la forma en que se accede y se comparte la información, lo que reduce el tiempo de búsqueda y acceso a los archivos.

9.2.5. ESCROTORIO REMOTO

El Escritorio Remoto es una característica de los sistemas operativos Windows que permite a los usuarios acceder y controlar de forma remota un equipo desde otro dispositivo, como una computadora portátil, una tableta o incluso un teléfono inteligente. En el caso concreto de este proyecto, se accederá desde un EFB o desde algún equipo del Ala 31.

Además, el escritorio remoto proporciona métodos robustos de autenticación de usuarios para verificar la identidad de quienes intentan acceder al servidor de forma remota. Esto puede incluir la autenticación basada en contraseñas, autenticación de dos factores, certificados digitales u otros mecanismos de autenticación seguros, dependiendo del sistema utilizado en la unidad. Por otro lado, todas las comunicaciones entre los clientes y el servidor a través de una sesión de Escritorio Remoto están encriptadas para proteger la confidencialidad de los datos transmitidos. Esto evita que terceros puedan interceptar y leer la información sensible que se envía entre el cliente y el servidor.

El hecho de que el escritorio remoto permita a los pilotos y militares acceder a la información crítica del servidor desde cualquier lugar con conexión a Internet, resulta beneficioso cuando están desplegados en misiones o destacamentos en ubicaciones desde las que no se tiene acceso físico al servidor en cuestión. Además, en estos casos, si surge algún problema o necesidad, los usuarios pueden recibir soporte técnico remoto a través del Escritorio Remoto, lo que les permite tanto resolver problemas como recibir asistencia de expertos sin necesidad de estar físicamente en el lugar donde se encuentra el servidor.

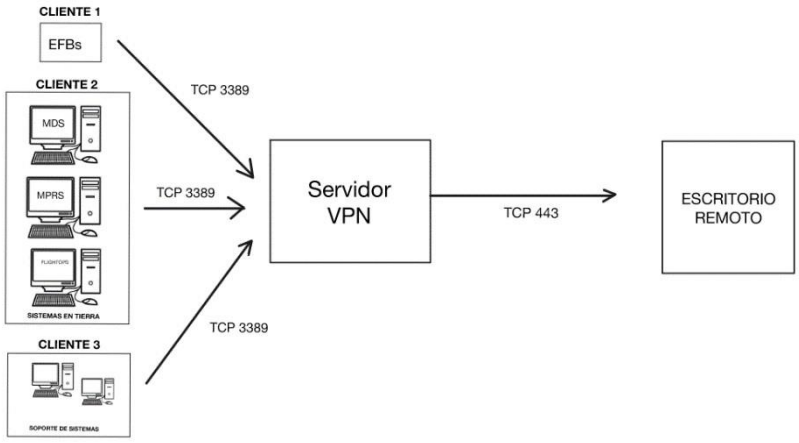


Tabla 8. Arquitectura de Escritorio Remoto. Elaboración propia.

Como se ha mencionado en el punto 8.2.1, las conexiones en este caso se realizan a través del protocolo HTTPS, que es una capa de seguridad que opera sobre TCP/IP.

En términos más detallados, lo primero que ocurre es el establecimiento de la conexión por VPN a través del puerto 443, por ello, antes de iniciar una sesión de Escritorio Remoto, los clientes establecen una conexión segura con el servidor principal a través de una la VPN (Red Privada Virtual) que proporciona un túnel seguro a través de Internet para el tráfico de red entre los clientes y el servidor. La conexión VPN, en este caso utiliza el puerto 443, que es comúnmente utilizado para conexiones HTTPS seguras, para encapsular y proteger el tráfico de la VPN.

Una vez que la conexión VPN está establecida, los clientes envían una solicitud de conexión al servidor principal utilizando el protocolo RDP (Remote Desktop Protocol). Es importante considerar que esta solicitud se envía a través del puerto 3389, que es el puerto estándar utilizado por el servicio de Escritorio Remoto para aceptar conexiones entrantes. Además, después de establecer la conexión RDP, se produce una negociación entre el cliente y el servidor para establecer los parámetros de la sesión de Escritorio Remoto y por ello, una vez que se establecen dichos parámetros, el protocolo RDP se encarga de transmitir los datos gráficos y de entrada entre el cliente y el servidor a través del túnel VPN. Esto incluye la transferencia de imágenes

de pantalla, acciones del ratón e incluso eventos del teclado, todo ello de forma segura gracias a la conexión VPN y al protocolo RDP.

Durante la sesión de Escritorio Remoto, el protocolo RDP permite al cliente controlar de manera remota el escritorio del servidor.

Para habilitar el servicio de Escritorio Remoto, al igual que en los casos anteriores, se añaden primeramente los roles y características correspondientes una vez se ha verificado que el servidor principal está seleccionado correctamente. En este caso, el rol que se añade es "*Remote Desktop Services".*

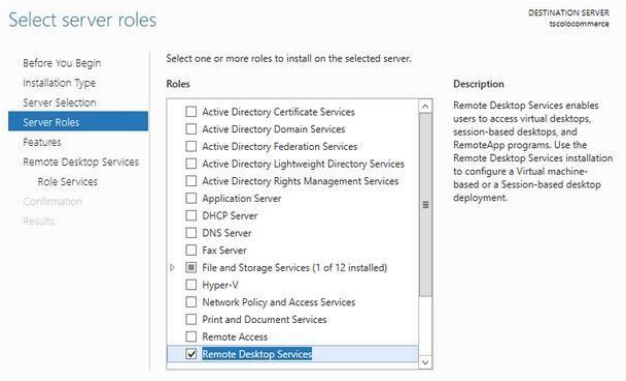


Figura 15. Habilitación del Escritorio Remoto. Elaboración propia.

Posteriormente se seleccionan las características requeridas y se comprueban para la posterior instalación del servicio.

