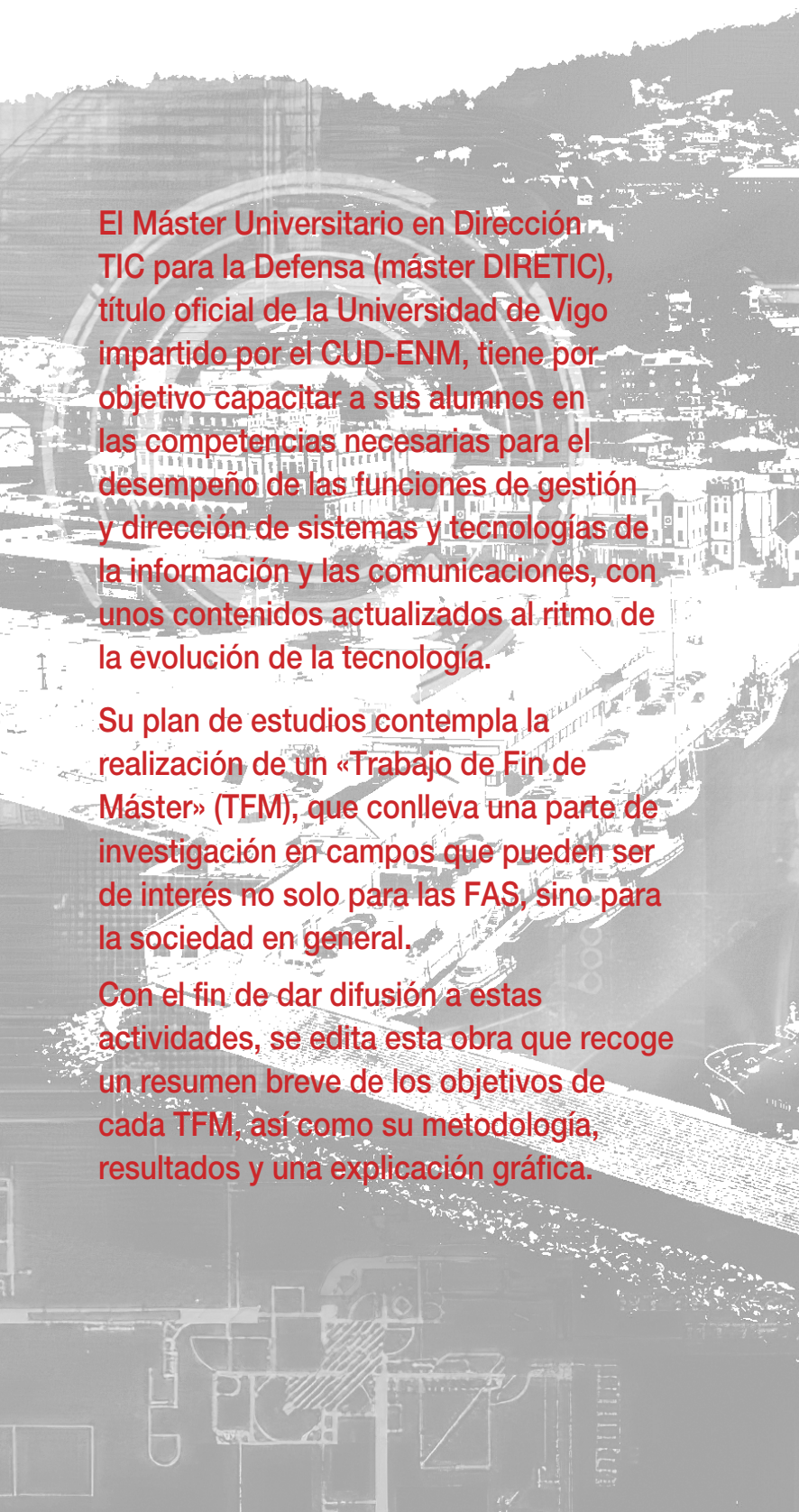
Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2022-2023

Centro Universitario de la Defensa en la Escuela Naval Militar

MINISTERIO DE DEFENSA



El Máster Universitario en Dirección TIC para la Defensa (máster DIRETIC), título oficial de la Universidad de Vigo impartido por el CUD-ENM, tiene por objetivo capacitar a sus alumnos en las competencias necesarias para el desempeño de las funciones de gestión y dirección de sistemas y tecnologías de la información y las comunicaciones, con unos contenidos actualizados al ritmo de la evolución de la tecnología.

Su plan de estudios contempla la realización de un «Trabajo de Fin de Máster» (TFM), que conlleva una parte de investigación en campos que pueden ser de interés no solo para las FAS, sino para la sociedad en general.

Con el fin de dar difusión a estas actividades, se edita esta obra que recoge un resumen breve de los objetivos de cada TFM, así como su metodología, resultados y una explicación gráfica.

Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2022-2023

RESÚMENES EXTENDIDOS

Centro Universitario de la Defensa en la Escuela Naval Militar

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
https://publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edición científica: Milagros Fernández Gavilanes y José María Núñez Ortuño

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-24-058-4 (edición impresa)
ISBN 978-84-9091-868-5 (edición impresa)

NIPO 083-24-057-9 (edición en línea)

Depósito legal M 4195-2024
Fecha de edición: febrero de 2024
Maqueta e imprime: Imprenta Ministerio de Defensa

En esta edición se ha utilizado papel procedente de bosques gestionados de forma sostenible y fuentes controladas.

Prólogo

El Centro Universitario de la Defensa en la Escuela Naval Militar (CUD-ENM), es un centro universitario público del Ministerio de Defensa (MINISDEF), adscrito a la Universidad de Vigo, que comenzó su actividad en el curso académico 2010-2011, en virtud de lo dispuesto en el Real Decreto 1723/2008, de 24 de octubre, por el que se crea el sistema de centros universitarios de la defensa. Su finalidad principal es la impartición de las enseñanzas universitarias que acuerde el MINISDEF, en función de las necesidades de la defensa nacional y las exigencias del ejercicio profesional de las Fuerzas Armadas.

Su objetivo prioritario es la impartición del título de grado en Ingeniería Mecánica (intensificación en Tecnologías Navales), título oficial de dicha universidad, pero el propio real decreto contempla que se puedan impartir enseñanzas de posgrado, en las modalidades de máster y doctor.

La Orden DEF/2639/2015, de 13 de diciembre, sobre Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, señala la necesidad de hacer una revisión de los cursos de perfeccionamiento y de altos estudios de la Defensa Nacional, a fin de obtener un mejor aprovechamiento de las capacidades del personal en el ámbito CIS/TIC del MINISDEF. Como consecuencia de esta necesidad nace el curso en Gestión y Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones (STIC) y de Seguridad de la Información, cuyo plan de estudios contempla una carga lectiva (60 ECTS), asignada al CUD-ENM en forma de máster, más un periodo de prácticas presenciales

(6 ECTS), cuya responsabilidad recae en el CESTIC. El curso comenzó su andadura en septiembre de 2017, con el máster impartido como título propio, por estar en proceso de verificación la memoria correspondiente al título oficial.

La verificación positiva del título se produjo en julio de 2019, año a partir del cual el máster es impartido como título oficial de la Universidad de Vigo, con la denominación de Máster Universitario en Dirección TIC para la Defensa (máster DIRETIC). En enero de 2021 se ha producido el egreso de la primera promoción de este máster.

El plan de estudios del máster DIRETIC contempla la realización de un Trabajo de Fin de Máster (TFM) dirigido por profesores del mismo, que conlleva una parte de investigación en campos que pueden ser de interés no solo para las FAS, sino para la sociedad en general. Con el fin de dar difusión a estas actividades, se edita el presente volumen que recoge, para cada TFM realizado durante el curso académico 2022-2023, un resumen de sus objetivos, metodología empleada y resultados obtenidos, así como una explicación esquemática en forma gráfica. Todos los resúmenes, así como los trabajos completos cuya difusión ha sido autorizada, se encuentran accesibles en el siguiente repositorio del centro: http://calderon.cud.uvigo.es, al que se puede acceder libremente.

Información adicional sobre el CUD-ENM o su actividad, tanto académica como de investigación o administrativa, se encuentra accesible en la página web: https://cud.uvigo.es.

José Martín Davila
Director del Centro Universitario de la Defensa
en la Escuela Naval Militar

Índice de contenidos

Las memorias completas de los trabajos fin de máster están disponibles en el repositorio institucional de este centro universitario de la Defensa y se pueden descargar a través del siguiente enlace:

http://calderon.cud.uvigo.es/handle/123456789/101

Índice de contenidos

Índice por autores

Trabajos fin de máster

Especialidad en Sistemas y Tecnologías de Información

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Trabajos fin de máster

Especialidad en Sistemas y Tecnologías de Información

El talento como factor estratégico organizacional en la Guardia Civil

Autor: Gabriel de la Coba Santana (gabriel.dlcs@gmail.com)
Director: Francisco Javier Rodríguez Rodríguez (fjavierrodriguez@cud.uvigo.es)

Resumen – El presente trabajo encamina su ámbito de estudio hacia la gestión de RR. HH. en la Guardia Civil y hacia el cambio de paradigma en la dirección de personas y la gestión del talento, junto a sus respectivos procesos. Se orienta la atención en la evaluación de la externalización de la gestión de talento como ventaja competitiva (outsourcing y headhunters), y en la adopción de la estrategia de employer branding o, en castellano, Marca del Empleador (ME), encaminada a generar una imagen positiva de una organización de cara a la atracción y retención del talento.

El empleo de estas técnicas ha permitido generar una serie de líneas estratégicas de actuación en el ámbito de la mejora en el proceso selectivo del personal de la Guardia Civil, también aportadas en el estudio.

Por otro lado, y para entender la situación actual de la institución armada, se realiza un análisis de los modelos de gestión estratégica directiva que plantean diversos expertos.

Asimismo, se aplica el instrumento de planificación estratégica cinco fuerzas de M. Porter para evaluar el entorno competitivo actual en relación con la atracción y retención del talento en la Guardia Civil. Además, se estudia la adaptación a los cambios del entorno, la evolución de los enfoques en la dirección de personas y el análisis del valor que aporta el talento en la institución, buscando nuevas formas de crear valor, focalizando en la ME.

En definitiva, el presente TFM aborda la importancia de la gestión del talento y de la dirección de personas como factores imprescindibles de la planificación estratégica organizacional, y su aplicación sobre la estrategia de dirección de personas, basada en el talento en el seno de la Guardia Civil.

Palabras clave – Talento, Dirección de personas, Marca del empleador, Planificación estratégica, Cambio de paradigma.

1. Introducción

Motivación

Actualmente, nos movemos, empresas y trabajadores, en un ambiente laboral convulso, en constante evolución y que trata de adaptarse al trabajador. La selección de personal no radica ya en la búsqueda del cumplimiento de un perfil determinado, sino en la captación de personas con talento que, además de cumplir con sus objetivos profesionales, puedan aportar valor añadido al resto de su entorno y a la empresa o institución.

El talento se constituye como factor de atracción por parte de las organizaciones, pues se busca que los trabajadores puedan servirse de sus capacidades para la consecución de objetivos eficaces dentro de la estructura corporativa.

En la Guardia Civil, a pesar de tratarse de un organismo público, la gestión del talento se advierte absolutamente necesaria a fin de ofrecer un mejor servicio a la ciudadanía. Su consideración como un factor estratégico organizativo de alta importancia permitiría a la institución posicionarse como marco de referencia en la gestión de personas en el ámbito policial.

Objetivos

A continuación, se reflejan los objetivos que pretende abordar el presente trabajo:

- Conocer los criterios que lo sustentan y analizar las posibles áreas de mejora en el proceso selectivo de la Guardia Civil (captación).
- Identificar cómo se gestiona el talento como factor estratégico organizacional en la Guardia Civil.
- Analizar la viabilidad de herramientas como outsourcing, headhunters o employer branding en la institución y su repercusión como ventaja competitiva.
- Evaluar el entorno competitivo actual en relación con la identificación, captación, desarrollo y retención del talento en la Guardia Civil (por ejemplo, con la aplicación del modelo de las cinco fuerzas de M. Porter).
- Detectar un plan de acción en dirección de personas para impulsar el talento dentro de la conceptualización estratégica del talento en la Guardia Civil que genere valor añadido a la Institución.
- Examinar las estrategias de mejora para la dirección de personas basada en el talento de la Guardia Civil, identificando las medidas de actuación susceptibles de ser aplicadas.

2. Desarrollo

Se pretende ubicar al lector en un contexto de comprensión suficiente para vislumbrar los motivos que han originado el cambio de paradigma en

la dirección de personas, permitiendo que la gestión del talento pueda ser considerada como un factor estratégico organizacional. Asimismo, se analizan los modelos de gestión formulados para la adopción de decisiones estratégicas institucionales.

Por otro lado, se estudia la externalización de la gestión de talento como ventaja competitiva: *outsourcing, headhunter* y la estrategia de Marca del Empleador (ME). Por último, y dentro del ámbito de la dirección de las personas en la Guardia Civil (GC), se detalla, en profundidad, el proceso selectivo de personal para la institución.

Se analiza el entorno competitivo de la institución y para ello se aplica el modelo de las cinco fuerzas de M. Porter. Posteriormente, se detalla la adaptación a los cambios del entorno y la evolución de los enfoques de la dirección de personas y el análisis del valor que aporta el talento en la institución.

Se constituye como elemento clave el plan de acción en dirección de personas para impulsar el talento y en la conceptualización estratégica del personal en la Guardia Civil, destacando los factores que influyen en la consecución del mismo. En este análisis se profundiza en la identificación, captación, desarrollo y retención de los trabajadores.

De dicho análisis se pudo aseverar que trabajar en la detección de personal más idóneo con base en sus capacidades y la posibilidad de explotación es un área de mejora que la Guardia Civil puede implementar en un futuro. También resulta imprescindible para cualquier organización mantener o retener ese talento, a fin de evitar que sea seducido por la competencia. Herramientas como un buen entorno laboral, condiciones satisfactorias de conciliación familiar, garantías de promoción interna y mejoras en la retribución salarial se han de disponer en los horizontes del personal con el propósito de lograr la fidelización corporativa. Asimismo, detectar los niveles de satisfacción del trabajador y sus motivos de descontento, y aplicar las medidas oportunas para subsanar la situación, se ha de contemplar como una tarea ineludible en el acompañamiento del personal.

Un perfil de estas características debe cimentarse objetivamente en el análisis de la posición a ocupar y en las metas de la organización. En su elaboración será aconsejable empezar por describir, con detalle, a través de un formato equilibrado, los requisitos del puesto; es decir, qué, cómo, por qué, dónde y cuándo se hace lo que es necesario en ese destino. De este modo se clarificarán los puntos de inflexión fundamentales, es decir, la misión u objetivo a desempeñar, las actividades que se han de desarrollar, las responsabilidades a asumir, las relaciones jerárquicas y funcionales a establecer y las condiciones de trabajo a enfrentar. Es recomendable, debido a los cambios susceptibles de ocurrir, que ese perfil se mantenga actualizado y vigente y que sea revisado al menos cada dos años. En conclusión, este plan de acción debería contener también un perfil de exigencias,

en el cual se haga constar el conjunto de características que debe tener un Guardia Civil en un puesto de trabajo donde desempeñe sus funciones con eficacia, eficiencia y seguridad.

En relación con el plan de acción en dirección de personas para impulsar el talento, se vislumbra la rentabilidad que obtendría la Guardia Civil con la estrategia del e*mployer branding*. El punto de partida de esta herramienta es la conocida como EVP, propuesta de valor del empleado. La EVP es un factor clave para optimizar el rendimiento del talento y debería estar vinculada con el perfil de exigencias explicado anteriormente. La misma da respuesta a dos preguntas tan básicas como recíprocas:

- Qué puede esperar el trabajador, ya sea integrante o candidato, de la empresa.
- Qué espera la empresa del trabajador, integrante o candidato.

La gestión del talento, como factor estratégico organizacional, en la Guardia Civil: posibles áreas de mejora en el proceso selectivo de la Guardia civil.

Se puede estimar que, si la mayoría de las actuaciones en el ámbito de la gestión de recursos humanos tienen como meta predecir quiénes, entre todas las candidaturas, tendrán un rendimiento más eficiente en sus puestos de trabajo, o qué acciones permitirán optimizar estos criterios, será preciso disponer de un sistema que asegure su efectividad. Esta es una de las razones fundamentales que ha llevado a aplicar un enfoque hacia las competencias. Según Boyatzis (1982), una competencia es «una característica subyacente en una persona, que está causalmente relacionada con un desempeño bueno o excelente en un puesto de trabajo concreto y en una organización determinada».

Al aplicar el enfoque de competencias se promueve un cambio sustancial respecto al planteamiento anterior, ya que se toma como premisa el estudio de la conducta de aquellas personas que realizan su trabajo con eficacia y, de este modo, el puesto se define en función de la misma. Mediante esta actuación, lo que conforma el perfil del puesto no es otra cosa que un conjunto de comportamientos que pueden ser observados directamente.

En la Guardia Civil, se puede concluir que la entrevista por competencias contribuye de modo valioso a los procesos selectivos de la institución, aportándoles manifiesta objetividad y criterios unánimes y convirtiéndola en un método de gran eficacia en la tarea de selección de personal, amén de reforzar la importancia de disponer de valoraciones uniformes en cuanto a las competencias de aquellos candidatos que aspiran a formar parte de la institución.

Por otro lado, la realización de pruebas psicotécnicas y la entrevista personal permiten, en primer lugar, llevar a cabo un cribado que favorezca la detección de aquellas personas que, ya en la fase de selección, presentan

disfunciones o rasgos de personalidad anómalos que puedan entorpecer su adaptación a la función policial y podrían causar desde la frustración personal hasta el absentismo laboral. Además, facultan a la institución para hacer una primera predicción sobre la adecuación y adaptación del candidato al puesto, tomando nota de conductas relevantes, partiendo de la tipología del sujeto y de cómo afrontó en ocasiones anteriores situaciones que pueden darse en el puesto de trabajo al que concurre. La evaluación de esos aspectos se lleva a cabo mediante la adaptación de las pruebas a cada proceso selectivo.

En la selección de personal para promoción interna se están aplicando, en exclusiva, entrevistas grupales previas a las individuales. Estas entrevistas en grupo, consistentes en pruebas situacionales, se han confirmado como herramientas útiles y precisas para la evaluación de competencias, pues durante su realización, los candidatos han de poner en práctica los conocimientos, destrezas y aptitudes necesarias para solucionar el problema o la situación concreta que se les plantea.

Las organizaciones han de hacerse, con un esquema capaz de integrar todos los sistemas subordinados a su método principal con las posturas estratégicas de sus procesos.

Es necesario operar con sistemas o métodos de evaluación del desempeño enlazados con el modelo gerencial por competencias y, estrechamente relacionados, con el ejercicio real del trabajador en su puesto, debido a que la actuación laboral observable formará parte de un flujo de aprendizaje dentro de la organización.

Tras todo lo indicado anteriormente, se exponen a continuación los siguientes extremos concluyentes relativos a las posibles áreas de mejora en el proceso selectivo de la Guardia Civil.

Durante el transcurso del presente trabajo se ha indicado que el *outsourcing* no es la mejor herramienta para proporcionar una ventaja en la gestión del talento como estrategia organizacional debido al carácter y naturaleza propia del Cuerpo. Sin embargo, tras analizar las ventajas del *employer branding* se podría determinar que es una herramienta útil y que aportaría el valor añadido que se pretende buscar en este trabajo de investigación.

Por tanto, para optimizar el rendimiento del talento y poder generar la atracción y fidelización de los integrantes de la Guardia Civil, actuales y potenciales, se propone el uso *del Internal branding* en la institución. Por consiguiente, los Guardias Civiles empleados internalizarían la imagen de marca deseada por el Cuerpo y externalizarían esa imagen a la sociedad.

Cabe destacar que, aprovechando los continuos e imparables avances en tecnología, la misma herramienta antes descrita podría ser empleada de forma más eficiente y eficaz, siendo el *employer branding digital* la mejor opción. Pues trata de incorporar las herramientas tecnológicas al proceso de atracción, selección y fidelización de los candidatos.

Ejecutando esta herramienta en la estrategia organizacional se conseguiría:

- Crear un sentimiento de pertenencia hacia la Guardia Civil por parte de los profesionales de la organización, no a nivel empresa.
- Fidelizar al talento sobre la base del plan de acción descrito en el capítulo anterior.
- Mejorar/mantener el compromiso con los integrantes del Cuerpo.
- Conseguir una buena reputación de la institución a nivel externo.

Queda constatado en la entrevista semiestructurada, basada en la selección por competencias, la manifiesta objetividad y criterios unánimes que aportan eficacia a la evaluación de las competencias de aquellos candidatos que aspiran a formar parte de la institución. Sin embargo, y en búsqueda de satisfacer las necesidades de los recursos humanos de la Guardia Civil, a la par que elegir a los candidatos más idóneos, ¿es esta opción la apropiada para la detección del talento?

Se considera que el proceso actual es correcto. Sin embargo, la posible adhesión del plan de acción en dirección de personas para impulsar el talento (identificación, captación, desarrollo y retención del personal) podría desembocar en un procedimiento de mayor eficiencia y eficacia, en cuanto a la gestión del talento. Asimismo, todo el proceso debe ir ligado a la conceptualización estratégica del personal en la Guardia Civil que se explica en el TFM.

3. Conclusiones

En las motivaciones del trabajo se contemplaba la necesidad de adaptación a los ambientes de incertidumbre actuales que desembocan en entornos laborales convulsos. También se postulaba acerca de la idoneidad de considerar la gestión del talento como un factor estratégico organizacional en la Guardia Civil para poder ofrecer un mejor servicio a la sociedad.

Se han podido identificar los criterios que sustentan el proceso selectivo de la Guardia Civil y se han aportado posibles áreas de mejora en el mismo. Concretamente, a raíz de analizar la viabilidad de las herramientas *employer branding* en la institución y su repercusión como ventaja competitiva.

Se ha materializado un análisis del entorno competitivo actual en relación con la identificación, captación, desarrollo y retención del talento en la Guardia Civil, aplicando el modelo de las cinco fuerzas de M. Porter. Asimismo, se ha detallado cómo se gestiona el talento como factor estratégico organizacional en la Guardia Civil.

De esta forma, se puede afirmar que el sector de la seguridad pública no es atractivo y que la inclusión de la Guardia Civil es latente con una cuota de mercado alta, lo cual la hace competitiva entre sus rivales. Para generar la diferenciación en cuanto a la adición de valor añadido se estipula, como un

área de mejora en el proceso selectivo y en su metodología de entrevista semiestructurada basada en la selección por competencias, la adhesión del plan de acción en dirección de personas para impulsar el talento podría desembocar en procedimiento de mayor eficiencia y eficacia en cuanto a la gestión del talento.

A lo anteriormente contemplado se debe añadir que, todo el proceso debe ir ligado a la conceptualización estratégica del talento en la Guardia Civil explicada en el presente trabajo. Asimismo, se debe recalcar, como factor clave, la motivación de los empleados, potenciando factores como el salario, la formación, la gestión de las expectativas y la frustración.

Se ha realizado un guion relativo a los factores fundamentales que debe recoger un plan de acción en dirección de personas. Este permite impulsar el talento dentro de la conceptualización estratégica del talento en la Guardia Civil, generando valor añadido a la institución.

También se han analizado las estrategias de mejora para la dirección de personas basada en el talento de la Guardia Civil, identificando las medidas de actuación susceptibles de ser aplicadas.

Del estudio del cambio de paradigma sucedido se puede aseverar que las mejores organizaciones son aquellas que valoran a sus empleados y el talento que aportan, aunque para que una organización llegue a ese punto ha de ir evolucionando, pasando previamente por un proceso de cambio y aprendizaje.

Mediante la apreciación de las transformaciones sociales, políticas, educativas y estructurales acontecidas a lo largo del tiempo en el entorno laboral, es posible distinguir cómo se han producido cambios notables en la división del trabajo. La gestión del talento humano implica, en la actualidad, mucho más que el reclutamiento del personal o la asignación de tareas. Involucra un conjunto integrado de procesos que busquen atraer, desarrollar, motivar y retener a los individuos y que den como resultado productos o servicios acordes a los estándares de calidad,cualificación y compromiso del personal con los objetivos institucionales.

La clave está en entender el talento como una cualidad que las personas atesoran y ponen en práctica para obtener excelentes resultados en entornos cambiantes y de incertidumbre a fin de alcanzar mejor rendimiento personal, de forma que este repercuta en una mayor eficiencia de la estructura a la que se vinculan, a la par que en un aumento de su eficacia empresarial u organizativa.

Como oficial de la Guardia Civil, se ha de recalcar la importancia de que la escala directiva encargada de la dirección de personas asuma el reto de atraer, identificar y mejorar las competencias correctas, el compromiso adecuado y la contribución que se detallaban en el concepto de talento en el capítulo segundo. Todo ello a fin de poder incrementar las capacidades de la persona y conseguir así una mayor productividad. Asimismo, se han

de construir capacidades organizativas (calidad, servicio al cliente, innovación, agilidad, etc.) que generen un todo (organización) frente a la suma de las partes (el talento de la persona), lo que dará como resultado final la totalidad del reto que se plantea en la gestión del talento.

4. Líneas futuras

En el presente trabajo, se contempla en el apartado relativo a la retención, que el plan de acción debería contener también un perfil de exigencias. Por consiguiente, se considera que una línea futura podría ser el análisis del perfil de estas características objetivas destinadas al análisis de la posición a ocupar y en las metas de la organización.

Se recalca, como se mencionó anteriormente en el presente trabajo, la necesidad de que el perfil de exigencias esté ligado a *la Guía Técnica de Buenas Prácticas en Reclutamiento y Selección de Personal* (R&S) del Colegio Oficial de Psicólogos de Madrid o algún documento de similar índole.

Asimismo, dicho perfil debería de describir con detalle, a través de un formato equilibrado:

- Los requisitos del puesto.
- La misión u objetivo a desempeñar.
- Las actividades que se han de desarrollar.
- Las responsabilidades por asumir.
- Las relaciones jerárquicas y funcionales a establecer.
- Las condiciones de trabajo a enfrentar.

Otra línea futura que se contempla pudiera ser el análisis de la EVP (Propuesta de Valor del Empleado*/ Employer Branding)* del Cuerpo en aras de establecer la oferta de valor que la Guardia Civil ofrece al profesional a cambio de su esfuerzo, rendimiento y compromiso.

En esta línea se deberían analizar los aspectos que la Guardia Civil quiere que se le asocien, estableciéndose las expectativas que se esperan del trabajador y las que el trabajador espera de la institución.

Referencias

Álvarez de Lara Galán, L. Responsable del Área Organizacional del Servicio de Psicología de la Guardia Civil.

Fernández-Lores, S. *et al.* (2014). 18 años de Employer Branding hacia una definición más precisa. *Revista Internacional de Investigación en comunicaciónaDResearch ESIC.*

Hartle, F. (1993). *Las competencias: clave para una gestión integrada de recursos humanos.* Madrid. Editorial Deusto.

Le Boterf, G. (2001). *Ingeniería de las competencias.* Barcelona, Gestión 2000.

Luna Arocas, R. (2018). *Gestión del talento. De los recursos humanos a la dirección de personas basadas en el talento (DPT).* Madrid, Pirámide.

Montes Adalid, G. M. (2020). Employer Branding digital y la atracción y retención del talento. Especial referencia al Plan de Igualdad. *Revista Internacional de Relaciones Laborales y Derecho del Empleo.*

Muñoz, G. A. D. y Lombeida, M. D. Q. (2021). *La gestión del talento humano y su influencia en la productividad de la organización.* Gestión Joven.

Rodríguez-Tarodo, A., Recuero Virto, N., y Blasco López, M. F. (2018). *Employer Branding: Atraer y comprometer el talento en 5 pasos.* Madrid, Pearson.

El Talento como factor estratégico organizacional en la Guardia Civil

Autor: Gabriel de la Coba Santana
Director: Francisco Javier Rodríguez Rodríguez

Introducción

Actualmente nos movemos, organizaciones y trabajadores, en un ambiente laboral convulso, en constante evolución y que trata de adaptarse al trabajador. La selección de personal no radica ya en la búsqueda del cumplimiento de un perfil determinado, sino en la captación de personas con talento que, además de cumplir con sus objetivos profesionales, puedan aportar valor añadido al resto de su entorno y a la empresa o institución. El talento se constituye como factor de atracción por parte de las organizaciones, pues se busca que los profesioanles puedan servirse de sus capacidades para la consecución de objetivos eficaces dentro de la estructura corporativa.

Metodología

Para el ámbito de investigación propuesto se ha empleado una metodología cualitativa. Se recurrió a fuentes primarias, como estudios estadísticos, análisis, libros, fuentes documentales, etc., pero sin dejar de lado las secundarias, como artículos, entrevistas o nociones colaterales.

Estrategia organizacional propuesta

La clave está en entender el talento como una cualidad que las personas atesoran y ponen en práctica para obtener excelentes resultados en entornos cambiantes y de incertidumbre a fin de alcanzar mejor rendimiento personal, de forma que este repercuta en una mayor eficiencia de la estructura a la que se vinculan, a la par que en un aumento de su eficacia empresarial u organizativa.

.

Posibles áreas de mejora en la Guardia Civil

Tras analizar las ventajas del *employer branding* se podría determinar que es una herramienta útil y que aportaría el valor añadido que se pretende buscar en este trabajo de investigación. Por tanto, para optimizar el rendimiento del talento y poder generar la atracción y fidelización de los integrantes de la Guardia Civil, actuales y potenciales, se propone el uso *del Internal branding* en la Institución. Por consiguiente, los Guardias Civiles empleados internalizarían la imagen de marca deseada por el Cuerpo y externalizarían esa imagen a la sociedad. Asimismo, y con el empleo de las nuevas tecnologías, el e*mployer Branding digital* permitiría:

- Crear un sentimiento de pertenencia hacia la Guardia Civil por parte de los profesionales de la organización.
- Fidelizar al talento en base al plan de acción descrito en el capítulo anterior.
- Mejorar/mantener el compromiso con los integrantes del Cuerpo.
- Conseguir una buena reputación de la Institución a nivel externo

Conclusiones

La entrevista semiestructurada actual, basada en la selección por competencias, la manifiesta objetividad y criterios unánimes que aportan eficacia a la evaluación de las competencias de aquellos candidatos que aspiran a formar parte de la institución se considera adecuado. Sin embargo, la posible adhesión del plan de acción en dirección de personas para impulsar el talento (identificación, captación, desarrollo y retención del personal) podría desembocar en un procedimiento de mayor eficiencia y eficacia en cuanto a la gestión del talento. Asimismo, todo el proceso debe ir ligado a la conceptualización estratégica del talento en la Guardia Civil.

Diseño y securización de un *rack* desplegable en zona de operaciones

Autor: Daniel Costa Fortea (dcosfort@ea.mde.es)
Directores: Fernando Suárez Lorenzo (presidente@cpeig.gal) y Norberto Fernández García (norberto@cud.uvigo.es)

Resumen – Debido a la inestabilidad política que ha tenido lugar en Europa en los últimos años, la OTAN se ha visto obligada a desplegar múltiples equipos de seguridad y observación en el continente.

Para que dichos equipos puedan cumplir la misión encomendada, se necesita disponer de una serie de servicios como son, Directorio Activo, impresión, aplicaciones, ficheros, DNS, DHCP, antivirus y correo, así como conexión a internet y telefonía IP, a través de satélite, aunque estos dos últimos no son objetivo de este proyecto. La jefatura CIS, responsable de los despliegues españoles en la OTAN, ha determinado lo siguiente: para el correcto desempeño de la misión en zona de operaciones, una comisión de seguridad necesita disponer de todos estos servicios mediante satélite, para veinte usuarios, en el momento inicial del despliegue, y para un máximo de cuarenta, *a posteriori* si el destacamento lo solicita. El presente trabajo trata de desarrollar un planeamiento previo de forma generalizada de los requisitos, arquitectura y montaje necesarios para ofrecer la conectividad requerida en los diferentes destacamentos.

Como resultado, permitirá que, en futuros despliegues, solo se necesite la realización de modificaciones de pequeña índole, acorde con las especificaciones particulares de cada nuevo destacamento. En definitiva, con la estandarización plasmada por escrito de los requisitos, arquitectura y montaje de un módulo desplegable con la acreditación del Centro Criptológico Nacional, la velocidad de despliegue de las redes de comunicaciones necesarias en los destacamentos se incrementa en gran medida. Además, también mejora la calidad del servicio prestado, debido a las ventajas que proporciona la uniformidad de la totalidad de redes telemáticas a desplegar en el futuro.

Palabras clave – Conectividad, Virtualización, Estandarización, Escalabilidad.

1. Introducción

Este trabajo de fin de máster tiene como objetivo fundamental el poder profundizar en el diseño y securización de la arquitectura de un módulo desplegable acreditable por el Centro Criptológico Nacional (CCN). Es así como este documento se caracteriza por ser más argumentativo y conceptual que práctico, aunque también involucra, como elemento nuevo en el marco referencial, la acreditación de seguridad.

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

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

2. Justificación

La relevancia del presente trabajo se puede justificar atendiendo a la trascendencia que tienen las misiones de la OTAN en el continente europeo. Esto hace que dar una serie de servicios básicos a los usuarios finales en un tiempo mínimo, así como ofrecer conectividad a internet y telefonía IP en zona de operaciones, sea una de las prioridades fundamentales en cualquier despliegue que se realice dentro del marco de la OTAN, siendo indispensable para el correcto desempeño de la misión encomendada a cada destacamento.

3. Objetivo

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

4. Desarrollo

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

Dentro del ámbito CIS/TIC la respuesta ante cualquier salida al exterior debe ser inmediata, dando una serie de servicios en el mínimo tiempo

posible. Esto motiva la necesidad de que el personal esté formado en su especialidad y tenga un documento por escrito en donde seguir las instrucciones básicas a la hora de realizar el primer montaje en cualquier parte del mundo con un número de personal bajo para poder hacer un primer reconocimiento *in situ*. Posteriormente, aumentaríamos los servicios según las necesidades de la misión encomendada, así como el aumento de *hardware* y *software,* ajustándolo al número de usuarios.

5. Resultados y discusión

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

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

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

6. Conclusiones

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

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

Seguidamente, se especifican algunas variables abiertas:

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

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

Referencias

CCN-STIC-530. Seguridad en Microsoft Office 2010.

CCN-STIC-550. Microsoft Exchange Server 2010 en Windows Server 2008 R2.

CCN-STIC-590. Recolección y Consolidación de Eventos con Windows Server 2012 R2.

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

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

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

DISEÑO Y SECURIZACIÓN DE UN RACK DESPLEGABLE EN ZONA DE OPERACIONES

Autor: DANIEL COSTA FORTEA
Universidad de Vigo
Director/es: FERNANDO SUÁREZ LORENZO y NORBERTO FERNÁNDEZ GARCÍA

Introducción

El presente trabajo trata de desarrollar un planeamiento previo de de los requisitos, arquitectura y montaje necesarios para el diseño y securización de un rack despalegable. Como resultado, permitirá que en futuros despliegues, sólo se necesite la realización de modificaciones de pequeña índole, acorde con las especificaciones particulares de cada nuevo destacamento.

Resultados

Metodología

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

1.Recopilación y estudio de la bibliografía básica necesaria para la realización del proyecto.

2.Diseño lógico de la arquitectura.

3.Implementación física de todos los componentes hardware, según lo determinado en el diseño lógico.

4.Instalación, configuración, securización y validación de los elementos que componen el módulo desplegable.

5.Elaboración de la memoria correspondiente justificando la realización del trabajo, detallando sus diferentes fases, proponiendo posibles mejoras e incluyendo las conclusiones obtenidas del trabajo realizado.

Conclusiones

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

Implementación de un servicio de atención al usuario en la Armada bajo el marco normativo del Ministerio de Defensa

Autor: Fernando Guinea Rodríguez (fguinrod@fn.mde.es)
Directores: Miguel Ángel Ares Tarrío (externo.miguelares@cud.uvigo.es) y Norberto Fernández García (norberto@cud.uvigo.es)

Resumen – Las Fuerzas Armadas tienen como misión principal la defensa de la soberanía nacional. Uno de los pilares fundamentales para alcanzar este objetivo son las Tecnologías de la Información y las Comunicaciones (TIC). Una buena gestión de los servicios TIC permite a los miembros de las Fuerzas Armadas centrarse en su misión principal y no en los medios o procedimientos para alcanzarla.

En este Trabajo de Fin de Máster (TFM) se mostrará el estado actual de la gestión de servicios en la que se encuentra el Ministerio de Defensa, su evolución y alcance y se identificará la ausencia de un servicio de atención al usuario como tal.

En el desarrollo del trabajo se expondrá, de manera lo más resumida posible, la actual normativa en vigor, incluyendo la estructura TIC desde el Ministerio de Defensa hasta la Armada, y la implementación de la gestión de servicios en las FAS, usando como base la normativa del Ministerio de Defensa, así como los estándares y metodologías que pueden ser de utilidad.

En la parte final del trabajo se realizará una propuesta realista de implementación de un servicio de atención al usuario en la Armada, bajo el marco de gestión normativo del Ministerio de Defensa. Esta abarcará los recursos humanos, procesos y tecnologías con el objetivo de alcanzar los tres pilares de un servicio TIC.

Este TFM se centra en los servicios de baja clasificación y, más concretamente, en los de uso oficial.

Palabras clave – ITIL, Atención al usuario, Servicio, Normativa, Armada.

1. Introducción

Tras tres años trabajando en un puesto donde se proporcionan servicios TIC en la Armada, resulta evidente que nos hemos quedado muy por detrás de las nuevas tendencias y metodologías. Seguimos trabajando como hace diez años.

El principal objetivo de este trabajo es entregar valor al cliente, pero esto en la Armada resulta difícil, ya que no somos una empresa en la que la entrega de valor es fácilmente cuantificable de manera económica. La única forma de dar valor al cliente es con algo más valioso que el dinero, con tiempo. Si un militar pierde un día en resolver su incidencia y está pendiente de ella, es tiempo que no se ha podido dedicar a su principal misión.

Para entregar ese valor a los miembros de la Armada debe haber una estructura, unos procedimientos y la tecnología que permita esa entrega de valor. Actualmente se hace, pero con una normativa y estructura que no están en consonancia con las nuevas tecnologías ni con el estado del arte.

En los últimos años se han sufrido muchos cambios en empresas y organizaciones debido a la imperatividad de satisfacer las necesidades de sus clientes, pero no por la satisfacción de la empresa de tener al cliente contento. La evolución de las empresas se puede resumir en dos frases: «el cliente siempre tiene la razón» y «la información es poder», pero con un cambio: «el cliente tiene la información» y «la información es dinero». Las empresas quieren cuantos más clientes satisfechos para conseguir su información y por ende dinero. Pero esta motivación es difícil de trasladar al mundo militar, lo que nos mueve es la eficacia y la eficiencia, véase alcanzar nuestros objetivos y lograrlos de la manera más rápida.

Por otro lado, la Armada no es un ámbito independiente con autonomía para decidir las líneas de actuación. El Ministerio de Defensa es el encargado de dar un marco normativo a todas las acciones que toman el Ejército de Tierra, la Armada o el Ejército del Aire y en el caso de las TIC no iba a ser menos. En mayo del 2022 se firmó el Pliego de Prescripciones Técnicas (PPT) que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D) [1]. En marzo de 2023 se realizó la formalización del mismo por un periodo de tres años.

Se considera que la Armada tiene la necesidad apoyar y aportar valor al usuario acorde con el despliegue geográfico, pero todo ello bajo el marco normativo del Ministerio de Defensa.

Gestión de servicio en el Ministerio de Defensa

El Centro Corporativo de Explotación y Apoyo (CCEA) [2] tiene la misión de asumir la dirección de la gestión y explotación de los sistemas de información, de la plataforma informática y de las telecomunicaciones del

Ministerio de Defensa. Dentro de sus cometidos generales está dar servicio de Atención al Usuario (SAU).

Para alcanzar su cometido define un organigrama, así como el Sistema de Control de Acuerdos de Nivel de Servicio (SCANS-DEF) como herramienta informática con la finalidad de dar cobertura funcional a la gestión del presupuesto y control del gasto en telefonía, gestión de incidencias y gestión de peticiones.

Como vemos en la figura 1 el usuario debe contactar con el CISPOC para crear una incidencia, no siendo este autónomo para la creación, seguimiento o cierre de la incidencia.

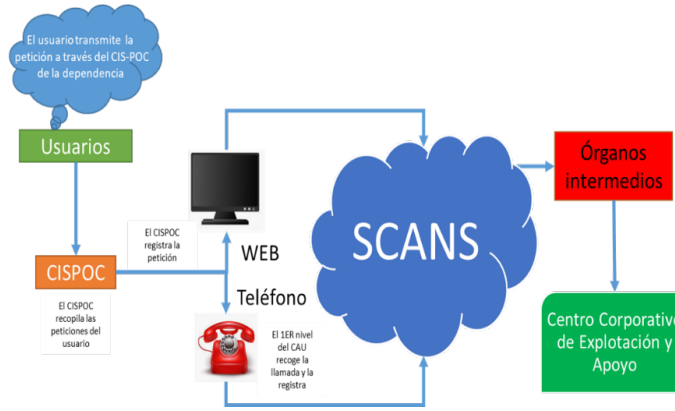


Figura 1. Proceso de peticiones CIS-POC al CCEA. *Fuente:* propia

Gestión de servicio de la Armada

Como hemos visto en el punto anterior, es necesario que en los diferentes Ejércitos haya una estructura que apoye al CCEA. La Armada define en el ACP-121 [3] una estructura que, no siendo *ad hoc* para satisfacer las necesidades del CCEA, sí que la apoya de manera eficaz. En dicha publicación [3] se definen los Centro de Explotación CIS (CECIS) distribuidos geográficamente según la Imagen 2:

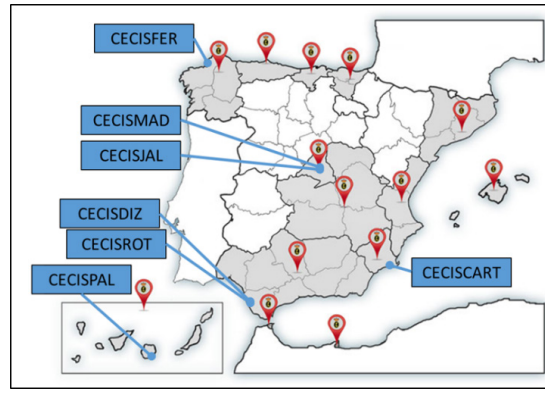
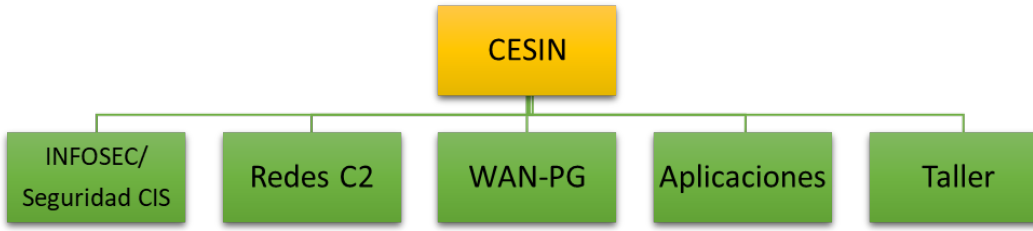


Figura 2. Distribución geográfica CECIS. *Fuente:* propia

Dentro de estos CECIS se define el Centro de Sistemas de Información (CESIN) que, según la referencia [3], además de otro cometido que no es tema de esta memoria, debe colaborar con las diferentes divisiones del CESTIC y con el MCCE, para mantener los niveles de servicio de los sistemas CIS del Ministerio de Defensa. Definiendo el organigrama 1 para alcanzar este cometido:



Organigrama 1. CESIN. *Fuente:* propia

En este punto nos centraremos en el CESIN de Ferrol (CESINFER), ya que ese centro cuenta con toda la casuística que hay en la Armada, véase, buques, unidades de tierra, cuartele, etc. Se definió una aplicación GESCAI (desarrollada con Métrica V3) para facilitar, entre otras, la interacción con los usuarios. Pero esta aplicación no solucionó el problema de gestión de las incidencias. Por decirlo así, GESCAI servía al CISPOC para gestionar las incidencias internamente, informando al usuario de la apertura y cierre de la incidencia. Este cierre de incidencia se producía sin el *feedback* del usuario afectado.

2. Desarrollo

En mayo de 2022 se firmó el Pliego de Prescripciones Técnicas que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D) (PPT I3D) [1] donde se definen los servicios a los que pueden acceder todos los miembros de las Fuerzas Armadas. Dentro de este PPT I3D se definen los siguientes lotes:

- Lote 1: servicios e infraestructuras de datos, telefonía y localización de la I3D del MINISDEF.
- Lote 2: servicios e infraestructuras de comunicaciones móviles de la I3D del MINISDEF.
- Lote 3: servicios e infraestructuras de comunicaciones satelitales civiles de la I3D del MINISDEF.
- Lote 4: servicios e infraestructuras de acceso a internet de la I3D del MINISDEF.
- Lote 5: servicios e infraestructuras de telemedicina de la I3D del MINISDEF.

- Lote 6: servicios e infraestructuras de soporte y atención a usuarios de la I3D del MINISDEF.
- Lote 7: servicios e infraestructuras de videoconferencia segura de la I3D del MINISDEF.
- Lote 8: apoyo técnico y logístico a los servicios e infraestructuras de la I3D del MINISDEF.

De todo ellos, y centrándonos en el Lote 6, vemos que el objeto es la prestación de los servicios de Soporte y Atención al Usuario TIC (CAU y SCANS). Este lote consiste en la implantación de un Centro de Atención a Usuarios del MINISDEF (CAU) y el mantenimiento y desarrollo del Sistema de Control de Acuerdo de Nivel de Servicio del MINISDEF (SCANS). En el PPT se menciona que se deben seguir las buenas prácticas ITIL, pero si nos vamos a las referencias que proporciona el PPT I3D vemos que usa Instrucciones Técnicas y Normas de 2006 y 2007 para el Servicio de Atención al Usuario y para la gestión de incidencias peticiones y avisos del CAU. Es por esto que se considera que, durante los próximos tres años, duración de la adjudicación del PPT, no habrá cambios en la metodología de trabajo.

Se plantea la necesidad de actualizar la metodología de trabajo en la Armada, orientándola hacia ITIL, ya que esta es la base de los servicios I3D. Este cambio no afectaría a la relación entre los CECIS y el CCEA, Debido a que, como hemos visto en el párrafo anterior, la tendencia es a modernizar SCANS, pero no cambiar la metodología, véase, el usuario no va a poder interactuar con el sistema y, por tanto, no podrá gestionar sus incidencias/peticiones. Sin embargo, se contempla que a nivel Armada sí que se puede hacer un cambio, no solo en la aplicación, sino también en la metodología hacia ITIL.

ITIL

En lo que a la metodología se refiere está definida por el Ministerio de DEFENSA (MDEF): esta es ITIL. Hoy en día la última versión de ITIL es ITIL 4, pero consideramos que ITIL V3, versión anterior, se adapta mejor a las necesidades del CECIS. El motivo por el que se ha elegido ITIL V3 en lugar de ITIL 4 es porque en la versión 4 las prácticas se focalizan en la realización de la tarea, independientemente del modo de llegar a ella y, sobre todo, sin una secuencia de acciones predefinidas, y esto no se alinea con el pensamiento militar. Por el contrario, ITIL V3 sí que se adapta a las necesidades, ya que para una entrada busca una salida o, lo que es lo mismo, busca un conjunto estructurado de actividades diseñadas, con una cierta secuencialidad, para conseguir un objetivo específico y esto se consigue con los procesos en ITIL V3.

GLPI

En el mercado existen numerosas aplicaciones ITSM (*Information Technology Service Management*) que puede satisfacer las necesidades

de la Armada y estar alineadas con la metodología ITIL. Para poder elegir la aplicación correcta es necesario cumplir lo definido por la normativa en vigor [4] que define que:

> «Los sistemas de información del Ministerio de Defensa tendrán en cuenta, con carácter preferente, las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados. Al efecto deberán consultarse, entre otros, directorios de aplicaciones reutilizables el CTT - Centro de Transferencia de Tecnología [5], con carácter previo, a la adquisición, al desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación informática».

Con estas premisas, teniendo cuenta la metodología ITIL, y tras buscar en el CTT, se identifica al GLPI, y a su agente (GLPI *Agent)*, como la ITSM que se adapta a las necesidades de la Armada.

3. Implantación

De los servicios definidos por ITIL nos vamos a centrar en la operación del servicio, ya que los restantes servicios; estrategia, diseño, transición y mejora continua; están definidos en la normativa en vigor del Ministerio de Defensa.

La operación del servicio se encarga de realizar todas las tareas operacionales que se vayan presentando y asegurar que los servicios de TI se ofrezcan efectiva y eficientemente. Esto incluye cumplir con los requerimientos de los usuarios, resolver fallos en el servicio, arreglar problemas y llevar a cabo operaciones rutinarias.

En el TFM se definen cada uno de los procesos y subprocesos necesarios en este servicio, así como su implementación, utilizando los procedimientos, organigramas y personal ya existente en los CESIN de la Armada.

4. Resultados y discusión

Tras conseguir la autorización del CESTIC para el uso de GLPI en la red de propósito general del Ministerio de Defensa la implantación inicial se realizó en el Centro de Sistemas de Información de la Jefatura de Apoyo Logístico de la Armada (CECISJAL) y el Centro de Sistemas de Información de Ferrol (CECISFER), en mayo del 2022, extendiendo su uso al resto de CECIS de la Armada, el 4 de julio de 2022. Hoy en día están implementados en la Armada los módulos de gestión de peticiones (eventos e incidentes) y gestión de activos. En la Ilustración 4 se puede ver el *dashboard* de GLPI donde se muestran los usuarios registrados (24,9 K), los activos (*hardware* y *software*) y desde donde se pueden extraer los KPI definidos en la memoria.

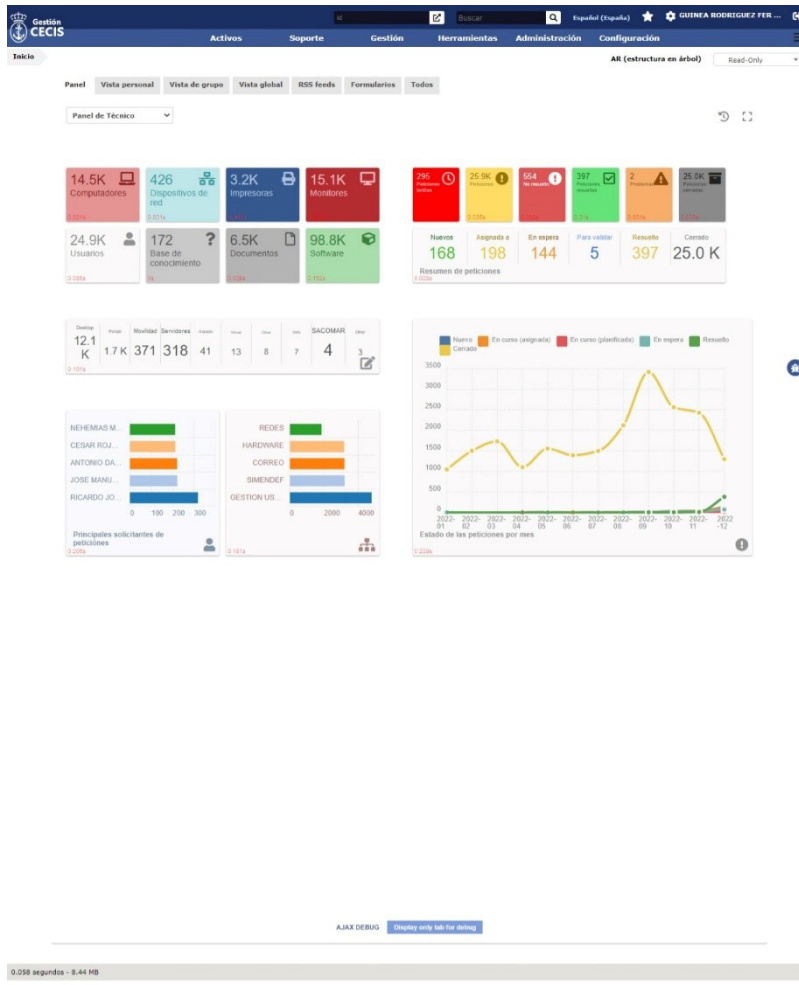


Figura 3. Dashboard GLPI. *Fuente:* propia

5. Conclusiones

Es necesario implementar en la Armada un servicio de atención al usuario, ya que actualmente los medios que proporciona, así como los que está previsto que proporcione, el Ministerio de Defensa no llegan al elemento más importante: el usuario, como dice ITIL [6]:

> «Independientemente de cómo se gestionan los servicios, procesos y la tecnología, todo está relacionado con las personas. Son las personas las que impulsan la demanda de los servicios de la organización y sus productos y son las personas las que deciden cómo se harán las cosas. En última instancia, son las personas las que gestionan la tecnología, procesos y servicios. El no reconocer esto resultará (y ha resultado) en el fallo de la gestión del servicio».

Ya se han definido las líneas futuras que guiarán la Política TIC del MINISDEF, así como los medios que nos permitirán alcanzarlas. Estas líneas futuras incluyen nuevos procedimientos para proporcionar nuevos servicios que están a disposición de los usuarios. Estos nuevos procedimientos convivirán con los anteriores, pero esto no es un impedimento, ya que gracias a la metodología ITIL esta transición debe ser natural.

En la memoria se ha propuesto una solución que actualmente está en funcionamiento en la Armada, el GLPI, con un coste tanto económico como humano razonable.

Lo más importante, el recurso humano que hay detrás del usuario: sin un técnico que resuelva las incidencias, lo anteriormente definido no tendría ningún sentido. El personal destinado en los CECIS de Apoyo de la Armada tiene la capacidad para satisfacer las necesidades mínimas de un SAU-AR.

Como conclusión, el GLPI es la solución que satisface las necesidades expuestas y se alinea con la normativa del Ministerio de Defensa,, permitiendo a la Armada dar un salto de calidad y ofrecer valor al usuario.

Referencias

Armada. (2020). Sección CIS de la Secretaría General del Estado Mayor de la Armada, Organización de las Comunicaciones Navales, Madrid.

España. (2002). Instrucción n.º 236/2002, de 7 de noviembre, del secretario de Estado de Defensa por la que se crea el Centro Corporativo de Explotación y Apoyo para los Sistemas de Información y Telecomunicaciones del Ministerio de Defensa. *BOD* 222, Ministerio de Defensa, p. 11312.

España. (2017). Instruccion Tecnic 01/07 sobre Arquitectura Técnica Unificada del Ministerio de Defensa. Madrid.

Gobierno de España. (s. f.). Gestión de Inventario Informático basado en OCS/GLPI. *Portal de la administración electrónica* [en línea]. Ministerio de Asuntos Económicos y Transformación Digital. Secretaría General de Administración Digital, «GLPI-CTT». Disponible en: https://administracionelectronica.gob.es/ctt/inventarioseap#.Y6aton3MLt4. [Consulta: 15 de noviembre de 2022].

Ministerio de Defensa. (2022). *Pliego de Prescripciones Técnicas que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la infraestructura integral de información para la defensa (I3D)*. Madrid.

TSO:The Stationery Office, ITIL Service Operation, Norwich: TSO Ireland. (2011), p. 4.

Implementación de un servicio de atención al usuario en la Armada bajo el marco normativo del Ministerio de Defensa

Autor: Fernando, Guinea Rodriguez
Directores: Miguel Ares Tarrío y Norberto Fernández García

Introducción

Las Fuerzas Armadas tienen como misión principal la defensa de la soberanía nacional. Uno de los pilares fundamentales para alcanzar este objetivo son las Tecnologías de las Información y las Comunicaciones (TIC). Una buena gestión de los servicio TIC permite a los miembros de las Fuerzas Armadas centrarse en su misión principal y no en los medios o procedimientos para alcanzarla.

En este Trabajo Fin de Máster (TFM) mostraré el estado actual de la Gestión de Servicios en la que se encuentra el Ministerio de Defensa, su evolución y su alcance e identificaré la ausencia de un servicio de atención al usuario como tal.

Metodología

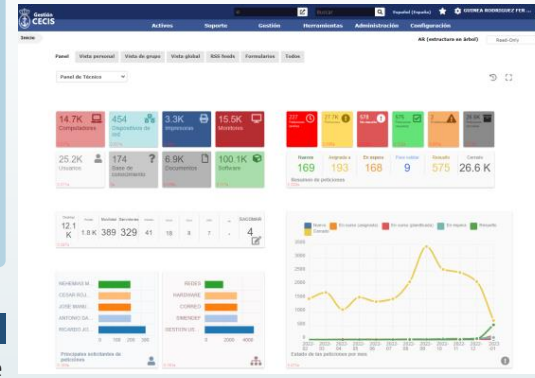
Se empleó un enfoque basado en el Pliego de Prescripciones Técnicas (PPT) que ha de regir el establecimiento de un acuerdo marco para la contratación de servicios e infraestructuras de telecomunicaciones de la Infraestructura Integral de Información para la defensa (I3D). En este PPT se define la metodología ITIL como marco para la definición de los servicios usando como base la organización actual.

Tras definir ITIL (*Information Technology Infraestructure Library*) , metodologías ágiles y herramientas ITSM *(Information Technology Service Managemet*) que hay en el mercado se eligen para la implementación de un servicio de atención al usuario en la Armada (SAU-AR) las siguientes:

- ITIL V3
- GLPI (*Gestionnaire Libre de Parc Informatique*)
- SCRUM
- KANBAN

Resultados

En mayo del 2022 se realiza la implantación inicial del GLPI en CECISJAL y CECISFER extendiendo su uso al resto de CECIS de la Armada el 4 de julio de 2023. A día de hoy están implementados en la Armada los módulos de gestión de peticiones (Eventos e Incidentes) y gestión de activos.



En esta imagen podemos ver, una vez implementado, el cuadro de mandos de GLPI. En él se diferencian dos áreas, la izquierda representa los activos en la red, mientras que la derecha muestra las peticiones de los usuarios. En la parte inferior se representan gráficas generales.

Mediante las herramientas nativas se pueden obtener estadísticas personalizadas para obtener, p.ej., los KPI (Key Performance Indicators).

Conclusiones

El GLPI es la solución que satisface las necesidades expuestas. Se alinea no solo con la metodología ITIL sino también con las instrucciones definidas por el Ministerio de Defensa, permitiendo a la Armada dar un salto al futuro, o mejor dicho al presente, en la atención al usuario.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Sistema de gestión integral de una flota de vehículos operativos

Autor: Rafael Martínez Mesones (rmesones@guardiacivil.es)
Director: Norberto Fernández García (norberto@cud.uvigo.es)

Resumen – Las unidades operativas sustentan gran parte de su trabajo en la flota de vehículos que tienen asignados para la realización de las labores que les son encomendadas.

Los medios de transporte se categorizan y se clasifican en relación con sus características: tipo de vehículo, cilindrada, kilómetros recorridos, antigüedad, color, etc., estableciéndose varias categorías donde ubicarlos.

Se necesita registrar y documentar todos los datos que generan estos vehículos durante su vida útil, como pueden ser: kilómetros recorridos mensualmente, reparaciones, revisiones mecánicas, accidentes, sustituciones de piezas, inspecciones ITV, seguros, etc., información que puede ser explotada con procesos de minería de datos con el objetivo de predecir fechas de mantenimientos, recambios e inspecciones.

El problema se plantea a la hora de realizar una adjudicación de los elementos de transporte a los distintos departamentos que componen una unidad operativa de una forma equilibrada y equitativa, sin que nadie se sienta perjudicado o desfavorecido en comparación al resto de grupos o departamentos.

El principal objetivo del presente trabajo es el diseño de una herramienta informática con la que administrar y gestionar este parque móvil, sus reparaciones, repostajes, accidentes, etc., que será fundamental para llevar un perfecto control de todos los elementos de transporte existentes.

Dada la importancia de esta herramienta, el sistema se sustenta en una arquitectura que puede escalar horizontalmente, con relación al número de usuarios y peticiones de proceso, realizando un despliegue en contenedores Docker y utilizando el orquestador Kubernetes para gestionar toda la plataforma.

Palabras clave – PHP, Docker, Kubernetes, Vehículos.

1. Introducción

Descripción

La gestión de una flota de vehículos comprende la administración y organización de todos los elementos de transporte asignados a una unidad. Con la ayuda de la informática, podemos controlar los vehículos de una flota con la finalidad de realizar un control holístico de la misma, al tiempo que pueda aumentarse la seguridad de los conductores y se reduzcan los riesgos de accidentes o siniestros con motivo de su utilización. Se pretenden aumentar la eficiencia y productividad, optimizando el estado del funcionamiento de los vehículos.

El primer objetivo de este trabajo es diseñar un sistema integral, basado en tecnologías de virtualización y contenerización, en el que se puedan ejecutar las aplicaciones informáticas de gestión de la flota de vehículos en contenedores que puedan escalar en función de la concurrencia de usuarios, de la ejecución de procesos de automatización, etc. Analizaremos las distintas herramientas de contenerización disponibles y nos centraremos en la instalación y configuración de una infraestructura basada en contenedores Docker [1] y en su orquestación mediante Kubernetes [2].

El segundo objetivo del proyecto es diseñar, así como desarrollar el embrión de una aplicación web, que se ejecute en el entorno virtualizado, programado en el lenguaje PHP [3], que cuenta con un *back-end* de base de datos, basado en MariaDB [4] y, cuya finalidad, sea la gestión integral de una flota de vehículos en una unidad.

Motivación

Las unidades soportan, en su día a día, una alta carga de trabajo en la gestión de su material y, sobre todo, en la administración, gobierno y registro de trámites que deben efectuar con la flota de vehículos que tienen asignados.

Si bien hoy en día la utilización de dispositivos informáticos, con los que procesar y almacenar la información, se ha convertido en una herramienta básica y con la que trabajan la mayor parte de las unidades, diversos procedimientos y actividades, que pueden ser calificadas como rutinarias, se realizan repetidamente y penalizan el rendimiento y producción del departamento encargado de llevar a cabo estas gestiones.

Se pretende obtener un beneficio en la productividad de la unidad, reduciendo procedimientos pautados y repetitivos, ofreciendo un entorno centralizado donde poder gobernar la flota de vehículos, con información en tiempo real y actualizada.

Uno de los hitos fundamentales del sistema lo compone el desarrollo de un módulo inteligente de adjudicación de los medios de transporte a los distintos departamentos y grupos que componen la unidad, de forma que

el reparto sea equitativo, neutral e íntegro, de acuerdo con unos parámetros configurables y definidos de antemano.

2. Desarrollo

Toda la infraestructura informática que compone este proyecto se sustenta en un conjunto de máquinas virtuales, con sistema operativo Linux, que se ejecutan en una plataforma *hardware* compuesta de dos procesadores Intel® Xeon® ES-2630 v3 @ 2.40 GHz, de ocho cores cada uno, con 32 GB de memoria RAM, un adaptador *Ethernet* con dos puertos RJ45 de 1 GB y dos HDs de 1 TB de capacidad en RAID 1.

El conjunto de VM está divido en dos grupos:

- Una VM de control, desde la que componer, ejecutar y procesar los playbooks de Ansible [5] para su despliegue en el resto de la infraestructura.
- Tres VM que componen el cluster básico de Kubernetes.

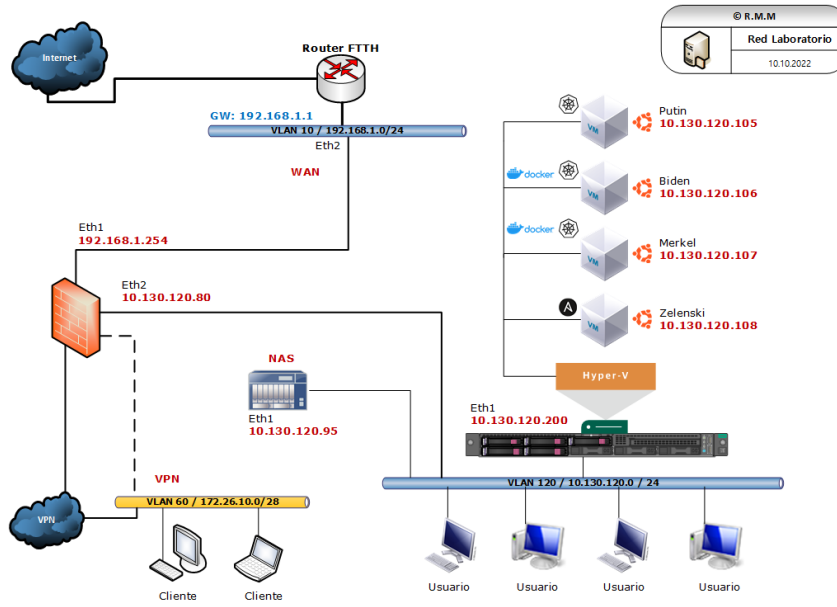


Figura 1. Esquema de conectividad e infraestructura. *Fuente:* propia

Todas estas VM, así como su plataforma base, están conectadas a una red *Ethernet* interna que se ha creado para este proyecto y que podemos observar en la figura 1.

En cuanto al almacenamiento, dado que está previsto que todos los sistemas accedan a un repositorio común en red, dispondremos de un NAS (*Network Attached Storage*), desde el que se exportará un volumen NFS (*Network File System*) al resto de componentes de la plataforma.

Utilizando los *playbooks* de Ansible, se realiza el despliegue y configuración de la infraestructura descrita en la figura 1, encargada de sustentar y ejecutar los distintos contenedores y el orquestador que administra todo el sistema.

Una vez se han instalado los servidores virtuales, se realiza la creación del *cluster* con Kubernetes y se configuran varios PV (*Persistent Volume*) y sus correspondientes PVC (*Persistent Volume Claim*), para que los contenedores de la aplicación utilicen un repositorio común, donde almacenar los ficheros e información compartida por todos ellos.

Como se ha comentado en el primer apartado, el segundo objetivo del presente trabajo es el diseño de una aplicación para la gestión integral de una flota de vehículos, basada en un modelo de tres capas (MVC), utilizando el lenguaje de programación PHP, servidor web Nginx y base de datos MariaDB (LEMP). En la figura 2 podemos observar las distintas entidades que forman parte de sistema.

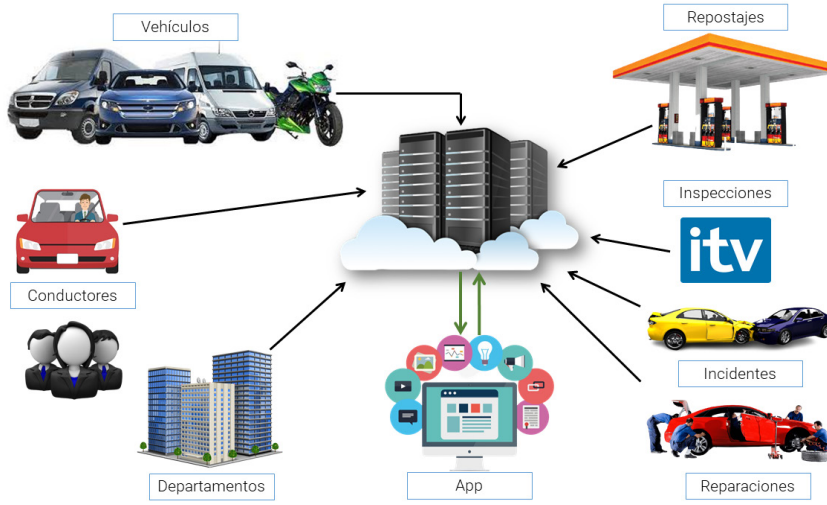


Figura 2. Entidades cuya información procesa el sistema. *Fuente:* propia

Mediante la utilización de varios ficheros en formato YAML, desplegamos toda la infraestructura de contenedores descritos anteriormente para ejecutar y dar soporte a la aplicación desarrollada.

3. Resultados y discusión

Empezamos realizando el despliegue de todos los contenedores que conforman el sistema con sus configuraciones particularizadas. Una vez completados estos pasos, se efectúa la configuración de las redes de comunicación entre los contenedores y entre estos y los clientes finales. Se comprueba la estabilidad del *cluster* y su operatividad.

En la figura 3 podemos comprobar la información asociada al servicio que se ha configurado para los contenedores Nginx, donde se muestra la información de direccionamiento IP (externo e interno), así como la redirección de puertos hacia el servicio web desplegado.

```
root@putin:~/resources# kubectl get svc -o wide
NAME            TYPE           CLUSTER-IP      EXTERNAL-IP      PORT(S)          AGE     SELECTOR
kubernetes      ClusterIP      10.96.0.1       <none>           443/TCP          15d     <none>
nginx-service   LoadBalancer   10.102.235.67   10.130.120.105   80:30858/TCP     2m20s   app=nginx
root@putin:~/resources# kubectl describe svc nginx-service
Name:                     nginx-service
Namespace:                default
Labels:                   app=nginx
Annotations:              <none>
Selector:                 app=nginx
Type:                     LoadBalancer
IP Family Policy:         SingleStack
IP Families:              IPv4
IP:                       10.102.235.67
IPs:                      10.102.235.67
External IPs:             10.130.120.105
Port:                     80-80  80/TCP
TargetPort:               80/TCP
NodePort:                 80-80  30858/TCP
Endpoints:                10.244.1.4:80,10.244.1.5:80,10.244.2.5:80
Session Affinity:         None
External Traffic Policy:  Cluster
Events:                   <none>
```

Figura 3. Servicio de red del contenedor Nginx. *Fuente:* elaboración propia

Se diseñan y especifican los requisitos, tanto funcionales como no funcionales, que debe contemplar la aplicación, se realiza un gráfico de actores y especificaciones de los casos de uso y, finalmente, se construye un modelo lógico de base de datos relacional, con las tablas, claves y relaciones entre todas ellas.

También se ha diseñado y proyectado un procedimiento gráfico con el que programar uno de los objetivos del trabajo, la adjudicación automática de vehículos a los distintos grupos de la unidad, como puede observarse en la figura 4.

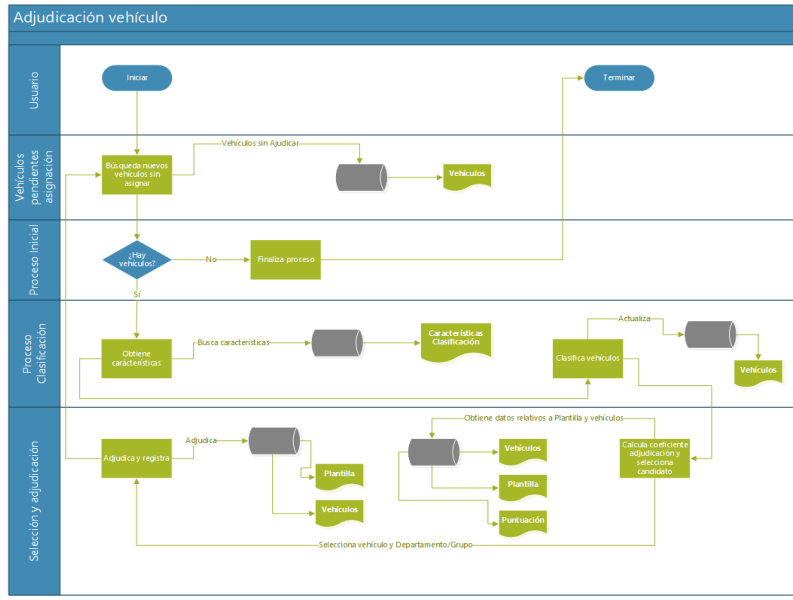


Figura 4. Procedimiento de adjudicación automática de vehículos. *Fuente:* elaboración propia

Con todos estos elementos definidos comentados anteriormente, se ha llevado a cabo la programación del núcleo de la aplicación, que cuenta con los siguientes componentes:

- Módulo de autenticación y validación de usuarios.
- Módulo de auditoría: registro de trazas de actividad realizadas por los usuarios.
- Alta, modificación, baja y consulta de vehículos registrados.
- Listado de vehículos por categorías o grupos asignados.
- Clasificación de nuevos vehículos dados de alta en el sistema.
- Adjudicación automática de vehículos a los grupos.

Se ha realizado una simulación, con diecisiete vehículos, que han sido clasificados en las tres categorías definidas en el sistema de forma automática y, posteriormente, se han adjudicado con el procedimiento programado en la aplicación, comprobando que ambos sistemas realizan su función tal y como se habían definido en el apartado de diseño.

4. Conclusiones

El primer objetivo planteado en este trabajo se ha completado diseñando, configurando e instalando un entorno de contenedores Docker, gestionados por Kubernetes. Apoyados en una herramienta de configuración para múltiples sistemas mediante la ejecución de *scripts* de Ansible, denominados *playbooks,* se ha desplegado una infraestructura *dockerizada*, compuesta por tres nodos, con la que se configuran los distintos elementos que albergan el sistema.

Con respecto al segundo objetivo expuesto en el proyecto, se ha acometido el diseño de los componentes que forman la aplicación de gestión, definiendo los objetivos que se pretenden alcanzar, estableciendo los requisitos funcionales y no funcionales que debe contemplar el sistema, diseñando el gráfico de actores y casos de uso global del sistema y finalizando con la documentación de los casos de uso especificados en el proyecto. Finalmente, se han programado y validado los procedimientos de clasificación y adjudicación de vehículos, con los que se pretende agilizar, automatizar y optimizar el trabajo que desarrollan los equipos de apoyo logístico en dichas tareas.

Por todo ello, podemos constatar que los objetivos que se han planteado al inicio de este trabajo se han alcanzado. Convendría finalizar la implementación de la aplicación, añadiendo los módulos y elementos que se consideran necesarios para completar su funcionalidad.

Referencias

Ansible. [en línea] [Consulta: 6 de noviembre de 2022] Disponible en: https://www.ansible.com

Docker Inc. [en línea] [Consulta: 11 de octubre de 2022] Disponible en: https://www.docker.com/

Kubernetes. [en línea] [Consulta: 24 de octubre de 2022] Disponible en: https://kubernetes.io/docs/concepts/overview/

MariaDB Foundation. [en línea] [Consulta: 1 de noviembre de 2022] Disponible en: https://mariadb.org/es/

PHP - Hypertext Preprocessor. [en línea] [Consulta: 1 de noviembre de 2022] Disponible en: https://www.php.net/manual/es/intro-whatis.php

Sistema de gestión integral de una flota de vehículos operativos

Autor: Rafael Martínez Mesones

Director: Norberto Fernández García

Universidad de Vigo

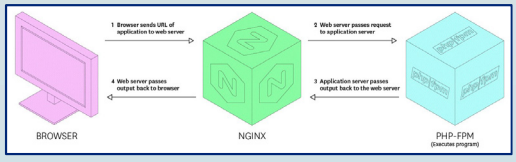
Introducción

La gestión de una flota de vehículos comprende la administración y organización de todos los elementos de transporte asignados a una Unidad/Organismo. Con la ayuda de la informática, podemos controlar los vehículos de una flota con la finalidad de realizar un control holístico de la misma, al mismo tiempo que pueda aumentarse la seguridad de los conductores y se reduzcan los riesgos de accidentes o siniestros con motivo de su utilización. Con este sistema se pretenden aumentar la eficiencia y la productividad, al tiempo que se mejora la seguridad de los conductores y se optimiza el estado del funcionamiento de los vehículos de la Unidad.

Metodología

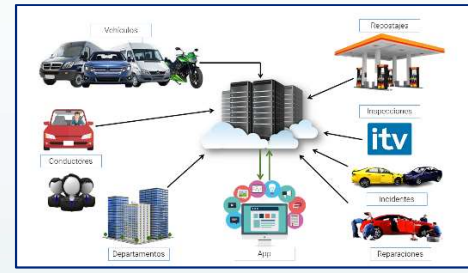
Para llevar a cabo el proyecto, se han utilizando los siguientes elementos:

- **Docker**. Contenedor de mayor utilización en la comunidad, de fácil despliegue y ejecución.
- **Kubernetes**. Herramienta de orquestación para administrar la infraestructura desplegada.
- **Ansible**. Software de automatización de tareas para llevar a cabo la implementación contínua.
- **Bootstrap**. Framework intuitivo y fácil de utilizar, con el que se han diseñado las páginas y elementos de la aplicación.
- **PHP**. Lenguaje abierto, portable, estándar, cuyo desarrollo puede procesarse en cualquier sistema operativo.
- **Nginx** y **PHP-FPM**. Servidor Web e intérprete de código PHP con los que mostrar y procesar páginas con código PHP.
- **MariaDB**. Base de datos relacional donde almacenar la información de la aplicación.



Resultados

Se ha diseñado, instalado, configurado y desplegado un entorno, basado en contenedores Docker y orquestado con Kubernetes, para llevar a cabo la gestión de la flota de vehículos de la Unidad.

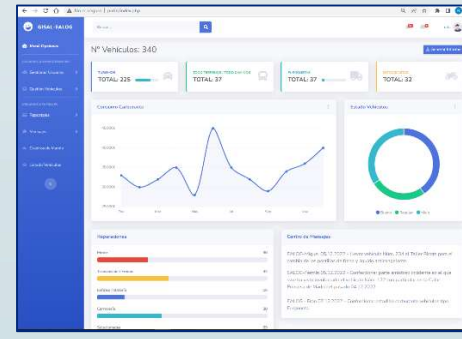


Conclusiones

El primer objetivo planteado en este trabajo se ha completado diseñando, configurando e instalando un entorno de contenedores Docker, gestionados por Kubernetes, apoyándonos en una herramienta de configuración para múltiples sistemas como es Ansible.

Con respecto al segundo objetivo, se ha diseñado la aplicación de gestión integral, se han definidos las vinculaciones entre todos los objetos que la componen y, finalmente, se han programado los dos procedimientos más importantes como son:

- Clasificación automática de vehículos
- Adjudicación a los distintos Grupos de la Unidad



Sistema de ciberinteligencia en apoyo a los procesos de decisión en la Armada: concepto y metodología

Autor: Juan Pablo Mesa Fernández (jmesfer@fn.mde.es)
Director: Francisco Javier Rodríguez Rodríguez (jjavierrodriguez@cud.uvigo.es)

Resumen – En los últimos años, la aparición de los asuntos del ciberespacio habría obligado a los ejércitos y otras organizaciones a adaptarse a un nuevo entorno operativo aún más complejo e incierto para lograr sus objetivos. Entender sus retos y oportunidades es un aspecto clave para la correcta toma de decisiones.

Las capacidades de ciberdefensa en la Armada están en continua adaptación y crecimiento para responder a esta situación. Sin embargo, en este trabajo se ha identificado la necesidad de cerrar un vacío en el ámbito de la inteligencia, desde la argumentación de que un sistema de mando y control robusto nace desde la mejor comprensión del entorno, incluyendo su componente de ciberespacio, por lo que necesita un sistema de ciberinteligencia propio que se la proporcione.

Si bien el nivel estratégico y operacional habrían reaccionado a esta circunstancia, en los niveles de conducción táctico y en las estructuras orgánicas de los ejércitos y de la Armada no habría permeado aún la importancia e influencia de la ciberintegencia; obviando así riesgos, retos, oportunidades y amenazas, comprometiendo con esta situación la propia misión. Este es el caso de la escasa integración de los asuntos del ciberespacio en el planeamiento y conducción de operaciones navales; o, desde un punto de vista orgánico, el sesgo que se produce en los procesos de adquisición de capacidades con tecnologías disruptivas como el *Big Data*, la inteligencia artificial o 5G, que en la búsqueda de la superioridad de la información, podría olvidar la seguridad por diseño al no contar con estructuras especializadas que planteen los riesgos asociados al ciberentorno.

En este contexto, el presente TFM propone la generación de una nueva capacidad militar que integre el entendimiento de lo ciber en los procesos de decisión de la Armada, tanto en su actividad orgánica como en la operativa. Se definen, así, los conceptos de empleo,

organización, formación, relación con otros entes y también la metodología de apoyo a la decisión, explicada a través de un caso práctico.

Palabras clave – Ciberinteligencia, Ciberespacio, Ciberdefensa, Entorno marítimo, Ciberamenazas, Inteligencia, Mando y Control, Decisión.

1. Introducción

Motivación y planteamiento del problema

Este trabajo pretende subrayar la necesidad de generar un sistema de cibertinteligencia como capacidad imprescindible para la toma de decisiones, proponiendo un modelo para la estructura de la Armada. Es un aspecto en el que la comunidad militar aún no ha delimitado siquiera su propia definición, alcance, procesos o responsabilidades.