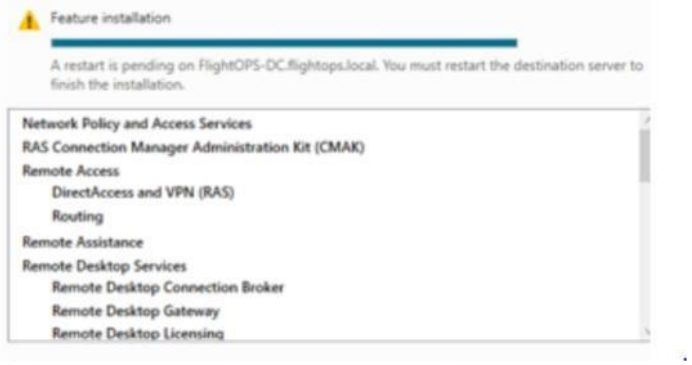


Figura 16. Instalación del Escritorio Remoto. Elaboración propia.

Una vez instalado el servicio de escritorio remoto, se reinicia el sistema y aparece en el Server Manager una notificación que indica que se requiere configuración de "Servicios de Escritorio remoto" y por ello se abre una ventana de configuración. Posteriormente se siguen los pasos que indica el asistente para configurar el Escritorio Remoto, incluida la asignación de licencias si es necesario, como se muestra en la siguiente imagen. Esta configuración debido a la naturaleza sensible de los datos, no se mostrará en el presente documento.

Figura 17. Asignación de licencia. Elaboración propia.

9.2.6. SERVIDOR DE IMPRESIÓN

El servidor de impresión gestiona las solicitudes de impresión de múltiples usuarios de la red, es decir, de los pilotos (a través de los EFBs), del personal de soporte de sistemas e incluso las solicitudes que se realizan desde los sistemas en tierra. En este caso, en lugar de conectar cada impresora directamente a los equipos individuales, estas se conectan a través de la red del servidor de impresión. De esta forma, cuando un usuario envía un documento para imprimir, este pasa directamente al servidor de impresión que lo procesa y posteriormente lo envía a la impresora encargada de la impresión física del documento en cuestión.

Además, en el contexto de este proyecto, el servidor de impresión contribuye a la centralización de la gestión de impresiones en la red, lo que facilita la administración y supervisión de las tareas de impresión en un entorno donde la eficiencia y la

seguridad son prioritarias. Por otro lado, el servidor de impresión se integra en los sistemas de control de acceso para garantizar que solo los usuarios autorizados puedan enviar documentos para imprimir, contribuyendo así a una mayor seguridad y la confidencialidad de la información.

El servidor de impresión lleva un registro detallado de todas las actividades de impresión que se realizan en la red proporcionando una trazabilidad importante para fines de cumplimiento normativo y posibles auditorías.

En este caso concreto, una vez está configurado correctamente el escritorio remoto, los usuarios que acceden al servidor principal a través de la conexión remota pueden imprimir los documentos desde el escritorio remoto, esto significa que los usuarios, ya sean EFBs, sistemas en tierra o equipos de personal, interactúan directamente con el Sistema Operativo (Windows Server) y pueden utilizar las aplicaciones y herramientas instaladas en el servidor incluidas las impresoras que estén configuradas y disponibles.

A continuación, se muestra una representación de dicho servicio:

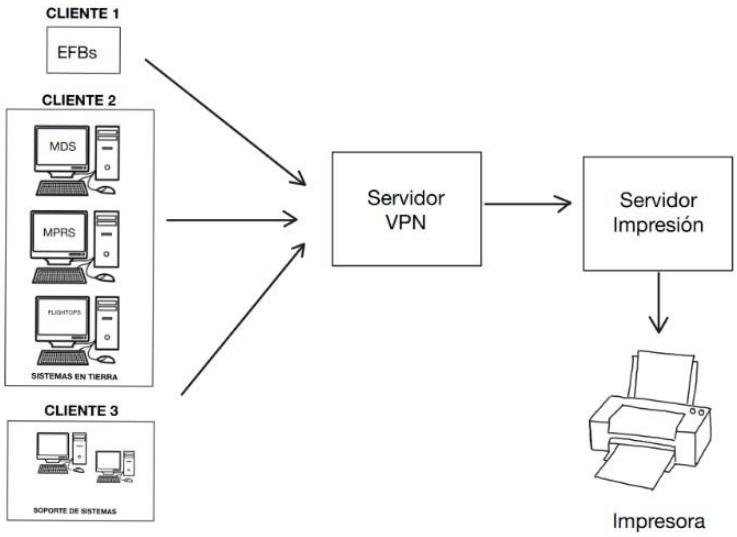


Tabla 9. Representación del servicio de Impresión. Elaboración propia.

Para la incorporación del servidor de impresión desde el Server Manager, al igual que en ocasiones anteriores, se añade el rol y las características correspondientes. Es importante asegurar que el servidor principal esté seleccionado como se muestra a continuación, aunque normalmente se encuentra seleccionado de forma predeterminada.

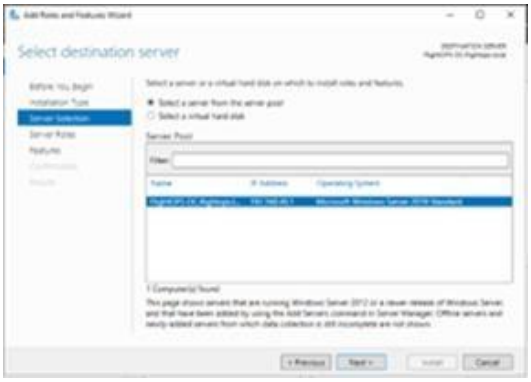


Figura 18. Configuración inicial de Servidor de Impresión. Elaboración Propia.

En la lista de roles, se marca "*Print and Document Services*" y de esta forma se instalan los componentes necesarios para el servidor de impresión.

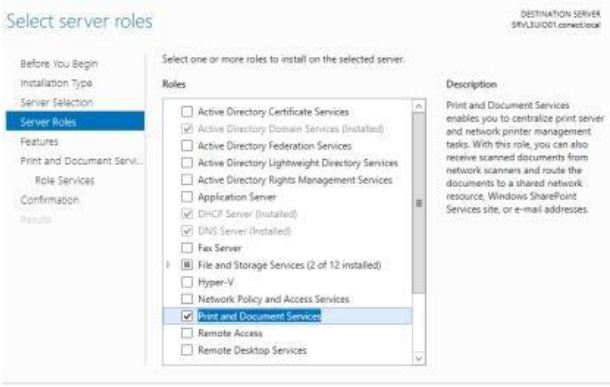


Figura 19. Roles del Servidor de Impresión. Elaboración propia.