El problema radica en que, a pesar de que en los últimos años el ciberespacio se haya erigido en un nuevo entorno de actuación, los ejércitos estarían aún en proceso de adaptación y no poseerían la capacidad ni la cultura operacional de considerar adecuadamente la influencia del ciberentorno sobre su actividad.

La situación actual reside en que el conocimiento de lo que ocurre, o bien se obvia, o bien se trata con medios y disciplinas tradicionales que no responden a los retos actuales. En el mejor de los casos, el estudio del ciberespacio se gestiona con capacidades retenidas a muy alto nivel de conducción, a menudo duplicando esfuerzos y sin una clara línea de responsabilidad entre las partes que tienen interés. Como consecuencia, el sistema actual es poco eficiente y ágil para responder a los retos a los que se enfrenta el decisor de la Armada.

Objetivos

El objetivo principal del presente trabajo reside en presentar una propuesta de capacidad de ciberinteligencia en la estructura de la Armada que le permita mejorar sus procesos de decisión para hacer frente a los retos y oportunidades del entorno cibermarítimo.

Para ello, se analiza cómo la irrupción de los asuntos del ciberespacio influye en la actividad y misiones de la Armada y condiciona el ejercicio del mando, siendo necesario integrar un sistema de ciberinteligencia para mejorar el proceso de decisión. Confirmando la hipótesis anterior, se define a continuación un concepto de empleo del sistema de ciberinteligencia de la Armada y se esboza la composición de la unidad que proporcionaría tal capacidad, estableciendo sus funciones, cometidos, relaciones y beneficios. Para finalizar, se realiza una descripción de algunos procesos de mando y control en los que la ciberinteligencia podría aportar valor.

2. Desarrollo

La Armada y el entorno cibermarítimo

La irrupción del ciberespacio no cambia la filosofía de mando y control, si bien introduce nuevos retos que obligan a los ejércitos a adaptar sus estructuras y procedimientos [1]. El entorno marítimo no es ajeno a tales cambios y sus condicionantes repercuten en la actividad de la Armada,

afectando todo el rango de operaciones navales: desde la seguridad y el conocimiento del entorno marítimo, a la disuasión o el enfrentamiento armado con un adversario híbrido o convencional [2] [3].

En este contexto, la capacidad de ciberinteligencia se identifica como clave en los procesos de decisión. La famosa niebla de la guerra se hace aún mayor con la inclusión de este nuevo dominio, idóneo para un adversario de estrategia híbrida o de zona gris que pretenda explotar nuestra dependencia de los sistemas CIS/TIC. No entender o identificar estas dinámicas significa ceder el terreno clave del ciberespacio, tan necesario para el empleo de sistemas TI/TO o la propia toma de decisiones.

Los decisores de la Armada no pueden ni deben renunciar a un sistema de inteligencia completo y propio. Este sistema, necesariamente, debe contemplar la perspectiva ciber para identificar no solo adversarios, capacidades o sus intenciones, sino también las oportunidades que este dominio puede ofrecer. La responsabilidad de dibujar el umbral del riesgo es del decisor, que poco podrá hacer si no posee la capacidad que lo vislumbre.

La estructura actual de la Armada no proporciona la mencionada capacidad. Su nuevo concepto de empleo de ciberdefensa [4] implícitamente asume el riesgo desde la argumentación de que el nivel táctico o la estructura de los ejércitos no son el nivel apropiado para introducir las capacidades de ciberinteligencia, pues ya se llevan a cabo en el MCCE y CIFAS. Sin embargo, un sistema propio mejora los principios de inteligencia sin repercutir en el control centralizado en el nivel superior. Una capacidad propia en la Armada cierra el círculo, engranando los mecanismos de decisión de nivel táctico y mejorando la capacidad de respuesta al situarse en una posición de privilegio entre el decisor marítimo y la relación funcional con estructuras de nivel superior, como MCCE y CIFAS.

Definición, alcance y concepto de empleo de la capacidad de ciberinteligencia en la Armada

Este capítulo se centra en proponer un concepto y metodología de un sistema de ciberinteigencia propio que posibilite afrontar los retos del entorno donde la Armada desarrolla su actividad. Está basado en las mismas prácticas, principios doctrinales y filosofías de mando y control e inteligencia, haciéndolos extensivos al estudio del ciberespacio [5-8].

A falta de una definición consensuada de ciberinteligencia, a los efectos de este trabajo se definiría como aquella capacidad militar que, con un enfoque en el ciberespacio y que, de manera continuada y coordinada con el ciclo de inteligencia, contribuye al entendimiento del entorno cibermarítimo, aportando a la mejora de los procesos de decisión, el óptimos empleo de capacidades navales y/o el mantenimiento de la libertad de acción en el ciberespacio asociado.

Así, la capacidad inicial de ciberinteligencia se visualiza organizativamente en el Grupo de Ciberdefensa de la Armada (GRUCIBER) y con relación funcional con el sistema de inteligencia. Es un modelo centralizado y desplegable, como estrategia más eficiente a corto y medio plazo, ante la dificultad de formar un equipo de analistas especializados en el campo de la ciberdefensa, inteligencia y operaciones navales.

El beneficio se identifica en tres diferentes dimensiones de toma de decisión:

- Dimensión táctico-técnica, con la generación de Inteligencia de Ciberamenazas (CTI) en apoyo a la ciberdefensa de los sistemas que la Armada tiene asignados en su zona de responsabilidad. Su fortaleza reside en la federación de fuentes de inteligencia y la automatización de la seguridad y defensa de redes y sistemas (Security Orchestration, Automation and Response, SOAR).
- Dimensión de las operaciones navales, mediante la integración en los procesos de planeamiento y conducción de las operaciones. Este ámbito, por ser el más demandante y razón de ser de la Armada, ha sido el elegido para profundizar en la metodología de integración de ciberinteligencia mediante un caso de estudio. La actualización del Cyber Situational Awareness (CySA), el Cyber Intelligence Preparation of the Operational Environment (CyIPOE), Análisis de CoG para Targeting e Influencia, valoración de las operaciones... son algunas metodologías presentadas.
- Dimensión estratégica, proporcionando apoyo de inteligencia estratégica al SIFAS y asesoramiento a la alta dirección en sus procesos de trabajo relacionados la actividad orgánica de la Armada. En este sentido, es especialmente interesante el beneficio de contar con un equipo de analistas de ciberinteligencia para la adquisición de nuevas tecnologías emergentes y disruptivas (5G, inteligencia artificial, etc.) y conseguir que la Armada, en plena transformación digital, obtenga superioridad tecnológica y de la información bajo el principio de seguridad por diseño.

Figura 1. Ciclo de ciberinteligencia y su contribución al nivel de decisión.
Fuente: elaboración propia

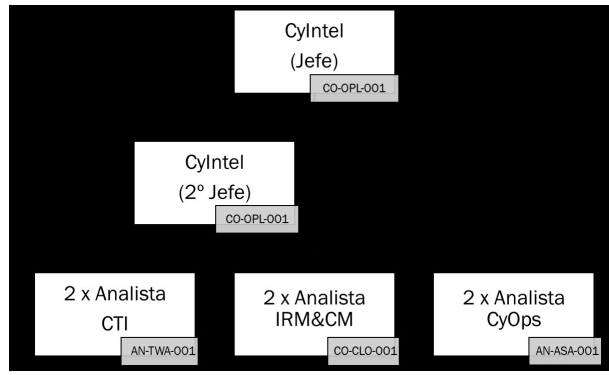


Figura 2. Propuesta de organización de unidad de ciberinteligencia de la Armada.
Fuente: elaboración propia a partir de [9]

El sistema de ciberinteligencia se ha diseñado en torno a un núcleo inicial compuesto por ocho miembros con una formación multidisciplinar. Sus perfiles profesionales se han diseñado a partir de competencias que incluyen desde las tradicionales técnicas de inteligencia y planeamiento de operaciones e influencia, hasta conocimientos técnicos de operaciones de ciberdefensa, análisis de sistemas e ingeniería inversa. Para configurar

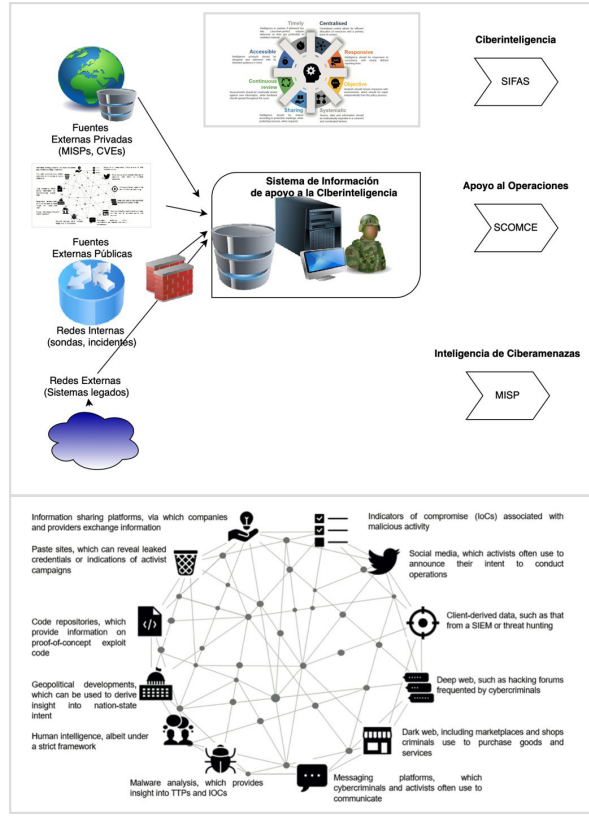


Figura 3. Sistema de Información en Apoyo a la Ciberinteligencia de la Armada (SIaCI).
Fuente: elaboración propia

el perfil profesional de cada puesto de trabajo se ha recurrido a un marco del *National Initiative for Cybersecurity Education* (NICE) [9], elaborando una detallada descripción de sus funciones, destrezas, conocimientos y habilidades.

La capacidad diseñada contempla el empleo de un sistema de información de apoyo a la Ciberinteligencia (SIaCI) que, basado en una filosofía de transformación digital, explota de manera sistemática las fuentes de interés y la información de los sistemas legados a los que está federado, facilitando las actividades del ciclo de ciberinteligencia de una manera particularizada para cada nivel de decisión.

3. Conclusiones

El desarrollo del trabajo abordado permite considerar que se han alcanzado y demostrado los objetivos planteados para este TFM, cuya argumentación se resume en los siguientes puntos:

- La irrupción del ciberespacio no cambia la filosofía de mando y control, si bien introduce nuevos retos que obligan a los ejércitos a adaptar sus estructuras y procedimientos. En la Armada, esa adaptación se identifica en la conveniencia de establecer una estructura orientada a extender la actividad de la inteligencia hasta el campo de la ciberdefensa, y viceversa, solapando dos ámbitos que aún no han establecido relación conjunta.
- La constitución e integración de un sistema de ciberinteligencia en la estructura de la Armada mejora sus procesos de decisión. La clave del éxito se identifica en la capacidad de entendimiento, enlace y aprovechamiento de las capacidades ciber y de inteligencia, residentes en niveles superiores, y su orientación a las necesidades del decisor para satisfacer las exigencias de su sistema de decisión con los condicionantes que incorpora el ciberespacio. Esta capacidad inicialmente se origina a través de la constitución de una unidad de ciberinteligencia con carácter centralizado, aunque desplegable, y formación multidisciplinar.

El segundo pilar de éxito se ha identificado en el sistema de información en el que se apoya. Se ha presentado la arquitectura de referencia del SIaCI como *hub* generador de apoyo a los procesos de decisión en cada dimensión mediante una metodología de integración de ciberinteligencia.

Agradecimientos

A mis compañeros de máster, por hacer de esta etapa una experiencia fantástica que me ha permitido conocer a grandes profesionales y mejores personas.

Referencias

Concepto de Empleo de Ciberdefensa de la Armada. (2022).

Departamento de Seguridad Nacional. (2021). *Gobierno de España, Estrategia de Seguridad Nacional 2021* [En línea]. [Consulta: octubre 2022]. Disponible en: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

EMAD. (2018). Doctrina para el empleo de las Fuerzas Armadas. PDC-01(a).

—. (2021). Doctrina de Operaciones en el Ámbito Ciberespacial. PDC 3-20.

Jefe de Estado Mayor de la Defensa. (2018). *Concepto de empleo de Ciberdefensa*.

Jordán, J. (2022). Una oscura 'zona gris' [En línea]. *Global Strategy.* [Consulta: octubre 2022]. Disponible en: https://global-strategy.org/una-oscura-zona-gris/

OTAN. (2020). AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security. NATO Standardization Agency.

Petersen, R. *et al.* (2020). Workforce Framework for Cybersecurity (NICE Framework) [En línea], *NIST.* [Consulta: noviembre 2022]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

U.S. Marine Corps. (1997). *MCDP 1 Warfighting*. Department of the Navy, Headquarters United States Marine Corps.

Sistema de ciberinteligencia en apoyo a los procesos de decisión en la Armada: concepto y metodología

Autor: Juan Pablo Mesa Fernández
Director: Javier Rodríguez Rodríguez

El problema

La irrupción del ciberespacio no cambia la naturaleza del conflicto pero lo hace aun más complejo e impredecible. Comprender sus retos y oportunidades es clave para el éxito de las operaciones navales.

El entorno ciber influye en las actividad y las misiones de la Armada. Nuestra dependencia a las TI y TO, favorecen al adversario con estrategia híbrida y de zona gris, poniendo en riesgo el empleo de las capacidades navales y el ejercicio del mando y control.

Un sistema de inteligencia está íntimamente ligado a la efectividad del proceso de decisión. Satisface las necesidades críticas de información de cada nivel de mando con la agilidad y la particularidad que requiere cada nivel del mando al que sirven.

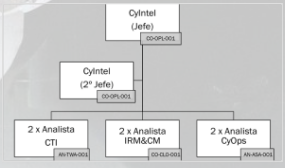
Las capacidades actuales están retenidas en un nivel mando que hace poco ágil el ciclo de ciberinteligencia en apoyo al decisor de la Armada. El *Concepto de Empleo de Ciberdefensa de la Armada 2022* no consigue solucionarlo.

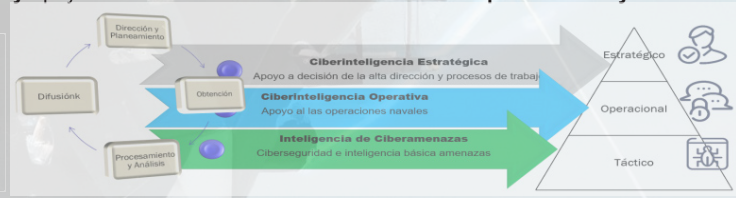
Hipótesis

La Armada debe constituir su propio sistema de ciberinteligencia para adaptarse a los requerimientos del entorno cibermarítimo actual, entendiendo riesgos y oportunidades y mejorando, así sus procesos de decisión.

Concepto

Se presenta un **sistema de ciberinteligencia** (personas-sistemas-procedimientos) **centralizado** en Ciber - Armada y relación funcional con el sistema de inteligencia. Es un concepto de unidad **desplegable y multidisciplinar**, compuesto de expertos en **operaciones, inteligencia y ciberdefensa** para apoyar hasta **a tres ámbitos de decisión y** apoyado en **sistemas de información de múltiples fuentes y federado** a los de nivel superior.





Metodologías, aplicaciones y beneficios

Mantenimiento de la *Cyber Situational Awareness* (CySA) y ciberinteligencia básica
Joint Preparation of the Opercional Cyber environment (CyIPOE)
Análisis de centro de gravedad y vulnerabilidades críticas de sistemas propios y adversarios
Elaboración de líneas de acción del ciberadversario (SITTEMP)
Apoyo al proceso *Targeting* con elaboración de línea de acción propia (Mecanismo de derrota)
Evaluación de la efectividad de las operaciones

"If you need a new idea, read an old book" (Proverbio popular)

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Amenazas de seguridad en redes de almacenamiento *fibre channel*

Autor: David Molina Vives (dmolvi1@fn.mde.es)
Director: Francisco Troncoso Pastoriza (ftroncoso@cud.uvigo.es)

Resumen – En este estudio, se aborda la situación en la que se instalan y explotan las redes de almacenamiento (SAN), usando uno de los protocolos más comunes, *fibre channel*. Estas redes son las que se utilizan para almacenar y procesar, cuando se requiera, el bien más importante de la organización: sus datos. Sin estos, la organización no puede desarrollar su actividad, lo que puede causar un grave perjuicio económico e incluso legal.

Cuando esta clase de redes empezó a surgir, la seguridad no era un aspecto crítico como sí lo es ahora. Además, a finales de los años ochenta, internet no era tan popular como en la actualidad. Ambos factores han provocado situaciones de vulnerabilidad en el diseño de las redes, que un atacante puede aprovechar en su beneficio.

Se verá lo sencillo que resulta obtener información de la red de almacenamiento, muy útil para encontrar puntos débiles. Así, el ataque podrá efectuarse con mayores posibilidades de éxito. Para ello, se ha utilizado una librería desarrollada por el mismo organismo encargado de la estandarización de los protocolos de *fibre channel*. A continuación, se expondrán algunas técnicas que podrían realizarse para burlar las pocas defensas que pudiera tener la red.

De esta manera, el atacante tiene la posibilidad de explotar las vulnerabilidades de los equipos que estén conectados a una red TCP/IP, y mover información entre ellos a través de *fibre channel*.

Por último, se tratará la cuestión de proporcionar una protección adecuada a la información, desde el momento en el que esta se encuentra almacenada en soportes de almacenamiento.

Palabras clave – Almacenamiento, Información, Redes, *Fibre channel*, Seguridad.

1. Introducción

Una red de almacenamiento *fibre channel* puede adoptar tres topologías distintas: punto a punto, bucle arbitrado (*arbitrated loop*) y malla conmutada (*switched fabric*). Estas dos últimas se pueden mezclar, formando una topología híbrida.

La más habitual es la de malla conmutada, o simplemente malla. Como mínimo, tiene que estar formada por un conmutador al que se conectan los distintos dispositivos que vayan a consumir o proporcionar recursos de almacenamiento (servidores, cabinas de discos, librerías de cintas, etc.).

Además de por los dispositivos y conmutadores, una malla requiere una serie de servicios para poder funcionar de manera correcta. Estos servicios se ejecutan en todos los conmutadores que forman parte de la malla, replicando la información necesaria entre todos ellos.

Uno de los más importantes, es el llamado «Servidor de Nombres», que almacena en una base de datos propia, una serie de información que posibilita la comunicación entre los distintos dispositivos conectados a la malla.

Estos dispositivos pueden ser muy heterogéneos y soportar distintas clases de servicio o protocolos de nivel superior. Antes de establecer la comunicación con uno de ellos, cada elemento solicita información a este servicio para saber cuál es la mejor forma para interactuar con el destinatario.

En las redes *fibre channel*, existe un mecanismo conocido como *zonning*, con el que un administrador de la red puede establecer qué dispositivos son accesibles por los que se defina. Así se evita que «todos hablen con todos».

2. Análisis de seguridad

Diseño de redes de almacenamiento

La seguridad debe ser tenida en cuenta desde el mismo momento en el que se inicia el diseño de cualquier proyecto, ya que luego puede resultar muy complicado o imposible corregir los problemas de seguridad que se puedan detectar una vez finalizado el montaje. Como muestra, se exponen dos situaciones donde pueden surgir problemas.

Elección correcta de la topología *fibre channel* a utilizar

Los primeros requisitos que una red de almacenamiento debe cumplir son los de la funcionalidad que la organización requiere para su buen funcionamiento. Es frecuente que una vez alcanzados estos, la seguridad se descuide.

Puede ocurrir que, a nivel físico, una red de almacenamiento parezca estar usando una topología, pero luego estar funcionando con otra distinta.

A modo de ejemplo, citar que existen cabinas de discos que pueden funcionar en cualquiera de las topologías descritas en el apartado anterior (punto a punto, bucle arbitrado o malla conmutada). Es el caso de la cabina de discos expuesta anteriormente, que por defecto viene configurada para funcionar como parte de una topología de bucle arbitrado.

Al usar la topología por defecto y conectar los servidores directamente a ella, todo parece funcionar de forma correcta y como el diseñador estableció en su diseño previo. Sin embargo, las tramas que los distintos componentes de la red de almacenamiento se envían entre sí, no fluyen como estaba previsto inicialmente en una topología punto a punto.

La diferencia entre una forma de trabajar y otra, tiene consecuencias en el aspecto de la seguridad y rendimiento. Por una parte, al viajar el tráfico en bucle, conlleva que todo el tráfico que un dispositivo envía deberá circular por el bucle hasta llegar al destinatario. Y una vez procesado, este deberá mandar la respuesta correspondiente, recorriendo el resto del bucle necesario hasta llegar al emisor inicial. Esto implica que todos los nodos del bucle verán una parte del tráfico, que no deberían. Esta situación no se produce en caso de una topología punto a punto. Además, el rendimiento de esta red no será óptimo porque utiliza el medio de transmisión directamente entre la cabina y sus clientes.

Uso de *fibre channel* en DMZ (zona desmilitarizada)

La tecnología de virtualización ha permitido que muchas organizaciones puedan requerir inversiones de menor importe para implementar los servicios necesarios en su propia infraestructura, incluyendo la parte dedicada a la prestación de servicios a sus clientes.

Desde hace unos años, internet y el comercio electrónico, han generado una gran cantidad de oportunidades, que muchas empresas han querido aprovechar. Esta situación, junto con la aparición de virtualización, ha llevado las redes de almacenamiento hasta la zona desmilitarizada de las redes de las organizaciones, sin tener en cuenta los problemas de seguridad que ello puede comportar.

No es imposible que un atacante pueda tomar el control de un equipo que se encuentre formando parte de una DMZ, incluso logrando efectuar una escalada de privilegios. Al lograrlo, se le ha abierto la puerta a la información que reside en ese equipo, así como a la que pueda almacenarse en la red de almacenamiento de la que forma parte.

Se puede llegar al extremo de que la red de almacenamiento se utilice para ofrecer recursos tanto a los equipos situados en la parte interna de la red, como a aquellos que forman parte de la DMZ. Muchas veces sin que ese tráfico pueda ser examinado por un cortafuego que pueda verificar el tráfico entrante y/o saliente para interrumpir aquel que no esté debidamente autorizado.

Este atajo permite que un atacante pueda aprovechar la red de almacenamiento en su beneficio, esquivando los cortafuegos de los que disponga la organización, que no podrán comprobar tráfico que no los atraviesa.

Ataque a la red de almacenamiento

Cada vez que un atacante debe enfrentarse a una red que desconoce, debe recopilar previamente toda la información que pueda, antes de iniciar el ataque. De esta forma, podrá efectuarlo con rapidez, reduciendo la probabilidad de ser descubierto y no poder alcanzar los objetivos que tenga establecidos.

— Fase de obtención de información de la red.

En las redes de almacenamiento *fibre channel*, puede realizarse esta fase de forma muy rápida y sencilla, a causa de la propia forma de funcionar de este tipo de redes. No es necesario recurrir a herramientas especializadas para ello.

Una de las alternativas que se proponen, es el uso de librerías como HBAAPI, que fue desarrollada por el organismo encargado de la estandarización de las propias redes *fibre channel*, INCITS. Además, el API que ofrece, sirve para varias plataformas, como Windows, Solaris, AIX, etc.

Su uso es tan sencillo, que en poco tiempo ha sido posible realizar dos pruebas de concepto para valorar las posibilidades que proporciona. Se han llamado hbainfo, y notify. La primera muestra por la pantalla toda la información que le resulta posible sobre la(s) tarjeta(s) HBA disponibles en el equipo. Además de los datos de la propia tarjeta, también presenta información de los puertos de la misma, así como de aquellos otros que hayan podido ser descubiertos por haberse realizado intercambio de algún tipo de información entre ellos. La segunda, registra una serie de funciones para que se invoquen cada vez que se produzcan ciertos tipos de eventos en la malla, de forma que el atacante puede saber cuándo se conectan o desconectan otros dispositivos.

El aspecto más delicado de esta librería es el que permite interactuar con los servicios de la malla, lo que podría permitir que un atacante modificara la configuración de seguridad de la red a su antojo y conveniencia.

Otras opciones incluyen la herramienta fcinfo, de Microsoft para sistemas operativos de la familia Windows. Con ella, es posible averiguar todos los dispositivos que se encuentran conectados al mismo conmutador al que está vinculado el equipo donde se ejecuta esta utilidad.

En ambos casos, el escaso tamaño de los ejecutables dificulta su detección cuando el atacante las intenta copiar al servidor vulnerado.

— Fase de ataque

Cuando el atacante ya ha decidido los pasos a realizar, puede usar alguna de las técnicas que se detallan a continuación para intentar obtener acceso a la información deseada:

- Debilidad de secuencias. Es un ataque que utiliza el mismo concepto que su correspondiente en redes TCP/IP, el ataque de predicción de secuencia. En este último, un tercero puede mandar tráfico al equipo víctima, haciendo creer que ese tráfico es legítimo y proviene del emisor. Para lograrlo, el atacante debe acertar con los valores adecuados de dirección origen y destino, puerto origen y destino, así como número de secuencia esperado. Los primeros cuatro valores se pueden obtener de las cabeceras de los paquetes y segmentos correspondientes. En cuanto al número de secuencia, debe adivinar el valor que espera recibir el receptor o víctima para que lo dé por bueno. Si lo logra, el tráfico generado será procesado adecuadamente. El atacante también deberá impedir que el emisor real, sea capaz de mandar tráfico a su destino.
- Suplantación de direcciones lógicas (WWN *Spoofing*). Aprovechando las herramientas de gestión que cada fabricante proporciona con la correspondiente tarjeta HBA, puede modificarse el valor de la dirección WWN usada a la hora de interactuar con conmutadores o sistemas de almacenamiento que pueda haber presentes en la red. Algunos mecanismos de seguridad en *fibre channel*, como el *zonning,* se pueden basar en estas direcciones, lo que les confiere una fiabilidad reducida.
- Envenenamiento del servidor de nombres. Cada vez que un dispositivo se conecta a la red de almacenamiento, debe seguir un procedimiento de registro, mediante el cual se anuncian sus distintas capacidades de comunicación en la red, como las clases de servicio que soporta, protocolos de capa superior que maneja, así como la dirección lógica de su puerto (WWPN) y de su tarjeta (WWNN). Esa información proporcionada se almacenará en la base de datos del servidor de nombres de la malla, para ponerla a disposición de quien la necesite. Un atacante puede aprovechar este proceso para registrar direcciones lógicas que corresponden a otros dispositivos de la red, con el objetvo de que, a partir de entonces, se haga llegar al atacante el tráfico que iba dirigido al dispositivo que anunció su dirección lógica correspondiente.

Cifrado de la información

Uno de los problemas más importantes que pueden producirse en una red de almacenamiento, es el de la pérdida o robo de soportes de almacenamiento, tales como discos duros y/o cintas. Por ello, se deben tratar dos situaciones diferenciadas.

Por un lado, el cifrado llamado en reposo, que corresponde al de la información una vez se almacena en el soporte correspondiente. Y que debe impedir que el robo de dicho soporte ponga en peligro la confidencialidad de la información. Para evitarlo, existen soluciones a distintos niveles:

- En el ámbito de medio de almacenamiento, mediante el uso de discos duros que disponen de capacidad de cifrar los datos que almacenan en su interior. Para ello, usan un algoritmo de cifrado de clave simétrica, como AES, implementado mediante hardware que tiene una penalización de rendimiento inapreciable. Pero solo se pueden usar en controladoras de discos preparadas para gestionarlos, ya que estos deben recibir del exterior la clave a usar para el proceso de cifrado. En caso de pérdida de esta, no existe forma de recuperación de la información guardada en el disco.

  En el caso de las cintas para copias de seguridad, existe la posibilidad de usar los llamados *token*, que se conectan al *drive* a través de una interfaz USB. Son capaces de generar claves y almacenar una cantidad muy limitada de ellas. Una vez agotado el espacio, debe sustituirse por otro. Pero para ello, debe revisarse la necesidad de disponer de alguna de las claves ahí alojadas, por si aún existe alguna cinta o juego de cintas, que contengan información que pueda necesitarse. Es una solución económica, pero que requiere intervenciones manuales del administrador, como la realización de copias de seguridad del contenido del *token* para posterior restaurado en otro similar. De lo contrario, se corre el peligro de que en caso de que se produzca un robo en las instalaciones, la organización pierda la capacidad de leer las cintas de cualquier copia de seguridad realizada anteriormente.
- A nivel de controladora de disco, que permite realizar el cifrado de forma transparente al sistema operativo y aplicaciones que se ejecutan sobre él, como en el caso anterior. Algunos modelos pueden cambiar la clave de cifrado sobre la marcha.
- En cuanto a sistema operativo o aplicación, lo que genera un consumo de tiempo de procesador para efectuar las tareas de cifrado y descifrado. Como ejemplo de la primera opción, se dispone de soluciones como BitLocker para sistemas Windows. De la segunda, tenemos software especializado como Crypt 2000 o McAfee Drive Encryption, que cifran todo el disco o partición elegida. Para efectuar el arranque del sistema, se inserta código adicional durante la fase de encendido, en la que se solicita u obtiene la clave de cifrado al usuario para poder acceder al contenido.

Para efectuar el cifrado de la información, se necesita una forma de generar las claves necesarias. Al usarse algoritmos simétricos, la misma clave se usa tanto para el cifrado como para el descifrado. Para las situaciones expuestas en el apartado anterior, existen varias alternativas:

- Utilizar una aplicación que genera las claves necesarias, y las envía al disco duro con capacidad de cifrado, o a la controladora correspondiente.
- En el caso de las lectoras de cintas, se puede usar un token que genera nuevas claves y las almacena en su interior. Tiene una capaci-

dad muy limitada y no se considera adecuado para una organización de tamaño mediano o grande.

- En el caso de la controladora de discos, esta dispone de generar claves localmente. Si se dispone de chip TPM, puede usarse para automatizar el proceso de arranque y no requerir presencia de un operador.
- Para organizaciones que dispongan de un gran número de equipos, se recomienda el uso de hardware específico, como los Enterprise Secure Key Manager (ESKM). Tiene capacidad para generar claves y almacenar una gran cantidad, incluso millones. Las solicitudes se realizan mediante el protocolo KMIP (por Key Management Interoperability Protocol). Además, está pensado para poder funcionar en cluster, de forma que el fallo de uno de ellos no produce un impacto en los dispositivos que lo utilizan, porque pueden acceder a los restantes, cuyo contenido se habrá replicado entre todos ellos previamente.

En la otra situación a plantear, se requiere cifrar la información en el momento previo a su envío por la fibra óptica, lo que requiere igualar la velocidad de cifrado con la de transmisión a través del medio para no perder rendimiento. Las velocidades actuales de *fibre channel* son muy demandantes y van a seguir aumentando en los próximos años. Actualmente, no resulta sencillo ni económico encontrar equipamiento con la capacidad de cifrar a la velocidad requerida. Y esa capacidad deberá repartirse entre todos los puertos que la requieran.

Normalmente, los conmutadores solo contemplan la posibilidad de cifrar el tráfico a transmitir, cuando el puerto elegido está configurado para la comunicación con otro conmutador. En ningún caso se cifran las tramas entre un dispositivo y el propio conmutador.

3. Conclusiones

La información que una organización maneja debe protegerse adecuadamente. Su pérdida o robo puede llevar al cierre de la misma. La seguridad debe estudiarse teniendo en cuenta que los ataques pueden proceder del exterior (por ejemplo, a través de internet), pero también del interior.

Con el empleo de la virtualización en DMZ, puede darse el caso de que un persona aproveche la red de internet para atacar los servicios que esa organización ofrece al público. Y desde ahí, tomar el control de la red de almacenamiento, en la que, históricamente, no se ha considerado nunca que hubiera algún peligro, por ser cerradas. Sin embargo, esta circunstancia ha cambiado de manera sustancial.

El uso de librerías como HBAAPI, permiten obtener mucha información de la red de almacenamiento, como se ha podido comprobar con el desarrollo de las dos pequeñas aplicaciones que se han elaborado como parte de este TFM.

Sin embargo, esta librería cuenta con una función llamada HBA_SendCTPassThru, que permite interactuar con los distintos servicios que proporciona la malla para su correcto funcionamiento. Las funcionalidades que cada servicio ofrece permiten obtener información de su base de datos correspondiente. Con esto, un atacante puede tener una imagen muy completa de cualquier dispositivo conectado a la red, aunque no pueda comunicarse con él debido a la configuración que el administrador tenga con las llamadas zonas (mecanismo de *zonning*).

Pero, además, existen funcionalidades que permiten añadir, modificar o eliminar contenido, por lo que el atacante también puede controlar el funcionamiento de la red, ya que esas funciones no parecen requerir que el usuario se autentique.

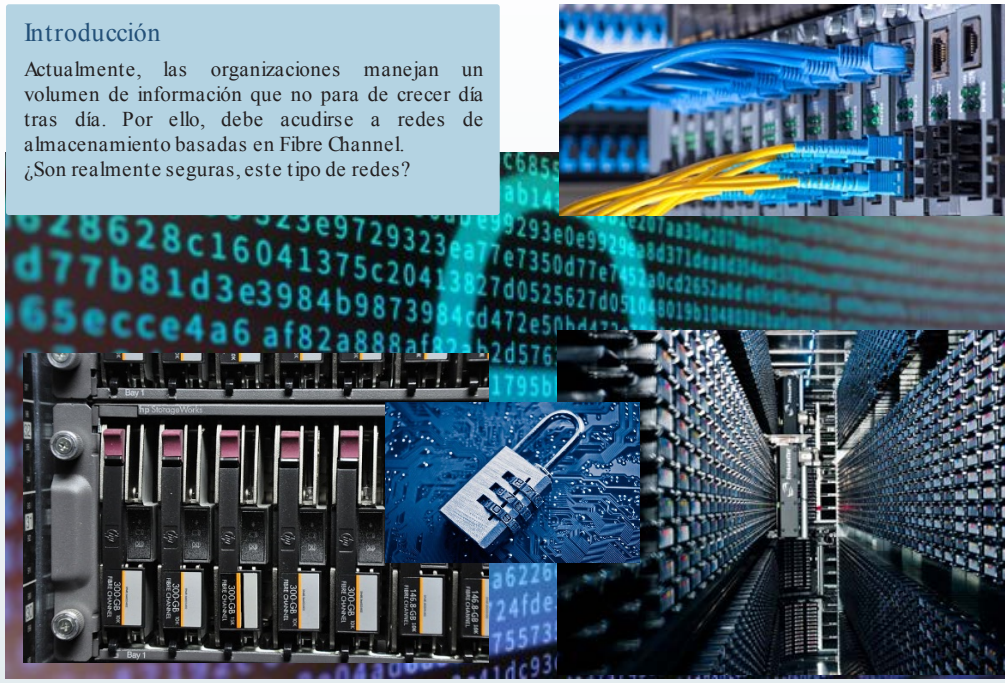
Amenazas de seguridad en redes de almacenamiento Fibre Channel

Autor: David Molina Vives
Director/es: Francisco Troncoso Pastoriza

Universidade Vigo

Introducción

Actualmente, las organizaciones manejan un volumen de información que no para de crecer día tras día. Por ello, debe acudirse a redes de almacenamiento basadas en Fibre Channel.
¿Son realmente seguras, este tipo de redes?



Consideraciones importantes

- Diseños incorrectos, pueden facilitar enormemente el trabajo de un atacante que pretende acceder a la información de la organización, un tesoro para cualquier ciber-delincuente.
- Existen librerías de código que permiten realizar muchas operaciones delicadas, sin autenticación.
- Cifrado de los datos, para evitar que robos o pérdidas perjudiquen confidencialidad.

Conclusiones

El uso de las redes de almacenamiento, requiere mucho cuidado a la hora de realizar un diseño seguro.

Tienen vulnerabilidades fáciles de explotar, como en TCP/IP hace unos años.

Existen herramientas que obtienen o permiten gestión de servicios en Fibre Channel.

Cualquiera, ¿puede gestionar los servicios de la red libremente?

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Diseño de un sistema automático de perfilado indirecto de la personalidad con base en datos extraídos de redes sociales

Autora: Laura Prada Rivero (laura.prada.rivero@gmail.com)
Directores: Luis Álvarez Sabucedo (lsabucedo@det.uvigo.es) y Milagros Fernández Gavilanes (mfgavilanes@cud.uvigo.es)

Resumen – Para el estudio de la personalidad, los modelos psicológicos tradicionales se basan en *tests* psicométricos y en entrevistas clínicas, identificando rasgos o características comunes entre las personas. Pero estas formas de estudio directas no son siempre posible. En medio de una investigación no se puede hacer un *test* a un sospecho, ni tampoco cuando se está seleccionando a las posibles fuentes para servicios de información. Existen modelos de la personalidad que permiten un estudio indirecto de los rasgos, partiendo de ciertos indicadores que se extraen del comportamiento de los sujetos.

El lenguaje humano muestra la personalidad del individuo. Por lo tanto, hay indicadores de comportamiento que se pueden extraer del lenguaje verbal. Hoy en día las redes sociales suponen unos de los canales de comunicación de la población, lo cual proporciona una fuente inmensa de información que puede ser tomada de muestra para inferir la personalidad.

Estudiando conocimiento experto en psicología, se seleccionará un modelo de personalidad de perfilado indirecto para definir los indicadores necesarios. Después se hará un recorrido por aquellas tecnologías que permitan realizar el diseño que cumpla los requisitos especificados. Entre estas tecnologías destaca el procesamiento del lenguaje natural (PLN), *Machine Learning* (ML) y diferentes modos de almacenamiento y generación de informes para los usuarios finales del sistema.

El resultado será una propuesta de diseño de un sistema de información que permitiría extraer los rasgos de la personalidad de un individuo a través de textos generados por él en sus redes sociales.

Palabras clave – Personalidad, Perfilado Indirecto, RR. SS., PLN, ML.

1. Introducción

La personalidad es la tendencia estable de una persona a pensar, sentir y actuar de una determinada manera [6]. Los llamados rasgos de personalidad expresan una tendencia a la hora de procesar e interpretar lo que sucede a cada persona, y con ello la forma en la que sienten [5]. La clasificación de la personalidad es objeto de estudio desde tiempos de la antigua Grecia, donde se evaluaban más aspectos físicos ligados a los humores, hasta nuestros días, donde la clasificación se basa en modelos de conducta [1][2][3][4][4]. Muchos de estos modelos están basados en rasgos [1][2].

Junto con cada modelo se crean *tests* de personalidad que, de forma directa, son utilizados para identificar los rasgos que cada individuo tiene, siendo la personalidad de cada uno un conjunto de varios o todos los rasgos de un modelo, cuantificándolos de forma individualizada.

Parece claro que estos métodos directos no siempre son aplicables. En particular, no son los más adecuados cuando se está tratando de clasificar masivamente a un grupo de población o a un individuo que no se debe sentir estudiado. La perfilación indirecta surge para dar respuesta a este tipo de necesidades como metodología igualmente válida que la directa para inferir la personalidad de los individuos estudiados [2][3]. Cuando la evaluación directa no se pueda realizar, el perfilado deberá realizarse por medio de la observación de la propia persona, de su entorno, de su comportamiento y de su lenguaje (verbal y no verbal) en lugar de acudir a las pruebas psicométricas y evitando que los sujetos se sepan evaluados.

Actualmente, las redes sociales (RR. SS.) constituyen una fuente inmensa de información. Hay teorías que exponen que los individuos seleccionan y crean sus ambientes sociales para encajar y reforzar sus características personales en los mismos [1][7][8]. Las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE) también tienen el foco puesto en estas redes como un *input* más en sus investigaciones. La importancia que tiene el perfilado indirecto con el objetivo de investigar es clara. Extraer el perfil de sospechosos o de posibles fuentes manipulables no puede ser abordado con un estudio directo de la personalidad.

El doctor James W. Pennebaker [12][13], profesor de Psicología del Centenario de Artes Liberales en la Universidad de Texas en Austin, ha centrado sus estudios dentro del campo de la psicología, concretamente en el ámbito del estudio del lenguaje humano. Es autor de la siguiente frase: «Eres lo que hablas». El lenguaje es vehículo de expresión de la personalidad de los individuos.