Ahora, se deben seleccionar las características específicas que deseas instalar. En este caso "*Print Server*" e "*Internet Printing*" según las necesidades requeridas, como se muestra en la siguiente figura.

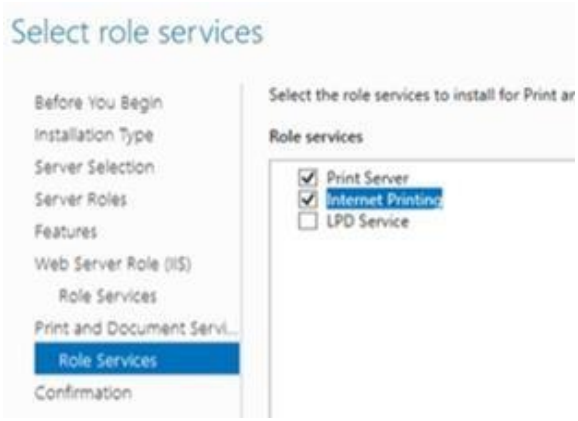


Figura 20. Servicios de Servidor de Impresión. Elaboración propia.

En esta ventana, se pueden seleccionar las características adicionales relacionadas con las impresoras, como la compatibilidad con impresoras UNIX o la administración de impresión web.

Por último, se verifican todas las opciones seleccionadas y se comprueba que se ajustan a las necesidades establecidas por la unidad y posteriormente, el asistente comenzará a instalar los componentes seleccionados.

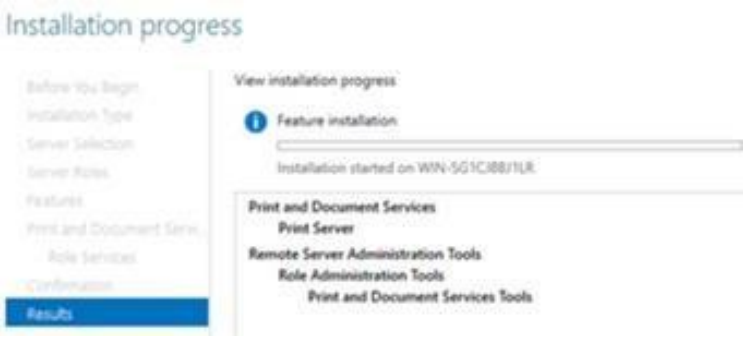


Figura 21. Servidor de Impresión. Elaboración propia.

De esta forma, ya se encuentra instalado el servidor de impresión para permitir la impresión de documentos.

9.2.7. WSUS (WINDOWS SERVER UPDATE SERVICES)

WSUS, acrónimo de "Windows Server Update Services", desempeña un papel esencial en el contexto de este servidor en la Ala 31, desde una perspectiva tanto profesional como técnica, con un especial enfoque en la seguridad ya que WSUS es una herramienta proporcionada por Microsoft que se encarga de la administración de las actualizaciones de software en entornos que utilizan sistemas operativos Windows.

WSUS opera como un servidor central dentro de la red y cumple el rol crucial de actuar como un depósito para las actualizaciones emitidas por Microsoft. Esto significa que, en vez de permitir que cada dispositivo descargue las actualizaciones directamente desde los servidores de Microsoft, WSUS descarga y almacena estas actualizaciones que posteriormente son distribuidas a los equipos en la red.

Esta estrategia proporciona múltiples ventajas, desde una perspectiva profesional, WSUS permite un control exhaustivo sobre el proceso de actualización debido a que los administradores pueden aprobar, rechazar o programar actualizaciones según las necesidades operativas, la compatibilidad y otros factores relevantes. Esto asegura que las actualizaciones se adapten a los requerimientos particulares del entorno en la Ala 31 y del servidor en cuestión.

Además, la implementación de WSUS afecta a los EFBs, sistemas en tierra y otros equipos ya que asegura que las actualizaciones de software se administran de manera centralizada y controlada, garantizando la seguridad y la estabilidad, que son características importantes del sistema objetivo. Los EFBs, los equipos de soporte y sistemas en tierra colaboran para garantizar que las actualizaciones se implementen de manera efectiva y sin impacto negativo en las operaciones.

En el ámbito técnico, WSUS optimiza el uso del ancho de banda. Al almacenar localmente las actualizaciones, reduce la demanda en la conexión a internet al distribuir las actualizaciones dentro de la red interna. Por otro lado, desde la perspectiva de la seguridad, WSUS tiene un impacto significativo ya que esta herramienta permite la rápida aplicación de actualizaciones críticas y de seguridad, reduciendo las vulnerabilidades conocidas en sistemas operativos y software de Microsoft. Esto minimiza las oportunidades para ataques cibernéticos que buscan explotar dichas vulnerabilidades.

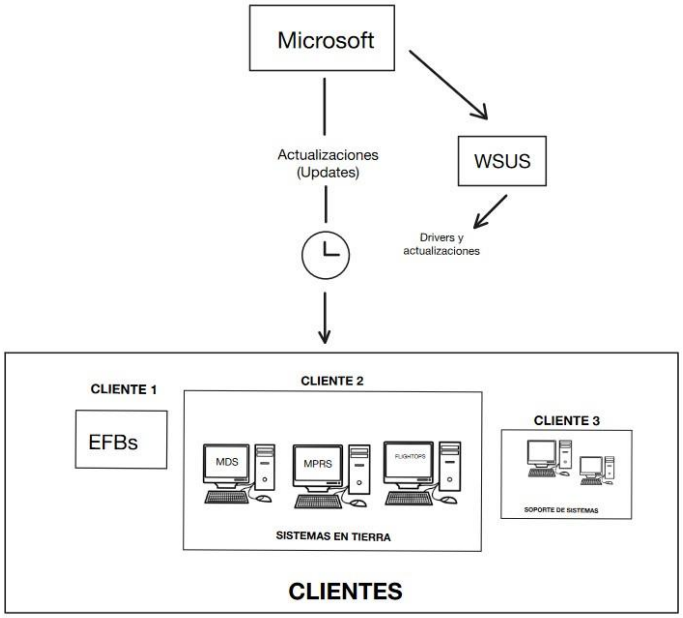


Tabla 10. Representación del servicio WSUS. Elaboración propia.

Como en casos anteriores, se instala el rol de Windows Server Update Services desde el asistente Server Manager de forma remota desde la ventana de Roles.

Para instalar WSUS, se debe seleccionar una ruta o path donde se guardarán todas las actualizaciones, en este caso, el directorio creado para este fin se denomina “Updates”.

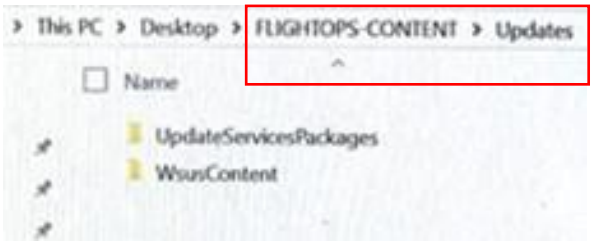


Figura 22. Directorio Updates. Elaboración propia.

9.2.8. DIRECTORIO COMPARTIDO

Compartir los recursos, en el contexto de este servidor, es uno de los objetivos ya que se prioriza la conectividad, centralización de información y eficiencia en la actualización y uso de esta. Además, si varios miembros del personal en la Ala 31 necesitan trabajar en los mismos archivos o proyectos, compartir recursos facilita la colaboración para que todos pueden acceder a los mismos datos y trabajar juntos de manera efectiva. Por otro lado, al centralizar los datos compartidos en el servidor, el proceso de respaldo y recuperación de datos se vuelve más eficiente, ya que no es necesario realizar copias de seguridad de cada dispositivo individualmente.

En este caso concreto, existirá un directorio compartido, de nombre “DATOS” que será donde se encuentre la información compartida y teniendo en cuenta la distribución de espacio de almacenamiento de este sistema, se deberá realizar lo siguiente para compartir dicho directorio.

Primeramente, se debe considerar que es necesario introducir las credenciales del usuario que tiene permisos de administrador en la ventana de “*Advanced Sharing*” respectiva al directorio DATOS.

Figura 23. Configuración de Escritorio Remoto. Elaboración propia.

A continuación, se marca la casilla "*Share this folder*" y se establece el nombre del recurso compartido, en este caso dicho recurso se denomina "zCOMPARTIDA" como se muestra a continuación:

Figura 24. Creación de directorio "ZCOMPARTIDA". Elaboración propia.

En un entorno militar como este, compartir recursos de manera estratégica puede ser crucial para facilitar la coordinación y la toma de decisiones efectivas.

En este caso, teniendo en cuenta todas las configuraciones realizadas y descritas en los puntos anteriores, los usuarios (EFBs, sistemas en tierra y sistemas de soporte)

se conectan a la red del servidor a través de una conexión VPN segura que establece un túnel cifrado entre los dispositivos clientes y el servidor. Una vez conectados a la red del servidor, los usuarios inician sesión en el servidor utilizando el protocolo de Escritorio Remoto (RDP), lo que implica abrir una conexión RDP desde el dispositivo cliente al servidor y una vez que los usuarios han iniciado sesión en el servidor a través del escritorio remoto, pueden acceder al directorio compartido utilizando el Explorador de Archivos, como se muestra a continuación.

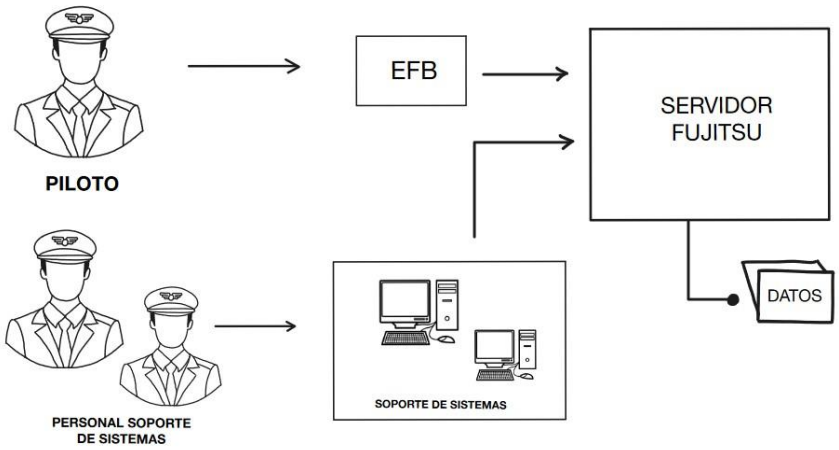


Tabla 11. Representación Directorio DATOS compartido. Elaboración propia.

El correcto funcionamiento del directorio compartido se comprueba en el apartado 10.2.

10. EVALUACIÓN Y PRUEBAS

En este capítulo, se detalla la fase de verificación y evaluación del sistema, por lo que se lleva a cabo una revisión para asegurar que el sistema esté operando correctamente y se cumplan todos los objetivos establecidos inicialmente, como se detalla en la sección 7.1.1 del documento.

La evaluación se lleva a cabo mediante la verificación de dos aspectos críticos: la capacidad de los usuarios principales (EFBs, Sistemas en Tierra y Sistemas de Soporte) para acceder al escritorio remoto y la disponibilidad de acceso a la carpeta compartida para una visualización adecuada de los archivos y documentos. Es importante destacar que para realizar esta evaluación se cuenta con el apoyo de un equipo auxiliar de soporte del área de Sistemas, ya que desempeña uno de los roles de usuario definidos para este sistema.

10.1. ACCESO A ESCRITORIO REMOTO

Con el fin de verificar la operación apropiada del escritorio remoto, se emprende una fase inicial que implica la conexión de una estación adyacente al switch que posibilita la conectividad de la red. Se debe considerar que, para llevar a cabo esta acción, es necesario instaurar un usuario en el dominio que previamente ha sido establecido (en el punto 9.2.8. Posteriormente se habilita la estación para establecer la conexión al escritorio remoto.