ENCUIST [4] es un modelo de personalidad desarrollado por la psicóloga Lucia Halty [3], directamente para trabajar en entornos policiales. Permite realizar un perfilado indirecto de los individuos, buscando y analizando variables que se pueden obtener de la observación del comportamiento.

Está muy orientado al perfilado indirecto con base en textos extraídos de charlas o entrevistas con los individuos estudiados, por lo que lo hace un buen modelo para trabajar en un sistema automático de perfilado indirecto basado en textos.

2. Objetivo

El objetivo es plantear un posible diseño de un sistema que permita perfilar a un individuo o a un conjunto de ellos basándose en la información de sus redes sociales, utilizando indicadores del lenguaje y metadatos asociados que se pueden deducir del modelo ENCUIST, una vez analizado en detalle.

Basándose en los principios de la arquitectura *software*, este trabajo se va a centrar en las etapas de análisis y diseño, dejando para futuros trabajos el desarrollo y las pruebas.

3. Perfilado indirecto de la personalidad. Modelo ENCUIST

ENCUIST es un modelo muy adecuado para el perfilado indirecto, ya que su diseño tuvo este objetivo como meta [2][3][4]. Se utiliza como requisitos del sistema las conclusiones a las que llega en modelo ENCUIST. Los rasgos de personalidad que propone ENCUIST.

- Extroversión/búsqueda de sensaciones (E): este rasgo se resumen en sociabilidad y búsqueda de estímulos. La emoción de la alegría está vinculada a este rasgo.
- Neuroticismo (ansiedad, ira y asco) (N): inestabilidad emocional. Emociones básicas. Los individuos con puntuaciones elevadas en neuroticismo suelen ser susceptibles a problemas basados en la ansiedad, el miedo y la tristeza.
- Insensibilidad emocional (CU): ausencia de culpa, falta de empatía, sentido desmesurado de autovalía.
- Impulsividad/agresividad (I): transgresor de normas, dificultad en el control de impulsos.
- Necesidad de cognición (NC): realización de tareas mentales. Búsqueda de información detallada.

4. Redes Sociales objetivo

Las RR. SS. seleccionadas para las descargas son Facebook y Twitter. Gran cantidad de los contenidos de los perfiles de Facebook son públicos y tienen texto suficiente para su estudio. Al ser una red social de bastante difusión, hay altas probabilidades de que los objetivos tengan perfil. Por lo tanto, Facebook es una red social adecuada para el estudio. Twitter es ideal para este estudio, ya que justamente su intención es la de mostrar la opinión de los usuarios en formato texto.

5. Arquitectura del sistema

La arquitectura planteada no pretende ser única, sino una de las múltiples posibilidades que pueden elaborarse y que den solución a la problemática planteada. La figura 1 muestra los subsistemas y flujos de información que se han considerado necesarios para cumplir los requerimientos del sistema.

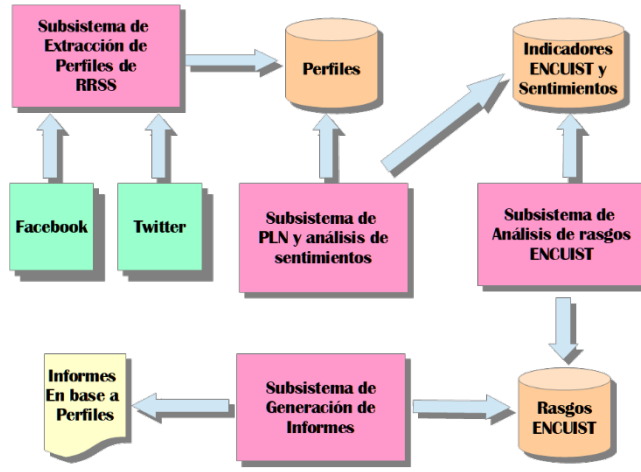


Figura 1. Análisis de subsistemas y flujos de información

El lenguaje de programación que se propone como base para el desarrollo del sistema de perfilado indirecto automático es Python [14]. Este lenguaje de alto nivel es el idóneo para el *data mining*, la inteligencia artificial, el *machine learning* y otros muchos tipos de proyectos. Como entorno de desarrollo se utilizará Jupyter Notebook [15]. Estos cuadernos (*notebooks*) permiten combinar texto y código, organizados en celdas, lo cual es más cómodo para desarrollar y documentar al mismo tiempo.

Extracción de información de RR. SS.

El web *scraping* es el proceso de recopilar datos web estructurados de forma automatizada. El *software* que se desarrolla se comporta simulando la navegación de un humano y están especializadas en sitios en concreto. En general, la extracción de datos web es utilizada por personas y empresas que desean hacer uso de la gran cantidad de datos web disponibles públicamente.

Diseño subsistema de extracción de perfiles de RR. SS.

Los desarrollos actuales con Selenium [13] copan todo el mercado especializado en tareas de *scraping*. Para ambas RR. SS. es necesario indicar cuáles serán los identificadores de los perfiles que se van a descargar.

Estos perfiles irán en un *array* de entrada y se irán procesando uno a uno. Será necesario el desarrollo de un Facebook *scraper* y de un Twitter *scraper*, ambos dos utilizando la herramienta WebDriver.

Machine learning

Inicialmente, debe existir un conjunto de datos de entrenamiento que consistirán en los *tests* ENCUIST de un cierto número de individuos junto con sus perfiles descargados de RR. SS.. Una vez que el sistema sea entrenado se podrá utilizar el modelo para inferir nuevos datos, es decir, que a partir de los indicadores descargados el modelo calculará valores para sus rasgos.

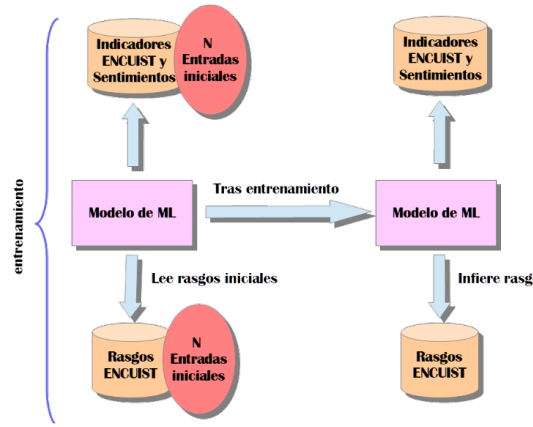


Figura 2. Subsistema de análisis de rasgos ENCUIST

De los requisitos del sistema se sabe que cada rasgo de la personalidad viene evaluado por un valor dentro del rango discreto, nulo, bajo, medio y alto. El subsistema deberá hacer una clasificación de los indicadores dentro de una de esas cuatro clases. El modelo a desarrollar será de clasificación supervisado para cada uno de los rasgos. Es importante subrayar que se implementaría un modelo por rasgo debido a que cada uno es independiente entre sí, al menos *a priori,* así se tratan en los *tests* psicológicos de perfilado directo.

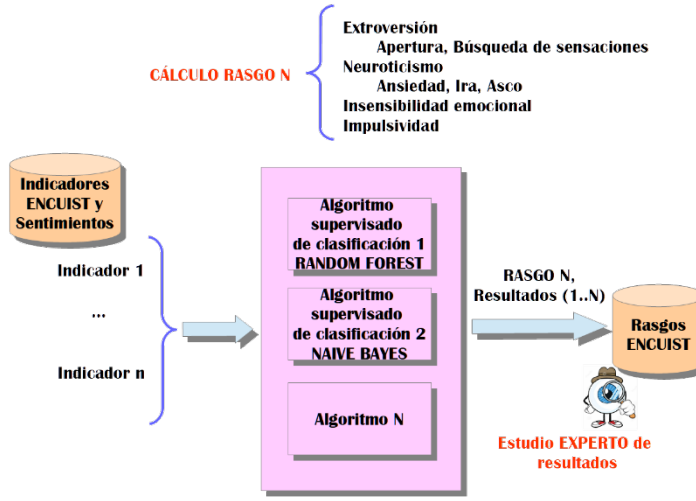


Figura 3. Cálculo de cada rasgo

Diseño subsistema de análisis de rasgos ENCUIST

- Modelo más conservador: algoritmos de clasificación supervisado. De tal manera que cada rasgo que se va a evaluar tendrá su propio modelo o modelos. De esta forma se gana independencia si a futuro se quieren añadir o eliminar rasgos. Será necesario aplicar inicialmente un entrenamiento con los vectores de ejemplo compuestos de: [Indicadores, Rasgon] siendo n el número de rasgo que se está calculando. Los algoritmos que se utilizarían en esta propuesta: Random Forest y Naïve Bayes y su resultado será almacenado en MongoDB en la Colección Rasgos.
- Modelo más innovador: algoritmo de deep learning. Como entrada del algoritmo introduciríamos los textos preparados para que el este aprendiera directamente de ellos y ver qué conclusiones extrae. Es más sencillo y eficiente que desarrollar una red neuronal partiendo de cero basarse en un modelo ya implementado como RoBERTa [12].

Procesamiento del lenguaje natural

El procesamiento del lenguaje natural (PLN) es una rama de la inteligencia artificial que se encarga de estudiar la comunicación de las máquinas con las personas a través de idiomas humanos. En el sistema de perfilado indirecto que se está diseñando es necesario el PLN para poder establecer los indicadores del lenguaje sobre la base de los que se podrán deducir los rasgos.

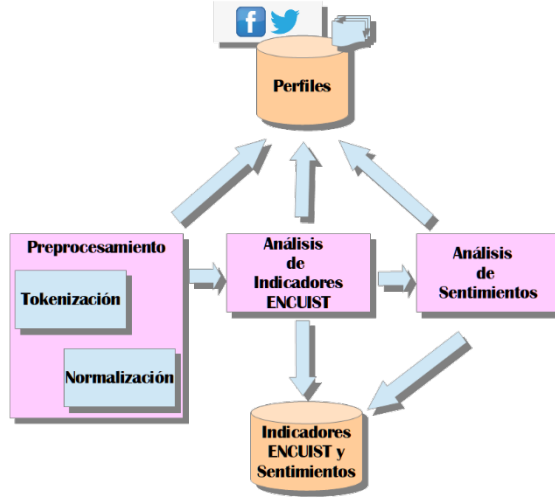


Figura 4. Subsistema de PLN y análisis de sentimientos

Para ello se pueden extraer dos acercamientos y dos propuestas de diseño:

- Tradicional: se propone utilizar NLTK para tokenizar los textos y normalizarlos, presentando todos el mismo aspecto para el posterior cálculo de los indicadores por LIWC [9].

— Innovadora: el deep learning, permite obtener resultados sin necesidad de una preparación tan exhaustiva de los textos, además, se aleja de fórmulas tradicionales basadas en el conteo de palabras, ya que el software realiza un análisis de los textos en su conjunto. Este diseño permitiría descubrir relaciones entre los rasgos y los textos que probablemente no han sido tenidos en cuenta. Con deep learning no será necesario el cálculo de los indicadores, sino que el entrenamiento consistiría en el vector de entrada compuestos por textos descargados de RR. SS. y el valor del rasgo ENCUIST para ese texto. Se propone el uso de los transformers ya desarrollados, y más en concreto, aquellos que tienen diccionarios en castellano y están basados en BERT como RoBERTa [14].

El análisis de sentimiento es el proceso de determinar el tono emocional que hay detrás de una serie de palabras. Entre los usos que tiene realizar este tipo de minería de textos está la de saber qué opinión tienen los autores de los textos o bien sus estados de ánimo. La propia herramienta NLTK permite realizar dicho análisis y se propone para formar parte del diseño en el cálculo de los sentimientos que se podrán inferir de los textos.

Diseño subsistema de procesamiento de lenguaje natural y análisis de sentimientos

Este subsistema contendrá tres módulos para trabajar sobre los ficheros textuales almacenados en JSON y descargados de las RR. SS..

— Módulo de preparación de los textos: se propone NLTK para la normalización y una tokenización de los textos y se almacenarán JSON.

— Módulo de cálculo de indicadores textuales ENCUIST: sobre los JSON normalizados y tokenizados se continúa con el cálculo de los indicadores textuales. Para ello se propone utilizar la herramienta LIWC [9]. Una vez calculados los indicadores del texto, se almacenarán en la Colección Perfiles de ENCUIST.

— Módulo de análisis de sentimientos: NLTK es una herramienta de Python muy valorada para el análisis de sentimientos a través de su librería SentimentIntensityAnalyzer.

Almacenamiento

Se opta por almacenamiento NoSQL debido a la flexibilidad a cambios en el modelo que este tipo de BB. DD aportan.

— BB. DD NoSQL documental: los datos descargados de RR. SS., una vez se hayan convertido en archivos JSON, se insertarán en esta BB. DD. Para el diseño propuesto se escoge MongoDB [11].

— BB. DD orientada a grafos: para poder analizar la información basándose en las relaciones entre los datos representadas a través de los grafos. De esta forma se podrán encontrar relaciones que no se han tenido en cuenta previamente y puede ser utilizada de forma sencilla

para el subsistema de informes. Su fácil representación gráfica la hace perfecta para el estudio de los datos y sus relaciones. Para la propuesta del actual diseño se elige el producto Neo4J.

Diseño Almacenamiento

La información descargada de las RR. SS. se va a almacenar en ficheros JSON. Esto implica una necesidad de gestión y almacenamiento de ficheros. Además, en esta unidad de datos, se pueden incluir más elementos que sean necesarios con pocos cambios en el código.

Se proponen cuatro colecciones en MongoDB: perfiles, indicadores, sentimientos y rasgos. MongoDB y Neo4J se comunicarán a través de un conector.

La representación en Neo irá relacionada con las preguntas que se vayan a realizar sobre el modelo. Estas preguntas pueden evolucionar a lo largo de la vida del sistema, ya que los grafos son fácilmente configurables y se necesitan pocos cambios en el código. Algunos ejemplos de preguntas son: devolver todos los patrones de rasgos que hay en función de su algoritmo; búsqueda de un determinado patrón de rasgos; encontrar los perfiles más influenciables para buscar fuentes; individuos que cumplan un perfil que encaje en un patrón criminal.

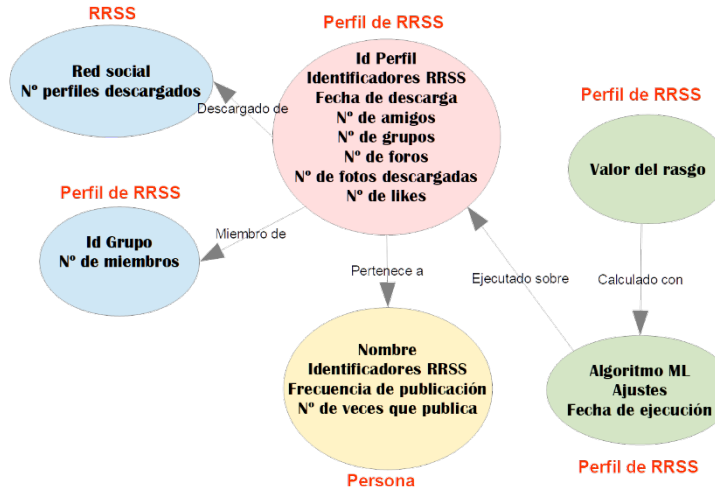


Figura 5. Modelo de grafos

6. Conclusiones

Una parte muy importante de investigación previa al desarrollo del presente trabajo fue encontrar un modelo de personalidad que permitiera realizar un perfilado indirecto. ENCUIST permite identificar los indicadores necesarios para hacer una perfilación indirecta y poderla automatizar mediante un sistema de información.

Con los requisitos identificados se estudiaron las posibilidades tecnológicas que plantea el mercado, para elegir aquellas que pueden dar una respuesta mejor a los requisitos elaborados. Los indicadores que se seleccionaron han sido básicamente textuales, por eso, el *machine lerning* y concreto el *deep learning* tienen una aplicación directa en este proyecto.

Este proyecto plantea una fórmula tradicional basada en algoritmos de *machine lerning* habitualmente utilizados, pero a la vez abierta para poder evolucionar, con una BB. DD NoSQL que almacenaría JSONs y que sería capaz de adaptar rápido su modelo sin tener que hacer grandes cambios de diseño. Y un segundo planteamiento, también con ese almacenamiento, pero basado en *deep learning*, con uso de *transformers*, herramientas punteras en el PLN.

Referencias

ENCUIST. *Modelo de personalidad para la realización de perfiles psicológicos*. [Consulta: septiembre 2022]. Disponible en: https://encuist.com/

GitHub Spanish BERT. (s. f.). *SpanBERTa: RoBERTa for* Spanish [en línea]. [Consulta: diciembre 2022]. Disponible en: https://github.com/chriskhanhtran/spanish-bert

González Élices, P. (2020). *Perfilación indirecta a través de la comunicación verbal y no verbal [tesis doctoral]*. Directores, Lucía Halty Barrutieta y José Luis González Álvarez. Madrid, Universidad Autónoma de Madrid. Disponible en: https://repositorio.uam.es/handle/10486/691839

Guijarro, M. Relación entre redes sociales y personalidad. *Drafts of economic intelligence*. La SEI. UAM. Vol. 1, n.º 3, pp. 23-34.

Halty, L., González, J. L. y Sotoca, A. (2017). *Modelo ENCUIST: aplicación al perfilado criminal. Anuario de Psicología Jurídica*. Colegio Oficial de la Psicología de Madrid. Vol. 27, pp. 21-31.

Investigación y Ciencia. Deconstrucción de La Memoria. *Mente y Cerebro*. [Consulta: diciembre 2022]. Disponible en: https://www.investigacionyciencia.es/revistas/mente-y-cerebro/deconstruccin-de-la-memoria-509/eres-lo-que-hablas-8301

Jupyter. [Consulta: diciembre 2022]. Disponible en: https://jupyter.org/

LIWC. [Consulta: octubre 2022]. Disponible en: https://www.liwc.app/

Thompson, S. *Managing Machine Learning Projects from design to deployment Version 4*. Manning Publications.

Martín Gómez, P. (2020). Ventajas y desventajas de MongoDB. *Openwebinars*. [Consulta: noviembre 2022]. Disponible en: https://openwebinars.net/blog/ventajas-y-desventajas-de-mongodb/

Psicología y mente. [Consulta: septiembre 2022]. Disponible en: https://psicologiaymente.com

Python. [Consulta: diciembre 2022]. Disponible en: https://www.python.org/

Selenium. [Consulta: diciembre 2022]. Disponible en: https://www.selenium.dev/

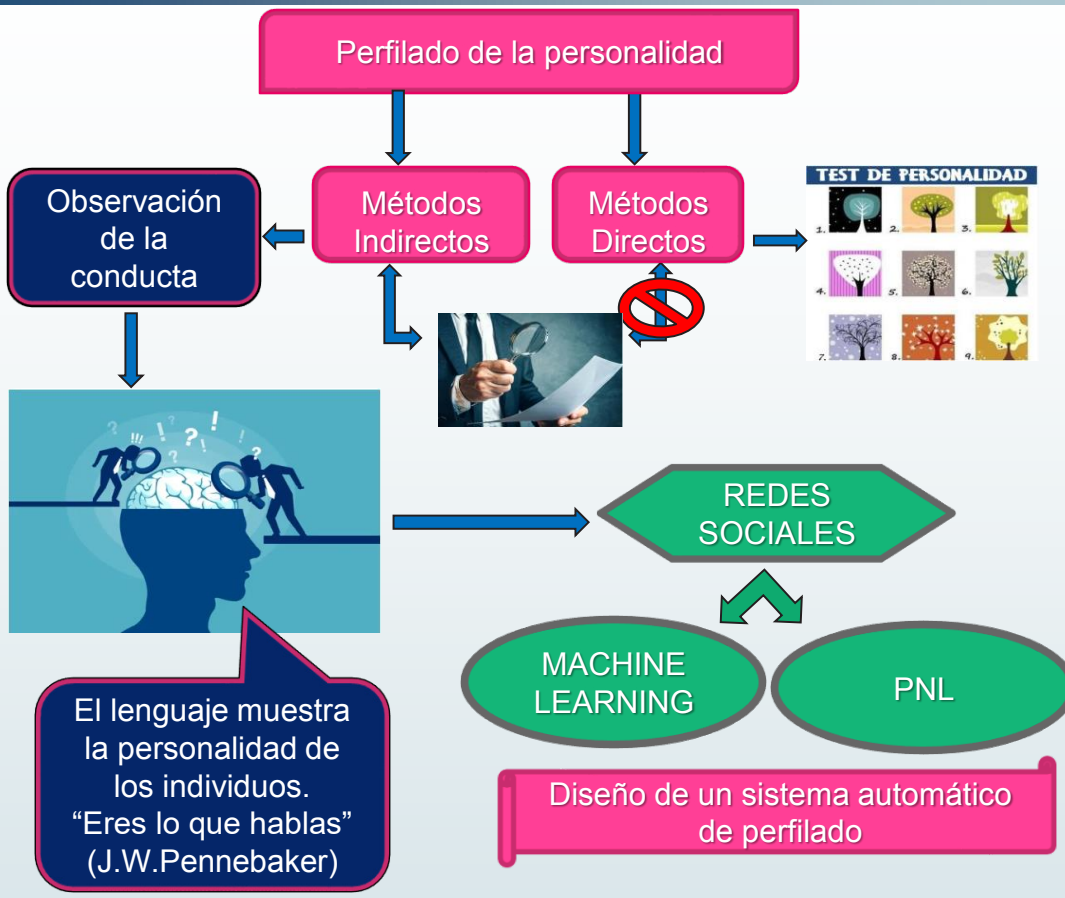
Serrano, J. (s. f.). Personalidad: Comprendiendo los rasgos de personalidad [en línea]. *Área Humana, investigación, innovación y experiencia en psicología*. [Consulta: diciembre 2022]. Disponible en: https://www.areahumana.es/que-es-la-personalidad/

Torregrosa López, F. J. y López, R. M. (2016). Personalidad y redes sociales: una revisión sistemática. *Research Gate Genios*.

Diseño de un sistema automático de perfilado indirecto de la personalidad en base a datos extraídos de redes sociales

Autor: Laura Prada Rivero
Director/es: Luis Álvarez Sabucedo y Milagros Fernández Gavilanes

Universidad de Vigo



El **objetivo** es plantear un posible diseño de un sistema que permita perfilar a un individuos o a un conjunto de ellos en base a la información de sus redes sociales, utilizando indicadores del lenguaje y metadatos asociados que se pueden deducir del modelo de personalidad ENCUIST basado en el perfilado indirecto.

El problema de la factorización de números enteros de gran tamaño y su resolución mediante computación cuántica

Autor: Rafael Romero Margaritti (margaritti@ea.mde.es)
Directores: Milagros Fernández Gavilanes (mfgavilanes@cud.uvigo.es) y Javier Vales Alonso (Javier.Vales@upct.es)

Resumen – El objetivo de este artículo es plasmar con un ejemplo cómo estarían amenazados los sistemas de encriptado actuales por la computación cuántica.

Para lograrlo se ha escogido el problema de la Factorización de números enteros de gran tamaño en la que se basa el algoritmo RSA. El algoritmo RSA es muy utilizado en la actualidad tanto para encriptar como para autenticar. Es un algoritmo asíncrono (clave pública, clave privada).

El algoritmo de Shor es la gran esperanza de mejora en la factorización de números enteros grandes si se llega a crear alguna vez un ordenador cuántico totalmente operativo.

Palabras clave – Algoritmo, Factorización, Shor, Qubit.

1. Introducción

En la actualidad se está especulando bastante que si la computación cuántica va a suponer un antes y un después en la computación. Al igual que lo que supuso la computación clásica que consiguió resolver problemas que nunca se habían pensado que fuésemos capaces de resolver, por ejemplo, el descifrado del genoma humano, la computación cuántica se supone que va a resolver problemas que hoy por hoy son irresolubles o irresolubles en un tiempo razonable.

Un ejemplo de los problemas que son actualmente irresolubles en un tiempo razonable es el problema de la factorización de números enteros grandes. Hay varios algoritmos de encriptación que se basan en la complejidad del cálculo de factorización de enteros, como por ejemplo RSA, y es un hecho que penden de un hilo si se consigue resolver este problema con los ordenadores cuánticos. No obstante, la computación cuántica puede traer también mejores algoritmos de encriptación.

2. Desarrollo

Shor ha desarrollado un algoritmo cuántico que factoriza números enteros grandes en un tiempo $O(\log(n)^3)$. Este algoritmo es mucho más eficiente que el mejor que existe en computación binaria, el Algoritmo General de Criba del Cuerpo de Números (*General Number Field Sieve*).

Tenemos un número n que proviene de la multiplicación de dos números enteros primos.

$$n = p*q$$

Este algoritmo se basa en calcular el periodo de la función $[m^x]_n$, cumpliéndose $1< m < (n-1)$. Esta función es periódica, con periodo $e < n$ y siempre toma el valor 1 cuando $x = e$. La notación $[t]_n$ se refiere al módulo de la división de $\frac{t}{n}$.

Si el periodo de la función es par entonces:

$$[m^{2a}]_n = 1 \Rightarrow m^{2a} = k*n +1$$

$$m^{2a} = k*n \Rightarrow (m^a-1)\,(+1)= k*n$$

Tres posibilidades:

$$(m^a-1) = h*n$$

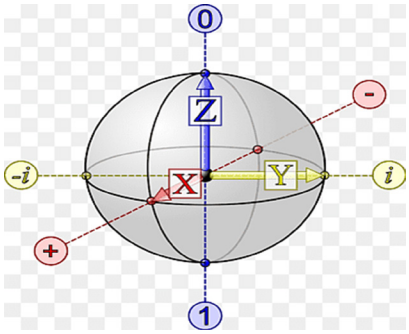
$$(m^a+1) = r*n$$

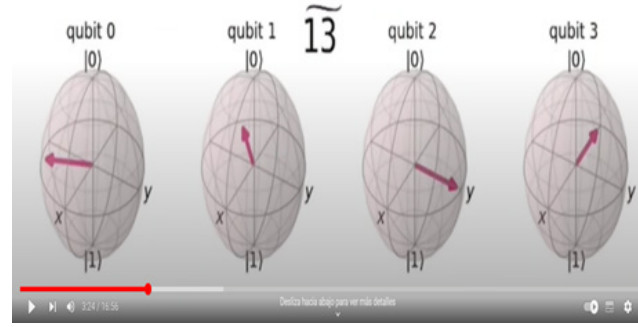
$$(m^a-1) = s*p \;\&\; (m^a+1) = u*n$$

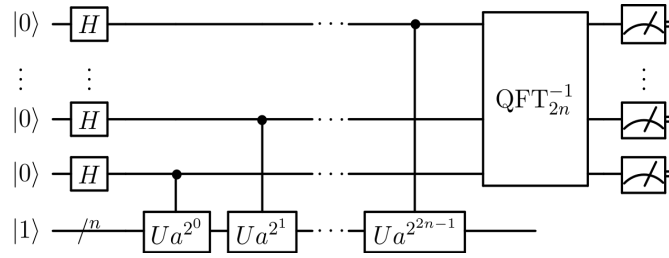
Si se da la última posibilidad hemos obtenido lo deseado y obtendríamos p y q, aplicando el algoritmo de Euclides. Si es impar o se da las otras dos posibilidades, se escoge otra m y se vuelve a calcular el periodo.

La parte novedosa del algoritmo de Shor es que utiliza la computación cuántica para calcular el periodo de la función $[m^x]_n$.

Para ello utiliza el Algoritmo Cuántico de Estimación de Fase y la Transformada Cuántica Inversa de Fourier. Y por supuesto las ventajas de la computación cuántica la superposición y el entrelazamiento es decir el paralelismo cuántico.







3. Conclusiones

En la computación cuántica al igual que con la clásica hay una parte matemática y otra física. Como hemos visto durante todo el trabajo la parte matemática de la computación cuántica se basa en las matrices y en los números complejos, al igual que la computación clásica se basaba en el Álgebra de Boole. La parte matemática de la computación cuántica no presenta ningún problema. El gran reto es la mecánica cuántica, es decir, conseguir un ordenador cuántico funcional con el número de qubits necesarios para implementar el Algoritmo de Shor u otro cualquiera. Otro gran problema es la decoherencia, los qubits de los ordenadores actuales son inestables y necesitan unas condiciones de uso muy estrictas (vacío, temperatura, ambiente limpio, etc.). Para finalizar, la unión o arquitectura de los ordenadores es compleja, ya que los qubits no se pueden unir uno con cualquiera, por lo cual hay hacer encajes de bolillos para implementar algunos algoritmos e incluso crear el ordenador para el algoritmo. Es decir, no se dispone de un ordenador universal en el que se puedan implementar cualquier algoritmo.

Por lo que, aunque matemática y teóricamente sea factible el algoritmo de Shor en la actualidad estamos muy lejos de disponer un ordenador cuántico totalmente operativo, los pocos que existen tienen muy pocos qubits y son muy inestables. Además, hay que recordar que la mayoría de los cálculos cuánticos son probabilísticos y no se tiene certeza 100 % de conseguir el resultado esperado.

Aunque con ordenadores cuánticos híbridos (parte cuántica y parte clásica) el *record* es mayor (hace una mezcla de algoritmos). El *record* actual con un computador cuántico puro es la factorización de veintiuno. Hay que construir el circuito expresamente según el n que queramos factorizar. Para un número RSA de los que tenemos ahora se requeriría un ordenador cuántico de cientos de miles de qubits.

Lo que sí es una realidad es que si se llega alguna vez a desarrollar un ordenador cuántico en el que se pueda implementar el algoritmo de Shor con el número de qubits necesarios se conseguiría factorizar los números RSA actuales. Aunque siempre queda el incrementar el tamaño de los números, pero está claro que estaría en duda la seguridad de RSA y de otros algoritmos de encriptación actuales. Pero como ya se ha dicho, la cuántica también abre el campo para que se desarrollen nuevos algoritmos de encriptación.

Referencias

Fuentes Izquierdo, S. (2017). *Análisis de los Nuevos Paradigmas de Computación* [trabajo de fin de grado]. Tutor, Pablo Ramos Sainz. Universidad de Alcalá Disponible en: https://ebuah.uah.es/dspace/bitstream/handle/10017/30585/TFG-Fuentes-Izquierdo-2017.pdf

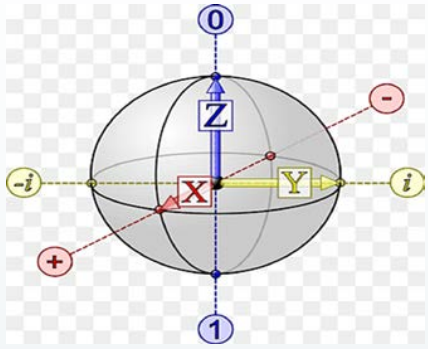
Paz, J. P. y Cormick, C. (2006). *Estimación de fase y algoritmo de Shor.* Depto. de Física, FCE y N, UBA. Disponible en: http://users.df.uba.ar/paz/pag_comp_cuant/resumenes/clase12.pdf

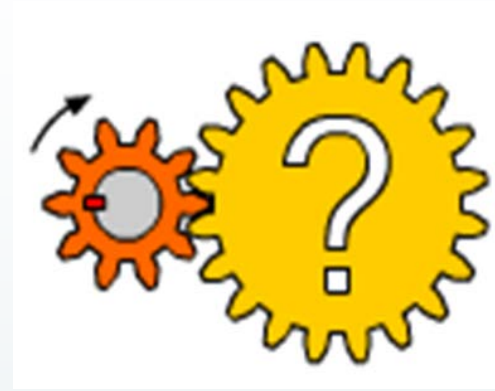
Villatoro, F. R. (2016). Factorizan el número 15 usando el algoritmo de Kitaev con 5 átomos atrapados [en línea]. *La Ciencia de la Mula Francis*. Disponible en: https://francis.naukas.com/2016/03/07/cifrado-con-un-ordenador-de-5-cubits/

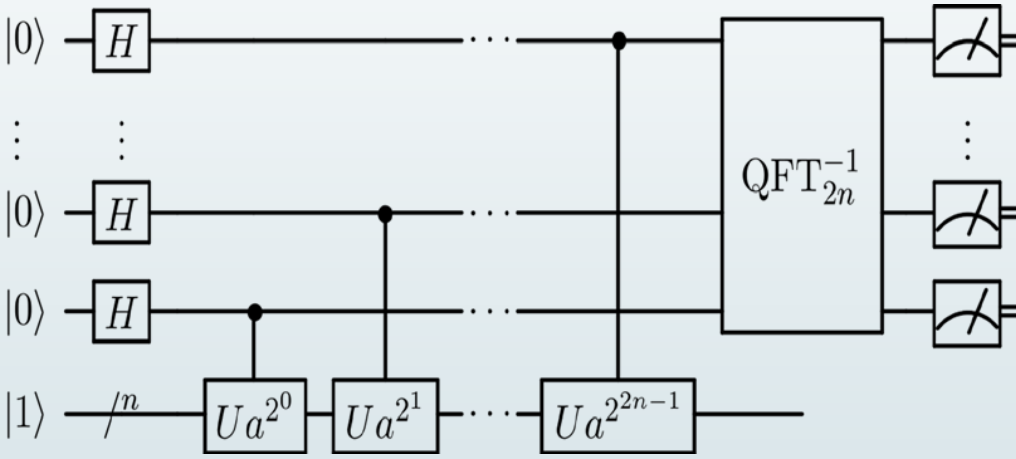
El problema de la factorización de números enteros de gran tamaño y su resolución mediante computación cuántica

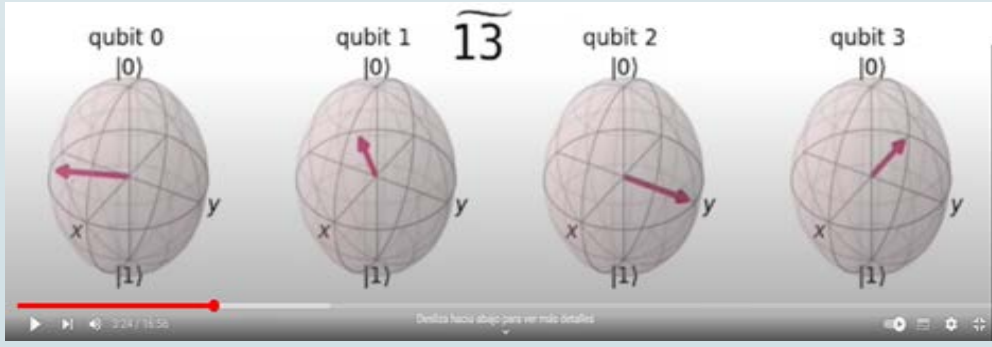
Autor: Rafael Romero Margaritti
Director/es: Milagros Fernández Gavilanes y Javier Vales Alonso

Universidad de Vigo









La ciberseguridad y sus herramientas. Diseño, organización y despliegue, en las redes de una gran corporación

Autor: Ángel San José Arranz (asanjosear@hotmail.com)
Director: Miguel Rodelgo Lacruz (mrodelgo@cud.uvigo.es)

Resumen: Este Trabajo Final de Máster (TFM) pretende profundizar en el campo de la ciberseguridad, aclarando conceptos en materia de seguridad de la información, relativa a los CIS/TIC y ciberdefensa entre algunos otros.

Se pretende abordar cómo debe estar implementada la ciberseguridad en una gran corporación y qué herramientas son fundamentales desplegar para que sea efectiva, fácilmente controlable y aplicable, con una descripción genérica de las mismas y sin referencia a productos de marcas determinadas.

Como algo de interés y novedoso, ya que empieza a ser muy demandado en el mundo de la ciberseguridad, pero a lo que aún no se ha dado una buena solución, se hará una descripción o esbozo de los requerimientos de una herramienta en particular, que integra a otras muchas herramientas de ciberseguridad, y sin la que muchas organizaciones o grandes empresas, no conseguirán una buena gestión de su seguridad en el futuro.

Dicha herramienta se trata de un Cuadro de Mando Integral, que permite la gestión y control de activos, de vulnerabilidades e incidentes, su seguimiento y resolución, todos ellos piezas fundamentales en materia de ciberseguridad e integrado en los diferentes niveles y roles de gobierno o actuación.

Se analizará el asunto desde el diseño para una gran red corporativa simulada con una casuística particular, en la que se pueden albergar dominios y sistemas sin clasificar, e incluso sistemas y servicios clasificados, adecuados al Esquena Nacional de Seguridad (ENS), en los que se integrarán tecnologías antiguas y modernas, como despliegues en la nube o equipos virtualizados.

Igualmente, se desarrollará como debe articularse la organización en los diferentes niveles, pasando desde los Comités de Dirección, Grupos de Trabajo o Gabinetes de Crisis y los Centros de Ciberseguridad (COSC) o SOC.

No pretende ser un trabajo de interés técnico, o solo para expertos en la materia de la ciberseguridad, sino ser una guía o referencia de inicio para los que pretendan abordar el diseño de la ciberseguridad, sin ninguna otra referencia de partida, o simplemente ser un texto de divulgación para enriquecer a quien lo lea en materia de ciberseguridad, que tan de moda está en la actualidad.

Palabras clave: Ciberseguridad, Gobernanza, Políticas, Guías, Herramientas.

1. Introducción

Hasta hace pocos años, podría decirse que no más de diez o quince, el término ciberseguridad era un vocablo con poca relevancia, o prácticamente desconocido para el común de los habitantes del planeta.

Hoy en día, por diversos motivos, ese vocablo tiene una relevancia superlativa, porque afecta a todas las naciones que componen la Tierra, independientemente de su ubicación, estado de desarrollo, riqueza, situación política, o incluso que estén en estado de paz, o de guerra.

Tanto es así, que relacionado con la ciberseguridad se desarrollan planes de nivel nacional e internacional, en grandes organizaciones como la OTAN, se dotan partidas presupuestarías bastante generosas para atender esta materia (ejemplo los fondos de la Unión Europea para ciberseguridad), se dictan políticas de actuación en las administraciones públicas y en las empresas, y de forma muy especial en el ámbito militar, encuadrándose ya en lo que se denomina el ciberespacio, catalogándolo como la cuarta dimensión del campo de batalla.

Pero de qué hablamos, ¿qué se entiende por ciberseguridad?

Si atendemos a los significados del prefijo ciber y del término seguridad:

- Ciber: indica relación con redes informáticas.
- Seguridad: cualidad de «seguro», término que a su vez significa, algo libre y exento de riesgos.

Es por ello que podemos obtener una primera aproximación sobre el significado de ciberseguridad, como la acción de mantener redes informáticas exentas de riesgo y en libertad frente a cualquier acción por impedirla. Pero es necesario profundizar en dicha acepción para una mejor compresión del vocablo y su campo de acción.

Tradicionalmente, se conoce la seguridad informática como la ciberseguridad, siendo su misión la de proteger, sistemas, redes y programas de ataques digitales, para preservar la confidencialidad, disponibilidad e integridad de la información.

Aunque una más reciente sería la del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) [1].

> «Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos».

No debiendo confundirla con la seguridad de la información, que se encarga de los métodos y procesos que procuran proteger los activos de

información en sus diferentes formas o estados, no centrándose únicamente en los sistemas computacionales.

Es por ello que puede decirse que la ciberseguridad para una gran organización está contenida dentro del proceso de seguridad de la información de esta y que será necesario que se establezca una estructura dentro de la organización, que se encargue de su diseño, organización, herramientas y despliegue en las redes informáticas.

2. Objetivos

Los objetivos fundamentales perseguidos, que ya se dejan entrever en el propio título, son los siguientes:

- Revisar las diferentes estrategias que a nivel del Estado se han ido desarrollando y llevado a la práctica, fruto de la situación o la coyuntura de cada momento, así como la revisión de parte de la legislación que en materia de ciberseguridad se está generando, como elemento intrínseco y fundamental de la ciberseguridad, ya que está asumiendo una relevancia muy considerable, tanto es así que parece ser uno de los motores que más impulsan el avance en materia de ciberseguridad en este momento.
- El estudio de los requerimientos de ciberseguridad de una gran corporación, analizando los motivos de los que emanan, confrontados con sus posibles consecuencias en caso de no aplicarlos, todo ello argumentado con diferentes casuísticas que pueden darse. Junto con un análisis organizacional, para atender al desarrollo y la implementación de la política de ciberseguridad, la generación de la múltiple y variada documentación a desarrollar, al objeto de resolver los incidentes que se produzcan. Así, poder comprender los diferentes roles en la organización, y diferentes situaciones que puedan darse.
- La exposición, análisis y diseño de las herramientas, que en materia de ciberseguridad se despliegan en una gran organización, basado en opiniones, casos de uso y experiencias con ellas. Describiendo de forma generalista los requerimientos fundamentales que deberá de cumplir el caso concreto de una instrumento de integración de herramientas de ciberseguridad. Esta deberá ser desarrollada en la organización o adquirida por la misma, si se quieren tener ciertas garantías de que se implementa adecuadamente la ciberseguridad y de que no se está derrochando capital, en soluciones que no solo no se integran, sino que dejan fisuras importantes en la seguridad de la organización.