En primer lugar, para añadir el usuario en cuestión al dominio, se abre el directorio "*Active Directory Users and Computers*" en el servidor. A continuación, desde el desplegable que ofrece el servidor, se accede al directorio "*Users"*.

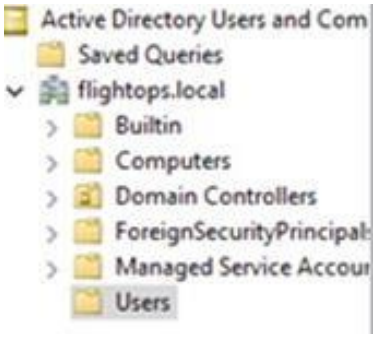


Figura 25. Ubicación de Usuarios. Elaboración propia.

En este punto, se ingresan los datos pertinentes para el nuevo usuario, en este caso se identifica como “Prueba”.

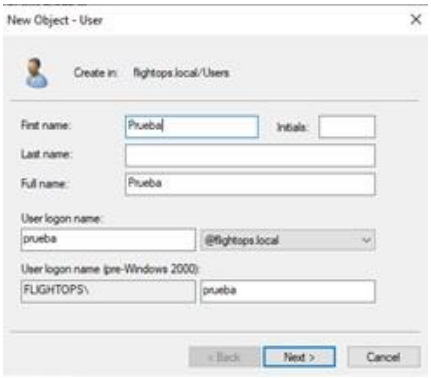
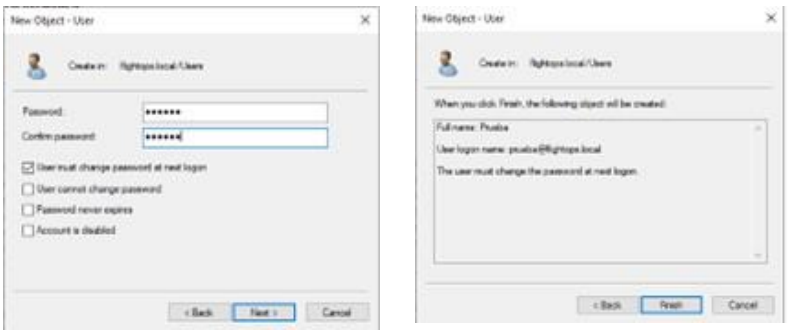


Figura 26. Usuario Prueba. Elaboración propia.

Una vez que los datos han sido registrados, se establece una contraseña. Dado el acento especial en la seguridad de este proyecto, es imperativo tener en cuenta la política de contraseñas del dominio configurado.



Figuras 27 y 28. Credenciales del usuario prueba. Elaboración propia.

Una vez realizado el proceso de creación del usuario "Prueba" dentro del dominio predeterminado, se continua desde el equipo auxiliar. Es imprescindible asegurar que equipo en cuestión cuente con conectividad de red, lo que implica que se encuentre dentro del rango de direcciones IP de la red local y que sea parte integrante del dominio establecido *("flightops.local")*.

En este contexto, la dirección IP establecida para el equipo auxiliar es 192.168.40.2, y la máscara de subred se sitúa en 255.255.255.0, tal como sucede en el servidor

Además, a parte de la dirección IP, otros parámetros que contribuyen a la configuración de red son la máscara de subred, la puerta de enlace y los servidores DNS.

Figura 29. Parámetros de configuración de red. Elaboración propia.

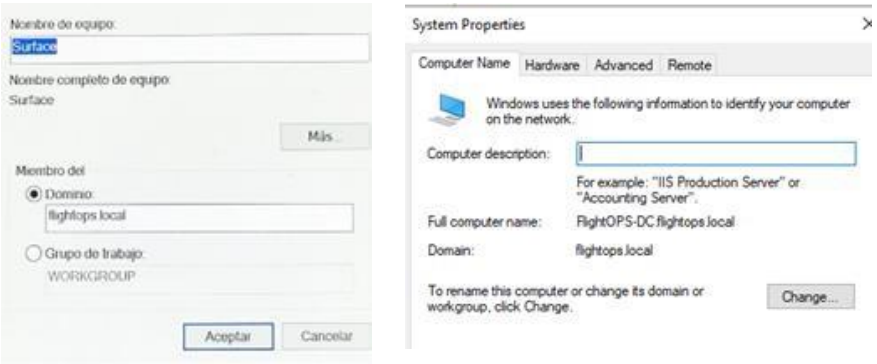
La puerta de enlace (Gateway) se cifra en 192.168.40.1. y la máscara de subred, por su parte, define los intervalos de direcciones IP que son considerados válidos en la Red de Área Local (LAN), que en este caso específico es la red interna a la que están conectados los dispositivos dentro del dominio *flightops.local*. Además, se establece una conexión a través de la WAN, que puede ser una red corporativa privada o a través de internet público, para acceder a un equipo en la LAN desde una ubicación remota.

Es esencial recordar que la puerta de enlace conecta la red interna (LAN) con la red externa (WAN), mientras que el servidor DNS (*Domain Name Server*) desempeña la función de traducir los nombres de dominio en direcciones IP.

Todos estos parámetros tienen su configuración dentro de la sección de propiedades de la conexión Ethernet del equipo auxiliar, y se debe tener en cuenta que es necesario asignar el dominio al equipo auxiliar. Con ese fin, se accede al panel de control de Windows y, dentro de la opción “Sistema y seguridad”, se selecciona la opción "Sistema". Desde allí, se opta por "Configuración Avanzada del sistema", abriendo así la ventana de “Propiedades del sistema” donde es posible ingresar el nombre de dominio correspondiente. Conforme se ha mencionado anteriormente, el dominio para este propósito es "flightops.local".

Es relevante destacar que, en este escenario, el equipo auxiliar que se quiere incorporar al dominio pertenece a un grupo de trabajo ya existente, por ello, es recomendable modificarlo a un grupo de trabajo distinto antes de emprender el proceso de adhesión al dominio.

Esta medida es sumamente beneficiosa, puesto que evita conflictos y agiliza la transición hacia el nuevo dominio.