3. Desarrollo

Es necesario reseñar que los datos aportados y contenidos en el presente ensayo son genéricos, con base en experiencias, análisis y estudios

del autor, refrendados con opiniones de especialistas en la materia, pero que, sin centrarse en ningún órgano en concreto, podrían extrapolarse a un gran número de administraciones o empresas de características similares, de forma total o parcial.

Todos los datos en los contenidos son de dominio público y accesible por las diferentes fuentes de información consultadas y referenciadas en el apartado correspondiente de la bibliografía.

Redes de una gran corporación

Para entender el mundo que abarca o, mejor dicho, sobre el que actuaría la ciberseguridad en el presente trabajo, lo primero que hay que delimitar es este, o, al menos, intentar que el mundo sea de alguna forma, tangible, medible, bajo ciertos parámetros, como mínimo, entendible, o reconocible por su estructura.

En el caso que nos compete, la red de la corporación se compondría a modo de ejemplo de:

- Una WAN de empresa distribuida en múltiples sucursales nacionales e internacionales.
- Conexiones a internet a través de un NODO frontera que hace de DMZ, estando esas conexiones contratadas a un proveedor de servicios.
- Interconexiones a otras empresas de un mismo holding, con las que comparte determinados servicios (intranet administrativa).
- Que dispone de tres CPDS propios, que actúan de respaldo entre sí.
- Realiza copias de seguridad sobre icloud privada e icloud pública.
- Tiene contratados servicios en icloud en modo SaaS.
- Emplea conexiones VPN con los empleados remotos.
- Tiene varias páginas web públicas para su negocio.
- Son unos cuarenta mil empleados en más de quinientas sedes.

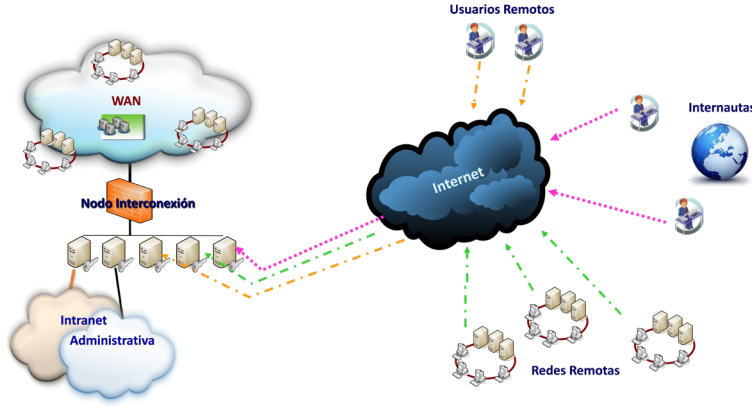


Figura 1. Red de una gran organización. Fuente: elaboración propia

En el desarrollo del TFM se abordan los siguientes puntos de interés:

- Políticas de ciberseguridad, su diseño y su implementación.
- Marco de gobernanza y estructuras.
- Órgano de dirección.
- Órganos de control y coordinación.
- Órganos de operación y resolución.
- Guías de gestión de la ciberseguridad.
- Herramientas de ciberseguridad, su diseño, su despliegue e integración.
- Herramienta de gestión integral.

Herramienta de gestión integral

Después de lo expuesto con anterioridad sobre la casuística de las múltiples herramientas en materia de ciberseguridad, que estando disponibles en el mercado podrán ser elegidas o no para dar la mejor solución posible, atendiendo a las necesidades y capacidades de cada organización, el lector de este TFM podría haberse preguntado ¿dónde está la herramienta maestra integradora?, es decir esa que le permite gestionar y controlar todas las demás y que puede implementar una organización para atender a sus necesidades.

Esa herramienta permitiría reducir la complejidad de tener que gestionar múltiples soluciones, aportarían resultados de manera independiente, pero no aprovecharían las acciones realizadas por las demás herramientas, y que podría contribuir a mejorar el resultado final, además de reducir costes en personal y equipos necesarios para el mantenimiento, y explotación de las múltiples herramientas.

Sin esta herramienta, el automatismo en acciones y reacciones para mitigar un ciberataque o asegurar los activos de la organización no existiría, salvo que la solución para la ciberseguridad esté implementada por una única firma o fabricante, que integre un gran número de campos de actuación, pero con el hándicap de no poder abarcar todos, al menos en la actualidad.

La situación actual es que los diferentes fabricantes y proveedores de herramientas están intentando abarcar la mayor parte de los campos de acción que se pueden identificar en la ciberseguridad de esta era. Y si bien es verdad que presentan posibles soluciones, a modo cuadro de control integral, que dirigen todas aquellas herramientas de su firma o empresa, además de asegurar que es totalmente compatible con la mayoría de las herramientas de la competencia, también es cierto que no existe ninguna que sea en realidad compatible y que pueda integrar al cien por cien las capacidades de todas las demás que se elijan en una organización si estas son de múltiples fabricantes.

La gran mayoría defiende que se pueden interconectar mediante enlaces API de código abierto, pero la realidad es que luego resulta que no es así, sino que hay que pagar por el desarrollo si se quiere que funcione a todo su potencial, y en muchos casos no siendo posible su propio desarrollo particularizado.

Es por ello que puede sentenciarse que, a fecha de hoy, no existe esa herramienta de gestión integral, pero que no cabe duda de que, a muy corto plazo, habrá múltiples fabricantes que si la ofrezcan, midiéndose su éxito por el grado de integración de herramientas y por el nivel de gestión ofrecido, sin importar la marca o fabricante que deba integrarse.

Para complementar esa herramienta en el caso de grandes corporaciones con despliegues en diferentes sedes y, sobre todo, con sedes internacionales, será necesario que pueda ingestar datos de plataformas que proporcionen juicios o partes de información o inteligencia, que permita variar el nivel de riesgo calculado, atendiendo a condicionantes particulares como pueden ser posibles catástrofes naturales, zonas de conflicto armado, o bajo tensiones políticas desestabilizantes, etc.

4. Conclusiones

Como parte final o colofón de este trabajo, se considera necesario exponer que el grado de consecución de los objetivos marcados al inicio del mismo, es, a criterio del autor, más que aceptable y satisfactorio, toda vez que la finalidad pretendida en este trabajo es totalmente didáctica, no requiriéndose por ello demostrar ninguna hipótesis, sino solamente divulgar conocimiento. Ello es así porque se han mostrado los requerimientos de ciberseguridad de una gran corporación y analizado los motivos de los que emanan, así como se ha mostrado la organización y la documentación a generar, todo ello perseguido en el objetivo primero.

Del mismo modo, lo señalado para el objetivo número dos relativo a la exposición, análisis y diseño de las herramientas necesarias a desplegar para implementar la ciberseguridad, ha quedado claramente conseguido, con numerosos argumentos y datos aportados en la elaboración del cuerpo propiamente dicho del TFM.

Por último, el objetivo número tres en el que se fijaba el revisar las diferentes estrategias a nivel del Estado, así como la revisión de parte de la legislación que en materia de ciberseguridad se está generando, igualmente parece más que acertado señalar que el objetivo ha sido cumplido, dado que se han recogido múltiples casos y se han analizado alguno de los más relevantes, como el reglamento europeo.

5. Consideraciones futuras

Todo lo descrito en el presente trabajo, son acciones del presente y que, sin lugar a dudas, tienen mucho de desarrollo, transformación y

aplicación en el futuro, pero a modo de inquietud personal o de motivación de los posibles lectores, cabría la posibilidad de preguntarse o de tratar de exponer en este apartado alguna reflexiones, sobre cómo afectará la ciberseguridad a los sistemas clasificados, o cómo afectara a sistemas desplegados en la nube versus a los que lo hagan *onpremise*, sin olvidarnos tampoco qué posibles consecuencias tendrá en las redes 5G, o en los prometedores sistemas que empleen la tecnología cuántica, aún relativamente en pañales.

6. Anexo. Estadísticas de ciberseguridad [2]

A continuación se muestran estadísticas y datos relevantes sobre ciberseguridad conocidos hasta 2020 en todo el mundo según la página www.websiterating.com. https://www.websiterating.com/es/research/cybersecurity-statistics-facts/

- El 85 % de las infracciones de seguridad cibernética son causadas por errores humanos.
- El 94 % de todo el malware se envía por correo electrónico (CSO en línea).
- Los ataques de ransomware ocurren cada 10 s.
- El 71 % de todos los ataques cibernéticos están motivados económicamente (seguidos por el robo de propiedad intelectual y luego el espionaje).
- 445 millones de ciberataques ocurrieron en 2020 a nivel mundial.
- Se estima que el costo global anual de la ciberdelincuencia será de 10.5 billones de dólares para 2025.
- Se estima que la industria de la ciberseguridad tendrá un valor de más de 400 mil millones de dólares para 2027.
- En 2021, la industria de la ciberseguridad tuvo una tasa de desempleo del 0 %.
- Más del 80 % de los eventos de ciberseguridad involucran ataques de phishing.
- Google descubrió más de 2.1 millones de sitios de phishing en enero de 2020.
- Hubo un ataque de ransomware cada 10 s en 2020.
- Durante la próxima década, el costo de los ataques de ransomware superará los 265 mil millones de dólares.
- 2020 vio la primera muerte conocida por un ciberataque relacionado con ransomware.
- En 2020, en promedio, se necesitaron doscientos siete días para identificar las brechas de seguridad informática.
- Marriott admite que una violación de seguridad en 2020 expuso los datos de al menos 5.2 millones de huéspedes.

- Más del 90 % del malware llega a través del correo electrónico.
- 1 de cada 36 teléfonos inteligentes Android tiene instaladas aplicaciones peligrosas.
- Hay 2.244 ciberataques por día y 164 ciberdelitos denunciados todos los días.
- Casi la mitad de todos los ciberataques se dirigen a pequeñas empresas.
- Las violaciones de datos expusieron 36 mil millones de registros a fines del tercer trimestre de 2020.
- Las brechas de ciberseguridad reducen el valor de las empresas públicas en un 8,6 % estimado.
- Una de las firmas de seguridad más grandes del mundo admite que fue víctima de un hackeo sofisticado en 2020.
- El 66 % de las empresas estuvieron expuestas al phishing en 2020.
- El 43 % de las pequeñas y medianas empresas (pymes) aún no han adoptado planes de mitigación y evaluación de la ciberseguridad.
- El 20 % de las pequeñas empresas permiten el trabajo remoto sin tener un plan de ciberseguridad.
- Los piratas informáticos robaron más de nueve millones de registros médicos en septiembre de 2020.
- Aproximadamente el 30 % de los trabajadores de la educación no aprobaron una prueba de phishing.
- Más del 40 % de los casos de ciberseguridad en la educación son causados por tácticas de ingeniería social.
- El 32 % de las empresas pagan un rescate para recuperar sus datos.
- Alrededor de sesenta millones de estadounidenses han sido afectados por el robo de identidad.
- Estados Unidos sufre la mayor cantidad de violaciones de datos por ubicación.
- 2.244 ataques ocurrieron todos los días que es casi un ciberataque cada 39 s.
- Rusia, Brasil y China son los tres principales países donde se originan los ciberataques.
- En promedio, toma alrededor de 280 días para detectar y detener un ciberataque.
- Hoy en día, las mejores técnicas de seguridad disponibles son el cifrado, antivirus, firewall, firmas digitales y autenticación de dos factores.
- Los aviones de combate F-35 enfrentan mayores amenazas de ciberataques que de misiles enemigos.

Agradecimientos

Al profesor Miguel Rodelgo Lacruz, en agradecimiento a su magistral dirección, sus acertadas correcciones y sugerencias, que han contribuido, sin lugar a duda, a proporcionarle mayor calidad y coherencia a este trabajo.

Referencias

España. (2022). Real decreto 311/2022, de 3 de mayo, por el que regula el ENS (Esquema Nacional de Seguridad). *BOE*, publicación 4 mayo 2022.

Web iterating. [En línea]. [Consulta: 16 diciembre 2022]. Disponible en: https://www.websitersting.com

La ciberseguridad y sus herramientas. Diseño, organización y despliegue, en las redes de una gran corporación.

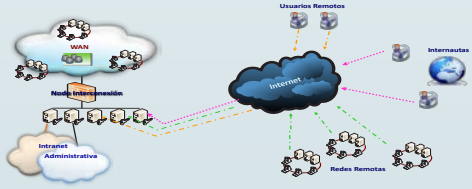
Autor: Ángel San José Arranz
Director: Miguel Rodelgo Lacruz
Universidad de Vigo

Introducción

El ciberespacio podría definirse, como la dimensión espacial creada mediante la interconexión de ordenadores y redes digitales por todo el mundo, pero que es algo que va más lejos aún incluso, de lo que algunos podrían estar identificando como Internet, dado que afecta además a leyes, normativas, procedimientos, organizaciones, países, personas, formas de uso e interacción, etc.

La ciberseguridad *(seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.*

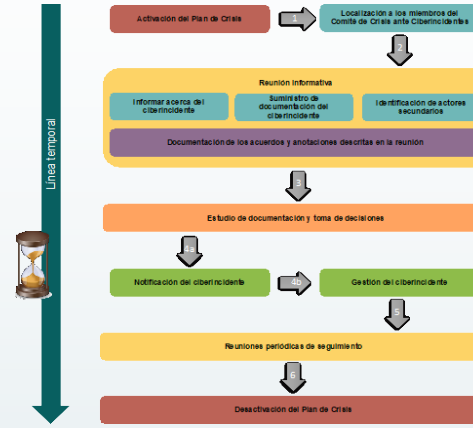
Elementos de análisis



- WAN de empresa en múltiples sucursales.
- Conexiones a Internet a través de una DMZ.
- Interconexiones de un mismo Holding.
- Dispone de 3 CPD,s propios interconectados.
- Copias de seguridad sobre icloud privada y pública.
- Contratados servicios en icloud en modo SaaS.
- Emplea conexiones VPN.
- Son unos 40000 empleados.
- Más de 500 sedes.

Herramientas

Plan de Crisis de una organización tipo.



Conclusiones

- La ciberseguridad en una organización, va mucho más allá de la mera implementación de ciertas herramientas o aplicaciones contratadas, sino que abarca también a la propia articulación del personal de la organización.
- Una herramienta de ciberseguridad, que en el futuro será fundamental tenerla desplegada, es la herramienta de gestión integral.
- La ciberseguridad y la ciberdefensa en una organización, deben actuar de forma conjunta y coordinada sin fisuras o divergencias.
- La legislación existente y la que está aún por desarrollarse, ya sea nacional o internacional, es un factor primordial para el éxito de la ciberseguridad.
- Una acción fundamental en materia de ciberseguridad que no debe ser pasada por alto, es la concienciación o formación del personal en dicha materia.

Datos en la actualidad

Se estima que el costo global anual de la ciberdelincuencia será de $ 10.5 billones para 2025.
Y que la industria de la ciberseguridad tendrá un valor de más de $ 400 mil millones para 2027.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

La cadena de custodia mediante *blockchain*

Autor: Diego Luis Santiago Gutiérrez (dlsantiago@guardiacivil.es)
Director: Luis Modesto Álvarez Sabucedo (lsabucedo@det.uvigo.es)

Resumen: – *Blockchain* es considerada una tecnología disruptiva que ofrece un nivel de madurez que permite dar soporte a nuevas aplicaciones de alto valor añadido en, prácticamente, cualquier sector de la sociedad. Sus implicaciones, que superan y trascienden la dimensión tecnológica, afectan a los modelos sociales existentes, adentrándose en el campo jurídico. Este ámbito, que requiere de complejos mecanismos que garanticen aspectos tan relevantes como los derechos fundamentales y las libertades públicas, puede beneficiarse de su potencial; pese a ello, su verdadera capacidad transformadora se encuentra aún por explorar debido a la carencia de soluciones concretas.

Este trabajo explora dicho potencial en una aplicación concreta: el aseguramiento de la cadena de custodia de cualquier evidencia de una investigación. *Blockchain* permite garantizar su trazabilidad, el registro de acciones, su integridad, unicidad y disponibilidad, sin necesidad de un tercero confiable. Este paradigma podrá aportar elementos de prueba altamente fiables, cuestión de suma importancia en el ámbito penal. Su aplicación requiere valorar multitud de opciones de diseño e implementación.

Blockchain engloba gran cantidad de modelos y protocolos específicos con diferencias tan notables que resulta obligatorio estudiarlos y analizarlos de manera minuciosa. De este modo, es posible seleccionar aquel que cumpla con los requisitos mencionados, permitiendo establecer un modelo que se adapte a las exigencias de un Estado de derecho y a las necesidades de la Guardia Civil. Además, se analizan los casos de uso que habrán de satisfacerse para que hagan de la propuesta una herramienta válida que dé soporte a la cadena de custodia.

Palabras clave: – *Blockchain*, Evidencia, Cadena de custodia, EBSI, REST.

1. Introducción

Motivación

La Ley de Enjuiciamiento Criminal, aprobada mediante real decreto de 14 de septiembre de 1882. Esencia de la garantía judicial en el proceso penal, no regula de manera explícita los requisitos que ha de tener la cadena de custodia en este ámbito. Sin embargo, sí se encuentra una primera alusión en su artículo 13 [1]: «Se consideran como primeras diligencias la de consignar las pruebas del delito que puedan desaparecer, la de recoger y poner en custodia cuanto conduzca a su comprobación y a la identificación del delincuente [...]».

Estas primeras diligencias constituyen el inicio de la cadena de custodia, puesto que ya se mencionan las pruebas que se pueden obtener y a su custodia, algo que en última instancia permitirá averiguar el delito y descubrir y asegurar el delincuente [2].

Asimismo, se alude a este procedimiento de manera implícita en los artículos 326, 334, y 338, en los que se dice respectivamente lo siguiente [1]:

> «Cuando el delito que se persiga haya dejado vestigios o pruebas materiales de su perpetración, el Juez instructor [...] ordenará que se recojan y conserven para el juicio oral si fuere posible, procediendo al efecto a la inspección ocular y a la descripción de todo aquello que pueda tener relación con la existencia y naturaleza del hecho.
>
> A este fin, hará consignar en los autos la descripción del lugar del delito, el sitio y estado en que se hallen los objetos que en él se encuentren, los accidentes del terreno o situación de las habitaciones y todos los demás detalles que puedan utilizarse [...]».
>
> «El Juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que este se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida. El secretario judicial extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.

La diligencia será firmada por la persona en cuyo poder fueren hallados, notificándose a la misma el auto en que se mande recogerlos».

> «[...] los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad

> y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito».

En esta segunda parte del texto normativo se detalla con mayor profundidad el proceso de cadena de custodia, en el sentido de que se ha de recopilar todo aquello que guarde relación con la prueba, de manera que se pueda asegurar en todo momento cuál es su estado y cómo ha variado hasta que la prueba es puesta a disposición de la autoridad judicial.

Por su parte, y en el ejercicio de sus competencias, la Sala de lo Penal del Tribunal Supremo, al no estar regulado explícitamente y al poder generarse incertidumbre al respecto, en su sentencia 208/2014, de 10 de marzo, considera que [3]:

> «Se viene entendiendo por la doctrina como «cadena de custodia» el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba».

De esta manera, el Tribunal Supremo, como órgano jurisdiccional superior en el territorio nacional, ha determinado, ante la falta de concreción de la Ley de Enjuiciamiento Criminal, esta definición de cadena de custodia, que sirve para establecer un criterio a la hora de materializarlo.

Tras realizar un breve análisis de los aspectos normativos y jurisprudenciales del concepto de cadena de custodia, puede observarse que en ningún momento se hace referencia a que esta pueda realizarse digitalmente. Sin embargo, por analogía, se trata de un concepto, como otros muchos, que puede extrapolarse a otros ámbitos, en este caso, el digital.

En la práctica, al ser compatibles y proporcionar una mayor garantía y seguridad en relación con la custodia de evidencias, en España se tienen dos tipos de cadena de custodia, que se emplean de forma simultánea: la cadena de custodia física y la cadena de custodia digital. En la primera, que se lleva a cabo físicamente, se refleja toda la información de los hechos en formato papel; en la segunda, en formato digital, se exponen los extremos de la cadena de custodia física en un documento electrónico.

Sin embargo, estos dos tipos de cadena de custodia tienen un claro componente subjetivo, pues toda acción que se lleva a cabo depende exclusivamente de las personas. Esto supone que se puedan dar errores y no exista una seguridad absoluta. Por todo ello, se hace necesario contar con un modelo que sea capaz de soslayar esos errores y que incremente la seguridad de la información relativa a las evidencias. Como se ha expuesto con anterioridad, la tecnología *blockchain* puede dar respuesta a esta problemática.

Por tanto, la motivación de este trabajo es establecer un modelo de cadena de custodia basado en tecnología *blockchain* con el que la Guardia Civil pueda garantizar la trazabilidad, integridad, unicidad y disponibilidad de las evidencias, tanto físicas como digitales, recogidas en el marco de las investigaciones que sus unidades y miembros lleven a cabo, teniendo en cuenta, en todo momento, lo que la legislación vigente y la jurisprudencia disponen.

2. Objetivos

En consonancia con la motivación anterior, puede formularse el objetivo de alto nivel de diseñar una plataforma holística que dé soporte para que se lleve a cabo una adecuada gestión de la cadena de custodia mediante el uso, si así resulta conveniente, a la luz del análisis previo, de la tecnología *blockchain*.

Se han planteado, para su consecución, los siguientes objetivos:

- O1: estudiar, debido a su relevancia en un Estado de derecho, el marco legal y jurídico de la cadena de custodia tanto de forma general como desde el punto de vista de la tecnología blockchain.
- O2: analizar la tecnología subyacente tras el modelo que se pretende establecer.
- O3: proponer un modelo de plataforma que ofrezca los servicios necesarios para la adecuada gestión de la cadena de custodia.

3. Modelo propuesto

Introducción

Tras el análisis realizado sobre la tecnología de las *blockchains* de Bitcoin, Ethereum y Hyperledger (Fabric y Besu), y teniendo en cuenta la confianza de las instituciones de la Unión Europea en la tecnología *blockchain*, se ha podido comprobar que la infraestructura de EBSI puede resultar una opción interesante si se quiere implementar la cadena de custodia con las debidas garantías y el respaldo de la Unión Europea.

Por ello, se ha propuesto un modelo de cadena de custodia basado en la tecnología *blockchain* empleando EBSI, como infraestructura de confianza al servicio de los Estados Miembro de la Unión Europea que proporciona un «ecosistema seguro e interoperable».

Infraestructura

La red está formada por diversos nodos físicos que se encuentran en los referidos Estados Miembro y que se corresponden, a su vez, con un nodo de la *blockchain*. Adicionalmente, se cuenta con una base de datos distribuida, accesible desde todos estos nodos.

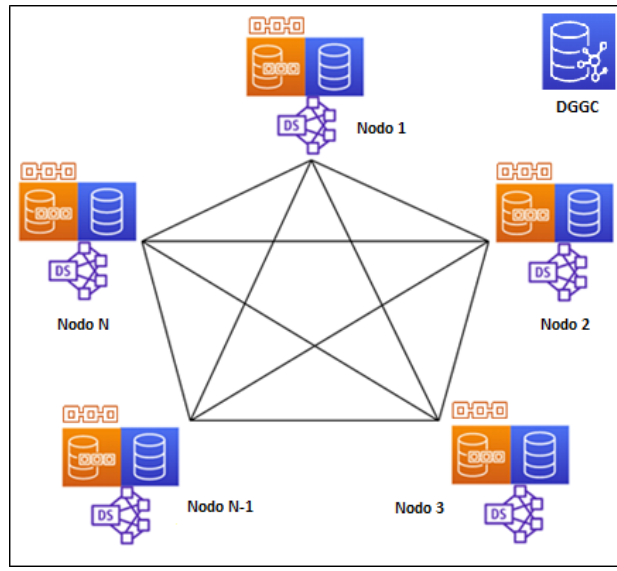


Figura 1. Arquitectura de implementación de la cadena de custodia

Al utilizar la infraestructura de EBSI, se asume implícitamente el empleo del algoritmo de consenso de *Proof-of-Authority* (PoA). Con él, los nodos del sistema seleccionarán a los nodos validadores en función de su identidad y de su reputación.

Los contratos inteligentes que se han de emplear deben asegurar que la información enviada a través de la API sea grabada correctamente y de manera confiable en la infraestructura.

Funcionamiento

En primer lugar, el agente de la policía judicial debe identificarse con una cuenta acreditada, que le permite acceder a través de un *token* válido de acceso. Una vez se haya autenticado, puede efectuar llamadas a la API REST a través de la aplicación diseñada.

El agente utiliza el modelo propuesto para llevar a cabo las diferentes acciones sobre la evidencia. Para ello, a través de la API REST, se solicita realizar una transacción al contrato inteligente. Esta, que debe ser previamente autorizada mediante el *token* de acceso y firmada por el agente, ha de ser verificada por el contrato inteligente que subyace tras la interfaz, incluyéndose en un bloque candidato. Cuando exista acuerdo entre los nodos validadores, se incorpora dicho bloque, quedando insertado en la *blockchain*, junto con los metadatos de la petición y el *hash* de la evidencia.

Por otro lado, se cuenta con la propia evidencia (digital o física —digitalizada—) y su cadena de custodia. La información relativa a estas dos figuras, de forma paralela y automática, se almacena en la base de datos distribuida mencionada con anterioridad.

Diseño

La interfaz debe ser consecuente con las acciones —y al menos permitir materializarlas— que se llevan a cabo en el proceso de la cadena de custodia tradicional y dar soporte técnico para su ejecución en el ámbito de la *blockchain*.

Para definir estas acciones en el modelo se han de tener en cuenta: la evidencia en cuestión, su cadena de custodia y sus registros o *records*, y la investigación en la que se enmarca, así como las personas que intervienen en el proceso. De esta manera, se tienen las siguientes figuras:

- La figura principal es la investigación, pues en ella se enmarcan todas las actuaciones que se realicen, las personas que intervengan y las evidencias que se hallen.
- La investigación es llevada a cabo por una unidad de policía judicial, que está integrada por diversos agentes. Los integrantes de este tipo de unidades, siempre que resulte pertinente, pueden realizar cualquier actuación con una evidencia en el marco de la investigación.
- Además de los agentes de policía judicial, se encuentran dos figuras de gran relevancia en las investigaciones: la autoridad judicial y, en caso de que el hecho delictivo se le haya imputado a alguien, la defensa.
- Por otro lado, se hallan las figuras de la evidencia y de su cadena de custodia, junto con los records de esta última. Toda evidencia es objeto de distintas actuaciones, de las que se debe dejar constancia en su cadena de custodia a través de sus records.

Teniendo en cuenta lo anterior y las acciones que se pueden llevar a cabo, en la figura siguiente se muestran los casos de uso existentes en el modelo propuesto:

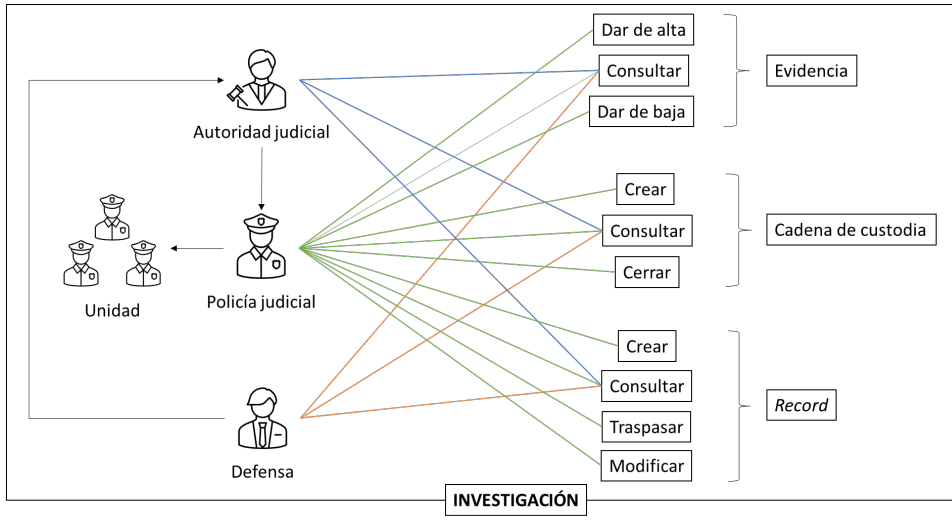


Figura 2. Casos de uso del modelo

En la figura puede observarse que, sin perjuicio de las consultas que pueden realizar tanto la autoridad judicial como, en su caso, la defensa sobre la evidencia y su cadena de custodia, de acuerdo con la legislación vigente, un agente puede dar de alta una evidencia, consultarla y darla de baja, y, además, crear su cadena de custodia, consultarla y cerrarla, así como crear, consultar y modificar los diferentes *records* de esta última y traspasar una evidencia.

Asimismo, para desarrollar la prueba de concepto, resulta imprescindible diseñar previamente el modelo. Este diseño, parcial, cubre cuatro de los casos de uso del modelo: dar de alta una evidencia y crear su cadena de custodia, y consultar tanto la evidencia como la cadena de custodia.

En primer lugar, se han de definir las características de la evidencia y de la cadena de custodia, las relaciones entre ambas y los métodos que se utilizarán, así como los *endpoints*.

Una vez se han definido, se procede a dar de alta la evidencia. Se inserta, así, un recurso denominado *evidence*, mediante una petición POST, en cuyo *body* se incluyen tanto los metadatos relativos a la evidencia como la propia evidencia o, en caso de ser una evidencia física, una versión digitalizada de esta:

POST /v1/evidence

Para consultar la información de la evidencia, se utiliza el método GET y se introduce el identificador asignado a la evidencia mediante el método anterior:

GET /v1/evidence/{id}

El siguiente paso es crear la cadena de custodia. En este caso, la información necesaria, incluida en el *body*, es el identificador de la evidencia, la fecha y el lugar de recogida, el agente interviniente, la unidad, la actuación realizada y las observaciones. De este modo, se crea un recurso denominado *custody_chain*, que está asociado a una evidencia, mediante una invocación con el método POST:

POST /v1/custody_chain/{id}/evidence

En último lugar, se puede realizar la consulta de la cadena de custodia indicando únicamente su número. El método empleado en este caso es GET:

GET /v1/custody_chain/{id}

4. Conclusiones

La eficacia procesal constituye un aspecto fundamental en la jurisdicción penal. Esta afirmación implica que aspectos como la cadena de custodia adquieran una importancia significativa para asegurar el normal

funcionamiento de esta jurisdicción, sobre todo en lo que respecta a la garantía de los derechos fundamentales y libertades públicas de las personas que se hallan implicadas en el proceso.

En la actualidad, la cadena de custodia se lleva a cabo de forma elemental y básica, desde un punto de vista tecnológico. En esencia, se emplean simultáneamente la cadena de custodia física —en formato papel— y la cadena de custodia digital —en documento electrónico, pero con los extremos de la cadena de custodia física—, dependiendo en última instancia del buen hacer y de la buena fe de las personas que participan en su elaboración o gestión.

La constante evolución de las tecnologías de la información y las comunicaciones, así como la digitalización de la sociedad y de la Administración Pública, han creado el ambiente y la situación propicios para que puedan plantearse nuevos escenarios para las figuras legales tradicionales, como la cadena de custodia.

Para ello, las diferentes formas de implementación de la cadena de custodia mediante tecnología *blockchain* hacen que sea necesario realizar un profundo estudio que dirima cuáles son las óptimas. Así, a través del análisis de la tecnología efectuado en este documento y teniendo en cuenta el respaldo de instancias europeas, se ha optado por emplear la infraestructura EBSI en el modelo propuesto. Esto ofrece al mundo de la investigación y a la cadena de custodia un nuevo paradigma, caracterizado por la descentralización, la escalabilidad y la confianza, así como por el estricto cumplimiento de las normas europeas.

Asimismo, EBSI posibilita que cada usuario que interaccione con la red esté debidamente identificado y autenticado, asegura la trazabilidad y el registro de acciones sobre las evidencias, su integridad, unicidad y disponibilidad, lo que garantiza una gestión adecuada de la cadena custodia a través de una única aplicación. De esta manera, se logra una mayor eficiencia y seguridad, además de que la información esté validada y sea inmutable, es decir, que no resulte posible su alteración o supresión tanto legítima como ilegítimamente.

Otra cuestión importante es la redundancia, pues, gracias a este sistema distribuido, se asegura que la información esté duplicada en cada nodo, haciéndola resistente a fallos y ciberataques. Asimismo, en caso de que el sistema no funcione correctamente o se produzca su desconexión por cualquier motivo relacionado con alguno de los nodos de la red, este puede continuar operando sin dificultad alguna, lo que le hace gozar de una mayor seguridad frente a ataques.

La simplicidad y ligereza de REST, así como la flexibilidad que proporciona en la integración de aplicaciones, ha hecho que se opte por este tipo de API en el modelo propuesto. Esta interfaz se convierte en un elemento clave, ya que permite realizar sobre una evidencia, a través de los métodos

diseñados, toda acción que se ha de llevar a cabo en la cadena de custodia tradicional.

Por otro lado, la cadena de custodia implementada mediante blockchain facilita al investigador la gestión de las evidencias, evitando los errores y accesos no autorizados que deriven en la comisión de ilícitos penales o en la vulneración de derechos fundamentales, sin perjuicio de la responsabilidad disciplinaria en que pudieren incurrir.

Por todo ello, y gracias a este modelo, se facilita la labor diaria de los investigadores, que pueden centrar su esfuerzo en los aspectos formales y operativos de la investigación, en lugar de tener una constante preocupación por las cuestiones burocráticas de la cadena de custodia. Además, la seguridad (confidencialidad, integridad y disponibilidad), característica de trascendental importancia en lo que respecta a la información, así como el cumplimiento de la legislación vigente europea y estatal, se garantizarán en todo momento.

Referencias

Cortes Generales. (1978). Constitución española. *BOE*, n.º 311.

Gobierno de España. (2022). EBSI: la infraestructura europea de blockchain en marcha [en línea]. *Portal de la Administración Electrónica*. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2022/Abril/Noticia-2022-04-08-EBSI-la-infraestructura-europea-de-blockchain-en-marcha.html

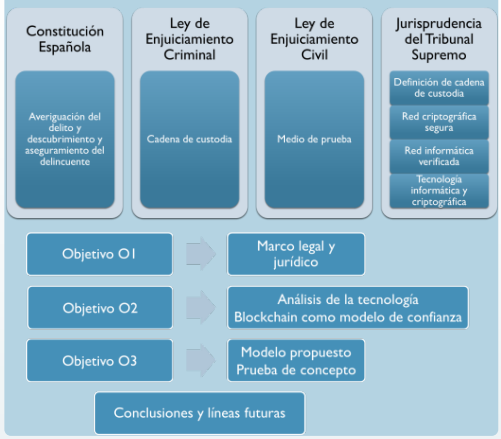
Ministerio de Gracia y Justicia. (1882). Real Decreto de 14 de septiembre de 1882, por el que se aprueba la Ley de Enjuiciamiento Criminal.

Tribunal Supremo. (2014). Sentencia del Tribunal Supremo 208/2014. Sala de lo Penal), de 10 marzo de 2014. Recurso 836/2013.

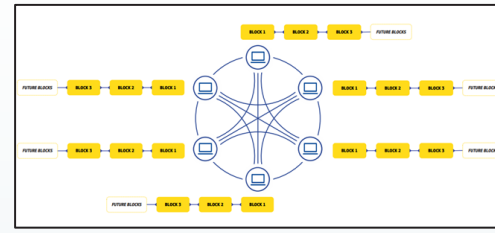
La cadena de custodia mediante tecnología Blockchain

Autor: Diego Luis Santiago Gutiérrez
Director: Luis Modesto Álvarez Sabucedo
Universidad de Vigo

Introducción



Blockchain como modelo de confianza



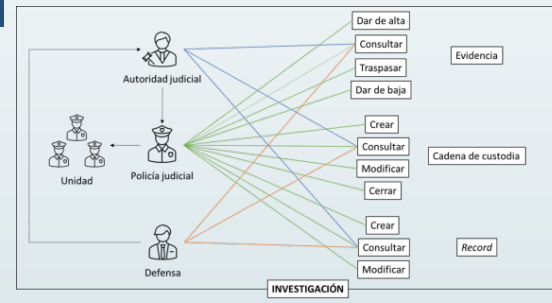
Fuente: European Comission, «European Comission» [En línea]. Disponible en: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/.

European Blockchain Services Infrastructure

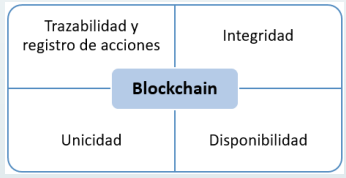
Infraestructura basada en tecnología Blockchain al servicio de los Estados miembro de la Unión Europea.

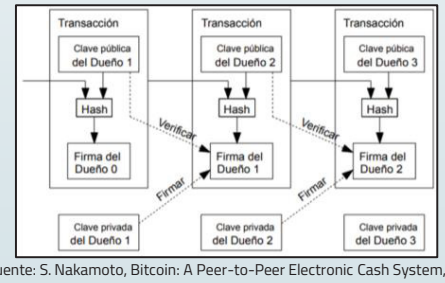
Ecosistema seguro e interoperable.

Modelo propuesto

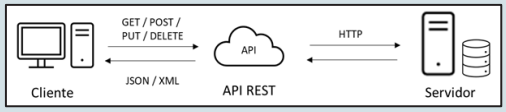


Análisis de la tecnología





Fuente: S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.



Conclusiones y líneas futuras

Conclusiones

- EBSI: respaldo de instancias europeas y cumplimiento normativo.
- API REST: simplicidad, ligereza y flexibilidad

Líneas futuras

- Implementar el modelo completo
- Incorporar oráculos

Agradecimientos

A mi madre.

Trabajos fin de máster

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Análisis de riesgos de la Red de Asistencia al Personal (RAP) del Ministerio de Defensa

Autor: David Alvarez Lanzarote (dalvalan@hotmail.com, lanzarote@et.mde.es)
Directores: Iago López Román (iago.lopez.roman@gmail.com) y
Rubén Nocelo López (rubennocelo@cud.uvigo.es)

Resumen: – El proyecto de Red de Asistencia al Personal comienza en 2018 con el fin de proporcionar un acceso a internet de calidad y protegido al personal de nuestras Fuerzas Armadas, tanto en instalaciones militares en territorio nacional, como cuando está participando en las distintas misiones en el exterior.

Estos servicios de internet seguro se proporcionan principalmente en emplazamientos donde existen dificultades para acceder por otros medios, o donde las situaciones de seguridad de la zona así lo aconsejan. Por ello, una de sus premisas de diseño inicial es la seguridad y protección de los servicios proporcionados. De este modo, se contribuye a la propia seguridad de las operaciones y del personal militar desplegado en el exterior. Para conseguirlo, todo el tráfico de navegación y servicios de valor añadido pasan primero por una infraestructura central de gestión y supervisión centralizada del sistema ubicada en CESTIC (Madrid) antes de conectarse a internet a través de una serie de dispositivos y mecanismos de seguridad.

En la actualidad, esta infraestructura de comunicaciones se extiende desde el Nodo Central de Gestión en el CESTIC hasta las principales misiones de las Fuerzas Armadas españolas en el exterior, buques de la Armada, y cerca de doscientas cincuenta bases, acuartelamientos y arsenales militares dentro del territorio nacional, con el fin principal de mejorar la calidad de vida del personal alojado en los mismos.

Si bien, como se ha dicho, una de las premisas de diseño de toda las TIC de este sistema es la de la seguridad, todavía no se ha realizado un análisis de riesgos de este, ni dispone de un plan de tratamiento de riesgos, ni una declaración de aplicabilidad (SOA). Sin embargo, por la complejidad y extensión de esta red, el presente documento se ceñirá en el análisis de riesgos.

Es por ello por lo que el trabajo, además de su utilidad académica, se considera de utilidad práctica de cara a la evolución y mejora del sistema.

Palabras clave: – Rap, Ens, Maguerit, Pilar, Seguridad.

1. Introducción

Una de las premisas principales del diseño de la Red de Asistencia al Personal del Ministerio de Defensa, es precisamente garantizar unas condiciones de seguridad en el uso de internet por el personal militar que está desempeñando sus cometidos en las distintas misiones de las Fuerzas Armadas en el exterior. Así pues, la seguridad es un aspecto que se ha tenido en cuenta de forma constante desde su concepción. Sin embargo, esta red es un tanto peculiar en el sentido de que, tratándose de una red corporativa de Ministerio de Defensa, por su naturaleza, función y tipo de interconexión con internet, puede procesar información sin clasificar de uso público exclusivamente.

No obstante, y de acuerdo con lo especificado en el artículo 2 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad [1], se trata de un sistema de información del Ministerio de Defensa, por lo que se considera que se aplica, a pesar de que no trata información clasificada, pero que precisa adoptar medidas complementarias de seguridad, específicas para dicho sistema.

Dado el interés que despertó en mí la materia de Gestión de la Seguridad y Análisis de Riesgos del presente máster, la consideré de mucha utilidad para los cometidos que estaba desempeñando por entonces en el CESTIC como responsable del contrato por el que se había iniciado en 2018 el Proyecto de la Red de Asistencia al Personal Militar en Zona de Operaciones (SAPZO), una de las dos partes principales de la infraestructura que pasó a denominarse Red de Asistencia al Personal (RAP) del Ministerio de Defensa.

2. Desarrollo

El trabajo se ha desarrollado siguiendo la siguiente secuencia:

- Recopilación de información referente a la RAP: para ello ha sido necesario estudiar todos los detalles de diseño y arquitectura de este sistema de información. Asimismo, se ha entrevistado a personal responsable de su gestión y administración de seguridad, con la finalidad de conocer detalles de su evolución, estado actual para valorar la madurez de la seguridad de este, y planificar si futuro desde el prisma de la seguridad.
- Estudio de la normativa en vigor, empezando por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad [1], y documentación referente a MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [2]. También las principales guías CCN-STIC relacionadas con la aplicación del ENS.
- Obtención, instalación y estudio del manejo de la aplicación PILAR del CCN, destinada a llevar a cabo todo el proceso de análisis y ges-

tión de riesgos que permite dicha herramienta. También fue preciso mantener una reunión con personal conocedor de la herramienta para recibir consejos prácticos sobre su uso.

— Carga de información en el sistema, siguiendo el proceso lógico de un análisis de riesgos.
— Analizar los resultados obtenidos tras completar este proceso de análisis y gestión de riesgos.
— Extraer todas las conclusiones como consecuencia del trabajo realizado, identificando aquellos aspectos en los que se podría seguir trabajando para mejorar y ampliar el TFM.

Descripción de la Red de Asistencia al Personal del Ministerio de Defensa

Los servicios de asistencia al personal tienen por finalidad mejorar la conectividad a internet del personal en las zonas de vida de las Bases, Acuartelamientos y Establecimientos militares (BAE) del Ministerio de Defensa.

En ningún caso se trata del acceso mediante tecnología wifi a una red corporativa. De hecho, de acuerdo con la arquitectura prevista, la infraestructura está caracterizada por la separación física (*air gap*) de esta infraestructura de cualquier otra infraestructura de red del emplazamiento.

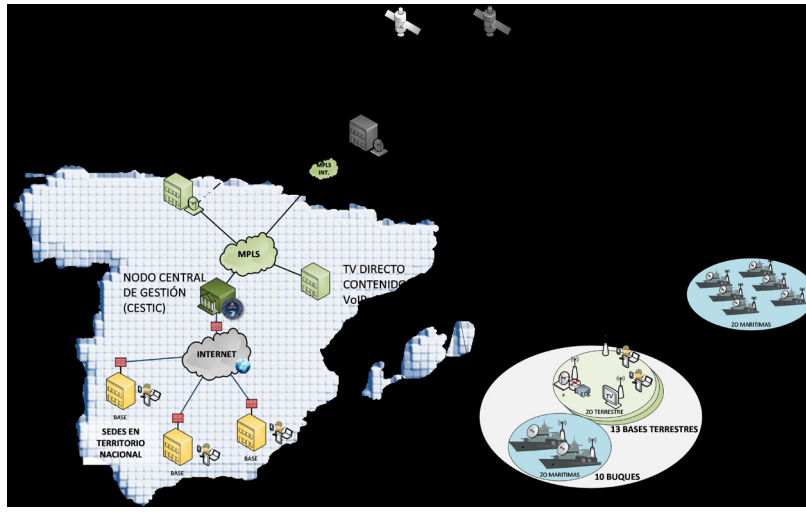


Figura 1. Alcance de la red de asistencia al personal del MDEF

Dichos servicios se proporcionan sobre la infraestructura *hardware* y *software* de la Red de Asistencia al Personal (RAP). La misma aúna dos infraestructuras distintas como consecuencia de los dos entornos operativos en los que se despliega que llevan asociados unos requisitos de seguridad diferentes.

— El Sistema de Asistencia al Personal Militar desplegado en Zona de Operaciones (SAPZO). Abarca bases terrestres en operaciones en el exterior y buques de la Armada que participan en distintas misiones internacionales.

  Por la naturaleza de estos escenarios, es muy probable que sea difícil disponer de un acceso a internet de calidad y que garantice unas condiciones mínimas de seguridad, teniendo en cuenta el riesgo que puede suponer el uso de infraestructura de telecomunicaciones locales.

  Además del acceso protegido a internet, se proporcionan otros servicios de valor añadido, con el fin de mejorar las condiciones de vida del personal desplegado:

  - Una serie de canales de TV en directo con una parrilla de contenidos exclusiva para el Ministerio de Defensa.
  - Contenidos de entretenimiento, principalmente películas y series de actualidad, así como cursos de idiomas, a los que se puede acceder bajo demanda.
  - Servicio de telefonía IP con numeración geográfica española, con la finalidad de facilitar el contacto con familiares y facilitar la realización de gestiones administrativas privadas desde la distancia.

  Todos estos servicios se proporcionan sobre una infraestructura de telecomunicaciones exclusiva para este sistema para así maximizar la confidencialidad y disponibilidad de las comunicaciones privadas. El enlace entre sedes remotas y el CESTIC se hace vía satélite gubernamental en banda X, lo que permite una mejor conectividad en los principales buques de la Armada al aprovechar el excedente de capacidad que tienen los terminales navales de mayor tamaño. En el caso de que el terminal en banda X embarcado tenga menos prestaciones, se recurre a un acceso a vía satélite comercial de alta velocidad en banda Ka civil Inmarsat Global Express (IGX).

— La Red WIFI de Asistencia al Personal Militar en Territorio Nacional (RAPNA). En este caso, sin dejar de lado el aspecto de seguridad, el objetivo es el de poder proporcionar un acceso a internet al personal en las zonas de descanso y vida de las bases, acuartelamientos y arsenales. La complejidad en este caso se encuentra en el número de usuarios, actualmente cerca de cincuenta mil, lo que requiere una alta exigencia en términos de disponibilidad del sistema.

  Aunque en el momento de creación de las dos redes en 2018, estas se concibieron como dos dominios diferenciados en cuanto a arquitectura de red y servicios proporcionados, enseguida se interconectaron sus infraestructuras en un único nodo central de gestión, ubicado en las instalaciones del CESTIC, en Arturo Soria, donde se lleva a cabo una gestión integral de todo el sistema.

Tras más de tres años en funcionamiento y constante evolución y mejora de su arquitectura, antes de acometer el análisis de riesgos del sistema, ya se intuía que había un alto grado de madurez en la seguridad del sistema como consecuencia de que en este tiempo se ha puesto en funcionamiento:

- Un equipo de personas responsables de la gestión y administración del sistema.
- Un centro de atención al usuario, incluyendo una Instrucción Operativa para Gestión de Incidencias y Peticiones de la RAP (IOP) [3], a través del Sistema de Gestión de Peticiones e Incidencias (SCANS) ya implantado en CESTIC para abordar todos los aspectos de atención de los usuarios de los distintos sistemas de su responsabilidad.
- Una normativa detallada de gestión de todo el sistema en todos los aspectos: operativos, logísticos, de formación [4].
- Se han realizado varias auditorías de seguridad en distintas sedes tanto en la geografía española, como en bases en zona de operaciones y buques. Las vulnerabilidades observadas se han ido corrigiendo de forma progresiva.
- Se dispone de la financiación necesaria para contratar todos los servicios de soporte necesarios, así como para incorporar personal externo para reforzar al equipo responsable de la administración del sistema.
- Periódicamente se imparten cursos de formación y actualización de conocimientos adaptados a las particularidades del personal que ocupa puestos relacionados con la administración, gestión y supervisión del sistema de distintas partes de la infraestructura de la RAP.

El proceso de análisis de riesgos

Este proceso comprende la identificación de activos informáticos, las vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de estas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. De este modo, nos permitirá determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema de información analizado, e implantar sus salvaguardas o contramedidas.

La RAP es un sistema de información del MDEF y como tal se le debe aplicar el Marco Operacional del ENS, constituido por las medidas a tomar para proteger la operación de dicho sistema como conjunto integral de componentes con la finalidad de facilitar un acceso a internet al personal del Ministerio dentro de sus instalaciones, tanto en TN como en ZO.

Para poder medir el nivel de cumplimiento del ENS, como se ha expresado anteriormente, se hará uso de la aplicación PILAR del CCN, que siguiendo

la metodología Magerit [2], nos ayuda a la adecuación de dicho nivel de cumplimiento. Una vez que se analizan las dimensiones de seguridad de la RAP, en el siguiente paso se abordará una evaluación de riesgos, una declaración de aplicabilidad (las medidas que se deberán tener en cuenta) y el perfil de cumplimiento que especificará la configuración de seguridad de las medidas incluidas en la declaración de aplicabilidad.

Pero antes que nada es preciso identificar la categoría de la RAP dentro del ENS, valorando el impacto que tendría un incidente que afecte a la seguridad de la información y el propio sistema. Para determinarlo, hay que tener en cuenta las dimensiones de la seguridad de sus activos, principalmente los esenciales que suelen ir asociados a la información y servicios del sistema. Tras el proceso que se describe en detalle en el TFM se llega a la conclusión de que la RAP se trata de un sistema de información de categoría media, lo que, de acuerdo con el anexo II del ENS 2022 [1], nos impone la aplicación de unos controles de seguridad concretos. Entre otros, la necesidad de realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. No obstante, en el TFM se ha realizado un análisis formal con la finalidad principal de conocer mejor las posibilidades que ofrece la herramienta.

Tras seguir una secuencia de carga de información, guiados por la herramienta, llegaremos a los primeros resultados que reflejan el índice de madurez del sistema en las distintas fases que hemos marcado en el proyecto inicial en el momento que se pusieron en servicio las primeras sedes en octubre de 2019 con una infraestructura precaria, actual, fechado en diciembre de 2022, y objetivo, estableciendo en diciembre de 2025 la fecha tope de duración del contrato en vigor.

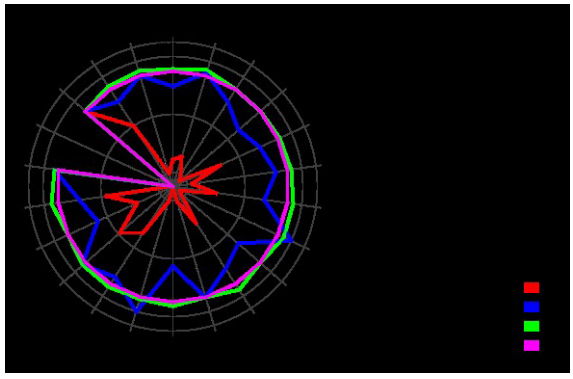


Figura 2. Nivel de aplicación de las medidas de seguridad

Figura 3. Índice de madurez y de cumplimiento del ENS del sistema

En la imagen se aprecia que actualmente, línea azul, hemos aplicado medidas de seguridad incluso por encima del nivel exigido por el propio ENS porque así lo he considerado necesario. Del mismo modo, ya nos orienta

hacia qué controles y tipos de protección debemos dedicar el esfuerzo por incrementar la seguridad del sistema.

3. Resultados y discusión

Llegados al apartado de informes, la herramienta facilita algunos que he encontrado de mucha utilidad como es el de valoración del cumplimiento del anexo II del ENS en el que se refleja la evaluación de cada uno de los controles que son de aplicación, de acuerdo con la declaración de aplicabilidad que hemos obtenido en el paso previo.

Para cada uno de ellos incluye un gráfico de rosa de los vientos que facilita la identificación de las medidas de seguridad que requieren mayor atención para alcanzar el nivel especificado por el ENS para el sistema, además de reflejar la evolución de la seguridad desde las fases previas del proyecto.

Como consecuencia de un análisis detallado del mismo, se llegan a identificar aquellas medidas de seguridad reflejadas en el punto siguiente, las cuales requieren de especial atención para mitigar el impacto y riesgo de las amenazas.

4. Conclusiones

A partir de los resultados obtenidos del análisis de seguridad, se observa que la RAP goza de buena salud, desde el punto de vista de la seguridad, teniendo siempre en consideración de que se trata de un sistema ENS medio como consecuencia de la valoración de sus activos e información a proteger.

Pero este grado de madurez no es fortuito, sino que, de forma indirecta, y gracias a la experiencia previa en el despliegue de sistemas de naturaleza similar, se habían exigido al contratista requisitos de seguridad que precisamente se encuentran recogidos dentro del conjunto de medidas de seguridad exigidas por el ENS 2022.

No obstante, con ocasión del comienzo del nuevo contrato de servicios de la RAP, que entró en vigor en diciembre 2022, con una duración máxima de tres años, se deberán aplicar las medidas de seguridad que se han identificado en este TFM:

- En relación con los procedimientos de seguridad, en la Norma de Gestión de la RAP [5] se incluirá un nuevo anexo con este mismo título en el que se refleje:
  - Cómo identificar y reportar comportamientos anómalos.
  - La forma en que se ha de tratar la información relativa a la gestión de la RAP, precisando cómo efectuar su control de acceso, almacenamiento, la realización de copias, el etiquetado de soportes,

su transmisión telemática empleando la herramienta de seguridad EP880 y cualquier otra actividad relacionada con dicha información.

- En la misma Norma de Gestión, se establecerá un proceso formal de autorizaciones que cubra todos los elementos de la RAP, abarcando la entrada de equipos, aplicaciones en producción, así como el establecimiento de enlaces de comunicaciones con otros sistemas.

— Sobre la base de la información introducida en la aplicación PILAR para la elaboración del análisis de riesgos objeto de este TFM, se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida.

— Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

— Se contratarán servicios de comunicaciones vía satélite LEO (por ejemplo, Starlink, con la que ya existe contacto) como vía alternativa y de alta capacidad a la comunicación vía satélite que da soporte a la comunicación. Ello mejorará la supervivencia del sistema, a la vez que tendrá un impacto muy positivo en la experiencia de uso del sistema.

— Se deberá redactar un documento de descripción de los deberes y responsabilidades en materia de seguridad de cada puesto de trabajo asociado a la RAP.

— Por parte del responsable de seguridad del sistema, periódicamente se impartirán charlas de concienciación al personal administrador del sistema acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

— Del mismo modo, se distribuirá, de forma periódica, entre los usuarios de la RAP y se hará difusión formal del tríptico ya existente, elaborado para dar a conocer los servicios de la RAP, uso básico, deberes y responsabilidades, así como concienciación sobre buen uso de los servicios de internet, y en especial de las redes sociales.

— Se potenciará la formación al personal administrador del sistema en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, tales como la configuración de los sistemas que forman parte de la RAP.

5. Sobre la aplicación PILAR

Se trata de una aplicación muy potente y compleja que necesita de muchas horas de trabajo y experiencia para maximizar su rendimiento. A pesar de ello, hace mucho más asequible y simplifica la aplicación de la metodología Magerit tal como propugna el ENS 2022.

Considero que se trata de una herramienta fundamental para quién desempeñe cometidos relacionados con la seguridad de las TIC, si bien requiere de mucha formación previa y conocer consejos y recomendaciones acerca de su uso por parte de personal experto.

Para mantener un proceso continuo de mejora de este sistema de información en cuestión, se deberán hacer revisiones periódicas del análisis de riesgos realizado, verificando que se estén aplicando correctamente las salvaguardas y medidas de seguridad que se habían identificado en fases anteriores.

6. Líneas futuras

Además de las medidas de seguridad propuestas en el apartado anterior, al tratarse de un sistema de categoría ENS media, deberá llevarse a cabo una auditoría para la certificación, tal como se expresa en el artículo 38 del ENS 2022 [1].

Además, se deberán programar las auditorías de seguridad previstas en el artículo 31 del ENS 2022, entre las que debe incluirse la del nodo central de gestión, todavía pendiente.

Por parte del autor, y con el fin anterior de elaborar el análisis de riesgos que se ha identificado que es necesario acometer, se cederán a CESTIC/DISEGINFO todos los archivos y documentación empleados para la elaboración de este TFM.

Referencias

CESTIC. (2020). *Instrucción Operativa para Gestión de Incidencias y Peticiones de la RAP*.

—. (2022). *NORMA 03/21 de Gestión de la Red WIFI de Asistencia al Personal.*Ministerio de Asuntos Económicos y Transformación Digital. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método* [en línea]. [Consulta: 9 de diciembre de 2022]. Disponible en: https://pilar.ccn-cert.cni.es/index.php/docman/documentos/1-magerit-v3-libro-i-metodo

Análisis de Riesgos de la Red de Asistencia al Personal (RAP) del Ministerio de Defensa

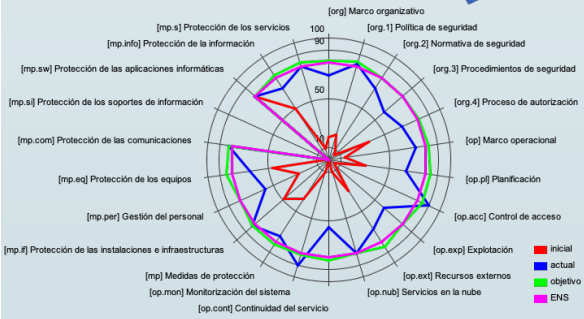
Autor: David Álvarez Lanzarote
Director/es: Iago López Román y Rubén Nocelo López

Introducción

Este trabajo tiene por finalidad realizar un análisis de riesgos de acuerdo al RD 311/2022, que regula el Esquema Nacional de Seguridad, de la Red de Asistencia al Personal del Ministerio de Defensa Se trata de un nuevo sistema de información nacido en 2019 con la finalidad de proporcionar un acceso a Internet de calidad y protegido al personal de nuestras Fuerzas Armadas tanto en instalaciones militares en territorio nacional, como cuando está participando en las distintas misiones en el exterior. Una de las premisas del diseño de la RAP es la seguridad, pero hasta ahora no se había abordado esta tarea.

Metodología

Empleo de la aplicación PILAR RA Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

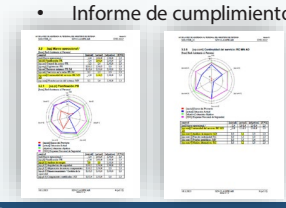


Resultados

ENS 2022 → controles de seguridad

Informes:

- Análisis de riesgos: disminución del riesgo en todas las dimensiones de seguridad de los activos
- ENS MEDIO:
  - Declaración de aplicabilidad: Controles
  - Informe de cumplimiento.



Aplicación práctica

Conclusiones

RAP → SISTEMA DE INFORMACIÓN **ENS MEDIO**

ENS 2022 → controles de seguridad:

- Ampliar NORMA 3/21 GESTIÓN RAP:
  - Nuevo anexo Procedimientos de Seguridad
  - Nuevo proceso formal de autorizaciones para entrada de equipos, aplicaciones en producción, o establecimiento de enlaces de comunicaciones con otros sistemas.
  - Incorporar anexo de descripción de los deberes y responsabilidades en materia de seguridad de cada puesto de trabajo asociado a la RAP.
- ANÁLISIS DE RIESGOS SEMIFOMAL
- ANÁLISIS DE IMPACTO:
  - Requisitos de disponibilidad de cada servicio
- Contratar vías alternativas de comunicaciones → ¿STARLINK?
- Charlas de concienciación en seguridad.
- Tríptico uso de servicios de la RAP y concienciación sobre buen uso de Internet, y redes sociales.
- Potenciar la formación en seguridad del sistema.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Estudio sobre implementación de comunicaciones BLOS (*Beyond Line of Sight*) alternativas al satélite a bordo de la F-110

Autor: Javier Antoranz Álvaro (jantalv@fn.mde.es)
Director: José María Núñez Ortuño (jnunez@cud.uvigo.es)

Resumen: – El requisito más importante de cualquier buque de guerra de la Armada española, es la capacidad de ofrecer una defensa eficaz frente a cualquier amenaza contra la soberanía nacional o algún país aliado de la OTAN. Para cumplir esta misión, es esencial disponer de una eficiente capacidad de Mando y Control (C2).

Una capacidad de Mando y Control adecuada (C2) garantizará que los comandantes navales en tierra emitan directivas oportunas a sus fuerzas desplegadas en el mar de manera efectiva en respuesta a una crisis emergente. Esto requiere proporcionar servicios IP basados en tierra a los comandantes en el mar, a través de comunicaciones BLOS rápidas, confiables, seguras y de alta capacidad, asegurando la seguridad de las comunicaciones.

Es por lo que las comunicaciones BLOS (*Beyond Line of Sight*) en el entorno naval son absolutamente primordiales, pues son necesarias para dotar a un buque desplegado en alta mar de la capacidad de ejercer el Mando y Control, y, por lo tanto, poder comunicarse con las estaciones en tierra.

Si bien es cierto que las comunicaciones por satélite (SATCOM) son la alternativa de comunicaciones BLOS más a menudo usadas actualmente en un buque de guerra debido a las elevadas tasas de datos y cobertura global que ofrecen, las comunicaciones satelitales presentan significativos inconvenientes como la fácil capacidad de interferencia, así como la frecuente indisponibilidad.

Para paliar estos inconvenientes, así como para ofrecer al buque de cierta capacidad de independencia frente al satélite, es necesario disponer de comunicaciones BLOS alternativas al satélite, tal y como las comunicaciones por HF (*High Frequency*) o la dispersión troposférica.

Este TFM tiene como objetivo analizar en detalle estas alternativas, sus estados del arte actuales, así como realizar un estudio de

aplicación práctica de alguna de estas alternativas a los buques de la Armada española, especialmente al futuro buque escolta F-110 y también a las actuales F-100.

Palabras clave: – BLOS, SATCOM, Dispersión Troposférica, HF, BRASS, BRE1TA.

1. Introducción

Panorámica de las comunicaciones BLOS

Las comunicaciones BLOS son esenciales para mantener la capacidad de un buque de guerra de ejercer el Mando y Control desplegado en el teatro de operaciones y, por lo tanto, alejado de la cobertura de las redes comerciales.

Son diversas las técnicas empleadas en la actualidad para dar cobertura y servicio a los diferentes escenarios marítimos en comunicaciones BLOS. Una de las más empleadas consiste en los sistemas basados en comunicaciones por satélite. Si bien es cierto que estas ofrecen grandes ventajas, tales como un elevado ancho de banda y una cobertura global, también presentan significativos inconvenientes, como la fácil capacidad de interferencia y la frecuente indisponibilidad.

Es por ello que resulta necesario disponer de distintas alternativas al satélite, que permitan establecer un enlace de comunicación seguro y fiable, más allá de la línea del horizonte y con suficiente ancho de banda, para garantizar la operatividad de las comunicaciones BLOS en caso de que el satélite no se encuentre disponible.

Entre estas alternativas de comunicaciones BLOS, se destacan dos que serán objeto de estudio de este documento: las comunicaciones por HF (*High Frequency*) y las comunicaciones basadas en la dispersión troposférica.

Comunicaciones en HF

Las comunicaciones por HF están basadas en varios mecanismos de propagación. De todos ellos, el predominante es la propagación por onda ionosférica, si bien es cierto que en la banda baja de HF se produce la propagación por onda de superficie y en la parte alta ya empieza a haber onda de espacio.

La propagación por onda ionosférica consiste en la reflexión de las señales radioeléctricas a frecuencias comprendidas entre 3-30 MHz (banda de HF). Esta reflexión se produce por la fuerte ionización surgida en la ionosfera causada fundamentalmente por la radiación solar.

Gracias a que las ondas electromagnéticas de HF se van reflejando una y otra vez en la ionosfera, la señal puede ir avanzando a lo largo de la superficie terrestre, superando todo tipo de obstáculo y sin que la curvatura de la tierra le afecte, consiguiendo una cobertura prácticamente global a lo largo de toda la tierra.

Comunicaciones basadas en dispersión troposférica

Están basadas en el fenómeno de la dispersión troposférica o *tropospheric scattering* (o simplemente, *troposcatter*) de las señales de UHF y

SHF. A grandes rasgos y a modo de breve introducción, este modelo de propagación basa su comportamiento en las propiedades físicas que componen la troposfera.

Estas propiedades se basan en la composición de áreas con diferentes constantes dieléctricas, además de existir en ella pequeñas partículas en suspensión, en su mayoría vapor de agua. Todos estos factores influyen en que una pequeña fracción de la señal de microondas transmitida hacia ella (normalmente con una frecuencia localizada en la banda alta de UHF y en la parte baja de SHF, en torno a los 2 GHz) sea dispersada de vuelta a la tierra.

Por consiguiente, esta pequeña parte de potencia puede ser captada por estaciones receptoras, estableciendo así un enlace de comunicaciones que, a pesar de no ser óptimo en cuanto a eficiencia (ya que la gran parte de la potencia se pierde en otras direcciones o se escapa hacia el espacio exterior), sí que puede resultar útil y funcional.

2. Motivación

Aunque en la introducción de este documento ya se han introducido razones para pensar en alternativas/complementos a las comunicaciones vía satélite, conviene hacer aquí una reflexión en mayor profundidad a ese respecto.

En primer lugar, hay que tener en cuenta los costes y la disponibilidad de uso de satélites. En la actualidad el Ministerio de Defensa cuenta con dos satélites propios (SpainSAT y XTAR-EUR), aunque no todos sus recursos están disponibles para uso oficial, puesto que parte del ancho de banda disponible se comercializa a través de la sociedad HisdeSAT. Por tanto, si la demanda de Defensa en un momento dado es suficientemente grande, será necesario recurrir al mercado para alquilar *transponders* de otros satélites, con el importante coste que ello supone. Ocurre lo mismo, si la misión lleva a unidades de la Armada a operar fuera de la zona de cobertura, presentando grandes zonas de sombra tanto en las regiones polares como en buena parte del océano Pacífico.

Un segundo aspecto a tener en cuenta es la vulnerabilidad de este tipo de sistema de comunicaciones. Dado que la situación de los satélites es conocida, se trata de sistemas fácilmente interferibles. Son susceptibles tanto a *jamming* convencional, como a un EMP-Jammer (Inhibidor de Generador de Pulsos Electromagnéticos, EMP).

Finalmente, en determinadas aplicaciones, tampoco puede obviarse la importante latencia que supone este tipo de enlaces (del orden de 600 m).

Por todos estos inconvenientes, se hace necesario disponer de alternativas de comunicaciones BLOS al satélite, tales y como las comunicaciones por HF, así como la dispersión troposférica.

3. Objetivos

El presente TFM tiene como objetivo estudiar los aspectos más relevantes, las ventajas y los inconvenientes de los dos tipos de comunicaciones BLOS alternativas al satélite, así como sus estados del arte actuales.

Adicionalmente, se estudiará en detalle el sistema BRE1TA, (evolución natural del actual sistema BRASS de comunicaciones HF de la Armada española), y se propondrá una solución técnica de aplicación, así como una arquitectura y un modelo de componentes. Por último, se estudiará la implantación de esta tecnología para la futura fragata F-110, así como la actual de tipo F-100.

4. Conclusiones

Las comunicaciones BLOS por HF y dispersión troposférica constituyen una buena alternativa a las comunicaciones satelitales y ofrecen una redundancia al satélite en caso de que este falle.

Si bien es cierto que actualmente no cabe ninguna duda de que las comunicaciones satelitales son mucho más rápidas y eficientes que las comunicaciones por HF y dispersión troposférica, estas comunicaciones presentan una serie de ventajas que las hacen ser muy atractivas.

En el caso de HF, las ventajas fundamentales que se han observado en el estudio realizado en el TFM son el bajo coste económico tanto de adquisición como de mantenimiento de los terminales de HF en comparación con los terminales satelitales, así como la independencia de cualquier autoridad externa a la Armada que proporciona el sistema de HF, en comparación con la fuerte dependencia que presenta el satélite de agentes externos a la Armada. Adicionalmente, son comunicaciones mucho más robustas y menos perturbables que las satelitales, por lo que en caso de conflicto pueden constituir una excelente alternativa.

Si bien es cierto que estas comunicaciones por HF presentan varias ventajas, en ningún caso sustituirían a las comunicaciones satelitales, ya que ofrecen un limitadísimo ancho de banda en comparación con las satelitales, que ocasiona que estas comunicaciones no sean aptas para los altos volúmenes de datos que se requieren actualmente. Además, el uso de las comunicaciones por HF no es nada fácil en comparación con el de los terminales satelitales.

Por todo ello, lo ideal sería que en barco estuviese presente tanto terminales satelitales como terminales de HF, pues en ningún caso son excluyentes.

Esta ha sido siempre la política de la Armada en esta cuestión, si bien es cierto que en ocasiones se ha reducido la inversión en el mantenimiento de los terminales HF debido a que el HF es incómodo de usar y las dotaciones prefieren siempre que sea posible usar el satélite. Este

escenario seguramente cambie con el nuevo concepto del HF basado en el BRE1TA, y el futuro BRE2TA, ya que estas dos tecnologías reducirán considerablemente los inconvenientes característicos de las comunicaciones por HF.

Además, como se ha analizado a lo largo del TFM, desde el punto de vista técnico es perfectamente abordable la modernización del BRASS, y, por lo tanto, su implantación del proyecto BRE1TA en los centros de mando y Control, así como en las estaciones radio y en la futura F-110 y en las F-100. También se ha observado en la solución técnica presentada, cómo reusándose elementos del antiguo sistema BRASS, se podrían ahorrar costes en dicha modernización.

En el caso de las comunicaciones por dispersión troposférica, es muy interesante destacar que se aprovechan las ventajas que, por un lado, presentan los sistemas *line of sight*, operando con altas frecuencias y permitiendo conseguir velocidades de transmisión elevadas, y, por otro lado, las que ofrecen los sistemas de comunicación por onda ionosférica, consiguiendo establecer enlaces BLOS más allá del horizonte sirviéndose de las propiedades físicas de las capas de la atmósfera.

También hemos visto que son una solución menos costosa que un sistema SATCOM. Además, ofrecen una alta fiabilidad y una velocidad de transmisión, fiabilidad y latencias bastante mejores que las comunicaciones por HF, y, por supuesto, soporta protocolos orientados a IP a diferencia del HF. Sin embargo, a pesar de estas ventajas tan interesantes, estas comunicaciones presentan una serie de inconvenientes, como el gran tamaño que requieren las antenas, (el espacio es una cuestión crítica en el diseño del *topside* de un buque) así como lo extremadamente sensibles que son estas comunicaciones al movimiento que presenta un buque.

Estos inconvenientes hacen que las comunicaciones por dispersión troposférica quizás no sea la mejor opción a la hora de ofrecer una alternativa al satélite en un buque de guerra. Esto afecta de manera directa el futuro buque escolta F-110, en donde el espacio en el mástil integrado es limitado y ya está totalmente copado por otros sensores. Es por ello que este tipo de comunicaciones pudieran ser más adecuadas para una instalación militar en tierra o para un buque muy grande (quizás un portaaviones) en donde el espacio no sea una cuestión crítica.

5. Líneas Futuras

Una vez desarrollado los diferentes puntos del presente TFM, se propone a la Armada española las siguientes líneas futuras de trabajo:

- Seguir avanzando en el proyecto BRE1TA y potenciar el HF como método de comunicación alternativa al SATCOM.
- Seguir adquiriendo transceptores de HF que cumplan los requisitos BRE1TA para los nuevos buques en construcción F-110 y modernizar

los transceptores de HF de los buques ya existentes (fundamentalmente las F-100) de tal manera que cumplan dichos requisitos.

- Iniciar una línea de investigación I+D de un sistema basado en dispersión troposférica buque-tierra, que calcule las fluctuaciones asociadas al movimiento del barco y sea capaz de corregir el enlace para optimizar la amplitud de potencia recibida
- Iniciar una línea de investigación para intercomunicar los Centros de Comunicaciones (CECOMs) con un enlace de comunicaciones troposféricas. De esta manera, se podría disponer de una comunicación de alta capacidad, segura y que actuase proporcionando redundancia, como recurso de seguridad en caso de caída de la red principal.
- Estudiar la posibilidad de desarrollar un sistema de comunicaciones táctico y portátil basado en dispersión troposférica para Infantería de Marina. Especialmente en escenarios donde la orografía impide las comunicaciones por visión directa.

Agradecimientos

Se agradece a la Armada, así como a la oficina de programa F-110 de la Subdirección General de Programas de la Dirección General de Armamento y Material todos los medios y el apoyo prestado para hacer el presente trabajo fin de máster.

Asimismo, agradezco a mi tutor todo el tiempo y la dedicación.

Estudio sobre implementación de comunicaciones BLOS *(Beyond Line of Sight)* alternativas al satélite a bordo de la F-110.

Autor: Javier Antoranz Álvaro
Director/es: Jose María Núñez Ortuño

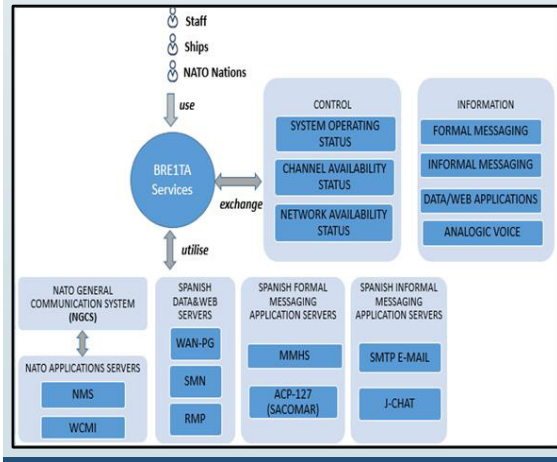
Introducción

El requisito más importante de cualquier buque de la Armada, es la capacidad de ofrecer una defensa eficaz frente a cualquier amenaza contra la soberanía nacional o contra algún país aliado de la OTAN. Para cumplir esta misión, es esencial disponer de una **eficiente capacidad de mando y control (C2).**

Las comunicaciones BLOS (*Beyond Line of Sight*) en el entorno naval son absolutamente primordiales, pues son necesarias para **dotar a un buque desplegado en alta mar de dicha capacidad** y por lo tanto poder comunicarse con las estaciones en tierra.

Si bien es cierto que las comunicaciones por satélite **(SATCOM)** son la alternativa BLOS más **frecuentemente usada** debido a las elevadas tasas de datos y cobertura global que ofrecen, también presentan **significativos inconvenientes** como la fácil capacidad de interferencia, así como la frecuente indisponibilidad.

Para **paliar estos inconvenientes**, así como para ofrecer al buque de cierta capacidad **de independencia frente al satélite**, es necesario disponer de comunicaciones BLOS alternativas al satélite tal y como las **comunicaciones por HF (*High Frequency*) o la dispersión troposférica**



Objetivos

- Estudio de comunicaciones por **HF y dispersión troposférica alternativas al satélite:**
  - ❖ Estado del arte
  - ❖ Ventajas e Inconvenientes.
  - ❖ Aplicaciones en la Armada Española
- Análisis del **BRE1TA** (*Broadcast Enhancement 1 Target Architecture),* evolución del sistema de comunicaciones HF actuales **BRASS** *(Broadcast, Maritime Rear Link and Ship-Shore) de la Armada*
  - ❖ Propuesta de Solución Técnica
  - ❖ Elaboración de Arquitectura y modelo de Componentes
  - ❖ Implantación en la futura fragata **F-110.**

Conclusiones

Las comunicaciones por HF a constituyen una buena alternativa a las comunicaciones satelitales, y ofrecen una redundancia al satélite en caso de que éste falle. **No son excluyentes**

Las comunicaciones por **dispersión troposférica** a pesar de sus ventajas **no son adecuadas** como alternativa al satélite para la F-110. Son más interesantes para una **instalación militar en tierra,** en la que el espacio no sea cuestión crítica.

La implantación del BRE1TA es abordable tanto en buques como la **F-110** y la serie existente F-100 como en tierra. Para ahorrar costes se podrían **reusar varios de los elementos del BRASS.**

El sistema BRE1TA permitiría **reducir los inconvenientes del HF y potenciar sus ventajas.**

Ciberatacando un buque de guerra: en la búsqueda de un sistema de ciberdefensa a bordo

Autor: Jesús Bayón Laguna (baylagchus@hotmail.com)
Directores: Carlos Zamorano Pinal (externo.czamorano@cud.uvigo.es) y Fondo Ferreiro, Pablo (pfondo@gti.uvigo.es)

Resumen: – La crisis actual en Ucrania está dejando en evidencia la importancia en la capacidad de los Estados para poder llevar a cabo ciberataques que pueden ser decisivos en un determinado momento. Esto les puede permitir llevar la iniciativa en el campo de batalla y tener efectos colaterales en el resto de los dominios físicos: terrestre, marítimo y aeroespacial.

Los buques emplean, cada vez más, tecnología altamente avanzada para poder desarrollar sus cometidos y misiones. Son todo tipo de sistemas, algunos de ellos conectados a internet. Sistemas tecnológicos de última generación que le proporcionan las capacidades operativas adecuadas para desarrollar su misión en el teatro de operaciones. Sistemas, como, por ejemplo, los integrados de control de comunicaciones, de control de la plataforma o de combate. En muchos casos interconectados entre sí.

El aumento, en los últimos años, de los ciberataques, el avance en nuevas técnicas, tácticas y procedimientos, y la cada vez más especialización y capacidad de ataque de grupos avanzados persistentes, en muchos casos financiados por los Estados, hace reflexionar sobre la necesidad de disponer de sistemas adecuados de ciberdefensa en los buques de guerra que les haga ciber-resilientes ante las amenazas en el ciberespacio.

En este trabajo se realiza un estudio detallado de los diferentes sistemas a bordo de un buque de guerra susceptibles de ser ciberatacados, para posteriormente proponer un sistema de ciberdefensa, dentro de un marco teórico, que permita la detección, monitorización y protección de los sistemas a bordo.

Palabras clave: – Buque de guerra, Ciberataque, Ciberespacio, Ciberdefensa, Sistema.

1. Introducción

Los buques emplean, cada vez más, tecnología altamente avanzada con la que poder desarrollar sus operaciones, cometidos y misiones. Son todo tipo de sistemas (IT/OT), algunos de ellos interconectados a internet.

Podemos pensar en cualquier tipo de sistema, desde los de comunicaciones hasta los de control de la plataforma. Los buques de guerra, además de los anteriores, emplean sistemas inherentes a su idiosincrasia, como es el sistema de combate, entre otros.

Se estima que existen cincuenta mil barcos navegando al mismo tiempo en un momento dado, siendo todos ellos altamente vulnerables a ciberataques [1]. En 2015, expertos en ciberseguridad presentaron, en una demostración, lo fácil que es hackear un buque [2]. Encontraron agujeros de seguridad en los sistemas de posicionamiento global (GPS; en inglés, *Global Positioning System*), sistema de identificación automática (AIS; en inglés, *Automatic Identification System*, sistema de información y visualización de cartas electrónicas (ECDIS; en inglés, *Electronic Chart Display and Information System*), este último utilizado para visualización de cartas náuticas.

Más recientemente, según se ha informado por diferentes medios de comunicación, a través de agencias de inteligencia, Rusia ha sido capaz de hackear al proveedor estadounidense de comunicaciones satélite Viasat el día de la invasión de Ucrania [3].

De todas las amenazas comentadas anteriormente no se escapa el buque de guerra. El impacto operativo que podría tener la pérdida, aunque sea momentánea, de las comunicaciones satelitales en el teatro de operaciones sería muy alto, ya que esto implicaría también la pérdida de redes y sistemas de Mando y Control principales o la pérdida de comunicación con los cuarteles generales. Sin mencionar, que se vea afectado el posicionamiento de un buque o algún mal funcionamiento del sistema integrado del control de plataforma.