Figuras 30 y 31. Añadir el equipo auxiliar a l dominio. Elaboración propia.

De esta forma, se añade el equipo auxiliar al dominio en cuestión, como se muestra a continuación.

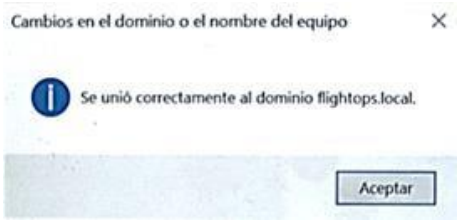


Figura 32. Unión correcta al dominio. Elaboración propia.

Una vez que la configuración se encuentra completa y el dominio ha sido asignado, la manera más eficaz de evaluar si existe una conexión entre el escritorio remoto del servidor y el equipo auxiliar es ejecutar el comando ping desde el equipo a la dirección del dispositivo al que se desea acceder, en este caso 192.168.40.1, correspondiente al servidor, por lo tanto, el comando a ejecutar es:

$ping 192.168.40.1

La presencia de una respuesta y la recepción de datos indican que existe conectividad en el rango establecido. En contraste, si se detecta la pérdida de datos, ello sugiere que alguna configuración presenta deficiencias.

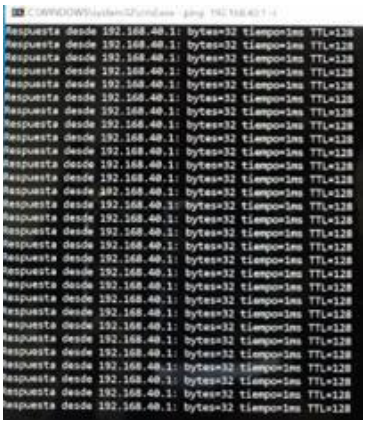


Figura 33. Ping de comprobación de conexión. Elaboración propia.

Como se puede observar en a figura, existe respuesta y, por consiguiente, existe conexión.

Una vez la conexión está establecida, se ingresan las credenciales con permisos de administrador provocando un reinicio del sistema. Al momento de reiniciar, se

introducen las credenciales del usuario "Prueba" que se ha creado, y se establece la conexión con el servidor introduciendo su dirección IP.

Es importante considerar que en el servidor se deben agregar los usuarios que se desean dotar de permisos para la conexión remota, como es el caso del usuario "Prueba".

Figura 34. Conexión remota. Elaboración propia.

Finalmente, se accede el escritorio del servidor de forma remota con éxito, como se muestra a continuación.

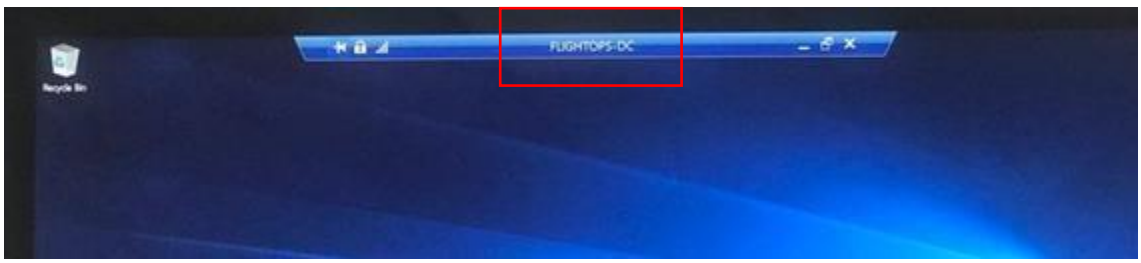


Figura 35. Conexión remota establecida. Elaboración propia.

En este contexto, dada la naturaleza crítica de un servidor de almacenamiento de datos del ejército y la información altamente sensible que contiene, los permisos de administrador son esenciales para garantizar la seguridad, la confidencialidad y el funcionamiento adecuado del sistema. Además, una buena práctica sería implementar medidas de seguridad adicionales, como la autenticación de múltiples

factores y la segmentación de redes, para aumentar la protección en entornos tan sensibles.

Una vez se haya comprobado el correcto funcionamiento del escritorio remoto, se puede incluir el hardware en la estructura del Centro de Procesamiento de Datos (CPD) del Ala 31 y continuar de forma remota con las tareas.

10.2. ACCESO A DATOS COMPARTIDOS

En el marco de este proyecto, tal y como se ha indicado en varias ocasiones, la optimización del tiempo y el acceso eficiente a la información almacenada en el servidor por parte de los usuarios de manera remota es uno de los objetivos fundamentales.

Para demostrar la viabilidad de este enfoque, se lleva a cabo a lo largo de este capítulo una prueba específica, teniendo en cuenta la creación y compartición de una carpeta designada como "zCompartida" (punto 9.2.8), cuya función de esta carpeta es servir como repositorio centralizado que aloja información crítica y datos relevantes que necesitan ser accedidos por los pilotos (a través de EFBs), sistemas en tierra y sistemas de soporte.

Desde el equipo auxiliar que se encuentra en la red y teniendo en cuenta la conexión remota establecida en el punto 10.1, se comprueba que la carpeta "zCompartida" es claramente visible en la estructura de directorios lo que proporciona una evidencia de que la compartición de recursos se ha implementado exitosamente y que la estructura de archivos está disponible para su acceso, como se puede observar en la Figura 36.

Para ello, en el equipo auxiliar se introduce en la ventana de red la dirección URL del recurso compartido, en este caso \\FLIGHTOPS-DC y así se visualiza el directorio.

Figura 36. Recurso compartido. Elaboración propia.

En el contexto de esta prueba, se realiza una interacción bidireccional con la carpeta compartida para comprobar la capacidad de descargar y cargar contenido desde y hacia la carpeta compartida. En este caso se confirma que la transferencia de datos es factible y que los usuarios pueden acceder a información vital de manera eficiente.

La capacidad de acceder y trabajar en archivos alojados en la carpeta "zCompartida" desde distintos dispositivos remotos brinda la posibilidad de colaboración remota. Esto es crucial para la coordinación de tareas y la toma de decisiones conjuntas por parte de los pilotos y el personal de tierra.