El aumento, en los últimos años, de ciberataques y la especialización, cada vez más, y capacidad de ataque de grupos de *Amenaza Avanzada Persistente* (APT; en inglés; *Advanced Persistent Threat*) en el ciberespacio, en muchos casos financiados por los Estados, hace reflexionar en tener sistemas adecuados de ciberdefensa en los buques.

Ante la necesidad de dotar con sistemas de ciberdefensa a las nuevas unidades y plataformas que formarán parte de las Fuerzas Armadas, el Ministerio de Defensa crea, a principios de 2021, el departamento de Jefatura de Sistemas Satelitales y de Ciberdefensa, dependiente la Dirección General de Armamento y Material (DGAM). Este nuevo departamento permitirá aportar una visión unificada para la obtención de sistemas de ciberdefensa.

Hasta el momento, los buques de guerra de la Armada, al igual que otras Armadas y Marinas, no habían contemplado la implantación de sistemas de ciberdefensa a bordo. El punto inflexión sobre esta perspectiva surge con el proyecto de las F-110, donde ya se contempla, desde la fase conceptual del programa, un sistema de ciberdefensa a bordo. Además, este se haría extensivo a los submarinos tipo S-80 [4].

En el ámbito internacional, ya por 2015, la Marina de EE. UU. se planteó la instalación de sistemas de ciberdefensa enfocados principalmente para la protección de sus sistemas de propulsión y de energía eléctrica [5]. También existen otras Marinas preocupadas en este nuevo dominio. Ejemplo de ello es la Marina alemana, que, con apoyo de la empresa Thales, va a implementar sistemas de ciberdefensa en la construcción de las fragatas tipo F-126 (MKS 180) [6]. También la Marina nacional francesa (en francés; *Marine Nationale*) contempla en sus proyectos de las fragatas FDI (en francés; *Fregate de defense et d´intervention*) la ciberseguridad por diseño, integrando lo que han llamado un sistema de gestión de ciberseguridad (CyMS; en inglés; *Cyberscurity Managment System*), lo que permite al buque ser ciber-resiliente [7].

2. Objetivos

Este trabajo plantea la consecución de una serie de objetivos estrechamente relacionados con lo expuesto antes. Dado que el buque de guerra moderno depende de redes y sistemas con tecnología de última generación (IT/OT) para poder llevar a cabo el cumplimiento de su misión, los cuales se ven expuestos a todo tipo de amenazas en el ciberespacio.

El objetivo general que se plantea es definir una posible solución de diseño para la implantación de un sistema de ciberdefensa a bordo que permita la detección, monitorización y protección de los sistemas a bordo de los buques de la Armada.

A raíz de este objetivo general se fijan los siguientes objetivos específicos:

- Identificar las diferentes amenazas que existen en el ciberespacio y que pueden tener impacto en los buques de guerra.
- Describir los sistemas y redes implantados en el buque modelo, fragata F-110.
- Identificar las vulnerabilidades que presentan las redes y sistemas del buque de guerra en general, aplicados en el buque modelo.
- Estudiar la tecnología y los requisitos que debe cumplir el sistema de ciberdefensa.

3. Desarrollo

La primera parte del trabajo se centra en dar a conocer una visión general de las amenazas existentes en el ciberespacio, realizando inicialmente

un estudio de los ciberinicidentes y ciberataques conocidos en las últimas décadas en el sector marítimo. La siguiente tabla muestra un resumen de ellos, así como sus consecuencias.

Año	Ciberincidente/Ciberataque	Consecuencias
2010	Ciberataque a una plataforma petrolífera de Corea del Sur	diecinueve días de inutilización y pérdidas de 700.000 $/día.
2011	Ciberataque a la naviera iraní IRISL	Pérdida de contenedores.
2012	Ciberataque a la plataforma petrolífera Noble Regina en construcción	Afectó a 89 trabajadores, estructura de apoyo y pérdidas económicas al astillero.
2013	Supuesto ciberataque del sistema ECDIS de un dragaminas de la US Navy	Encalla en arrecifes de coral cuando navegaba en el mar de Sulú, al sur de la isla filipina de Pawalan
2013	GPS *Spoofing* (Universidad de Austin, Texas)	El yate White Rose of Drax recibe durante treinta minutos señales falsas de GPS mientras navegaba en el Mediterráneo.
2017	Sistema de navegación a buque mercante	Carguero pierde acceso al sistema de navgeación durante diez horas cuando navegaba rumbo Yibuti. Piratas somalís abordan el buque.
2017	Ciberataques a los sistemas de navegación de dos buques de guerra de la US Navy desplegados en el pacífico	Ambos sufren colisiones con otros buques mercantes. Se pierden diecisiete vidas humanas.
2017	GPS *Spoofing*	Veinte buques informan de anomalías en su posición de GPS cuando navegaban en el mar Negro. Todos fueron situados en una misma posición, el aeropuerto de Gelendzhik (Rusia), muy próximo a la zona de navegación.
2019	Buque con destino Nueva York alerta de incidente con impacto significativo en sus redes y sistemas.	El análisis realizado por la Guardia Costera (U.S. Coast Guard), concluye que el *malware* degradó significativamente la funcionalidad de los sistemas a bordo.
2020	*Ransomware* Hermes 2.1	Múltiples estaciones de trabajo en las redes de administración del buque se vieron afectadas

Tabla 1. Resumen de ciberinicidentes/ciberataques conocidos en el sector marítimo

Seguidamente, se identifican las diferentes amenazas que existen en el ciberespacio y que pueden tener impacto en los buques de guerra. El interés de los diferentes actores o agentes amenaza en el ciberespacio no tiene límites ni fronteras. Es cierto también, que no todos disponen de los mismos recursos para poder llevar a cabo un ciberataque. Son los Estados los que se han dado cuenta del potencial que pueden tener las acciones ofensivas en el ciberespacio y los efectos que puede causar en el adversario. Muchos a través de sus propios medios o de *proxies* efectúan acciones en lo denominado «zona gris». Esto les permite fijar objetivos, prepararse con el tiempo necesario y en el momento adecuado llevar a cabo sus acciones ofensivas.

Tampoco nos podemos olvidar del *insider* o actor interno, especialmente de aquel que está descontento con la organización y quién podría tener acceso directo a los diferentes sistemas del buque. Ambos, aunque también otros ciberactores pueden causar estragos a un buque en zona de operaciones si el ciberataque tuviese existo.

Lo comentado hasta el momento supone un cambio de paradigma para las operaciones militares. El ciberespacio es un nuevo dominio, transversal a los dominios físicos y donde, además, pueden tomar parte un gran abanico de ciberactores.

Tal como demuestra la tabla 1 el sector marítimo no está exento de todo ello. Pensar que los buques de guerra son inmunes, dado que emplean cifradores y canales específicos de comunicaciones, puede ser un poco temerario e ingenuo al mismo tiempo. Es por ello, que existen dos tipos de buques: «los que ya han sido ciberatacados y los que lo serán».

Por todo lo anterior, se cree necesario dotar a los buques de guerra con sistemas que sean capaces de aportar una protección extra al resto de sistemas y, por ende, al propio buque. Tanto es así, que se empieza a apreciar un interés por las marinas de guerra en implementar sistemas de ciberdefensa. Algunos ejemplos son las de EE. UU., Alemania, Francia y España, como ya se ha comentado en la introducción. A medida que pasen los años es probable que estos sistemas sean simplemente uno más a bordo de todos los buques de guerra.

Para poder llevar a cabo el diseño del sistema de ciberdefensa se ha elegido un buque como modelo. En este caso se ha escogido la fragata F-110 que será uno de los buques que en un futuro próximo llevará este sistema instalado. En realidad, podría haber sido cualquier otro, pero para el autor suponía un pequeño reto al ser este el más moderno de la Armada que dispondrá de él.

Una vez presentados cada uno de los sistemas de la F-110, se lleva a cabo el estudio detallado de la superficie de exposición y vulnerabilidades de cada uno de ellos. Tal y como se ha comentado en el párrafo anterior, de un modo genérico. Cabe destacar el empleo en alguno de ellos de *hardware* y *software* comercial. Esto unido a la interconexión de sistemas y la posibilidad de conexión de internet hace que la superficie de exposición a los ciberataques se amplíe. El hecho de que un sistema sea infectado podría, en un momento dado, permitir la libertad de movimiento a través de las distintas redes a un ciberatacante.

Finalmente, se menciona las ya conocidas debilidades de algunos sistemas que ya han sido hackeados como son los AIS o los sistemas de comunicaciones satélite comerciales.

Requisitos del sistema de ciberdefensa

Lo expuesto anteriormente no hace más que reforzar la idea de la necesidad de implementar un sistema a bordo de los buques que sea capaz de

identificar, proteger, detectar, responder y recuperar los sistemas en caso de ser ciberatacados, incorporando para ello un diseño y procedimientos que lo haga ciber-resiliente.

El sistema de ciberdefensa que se propone para la F-110 deberá reunir principalmente las siguientes funcionalidades: defensa en profundidad de los sistemas (protección), monitorización de eventos de ciberseguridad (detección). Dado que lo que buscamos es un sistema ciber-resiliente deberíamos implementar las funcionalidades de respuesta y recuperación de este. Adicionalmente, es interesante contar con una conexión de nuestro sistema con el Centro Operativo de Ciberseguridad (COCS) de la Armada y/o del Ministerio de Defensa que proporcione una monitorización remota.

Figura 1. Requisitos del sistema de ciberdefensa

Defensa en profundidad

Esta estrategia consiste en introducir múltiples capas de seguridad o barreras que permitan reducir la probabilidad de compromiso, en caso de que una de estas falle, y, en el peor de los casos, minimizar el impacto.

El objetivo final es la protección de los sistemas, de sus activos y, por ende, de la información alojada en ellos.

En este apartado se analiza cada uno de los dispositivos a emplear en cada uno de los sistemas a defender del buque y que, por tanto, formarán parte del sistema de ciberdefensa. Entre ellos, podemos incluir, como no puede ser de otra manera, los cortafuegos, diodos de datos, IDS e IPS, así como configuraciones de DMZ o pasarela de intercambio de datos, sin olvidarnos de protección en los *hosts* con el empleo de HIDS o EDR.

Monitorización

El sistema permitirá realizar la monitorización de todos los sistemas que integra la F-110. Esto lo llevaremos a cabo a través del ya mencionado antes SIEM, basado principalmente en las soluciones propuestas y a lo establecido en las guías del Centro Criptológico Nacional (CCN).

Monitorización desde el COCS de Armada/MDEF

Por diferentes razones puede ser interesante contemplar que desde un COCS remoto, bien sea el COCS Armada o bien desde el COCS MDEF del Mando Conjunto de Ciberespacio (MCCE), se pueda visualizar o monitorizar el estado de las redes y sistemas de los buques que se encuentran principalmente en zona de operaciones, pero también, desde luego, de los que se encuentran en puerto base. Esto permitirá, por ejemplo, en un momento dado, poder emplear recursos humanos en el buque para otros

puestos en una situación de mayor complejidad o estrés en zona de operaciones, al mismo tiempo que desde remoto se está llevando a cabo esta monitorización de todos los sistemas.

Gestión de ciberincidentes

El sistema de ciberdefensa debe contar con una herramienta que permita realizar una gestión de los ciberincidentes, de forma eficaz, que ocurren en cada una de las redes y sistemas del buque. Para ello, debe permitir el acceso a la información de los registros recogidos en los SIEM, para poder realizar la notificación con empleo de un lenguaje común en cuanto a la clasificación de ciberincidentes, niveles de amenaza y trazabilidad de estos.

Requisitos del personal. Personal cualificado

Todos los requisitos tecnológicos expuestos anteriormente para el sistema no servirán si no lo dotamos con el personal cualificado y la formación adecuada en esta materia.

El personal formado por la Armada en las TIC no contempla una formación específica en ciberdefensa. Por tanto, debe existir una plantilla específica en la F-110 para desempeñar estas funciones. Existe una formación en esta materia dentro del ámbito conjunto de las Fuerzas Armadas que cubre, en parte, los conocimientos teóricos y técnicos que debe adquirir este personal. Aun así, esta debe ser complementada con otros cursos específicos desarrollados por otras organizaciones e instituciones como son los del CCN-CERT o el instituto SANS que proporcionarán la formación requerida a los operadores del sistema.

Finalmente, se plantea un sistema básico de ciberdefensa que contempla todas las particularidades de cada uno de los sistemas a defender. Para el diseño se ha querido diferenciar entre aquellos sistemas a defender que manejan información clasificada y los que no, así también, atendiendo al tipo de información que maneja cada uno de ellos. Esto tiene relevancia, ya que el sistema de ciberdefensa propuesto en realidad constará de dos subsistemas. El objetivo final es no interconectar el sistema de ciberdefensa no clasificado al que sí lo es, aunque luego se pueda plasmar toda la información disponible para el analista en un mismo panel.

4. Conclusiones

Ha quedado constancia de la necesidad de contar en los buques de guerra con un sistema de ciberdefensa que les permita saber en cada momento el estado de las redes y sistemas empleados a bordo, y realizar su misión. El conocimiento de ello puede, en un momento dado, prevenir daños mayores en los sistemas, evitar accidentes y facilitar el desarrollo de las operaciones navales, además de mantener en todo momento informado y asesorado al comandante del buque y mandos superiores en la cadena orgánica y operativa en lo relativo a esta materia.

La cada vez mayor capacidad de los diferentes actores en el ciberespacio, el aumento de recursos, tanto humanos como económicos, la mejora de conocimientos y el avance en las TTP, la creación de nuevas ciberarmas, la mayor capacidad de algunos Estados este ámbito, la financiación del algunos Estados a *proxies,* sumado a la difícil atribución de las acciones en el ciberespacio, evidencia la tendencia progresiva hacia un incremento de amenazas y estrategias no convencionales e híbridas, y hacia una actuación, cada vez mayor, en la «zona gris» de nuestros potenciales adversarios.

Durante las últimas décadas se han producido ciberataques en el sector marítimo, no solo a navieras, sino también a buques, incluidos a buques de guerra.

El empleo de tecnología COTS y algunos casos de *software* obsoleto y fuera de soporte, pone más fácil al adversario el empleo de sus ciberarmas.

Se ha querido hacer un diseño de modo que la detección pueda realizarse de forma duplicada, tanto desde el COCS del buque como el de Armada o el del Mando Conjunto del Ciberespacio en tierra. Eso permitiría que desde los cuarteles generales se tuviese la información del estado de los sistemas casi en tiempo real.

No se ha querido mezclar dominios de seguridad. El hecho de interconectar los dominios supondría aumentar la superficie de exposición de los sistemas que necesitan la mayor protección posible o que manejan información clasificada, y, por tanto, hacerlos más vulnerables.

De este modo, aunque supone tener el doble de elementos, SIEM y puestos de operador, se considera conveniente que no exista interconexión entre ambos dominios.

Aun así, todo lo anterior, no tiene sentido si no se dispone de un personal cualificado y específicamente formado en la materia de ciberdefensa. Por lo tanto, se considera imprescindible para poder tener un sistema completo, no solo el recurso material adecuado, sino un recurso humano de calidad.

Referencias

Corera, G. (2022). Russia hacked Ukrainian satellite communications, officials believe. *BBC*. Disponible en: https://www.bbc.com/news/technology-60796079

EDR: European Defense Review. (2022). Naval Group launches the first defense and intervention frigate (FDI) for the French Navy [en línea]. *Revista EDR online*.

Freeman, B. (2015). A New Defense for Navy Ships: Protection from Cyber Attacks. *Press Release US Navy*. Disponible en: https://www.navy.mil/Press-Office/News-Stories/Article/2263855/a-new-defense-for-navy-ships-protection-from-cyber-attacks/

Karremann, J. (2021). *Cyber security at sea, defending against digital attacks on ships.*

Kochetkova, K. (2015). Maritime industry is easy meat for cyber criminals. *Kaspersky daily.* Disponible en: https://www.kaspersky.com/blog/maritime-cyber-security/8796/

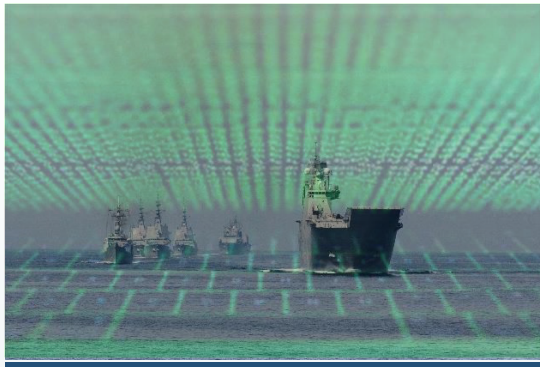
Navantia. (2021). Navantia y Telefónica Tech instalarán un sistema de ciberseguridad reforzado en los submarinos de la clase S-80. *Navantia Notas de prensa.* Disponible en: https://www.navantia.es/es/actualidad/notas-prensa/navantia-y-telefonica-tech-instalaran-un-sistema-de-ciberseguridad-reforzado-en-los-submarinos-de-la-clase-s-80/

Rory Hopcraft, K. M. (2018). 50,000 Ships worldwide are vulnerable to cyberattacks. *Independent*. Disponible en: https://www.independent.co.uk/tech/ships-cyberattacks-vulnerable-worldwide-a8404191.html

Ciberatacando un buque de guerra: en la búsqueda de un sistema de ciberdefensa a bordo

Autor: Jesús Bayón Laguna

Director/es: Carlos Zamorano Pinal, Pablo Fondo Ferreiro.



Introducción

Los buques emplean cada vez más, tecnología altamente avanzada para poder desarrollar sus cometidos y misiones.

El aumento en los últimos años de los ciberataques, el avance en nuevas técnicas, tácticas y procedimientos, y la cada vez más especialización y capacidad de ataque de grupos avanzados persistentes, en muchos casos financiados por los Estados, hace reflexionar en la necesidad de disponer sistemas adecuados de ciberdefensa a bordo de los buques de guerra.

Objetivos

General: definir una posible solución de diseño para la implantación de un sistema de ciberdefensa a bordo que permita la detección, monitorización y protección de los sistemas a bordo de los buques de la Armada.

1. Identificar las diferentes amenazas que existen en el ciberespacio y que pueden tener impacto en los buques de guerra
2. Describir los sistemas y redes implantados en el buque modelo (fragata F-110).
3. Identificar las vulnerabilidades que presentan las redes y sistemas del buque de guerra en general, aplicados en el buque modelo.
4. Estudiar la tecnología y los requisitos que debe cumplir el sistema de ciberdefensa.

Resultados

El sistema de ciberdefensa que se propone para la F-110 deberá reunir principalmente las siguientes funcionalidades:

Conclusiones

- Aumento de ciberataques en las últimas décadas en el sector marítimo.
- Aumento en capacidades y recursos por partes de los Estados y grupos avanzados persistentes.
- Mejora de conocimientos y avance en las técnicas, tácticas y procedimientos empleadas.
- Mayor conciencia por implantar estos sistemas en buques de guerra (EE.UU, Alemania, Francia, España).
- El sistema no solo le permitirá conocer en todo momento al Comandante del buque el estado de las redes y sistemas de su buque sino también estar más protegido.
- La monitorización externa ofrece una capa extra y comunicación directa para gestión de ciberincidentes
- Es primordial dotar al sistema de personal altamente cualificado y formado.

Sistema global contra drones

Autor: José Antonio Cebrián de Barrio (jac@interior.es)
Directora: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen: – El crecimiento exponencial en las tecnologías *drone*, la gran cantidad de modelos de ámbito comercial, diferentes usos para los que son útiles, unido a la reducción de costes de compra y mantenimiento, facilidad de pilotaje y programación, incluyendo el desarrollo legislativo, hace que cada vez más empresas, organismos públicos, particulares, etc., se planteen la utilización de este tipo de aeronaves. Por este motivo, las Fuerzas y Cuerpos de Seguridad han de estar preparadas para hacer frente su uso malintencionado.

Inicialmente, se han definido las siguientes fases para hacer frente a la posible amenaza:

- Detección: se detecta algo extraño, inicialmente no se puede saber si se trata de un dron, a dónde se dirige, las intenciones que tiene, etc.
- Identificación: discernir si realmente se trata de un dron y tratar de obtener el mayor número de datos posibles del mismo. Incluyendo la posición del piloto.
- Seguimiento: dará indicios de a dónde se dirige y posibles intenciones.
- Neutralización: en caso necesario.
- Inteligencia: todas estas fases han de disponer de una cierta inteligencia que ayuden al operador a tomar decisiones en tiempo real.

El 11 de julio de 2019, en España se produjo un punto de inflexión, la Secretaría de Estado de Seguridad firmó una resolución por la que se declaraba de emergencia la contratación de un servicio, llamado Sistema Global Contra Drones (SIGLO-CD), con el objetivo de detectar, identificar y seguir drones comerciales en el área Metropolitana de Madrid, y, en su caso, neutralizar si se considera que amenaza a algunas de las mayores instituciones del Estado.

Palabras clave: – *Drone*, Contradrones, CUAs, Seguridad ciudadana, SIGLO-CD.

1. Introducción

«Lo consiguieron porque no sabían que era imposible» Jean Cocteau.

Gracias a la velocidad a la que se están produciendo los avances tecnológicos, nos encontramos que, en el mercado de los drones, hay una gran variedad de marcas y modelos comerciales de coste reducido, facilidad de mantenimiento y pilotaje, posibilidad de programar diferentes funciones, entre ellas, las rutas mediante *waypoints*, añadiendo los diferentes usos para los que son útiles, incluyendo una legislación que permite que cada vez más empresas, organismos públicos, particulares, etc., se planteen la utilización de este tipo de aeronaves para diversos objetivos.

El problema es que la delincuencia organizada también trata de aprovechar los avances tecnológicos y este tipo de aeronaves son cada vez más utilizadas con fines ilegales. Desde el punto de vista estadístico, el uso no legal, alegal, ilegal, en la mayoría de los casos, es por desconocimiento de la ley, por imprudencia. Existen otros casos en los que conscientes de la ilegalidad del vuelo, estos no son conscientes de las posibles consecuencias, para ellos (sanciones), ni para terceros (daños colaterales en caso de accidente). El siguiente escalón es el uso de este tipo de tecnología para favorecer actividades ilegales, como, introducir droga en un centro penitenciario, invadir la intimidad de las personas y una gran variedad de comportamientos. En los casos más graves, el uso de estas aeronaves se hace para producir atentados. Por todos estos motivos, las Fuerzas y Cuerpos de Seguridad, tienen que estar preparados tecnológicamente para proteger la seguridad ciudadana y las libertades públicas.

El objetivo del presente trabajo es doble:

- Hacer una comparación de los diferentes sistemas que existen para neutralizar el uso malintencionado de los drones comerciales.
- En segundo lugar, se plantea como habría que desplegar una solución contradrones «C-UAVs».

Al ser una tecnología reciente, existe relativamente muy poca documentación al respecto, por lo que todo lo expuesto se basa en la experiencia personal.

2. Drones

Dron es la adaptación al español del inglés *drone* (abeja macho o zángano), para referirse a los vehículos aéreos no tripulado. Ha sido este año cuando ha empezado a figurar la palabra en el diccionario de la Real Academia de la Lengua. Los drones tienen diferentes denominaciones: UAV, UAS, RPA, RPAS...

Igualmente, hay diversas clasificaciones, las más conocidas son las basadas en el peso (clasificación OTAN) y por forma (ala fija, multirrotores, globos y dirigible). En la figura 1, vemos la clasificación OTAN.

Class I w < 150	Small w > 20 kg	Tactical Unit (employs launch system)	h ≤ 5000 AGL	50 (LOS)	Luna, Hermes 90
	Mini 2 ≤ w ≤ 20 kg	Tactical Unit (manual launch)	h ≤ 3000 AGL	25 (LOS)	ScanEagle, Skylark, Raven, DH3, Aladin, Strix
	Micro w < 2	Tactical Patrol/section, Individual (single operator)	h ≤ 200 AGL	5 (LOS)	Black Widow

Figura 1. Clasificación OTAN. Fuente: Plan Director de RPAS de 2015 (DGAM)

El interés de las FFCCS para proteger la seguridad ciudadana se centra en los de clase 1 y dentro de ellos, los micro y mini, ya que este tipo de drones son utilizados por delincuentes, bandas organizadas y organizaciones terroristas. DAESH e ISIS han empleado drones comerciales con pequeñas modificaciones, para cometer atentados. En España, hasta el momento, solo se ha detectado un intento de atentado terrorista utilizando este tipo de tecnologías.

Por lo expuesto, cuando se detecta un vuelo no autorizado, inicialmente se desconoce la intención del piloto, por lo que debe ser tratada como una posible amenaza hasta descartar que se trate de un peligro real. Téngase en cuenta, igualmente, que un vuelo lúdico cerca de un aeropuerto, se convierte en un peligro grave, aunque no hay ninguna intención de causar daño.

En definitiva, las FFCCS han de estar preparados para prevenir, detectar, identificar y, en su caso, neutralizar este tipo de amenazas, diferenciando entre *security* y *safety*.

- Security: evitar el uso de estas aeronaves en vuelos no autorizados o para cometer acciones ilegales.
- Safety: evitando los daños que estás aeronaves puedan producir a terceros por su uso inadecuado. A la hora de neutralizar los daños producidos nunca deben ser iguales o mayores de los que se quieren evitar.

Partimos de la premisa de que la seguridad 100 % no existe, por lo que el punto de partida será analizar cuáles son los drones comerciales más vendidos y centrarnos inicialmente en estos. Al respecto, tres marcas de drones comerciales ocupan más del 90 % de las ventas y, en el caso de España, podemos decir que más del 95 % se concentra en DJI (90 %), Parrot y Yuneec. El motivo es sencillo: precio bajo, facilidad de pilotaje y mantenimiento, aumento de las prestaciones, cargas de pago de mayor calidad.

3. Fases para hacer frente a la posible amenaza

Para conseguir neutralizar la posible amenaza, se han definido las siguientes fases, tal y como recoge la figura 2:

- Detección: se detecta algo extraño, inicialmente no se puede saber si se trata de un dron, a dónde se dirige, las intenciones que tiene, etc. Tendremos que diferenciar entre falso positivo, detección no real o equivocada que hace saltar la alarma y falso negativo, dron real no detectado, hay que reducir a cero este tipo de falsas alarmas, desde el punto de vista de la seguridad una amenaza real no detectada, es inasumible; ambos tipos de falsas alarmas son inversamente proporcionales, por lo que para reducir a cero los falsos negativos, debemos aumentar la sensibilidad del detector, con lo que aumentarán los falsos positivos.
- Identificación: discernir si realmente se trata de un dron y tratar de obtener el mayor número de datos posibles del mismo. Incluyendo la posición del piloto.
- Seguimiento: dará indicios de a dónde se dirige y posibles intenciones.
- Neutralización: en caso necesario.
- Inteligencia: todas estas fases han de disponer de una cierta inteligencia que ayuden al operador a tomar decisiones en tiempo real.

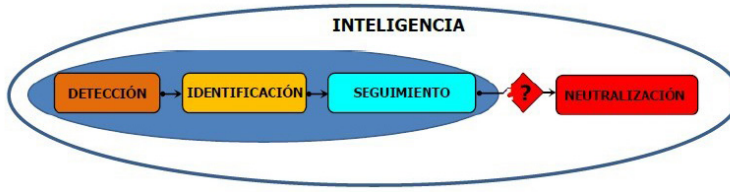


Figura 2. Fases para neutralizar un dron

4. Clasificación de las tecnologías de detección e identificación

Podemos distinguir diferentes clasificaciones atendiendo a:

- Sonido o ultrasonido

  Mediante la marca acústica característica que dejan este tipo de aeronaves, el problema es la distancia de detección que se vuelve crítica en entornos urbanos. No son soluciones muy populares debido a la escasa distancia de detección.

- Sistemas ópticos

  Solución bastante extendida, sobre todo en la fase de identificación. Como sistema único de detección ha sido descartado, ya que para detectar a larga distancia se necesita que la distancia focal de los objetivos sea alta, reduciendo el ángulo de captación.

- Radar activo

  Basados en el efecto Doppler, detectan el cambio de frecuencia de onda aparente de un objeto con movimiento con respecto a un observador. Teóricamente, funcionan bastante bien en entornos no urbanos, las distancias de detección son altas, necesitan un *software*

de apoyo para clasificar las alarmas y hay que ajustar la sensibilidad para detectar los actuales drones de tamaño pequeño.

— Radar pasivo

Utilizan las señales emitidas por otros sistemas radio como iluminadores de oportunidad en lugar de un transmisor propio. Se aprovechan infraestructuras ya desplegadas como iluminadores, siendo las más comunes la DVB (T y S), LTE, GSM, radio FM, GPS.

— Sistemas de radiofrecuencias

Escuchan las señales de radio en determinadas frecuencias, al tener clasificadas las tramas que se envían entre el *handcontrol* (piloto) y el dron, permite una detección bastante precisa. Constan de una o varias antenas para recibir ondas de radio e intentar detectar la comunicación entre un dron y su controlador. En 2017 DJI empieza a comercializar el sistema de detección Aeroscope, el cual detecta en un radio de 5 km con las antenas básicas (carezco de datos de dB), todos los drones de DJI y al descifrar la trama se obtienen datos precisos del modelo, número de serie, altura de vuelo, velocidad, etc.

— Inteligencia

Es importante que los futuros desarrollos incluyan inteligencia que ayuden al operador a clasificar las alarmas, esto es algoritmos de *machine-learning*, *deep-learning*, aprendizaje neuronal, que estudien patrones y con base en ellos mostrar probabilidades de intenciones.

5. Clasificación de las tecnologías de neutralización

Los sistemas de neutralización los podemos dividir en dos grandes bloques: cinéticos y no cinéticos.

Sistemas cinéticos

Mayoritariamente dispositivos balísticos y similares.

- Utilización de munición no letal.
- Sistemas bloqueadores del vuelo basado en redes.
- Sistemas dron contra dron y sus variantes.
- Hard killing, balística convencional.

El problema fundamental de estos sistemas es que hay que estar cerca de la amenaza y la distancia de efectividad es muy escasa, dependen fundamentalmente de la pericia y reacción del operador.

Sistemas no cinéticos

Dentro de este bloque podemos encontrarnos con:

— Bombardeo electromagnético de alta potencia: basado en la utilización de microondas de alta potencia (HPM) que generan un pulso electromagnético (EMP) de frecuencias comprendidas entre 1 y

10 GHz, enviadas directivamente. Son efectivos a distancias cortas, pudiendo generar graves daños colaterales en los dispositivos electrónicos y en las personas.

- Hack: tomar el control del dron remotamente mediante técnicas de hacking; hay que estudiar el enlace entre el handcontrol y el dron. Son soluciones ideales, pero presentan diversos problemas, suelen ser caras y tardías.
- Spoofing GPS: suplantar la señal GPS del dron, permitiendo llevarlo a zona segura, medida muy eficaz si el dron está programado para volar mediante waypoints. No está permitido en ningún caso este tipo de medida por legislación.
- Láser: dispositivo óptico de alta potencia que produce un haz de luz coherente (muy focalizado). Destruye la estructura y la electrónica.
- Inhibidores de frecuencia: es uno de los métodos más utilizados en estos momentos por su eficacia, fácil manejo, despliegue y precio. Son dispositivos que transmiten una gran cantidad de energía de radiofrecuencia hacia el dron o handcontrol, anulando la señal, por lo que el dron deja de recibir instrucciones.

6. Pruebas reales de sistemas

Una vez analizadas las tecnologías existentes, se realizaron pruebas reales en diferentes entornos, destacando:

- Pruebas de evaluación de sistemas contra drones, Aeropuerto de Asturias, celebradas entre los días 14 al 18, del mes de septiembre de 2020.
- Participación en la prueba de campo de la licitación de la Liga Nacional de Fútbol Profesional (LaLiga) en agosto de 2021.

Pruebas en el Aeropuerto de Asturias

Detección:

- Apantallada por un camión de bomberos.
- Apantallada por un edificio.
- Drones volando a baja cota.
- Drones volando a alta cota.
- Drones volando a distancia.
- Drones volando en modo autónomo.
- Detección de enjambres formados por drones autorizados y no autorizados.

En el siguiente gráfico se ven los resultados globales obtenidos por las diferentes empresas sobre un total de cien. El color amarillo indica detección mediante radiofrecuencia, el naranja la detección radar y el verde ambas.

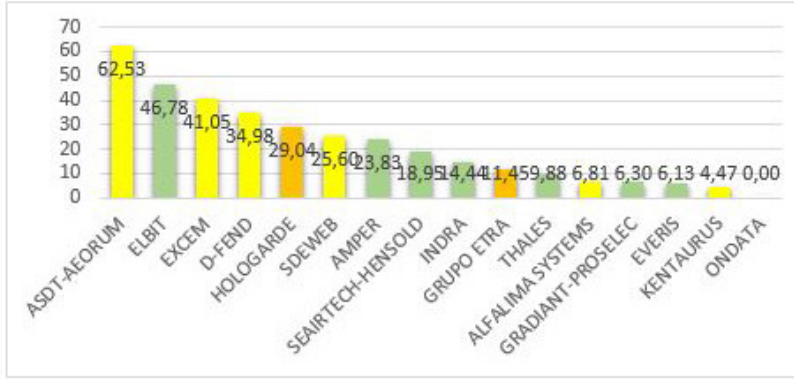


Figura 3. Resultados Asturias global

Globalmente se puede observar que solo una empresa (el 5,5 %) supera el 50 % y solo seis empresas (el 33 %), de dieciocho, superan el 25 %, resultados muy malos desde el punto de vista de la seguridad, esto significa que de cada cuatro drones comerciales que vuelan solo detectamos uno.

7. SIGLO-CD

La Secretaría de Estado de Seguridad (SES) dispuso en 2019 el diseño y la implementación de una plataforma tecnológica que pudiera llevar al desarrollo de un sistema integral contra drones, como protección ante hechos presuntamente ilícitos (vuelos imprudentes o con intención ilegal), así como intrusiones en la privacidad personal, uso por crimen organizado y, en los casos más graves, posibles acciones terroristas. La Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), fue la encargada de poner en marcha el Sistema Global Contra Drones (en adelante, SIGLO-CD). A continuación, vamos a desglosar las fases llevadas a cabo:

Fase O, inicial

El 11 de julio de 2019 se firmó, por parte de la Secretaría de Estado de Seguridad, la resolución por la que se declaraba de emergencia la contratación del servicio de un sistema global.

La premisa inicial fue huir de sistemas *stand-alone*, por lo que se decidió basarse en la arquitectura cliente-servidor, donde los detectores y neutralizadores serían periféricos del sistema y se podrían instalar en el lugar más adecuado. Todas las soluciones tenían que ser interoperables, independientemente del fabricante. La segunda premisa fue, hay que proteger el mayor número de ciudades e infraestructuras, con la mayor eficacia posible, por lo que la balanza calidad-precio es fundamental.

Esta arquitectura cliente-servidor se articula en torno a servidores dedicados pertenecientes a un CPD principal (sede central), sobre el que

transmiten y reciben información, a través de una VPN mallada (no todos los sistemas, los más críticos se conectan mediante APN), los diferentes detectores, neutralizadores y usuarios de la red.

Los sistemas de detección seleccionados inicialmente son pasivos y están basados en detección de radiofrecuencias (RF), ya que el entorno en el que se desplegaron es urbano, también permiten obtener datos de marca, modelo, número de serie, *tracking*..., de los drones comerciales más extendidos, siendo una solución bastante eficaz. Su radio de cobertura es superior a 10 km. La figura 4 muestra la detección de un dron en el barrio de Hortaleza de Madrid.

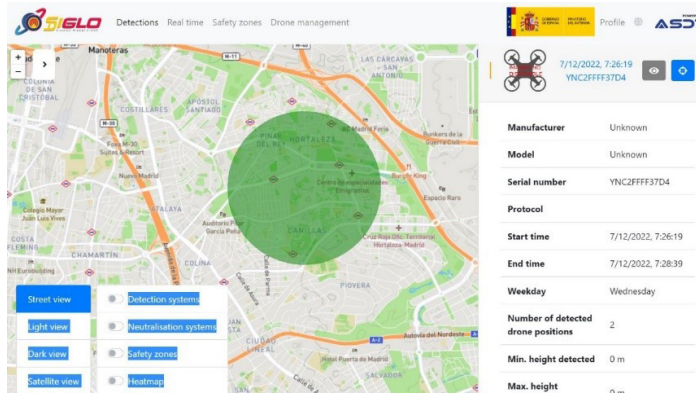


Figura 4. Captura real de pantalla, detectores en Madrid

Respecto a los sistemas de neutralización, se seleccionaron los basados en *jamming*, por las mismas razones que se han descrito. Salvo excepciones, se han seleccionado antenas directivas, para evitar al máximo los daños colaterales que este tipo de soluciones pueden causar.

El Centro de Mando y Control permite la gestión de usuarios. Tiene dos vistas principales sobre un mapa GIS, tipo Google Maps: detecciones en tiempo real, historial de detecciones.

Fase 1

El contrato fue adjudicado en el mes de julio de 2022 y hay de plazo hasta el 31 de diciembre de 2023 para suministrar y realizar el siguiente despliegue: trece puestos de Mando y Control, tres sistemas estacionarios de detección, diez sistemas portátiles de detección con módulo DJI, nueve sistemas estacionarios de neutralización direccional, doce sistemas de neutralización de mano, cuatro sistemas portátiles de neutralización omnidireccional.

Fase 2

Actualmente en intervención, plazo de ejecución de 2023 a 2025. En esta fase se pretende poder desplegar el sistema en 32 ciudades españolas con antenas fijas, incluyendo 86 maletas de detección portátiles.

Estadísticas

Durante el pasado 2021, se han detectado un total de 14.266 vuelos de drones en el casco urbano de Madrid.

8. Conclusiones

Tras analizar más de cien soluciones existentes en el mercado se llegó a la conclusión de que, no existen soluciones globales para dar respuesta a todas las situaciones; la gran mayoría son soluciones *stand-alone*, pero hay muchos escenarios diferentes, con características muy distintas. Por lo que el sistema debe ser escalable, modular, integrable, adaptable al lugar y a la situación.

- Integral. Todos los elementos del sistema, independientemente del fabricante, formarán parte de un todo.
- Modular. El sistema estará formado por diferentes subsistemas de detección, identificación, seguimiento y mitigación de drones. Formado por diferentes piezas, como un puzle, se irán seleccionando las piezas adecuadas dependiendo de la situación y la zona a proteger.
- Escalable. La infraestructura debe ser escalable, con el fin de extender y optimizar la plataforma TIC con el tiempo y garantizar su disponibilidad y sostenibilidad en futuras ampliaciones.
- Adaptable: los sistemas se van a desplegar en diferentes lugares y situaciones, por lo que los mismos han de adaptarse a circunstancias cambiantes, como trabajar en zona urbana o no urbana, o ser fijo o móvil, entre otros.

Sobre la base de los resultados obtenidos en las pruebas y teniendo en cuenta la balanza calidad-precio, para soluciones globales, hoy en día, los mejores sistemas de detección son los basados en radiofrecuencias y los de neutralización los basados en inhibición.

Futuro

El *software* de Mando y Control deberá incorporar ayudas y capacidades de procesamiento basadas en técnicas de inteligencia artificial.

- Algoritmos de inteligencia artificial que permitan la toma de decisiones de modo rápido e intuitivo.
- «Previsión de zonas de intercepciones de drones», en función de los datos proporcionados, basado en patrones del histórico de vuelos con características similares.
- Funcionalidad, «predicción de la acción del piloto» y predicción de trayectoria de vuelo, basada en la velocidad del dron, ubicación, franja horario y expediente del dron, entre otros.

Figura 5. Logo de SIGLO-CD

Referencias

Para la realización de este resumen, no se ha consultado ninguna referencia, salvo la figura 1 obtenida del Plan Director de RPAS de 2015 (DGAM).

Sistema global contra drones.

Autor: José Antonio Cebrián de Barrio
Directora: Milagros Fernández Gavilanes

Introducción

En 2019 la SES del Ministerio del Interior, firmó una resolución por la que se declaraba de emergencia la contratación de un servicio, llamado Sistema Global Contra Drones (SIGLO-CD), con el objetivo de detectar, identificar y seguir drones comerciales en el área Metropolitana de Madrid, y en su caso neutralizar si se considera que amenaza a algunas de las mayores instituciones del Estado.