Sin embargo, para que a los usuarios se les muestre dicho recurso directamente, sin necesidad de introducir la dirección URL, se crea una GPO (Group Policy Object) llamada "*MAPEO Z COMPARTIDA"* como se muestra a continuación.

Figura 37. Acceso directo al recurso. Elaboración propia.

Una GPO es un componente fundamental en el sistema operativo Windows que permite a los administradores de sistemas definir, configurar y gestionar una amplia variedad de configuraciones y políticas para usuarios y equipos en una red. Además.

se utilizan para establecer y mantener consistentemente la configuración de seguridad, el entorno de usuario, las restricciones y muchas otras opciones en un entorno de red de Windows.

Después de realizar la configuración pertinente para la GPO y establecer las políticas necesarias desde la consola de comandos, se puede visualizar la carpeta compartida directamente, sin tener que introducir la URL, lo que facilita el acceso y optimiza el tiempo de este facilitando el trabajo y las tareas de los usuarios que se quieran conectar.

Figura 38. Acceso directo establecido. Elaboración propia.

La misma situación ocurre en el lado del servidor como se muestra a continuación:

Figura 39. Acceso directo del lado del servidor. Elaboración propia.

11. CONCLUSIONES Y RESULTADOS

A lo largo del proyecto se han considerado aspectos clave como las cinco dimensiones de la ciberseguridad (trazabilidad, autenticidad, disponibilidad, confidencialidad e integridad), teniendo en cuenta la normativa y las regulaciones pertinentes tanto a nivel nacional, como a nivel europeo e internacional. Además, se ha tenido en cuenta el carácter crítico y confidencialidad de los datos.

Por otro lado, se han cumplido los objetivos establecidos ya que se ha optimizado el proceso de gestión e intercambio de información entre los diferentes usuarios y personas pertenecientes al Ala 31 contribuyendo así a la evolución y mejora tecnológica de esta unidad esencial para el Ejército del Aire y, por consiguiente, para las Fuerzas Armadas Españolas.

Además, se han tenido en cuenta términos como la escalabilidad y la accesibilidad de los usuarios, creando un sistema de fácil acceso para todos ellos, siempre que hayan sido autorizados y que permite mejoras y actualizaciones futuras.

Por otro lado, se ha mejorado la centralización y el orden de la información gracias a la implementación del sistema de gestión de información propuesto como solución, contribuyendo a facilitar la actualización en tiempo real y transferencia eficiente de datos y asegurando su correcto funcionamiento en conjunto con el software creado previamente para este fin.

En resumen, el presente trabajo constituye a un análisis exhaustivo, implementación y operación con éxito de un sistema de gestión de información dentro del sector militar del Ala 31 que cumple con requisitos de seguridad e incorpora funcionalidades útiles para las tareas diarias de todos sus servicios.

La descripción del procedimiento que se ha seguido se complementa con imágenes, esquemas y referencias bibliográficas para una mayor comprensión de la situación inicial, la solución propuesta y la implementación de dicha solución difundir y explicar cómo reaccionar ante una sociedad cada día más tecnológicamente dependiente.

12. REFERNCIAS

[1] Ministerio de Asuntos Económicos y Transformación Digital. 2022. Esquema Nacional de Seguridad.

https://www.boe.es/boe/dias/2022/05/04/pdfs/BOE-A-2022-7191.pdf

[2] Centro Criptológico Nacional. 222. Gobernanza de Seguridad Nacional. https://gobernanza.ccncert.cni.es/ens-navegable

[3] Ministerio del Interior. 2011.

https://www.boe.es/buscar/pdf/2011/BOE-A-2011-8849consolidado.pdf

[4] Ministerio de Presidencia, Relaciones con las Cortes y Memoria democrática. 2021. Real Decreto-ley Seguridad de las redes y sistemas

https://www.boe.es/boe/dias/2021/01/28/pdfs/BOE-A-2021-1192.pdf

[5] Ministerio de Defensa. Abril 2018. Revista de Aeronáutica y Astronáutica.
https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/a/raa_872.pdf

[6] Microsoft. 2023. Windows Server. https://www.microsoft.com/es-es/windows-server

[7] Microsoft. 2023. Administrador de Servidores. https://learn.microsoft.com/es-es/windowsserver/administration/server-manager/server-manager

[8] Dinahosting. 2023. Servidor DNS. https://dinahosting.com/ayuda/que-es-un-servidor-dns/

[9] Axarnet. 2023. Servidor de Archivos. https://axarnet.es/blog/servidor-de-archivos

[10] Microsoft Soporte técnico. Servidor de Impresión. https://support.microsoft.com/eses/topic/administraci%C3%B3n-de-la-

impresi%C3%B3n-en-red-en-un-entorno-windows-8e06c364e4bf-8842-915a-ba9f077f3bda

[11] Asperix Security. 2023. Controlador de Dominio. https://www.asperis.es/blog/controlador-dedominio/

[12] Microsoft. 2023. Guía Oficial de Server Manager. https://learn.microsoft.com/es-es/windowsserver/administration/server-manager/manage-the-local-server-and-the-server-manager-console

[13] SSL.com. 2023. Apretón de manos. https://www.ssl.com/es/art%C3%ADculo/ssl-tls-apret%C3%B3nde-manos-que-garantiza-interacciones-seguras-en-l%C3%ADnea/

[14] IBM. 2023. Cifrado extremo a extremo. https://www.ibm.com/es-es/topics/end-to-end-encryption

[15] Microsoft. 2023. Bosque de dominio organizativo. https://learn.microsoft.com/es-es/windowsserver/identity/ad-ds/plan/using-the-organizational-domain-forest-model

[16] Centro Criptológico Nacional. Septiembre 2023. Guía de Ciberseguridad de las TIC CCN-STIC 140.

Taxonomía de referencia para productos de Seguridad TIC (cni.es)

[17] Centro Criptológico Nacional. Abril 2024. Guía de Ciberseguridad de las TIC CCN-STIC 105.

file.html (cni.es)

ANEXOS

ANEXO A. ARTÍCULOS DEL ENS EXCLUIDOS

ARTÍCULOS EXCLUIDOS DEL ESQUEMA NACIONAL DE SEGURIDAD

Se debe tener en cuenta que el análisis de los artículos a cumplir o a excluir se hace desde el punto de vista de políticas de seguridad y requisitos mínimos de seguridad del Esquema Nacional de Seguridad.

Artículo 3. Sistemas de Información que traten datos personales. En este caso, el sistema no almacena información personal de los usuarios. Solamente almacena datos referentes a los usuarios en termas de nombres de usuario y contraseñas.

Artículo 19. Adquisición de productos de seguridad y contratación de servicios de seguridad. En este caso, las instalaciones donde se encuentra el sistema cuentan con mecanismos de seguridad rigurosos ya que solo pueden acceder a dichas instalaciones le personal autorizado. A su vez, dentro de las propias instalaciones, el sistema se encuentra en un área restringida cuyo acceso solo está permitido a cierto personal autorizado de la unidad de Soporte de Sistemas.

Se puede decir, por lo tanto, que el sistema se encuentra en un entorno con doble factor de seguridad.

Artículo 23. Prevención ante otros sistemas de información interconectados. En este caso, el sistema no se conecta a redes públicas. Además, para tener acceso a la red se utiliza una Red Privada Virtual.

ANEXO B: GOBERNANZA DE CIBERSEGURIDAD NACIONAL APLICADA

A continuación, se muestran las medidas de seguridad que se aplican en este proyecto según marca la Gobernanza de Ciberseguridad Nacional proporcionada por el Centro Criptológico Nacional Español (CCN).

MEDIDAS DE SEGURIDAD - GOBERNANZA DE CIBERSEGURIDAD			
	Org	**Medida**	**Comentario**
Control de Acceso	op.acc1	Identificación	Se utiliza una técnica de identificación interna del EA utilizando tarjetas.
	op.acc.2	Requisitos de Acceso	Los recursos del sistema se protegen para que solo puedan ser utilizados por usuarios con permisos suficientes que se establecen según las responsabilidades de cada usuario.
	op.acc.3	Segregación de funciones y tareas	Se diferencian responsabilidades y tareas
	op.acc.4	Proceso de gestión de derechos de acceso	Accesos prohibidos sin autorización, los usuarios solo están autorizados a acceder a información relativa a sus
	op.acc.6	Mecanismos de autenticación (usuarios	Se utiliza un nombre de usuario y una contraseña segura
Protección	mp.if.1	Areas separadas con control de acceso	El servidor se encuetra en un lugar separado y aislado, dentro de un CPD
	mp.if.2	Identificación de personas	Solo pueden acceder al lugar dónde se encuentra el sistema personas con un permiso muy restrictivo
	mp.if.3	Acondicionamiento de los locales	cuenta con un sistema de aislamiento bajo llave
	mp.if.4	Energía eléctrica	Se dispone de toma de corriente eléctrica en el entorno del sistema
	mp.if.5	Protección frente a incendios	El lugar donde se encuentra el servidor cuenta con un sistema anti incendios
	mp.if.6	Protección frente a inundaciones	El lugar donde se encuentra el servidor cuenta con un sistema anti inundaciones
	mp.if.7	Registro de entrada y salida	Se tiene control sobre los accesos a la unidad donde se encuentra el sistema
Explotación	op.exp.1	Inventario de activos	Se tienen identificadas las partes esenciales que forman el sistema
	op.exp.2	Configuración de seguridad	Se configuran los equipos previamente a su entrada en operación
	op.exp.3	Gestión de la configuración de seguridad	Se mantiene el equipamiento físico y lógico que constituye el sistema
	op.exp.4	Mantenimiento de las actualizaciones	Se atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluye un seguimiento continuo de los anuncios de defectos.
	op.exp.5	Gestión de cambios	Se mantiene un control continuo de los cambios realizados en el sistema

Tabla 12. Análisis de medidas de seguridad CCN. Elaboración propia.

Teniendo en cuenta el análisis anterior, cabe destacar que existen medidas de seguridad que no aplican en este contexto prestando especial atención a la medida de seguridad respectiva a Marco Operacional con identificativo **Op.pl.5** como se explica a continuación.

Op.pl.5. Componentes certificados: No se utilizan componentes proporcionados por terceros.

Existen dispositivos y componentes que el Esquema Nacional de Seguridad, mediante el Real Decreto 311/2022, de 3 de mayo, ha clasificado como proveedores de seguridad y dichos dispositivos se recogen la Guía de Seguridad de las TIC CCN-STIC 140.

Tras revisar dicha guía y el inventario de activos, se ha comprobado que el Sistema Operativo, en este caso Windows Server, está clasificado como servicio de seguridad y por ello debe tener una certificación asociada. Además, existe la Guía de Seguridad de las TIC CCN-STIC 105 que indica qué componentes están validados por el CCN (Centro Criptológico Nacional). En dicha guía se comprueba si el sistema operativo que se ha utilizado en este proyecto se encuentra entre los componentes validados en términos de seguridad. En este caso, Windows Server 2016 y superiores están validados y por ello se concluye que cumple con los requisitos.

Además, se deben considerar la aplicación y seguimiento de los estándares establecidos en las Guías de Configuración Segura enfocado a los servicios y funcionalidades del sistema como punto de mejora para futuras modificaciones de este.

Op.acc.5. Mecanismos de autenticación a terceros. En este caso, personas externas a la organización, al Ala o pertenecientes a cualquier área externa no tienen autorización, por ello, esta norma de seguridad no aplica para este sistema.

Es importante destacar que la configuración que se ha realizado cumple con las medidas de seguridad anteriormente mencionadas, sin embargo, se debe destacar

como posible punto de mejora la implementación de un sistema de métricas que notifique y alerte del estado del servidor para poder tener control sobre la carga de accesos e información a la que está sometido el sistema. Dicho Sistema de Métricas se considera en la medida de seguridad Op.mon.1 que, en este contexto podría contemplarse en conjunto con la medida Op.pl.4 respectiva al dimensionamiento y gestión de la capacidad del servidor. La aplicación de estas normas implica un estudio sobre las necesidades de procesamiento, de almacenamiento, de comunicación, de personal y necesidades de instalaciones o medios auxiliares.