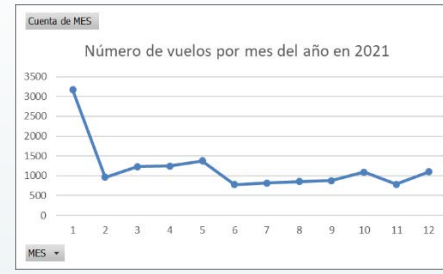
Metodología

Fase para neutralizar un drone:

1. Detección: se detecta algo extraño, inicialmente no se puede saber si se trata de un dron.
2. Identificación: discernir si realmente se trata de un dron y tratar de obtener el mayor número de datos posibles del mismo.
3. Seguimiento: dará indicios de a dónde se dirige y posibles intenciones.
4. Neutralización: en caso necesario.
5. Inteligencia: todas estas fases han de disponer de una cierta inteligencia que ayuden al operador a tomar decisiones en tiempo real.

Resultados

En el año 2022 se han detectado más de 14.000 drones comerciales, volando sobre el casco urbano de Madrid.

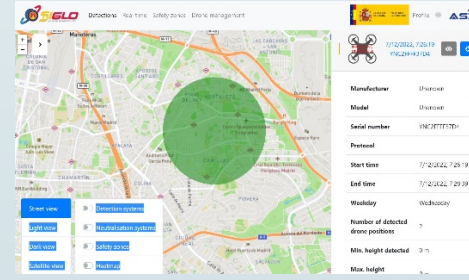


Conclusiones

Siglo CD está operativo en las ciudades de Madrid y Valencia con 13 puestos de mando y control, 13 sistemas estacionarios de detección y 9 sistemas estacionarios de neutralización direccional.

Entre los años 2023 a 2025, se pretende poder desplegar en 32 ciudades españolas, además de disponer de 85 unidades de detección portátiles.

En la imagen, detección real de un drone en el barrio de Hortaleza de Madrid



Evolución del sistema satélite de la Unidad Militar de Emergencias

Autor: Pedro José González Cañas (pedrojosegc@hotmail.com)
Director: José María Núñez Ortuño (jnunez@cud.uvigo.es)

Resumen: – La Unidad Militar de Emergencias (UME) es una unidad militar que por la naturaleza de sus misiones debe estar preparada para actuar en cualquier circunstancia imprevista. En cualquier situación, debe de mantener la operatividad, para ello, es imprescindible dar continuidad al Mando y Control.

Para el apoyo del Mando y Control es elemento básico contar con unos medios de telecomunicaciones e información que, al igual que la propia unidad, se mantengan operativos durante una emergencia.

El medio que puede aportar la suficiente autonomía a la unidad, para no depender del entorno y así, que no se vea afectado por las circunstancias, es el enlace satélite militar. Este tipo de enlace es un sistema robusto y con gran supervivencia. La UME cuenta con un segmento propio para su sistema satélite, dentro de la capacidad satélite gubernamental. La UME gestiona y administra su segmento de forma autónoma.

Este sistema, al igual que la unidad, se creó en 2006 y no ha evolucionado desde entonces, aunque se mantiene operativo y en servicio. Desde 2006, y hasta hoy, las necesidades de comunicaciones han crecido, aunque la capacidad del servicio sigue siendo la misma.

En la época actual, de recortes presupuestarios, se hace difícil la sustitución del sistema completo y, aún más, la adaptación a otras bandas. Por este motivo se pretende estudiar una solución que aporte mayor capacidad al sistema, evolucionando solo algunas partes de este (módems), de tal forma que se obtenga mayor eficiencia del segmento satélite de la UME.

Este estudio es teórico y práctico, de donde se obtendrán unos resultados y unas conclusiones. Del resultado se determinará la conveniencia técnica de realizar la evolución y se propondrá un plan de actualización.

Palabras clave: – UME, Satélite, Modems, MODCOD, Heights, Vipersat.

1. Introducción y objetivos

Introducción

Para su funcionamiento, la Unidad Militar de Emergencias (UME) cuenta con numerosas capacidades. Una de ellas es el Mando y el Control. Esta capacidad es similar al cerebro que controla todas las actividades de un cuerpo, siendo esencial para la correcta y oportuna coordinación de los esfuerzos, tareas y cometidos, que se realizan durante una operación.

El Mando y Control precisa, hoy en día, de un elemento de apoyo esencial: las comunicaciones.

Los sistemas y tecnologías de información y telecomunicaciones (CIS/TIC) proporcionan la capacidad de comunicación y enlace necesaria para dar continuidad al Mando y Control. Dentro de la multitud de medios CIS/TIC con los que cuenta la UME, uno de ellos es el sistema satélite asignado del Sistema Español de Comunicaciones Militares por Satélite (SECOMSAT). La gran ventaja y principal cualidad de este sistema es su autonomía, en referencia a la soberanía que se tiene sobre el mismo.

Objetivos

Este trabajo se basa en un objetivo principal y único: «analizar y valorar si los sistemas de modulación actuales posibilitan un incremento en la eficiencia que se puede obtener del sistema satélite de la UME, para aumentar su rendimiento sin la sustitución de la mayor parte del sistema».

En la línea de acción a recorrer para alcanzar este objetivo principal, es necesario lograr unos objetivos secundarios. Entre estos se incluyen: conocer y entender el funcionamiento operativo de la UME y de su sistema satélite actual; estudios teóricos de las capacidades de modulación actuales; establecimiento de unas condiciones que indiquen la conveniencia de actualizar los módems de la UME; unas pruebas técnicas reales y el contraste de estas con las condiciones establecidas previamente; y, por último, un plan de implantación de un nuevo sistema.

El nivel de autonomía de un sistema podría medirse dependiendo de cuantos y, en qué cantidad, de los siguientes elementos se encuentran bajo el control propio:

- Equipos clientes que dan servicio al usuario y equipos de administración.
- La red de comunicaciones que une los equipos de clientes y administración entre sí.
- La energía que permite el funcionamiento de los equipos.

2. Desarrollo

El sistema satélite de la UME

Consta de un segmento espacial basado de la red SECOMSAT. A diferencia de otras unidades militares, que para hacer uso del SECOMSAT realizan

una solicitud de acceso satélite, la UME tiene asignado un ancho de banda de forma permanente, para ser gestionado de forma autónoma.

Por lo general, la UME no realiza sus enlaces sobre las estaciones de anclaje, sino contra un terminal fijo (TFUME) situado en la Base Aérea de Torrejón, en las instalaciones de la UME. También, como respaldo, pueden realizarse contra la EAN Torrejón y contra dos estaciones móviles de alta capacidad, véase figura 1.

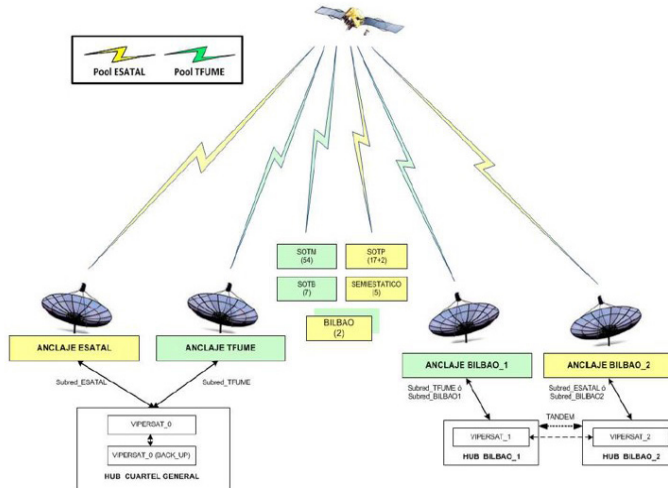


Figura 1. Arquitectura satélite de la UME (diagrama del 2007). Fuente: [1]

El sistema satélite de control dinámico satélite de la UME se denomina Vipersat. Toda la gestión de las comunicaciones satélites depende del terminal de gestión y administración, de los módems CDM-570L y CDD-564L que equipan los terminales fijos y desplegables, y el *software* Vipersat Management System (VMS). Este *software* controla de manera global una red de comunicaciones satélite (espectro asignado a UME: 7 MHz), optimizando dinámicamente el segmento espacial empleado.

La comunicación desde el terminal fijo de la UME hasta los terminales remotos consume un ancho de banda aproximado de 3,71 MHz. Este *outbound* se compone de cuatro portadoras:

- Tres portadoras de 512 kbps (QPSK de modulación) para las estaciones con antenas on the move y terminales ligeros.
- Una portadora de 4096 kbps (16 QAM de modulación) para las estaciones de antenas más grandes.

La comunicación desde los terminales desplegados hasta el terminal fijo consume aproximadamente 3,29 MHz, existiendo un solo TDM, véase la figura 2. Este *inbound* se basa en STDMA (*Selective Time Division Multiple Access*) con posibilidad de conmutar a *simple carrier per channel* (SCPC) de forma dinámica cuando un enlace lo necesita.

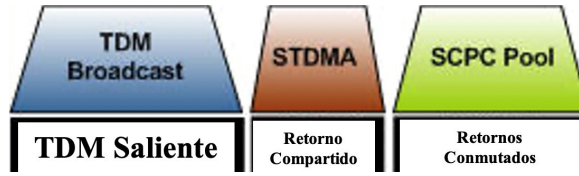


Figura 2. Esquema del outbound y los inbound de Vipersat. Fuente: [1]

Evolución tecnológica

La evolución tecnologíca actual, con respecto a la tecnología instalada con la creación de la UME, atiende a las siguientes características:

- Empleo de un outbound único, gracias a tecnologías de adaptación especifica a cada tipo de terminal remoto. Estas tecnologías aplican diferentes tipos de modulación y codificación (MODCOD) sobre la misma señal, para cada slot de tiempo de cada terminal, dependiendo de sus características.
- Adaptación dinámica a la situación del enlace, para mantener un enlace estable y con la máxima eficiencia posible, adaptándose a las circunstancias externas.
- Menores valores de Roll-off.
- Mejores y más eficientes técnicas de modulación.
- Sistemas de corrección de errores más eficientes.

Condiciones

Las condiciones que, de alcanzarse, apoyarán la recomendación del cambio, son las siguientes:

- Teniendo en cuenta que la mayor parte del sistema se mantiene, incluido el ancho de banda disponible, se obtiene un incremento sustancial de la tasa de datos resultante.
- Disminución del número y tipo de equipos implicados en el funcionamiento, que simplifique la estructura y funcionamiento del sistema.
- Mejora de las técnicas de corrección de errores, que disminuyan el tráfico redundante, aumentando, por tanto, la tasa de datos dedicada a carga útil.
- Mayor aprovechamiento del ancho de banda útil, sin tener en cuenta la tasa de datos.
- Número de estaciones remotas conectadas al sistema al mismo tiempo.

Pruebas

Para probar la compatibilidad de diferentes antenas, sobre el mismo TDM, se realiza una prueba de comunicaciones con el Mérida Bravo (*on the move*) con 321 KHz y el León Alfa (*on the pause*), empleando 315 KHz. Véase espectro de la señal en figura 3.

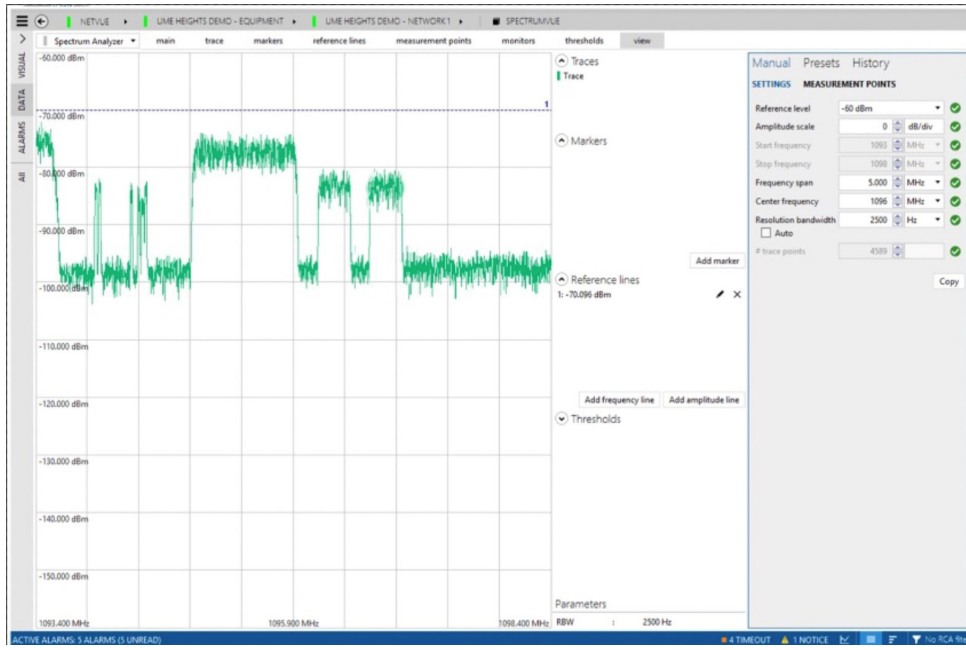


Figura 3. Representación espectral

El León emplea un MODCOD de 32APSK 4/5 para el *outbound,* mientras el Mérida se mantiene con QPSK 2/3. Sin duda, la mayor ganancia de la antena favorece la modulación y la codificación con la potencia existente.

La comunicación de recepción es adecuada en el *outbound* compartido sin necesidad de contar con un TDM especifico, lo cual evita la necesidad de *outbound* dedicados, como se hacía en Vipersat, que restan flexibilidad a la gestión del espectro disponible.

En el *inbound*, el León emplea un VersaFEC-2 de 32-ARY 0.733, mientras que el Mérida mantiene VersaFEC-2 de 32-ARY 0.635.

En cuanto a tasas de datos en descarga, el Mérida, con su antena *on the move*, mantiene tasas entre los 512 y los 1000 kbps de manera estable, mientras que el León alcanza los 1,4 Mbps. En emisión, el Mérida se mantiene en torno a 1 Mbps y el León los supera, alcanzando en torno a los 1,2 Mbps.

3. Resultados y discusión

Una vez concluidas las pruebas y analizando los datos obtenidos, se pueden concretar los siguientes resultados:

Adaptación MODCOD

Se observa cómo se adapta el MODCOD al estado del enlace. Esto es beneficioso para mantener la estabilidad en los enlaces y para sacar el máximo rendimiento cuando las circunstancias los permitan.

Roll-off

En la representación espectral de Heights de la figura 4, se observan unas caídas de las portadoras bastante verticales. Esto es debido al *roll-off* reducido. Gracias a unos valores bajos de este factor hay más aprovechamiento del ancho de banda disponible. En el siguiente gráfico se pueden observar las diferentes caídas entre Vipersat y Heights.

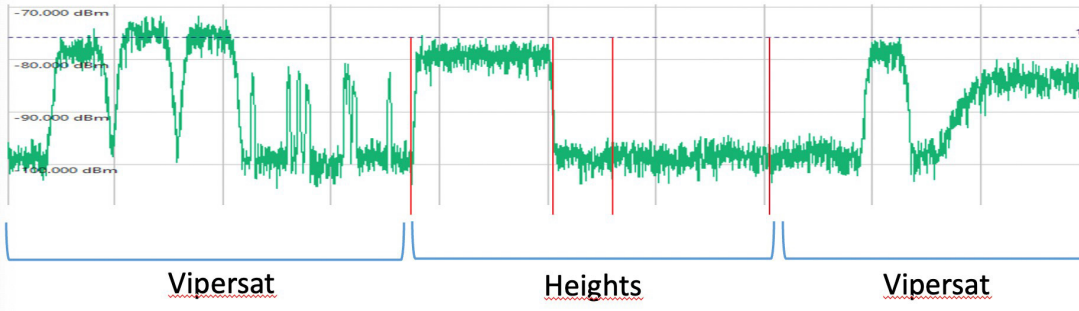


Figura 4. Diferencias en caídas de las portadoras

En un ejemplo matemático, para un ancho de banda de 1 MHz, con un 35 % de *roll-off*, tan solo nos quedarían 650 KHz para la transmisión de símbolos, por los 950 kHz que estarían disponibles con un factor del 5 % para el mismo ancho de banda.

Portadora única

Se ha comprobado en las pruebas como dos estaciones de transmisiones con equipos de comunicaciones satélite diferentes conviven en la misma portadora, con MODCOD diferentes. Así ha sido el caso del Mérida Bravo y el León Alfa en las mismas circunstancias meteorológicas, cuando el Mérida trabajaba en QPSK ¾ mientras que el León empleaba 32 APSK 4/5.

Eficiencia del *inbound*

Las mejoras en modulación hacen que se haga un empleo más eficiente del ancho de banda dedicado al *inbound*. Gracias a este hecho, se consiguen tasas de tráfico mayores con menores anchos de banda, aumentando la eficiencia del sistema, no siendo necesario tener ancho de banda reservado para enlaces SCPC.

Así resultó en las pruebas sobre el Mérida, donde, con los 321 KHz, se obtenían tráficos de más de 1 Mbps con VF2 32-ARY 0,635,. frente a los 500 kbps obtenidos en 8 PSK 3/4 en 384 KHz. Esto supone un 243 % sobre Vipersat para este ejemplo.

FEC

No se ha podido comprobar, durante la realización de estas pruebas, las mejoras técnicas de las nuevas tecnologías de FEC, que ayudarían a

mejorar las correcciones de errores y disminuir el número de paquetes repetidos, así como el número de bits dedicados a corrección. Al reducirse la cantidad de información dedicada a corrección de errores y el número de mensajes repetidos, aumenta el número de símbolos destinados a remitir información útil, aumentando la velocidad de transmisión.

Estabilidad

Con varios equipos remotos simultáneamente, el sistema se mantiene estable, soportando unos valores altos de transmisión que garantizan videoconferencias en buenas condiciones, mientras se envían datos o se realizan llamadas de VoIP al mismo tiempo.

Capacidad

Se ha podido observar claramente, con una de las estaciones empleadas en las pruebas de carga, que el valor de CIR puede ser superado si es preciso, siempre que se mantenga dentro del valor marcado como MIR.

También se ha podido establecer una tasa máxima teórica (no probada) en las circunstancias en las que se realizaron las pruebas, de 10 Mbps de bajada + 9 Mbps de subida. Estas tasas de tráfico en los 7 MHz suponen más de 3,2 bits por hercio.

4. Conclusiones

De las pruebas realizadas se han extraído unos resultados, que verifican que cuatro (4) de las cinco (5) condiciones se cumplen. A continuación, se recoge un extracto de los resultados.

Primera condición

De los resultados obtenidos en las diferentes pruebas realizadas, en el caso de la antena *on the move*, se obtienen unas tasas de datos por hercio que son superadas por Vipersat en el *outbound*, aunque bastante igualadas; y favorables a Heights en el *inbound,* con amplia diferencia.

Este resultado desfavorable a Heights puede ser debido a las combinaciones MODCOD que el sistema selecciona para las antenas *on the move*, que es similar a la máxima modulación empleada por Vipersat. En las pruebas del León Alfa, con la antena *on the pause*, de mayor ganancia, si se llega a un MODCOD de 32 APSK 5/6, muy superior al 16 QAM que ofrece Vipersat como máximo en el *outbound*. En este caso, Heights supera en tasa de datos a Vipersat, tanto en bajada como en subida.

Segunda condición

Para poder dar respuesta a esta condición, ha sido necesario estimar cuál sería la equipación necesaria para el sistema Heights a partir de los datos obtenidos de las pruebas.

Reduciendo la diferencia de equipamiento solo a los terminales centrales (TFUME y EAN Torrejón) y el respaldo de los Bilbao 001 y 002, ya que, en los terminales remotos, el número de módems es similar, se obtiene una cantidad de 67 equipos en Vipersat entre módems y demoduladores. En Heights, se obtiene una cantidad de tan solo doce equipos. Además, con Heights no se precisa el empleo de la EAN Torrejón como respaldo.

Tercera condición

Esta condición no ha podido ser comprobada durante las pruebas, ya que no se ha detectado ningún parámetro del sistema de gestión que aportara los datos adecuados para comprobar mejoras en este aspecto.

Por lo tanto, se considera que esta condición no puede ser concluida como superada, por falta de datos que la apoyen.

Cuarta condición

Esta condición se refiere a los factores que de forma directa influyen en un mayor aprovechamiento del ancho de banda disponible: *roll-off* y modulación.

Con los factores de *roll-off* del 5 % en Heights y del 35 % en Vipersat:

— Heights. 7 MHz x 5 % = 0,350 MHz

— Vipersat. 7 MHz x 35 % = 2,450 MHz

Por lo tanto, el ancho de banda útil para transmisión es de 6,650 MHz en Heights frente a los 4,550 MHz de Vipersat.

La modulación, diferenciada entre bajada y subida:

— Inbound. En Heights se pueden llegar a transmitir 5 bits/símbolo (VersaFEC 32 ARY), mientras que en Vipersat se alcanza un máximo de 4 bits/símbolo (16 QAM).

— Outbound. En Heights se pueden llegar a transmitir 5 bits/símbolo (32 APSK), mientras que en Vipersat se alcanza un máximo de 4 bits/símbolo (16 QAM).

Quinta condición

Se estudia cuantas estaciones pueden entrar en el *inbound* para 300 kbps, que se considera una cantidad media empleada en estas comunicaciones. Para esa tasa, se calcula su ancho de banda asociado, para posteriormente, comprobar que el *hardware* instalado soporta dicha cantidad. Este cálculo se hará de forma teórica, matemáticamente, una vez se ha visto en las pruebas que el sistema Heights soporta este tipo de transmisiones.

Para Vipersat tenemos un *inbound* de 3,71 MHz. Empleando 16 QAM, para conseguir una comunicación de 300 kbps se precisarían 75 KHz. Esta

portadora, con un *roll-off* del 35 % emplea 101,25 KHz. En los 3,71 MHz, supondrían 36 portadoras, que darían enlace a 36 terminales remotos.

Para Heights tenemos un *inbound* de 3,5 MHz. Empleando 32 ARY, para conseguir una comunicación de 300 kbps se precisarían 60 KHz. Esta portadora, con un *roll-off* del 5 % emplea 63 KHz. En los 3,5 MHz, tendrían entrada 55 portadoras para 55 terminales remotos.

Con los módems 570L de Vipersat instalados en TFUME, EAN Torrejón y los Bilbaos, habría cabida para cincuenta terminales, sin tener en cuenta los demoduladores 564L. Con lo cual se podrían conectar los 36 terminales remotos para los que habría portadora.

Con los HRX de Heights, hay capacidad para veinticuatro terminales remotos a un máximo de 5 Mbps. En una propuesta de instalación adecuada a las necesidades operativas, se instalarían dos HRX, uno en TFUME y otro en el Bilbao 002. Por lo tanto, habría cabida para 48 terminales remotos de los 55 para los que habría portadora.

Aunque la propuesta de instalación de Heights es inferior a las capacidades resultantes, la capacidad de 48 terminales supera a los 36 terminales de Vipersat. Por lo tanto, esta condición se considera superada.

Además de los resultados relativos a las condiciones, se pueden extraer otras conclusiones a raíz de las pruebas realizadas:

- El empleo de un solo TDM en el outbound aumenta la flexibilidad y simplifica la gestión de los terminales activos.
- El impacto sobre el sistema actual es mínimo, ya que solo debe sustituirse el subsistema de modulación.
- Con la simplificación de TDM de Heights no se precisa el empleo de la EAN Torrejón como respaldo.
- Con las tasas de datos obtenidas en las pruebas se comprueba que la probabilidad de necesitar enlaces SCPC en Heights es muy reducida.

Referencias

Unidad Militar de Emergencias. (2007). *Arquitectura de Referencia de los CIS de la UME*.

Evolución del sistema satélite de la UME

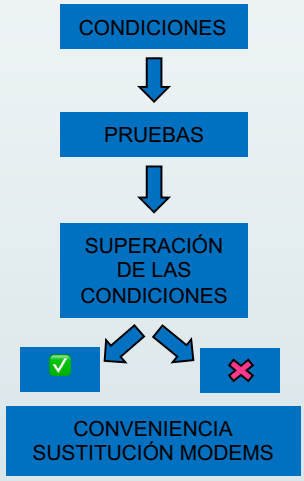
Autor: Pedro José González Cañas
Director: José María Núñez Ortuño
Universidad de Vigo

Introducción

La Unidad Militar de Emergencias cuenta con un sistema satélite del estado, sistema imprescindible por su autonomía, que le hace resistente a casi cualquier fenómeno que se encuentre en una emergencia.
El sistema es estable, pero desde su implantación en 2006, no ha sufrido actualizaciones.
Durante los años que transcurren desde su implantación hasta la actualidad, los módems satelitales han evolucionado, pudiendo ofrecer importantes mejoras al sistema sin sustituir el resto de componentes.

Metodología

La metodología empleada es la científica. Para llevarla a cabo, se han establecido una condiciones que deberán ser superadas en su mayoría para que el resultado de las pruebas técnicas se pueda dar por valido. De esta forma se podrá recomendar la conveniencia de sustituir los módems del sistema satélite de la UME para obtener un rendimiento mucho mayor del mismo, y así actualizarlo a las tecnologías actuales.



Resultados

De las condiciones planteadas previamente a las pruebas, se obtiene que:
1- Se obtienen mejores tasas de bit.
2- La nueva instalación reduciría el número de equipos y simplificaría la instalación.
3- Los factores característicos de los nuevos módems, hacen un uso más eficiente del ancho de banda disponible.
4- La capacidad de conectar terminales remotos aumenta en número con el nuevo sistema.

Conclusiones

1- Se realiza un mejor aprovechamiento de las características técnicas de cada tipo de terminal satélite remoto, mejorando la eficiencia del sistema.
2- Se mejora el aprovechamiento del ancho de banda disponible con los factores de roll-off reducidos.
3- El empleo de un solo TDM en el *outbound*, aumenta la flexibilidad en la gestión de los terminales activos.
4- Se obtienen mayores eficiencias de las modulaciones, que aumentan el tráfico con el mismo ancho de banda.
5- El impacto sobre el sistema actual es mínimo, ya que solo debe sustituirse el subsistema de modulación.

Agradecimientos

A la J6 de la UME. Por darme la posibilidad de cursar este máster y colaborar en la cumplimentación del TFM.
A mis compañeros del V Máster DIRETIC. Porque solo estando todos a una, hemos superado este máster con un compañerismo ejemplar.

Redes de comunicaciones militares Intra-Teatro basadas en tecnología 5G mediante empleo de drones

Autor: Rafael López Lucendo (rlopluc@fn.mde.es)
Director: José Pablo González Coma (jose.gcoma@cud.uvigo.es)

Resumen: – En este trabajo se pretende identificar la aplicabilidad del empleo de una red de comunicaciones en malla mediante el despliegue de un «enjambre» de drones con transceptores 5G, con el propósito de suministrar servicios de telecomunicaciones seguros con un alto ancho de banda y baja latencia, para la ejecución de Mando y Control de un contingente militar desplegado en un escenario alejado del territorio nacional, o cualquier escenario inhóspito en el que no exista una infraestructura que pueda garantizar el adecuado flujo de información de forma inmediata.

La red debe ser capaz de soportar el tráfico de los principales sistemas de Mando y Control de una fuerza desplegada, permitiendo el seguimiento en tiempo real (por geolocalización) de cualquier unidad que pueda ser equipada con un emisor, así como la transmisión de audio y video en alta definición. Asimismo, los drones deben poder operar en modo semi-desatendido durante el tiempo de operación, garantizando una permanencia en servicio elevada y con capacidad de interconexión en malla con otros drones para extender el alcance de la red en función de la demanda.

Esta arquitectura de red permite resolver tres problemas actuales de comunicaciones en zonas de operaciones: la dependencia de sistemas satelitales o de infraestructuras de comunicaciones no propias o inseguras, la disponibilidad del servicio (ya que la red no se puede establecer hasta que la fuerza despliega el equipamiento de comunicaciones) y la dependencia de conexiones físicas (los puestos de mando tienen que ubicarse en proximidad a los terminales satélite).

Palabras clave: – 5G, Dron, Estación base, Malla, Mando y Control, Infraestructura.

1. Introducción

El Mando y Control en las operaciones militares

El éxito de cualquier operación militar radica en un adecuado empleo del Mando y Control (C2) por parte del mando de la operación, entendido el Mando y Control como el ejercicio de la autoridad, la conducción y seguimiento por parte de un comandante o Mando Operativo expresamente designado, sobre las fuerzas asignadas para el cumplimiento de una misión.

Para el adecuado ejercicio del C2, el Mando Operativo debe dotarse de una gran variedad de elementos y capacidades, destacando de una forma muy relevante los sistemas de comunicaciones e información (CIS), que se pueden considerar como el principal medio capacitador en la alimentación de información necesaria para el proceso de decisión.

Los medios y sistemas CIS, por tanto, se consideran un elemento crítico para el desarrollo de las operaciones militares de cualquier índole, por lo que deben estar sostenidos por cimientos robustos que garanticen, no solo la capacidad mínima de conocimiento de la situación, sino una ventaja estratégica sobre el adversario.

El contexto de las operaciones expedicionarias

Las operaciones expedicionarias son, por definición, aquellas que se desarrollan en una nación diferente a la del contingente militar que participa en ella. Si bien el desarrollo de operaciones expedicionarias de combate ha sido residual en las últimas décadas, es muy frecuente la participación de fuerzas militares en operaciones expedicionarias de paz, principalmente en misiones de ayuda humanitaria en escenarios donde se han producido catástrofes naturales. En un escenario de este tipo, existirán daños graves a las infraestructuras de todo tipo, incluyendo las de servicios de telecomunicaciones, además de que existirán dificultades para el acceso a redes de suministro energético, áreas aisladas o de difícil accesibilidad, etc.

Las operaciones expedicionarias pueden desarrollarse en diferentes tipos de escenarios, como, escenarios de crisis, donde existe algún tipo de conflicto que impide unas condiciones mínimas de estabilidad, escenarios de paz, en los que no existen conflictos armados o sociales, y escenarios híbridos o ambiguos, en los que, sin darse las condiciones típicas de un escenario de crisis, se da un entorno de incertidumbre que, de algún modo, puede impactar en la estabilidad.

Bajo estas premisas, un contingente militar que debe desarrollar una operación expedicionaria deberá desplegar desde su base contando con unos medios de comunicaciones e información que le permitan establecer una red de Mando y Control robusta y que cubra todas las necesidades de los sistemas que contribuyen a los diferentes servicios (logística, comunicaciones, inteligencia, intercambio de información y órdenes, vigilancia, etc.).

Las capacidades para el ejercicio del Mando y Control

Las capacidades estándar actuales a disposición de una fuerza militar permiten el establecimiento de un sistema de Mando y Control basado en comunicaciones tácticas de voz y datos en frecuencias HF-VHF-UHF y en enlaces satelitales en bandas X, Ka militar y UHF, mediante el empleo de satélites militares dedicados, o en su defecto, canales protegidos de comunicaciones, a través de satélites comerciales, con capacidad muy limitada, en cuanto a tasa de transferencia, latencia e incluso disponibilidad. Esta limitación constituye un factor crítico en situaciones en las que se debe efectuar un despliegue inmediato de fuerzas y se debe intercambiar un gran volumen de información entre las unidades militares desplegadas y el puesto de mando desde el que se dirigen las operaciones. Por este motivo, es necesario disponer de un método que permita contar con capacidad de intercambio de información a demanda, desde el momento en el que surja la necesidad, con un sistema que pueda garantizar altas prestaciones en cuanto a tasa de transferencia de datos y latencia, y que garantice disponibilidad y flexibilidad en su empleo para poderse adaptar a las condiciones dinámicas de una operación militar.

2. Desarrollo

Arquitectura tipo en un despliegue expedicionario

La arquitectura de C2 en un despliegue expedicionario se debe definir durante la fase de planeamiento de la operación y debe contemplar todos los mecanismos para garantizar el ejercicio del Mando y Control durante todo el desarrollo de la misma. En una operación expedicionaria tipo figura 1, con las capacidades estándar disponibles en la actualidad, la arquitectura de Mando y Control debe proveer los servicios de voz en claro y cifrado entre las fuerzas que despliegan y el mando operativo, enlace de datos para los diferentes sistemas de Mando y Control, y *streaming* de video para dispositivos de vigilancia y exploración.

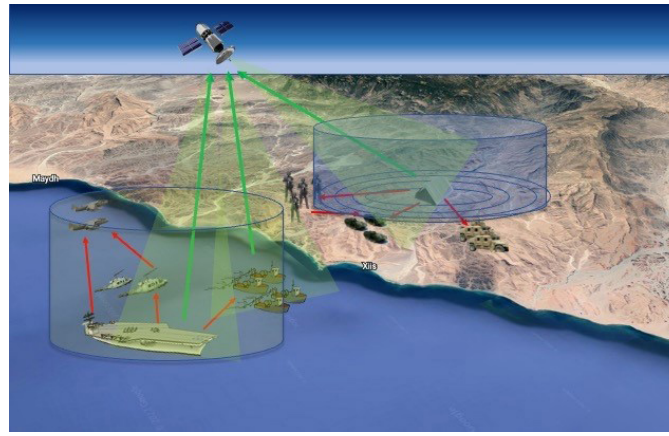


Figura 1. Arquitectura de comunicaciones tipo en un despliegue expedicionario

Para ello, se basará en los siguientes sistemas:

- Enlaces satelitales seguros, a través de los satélites de uso militar dedicado (SECOMSAT).
- Enlaces satelitales de respaldo, a través de satélites comerciales (COMSATCOM).
- Enlaces radio en voz y datos, a través de transceptores de UHF-VHF-HF.
- Dependiendo de las características del escenario y de los requisitos de seguridad de la misión, estas redes se pueden complementar con otros sistemas no securizados, como la red de telefonía móvil.

Limitaciones en la arquitectura tipo

El modelo planteado permite establecer unos enlaces cuya capacidad de servicio está limitada por la propia capacidad del sistema. Aunque la programación de la arquitectura CIS contempla planes de contingencia y alternativos, en caso de falta de disponibilidad de alguno de los medios de mayor capacidad, la arquitectura de reserva puede no ser suficiente para cubrir las necesidades. Este caso se agrava en escenarios donde se tienen que desarrollar las operaciones en terrenos con elevados gradientes orográficos, áreas aisladas o en lugares donde la mayor parte de las infraestructuras han sido dañadas por algún evento catastrófico.

En este tipo de situaciones, es necesario disponer de medios alternativos que puedan complementar la capacidad de los sistemas disponibles en la actualidad, permitiendo su despliegue inmediato desde el momento en el que sea necesario, con facultad para cubrir todos los servicios C2 (alta tasa de transferencia de datos y baja latencia), y con adaptabilidad escalable para permitir la integración de nuevos servicios que puedan ser necesarios. Del mismo modo, los medios alternativos deben poder establecer y mantener enlaces más allá del alcance visual (BLoS), para garantizar las comunicaciones con elementos del contingente que pudieran quedar aislados, y todo ello con unas adecuadas condiciones de confidencialidad, integridad y disponibilidad.

Una posible solución a las limitaciones planteadas es la integración de redes basadas en comunicaciones 5G que puedan ser desplegadas *ad hoc,* empleando vectores que permitan cubrir alcances y zonas de cobertura en función de la demanda. La solución más adecuada, por tanto, es el empleo de drones con transceptores 5G que puedan actuar de forma semiautónoma sorteando las limitaciones mencionadas y dotando a la arquitectura CIS estándar de capacidades ampliadas.

El 5G como alternativa

El 3GPP define al 5G como la quinta generación de la telefonía móvil. Su característica principal es que permite velocidades de transferencia de datos hasta 10 Gbps y con muy baja latencia (1 ms), lo que la sitúa como

una opción a tener en cuenta como alternativa complementaria a los sistemas de comunicaciones disponibles en la actualidad.

Para poder contar con esta tecnología es necesario disponer de estaciones base (BS) que actúen como nodos de anclaje para la conexión de los usuarios (UE) a la red. En una operación militar, y más concretamente en las de carácter expedicionario, para poder contar con tecnologías de este tipo se debe disponer de infraestructura propia, tanto por motivos de seguridad en las comunicaciones, como por las cuestiones obvias de disponibilidad. No obstante, el principal reto que presenta el 5G es la degradación de señal fuera del alcance visual (LoS). Para solventar esta limitación, una solución idónea sería disponer de estaciones base aéreas que pudiesen ubicarse en función de la necesidad para establecer los enlaces óptimos. Esta se podría materializar mediante el empleo de drones como estaciones base, equipando transceptores de 5G para formar redes de comunicaciones de alta capacidad que den cobertura a todo el teatro de operaciones. Además, el disponer de equipamiento propio permite garantizar la disponibilidad, al no depender de infraestructuras externas.

Existen otras alternativas de alta capacidad y baja latencia, como pueden ser la tecnología WIMAX, enlaces satelitales con constelaciones de baja órbita, sistemas de distribución local multipunto (LMDS), sistemas de distribución de microondas multipunto (MMDS), sistemas ópticos punto a punto, redes tácticas de radio, redes WLAN con multisalto, etc., si bien, las características de cada una de ellas presentan diferentes desventajas respecto del empleo del 5G.

Más allá de las desventajas descritas, el Ministerio de Defensa del Gobierno de España definió una «Estrategia de comunicaciones móviles de quinta generación» [1], en la que considera al 5G como una tecnología disruptiva que constituye un componente tecnológico esencial de transformación de la fuerza conjunta, que proporciona soluciones óptimas para habilitar e integrar el empleo de otras tecnologías, como el IoT, la robótica, la realidad mixta, la inteligencia artificial, *Big Data* o el procesamiento en la nube.

Drones como estaciones base

La tecnología asociada al desarrollo de vehículos aéreos no tripulados (UAVs) o drones, ha experimentado un crecimiento vertiginoso en la última década. En la actualidad existe una gran variedad de dispositivos con características muy diferentes que pueden tener aplicación en casi cualquier actividad o sector.

La cantidad de opciones disponibles en la actualidad en el mercado permite combinar perfiles de velocidad, altura de vuelo, autonomía, capacidad de carga, sigilo y prácticamente cualquier otra variable.

Las ventajas del empleo de drones como estaciones base aéreas radican en su facilidad y velocidad de despliegue (se trata de equipos

preconfigurados que se pueden desplegar de forma casi inmediata), su movilidad (al poder ubicar la estación base en cualquier punto del espacio tridimensional libre de obstáculos se pueden establecer enlaces óptimos en LoS) y su seguridad (al no depender de infraestructuras físicas sobre las que se puedan producir daños deliberados).

Estado del arte

Existe una gran variedad de estudios que tratan el empleo de drones como estaciones base aéreas de 5G, desarrollando su aplicabilidad para diferentes funciones y planteando los retos a los que se expone la implantación de esta tecnología. Una lista de los más relevantes se detalla en la siguiente tabla.

Enfoque de aplicación	Papel del dron	Función alcanzada	Referencia
Redes inalámbricas celulares	BS aérea	Acceso y cobertura ubicua	[2][3]
Redes de retransmisión inalámbricas	Relé aéreo	Conectividad inalámbrica	[4][5]
Redes aire-tierra multinivel	BS aérea	Mayor eficiencia espectral en enlace descendente	[6][7]
Redes aéreas *ad hoc*	Enjambre de drones	Eficiencia de uso mejorada de drones individuales	[8]
Malla aérea	Relé aéreo	Redes de drones totalmente conectadas	[9]
Redes alimentadas de forma inalámbrica	Fuente de energía aérea	Transferencia de energía inalámbrica	[10]
Redes inalámbricas asistidas por caché	Caché aéreo	Carga de *backhaul* inalámbrico reducida	[11]
Redes de acceso radio en la nube	Caché/acceso radio aéreo	Distribución de caché y conectividad inalámbrica	[12]
Redes de emergencia	BS/relé aéreo	Cobertura y retransmisión de la información	[13]
Redes radio cognitivas	Dispositivo cognitivo aéreo	Acceso a espectro dinámico	[14]

Tabla 1. Estudios relevantes sobre empleo de drones como BS aéreas 5G

Escenarios de estudio

Se plantea el estudio de arquitecturas C2 para escenarios de paz o de baja y media intensidad, donde se debe desplegar un contingente militar para desempeñar una operación expedicionaria en un entorno en el que no existe una amenaza ni una oposición a la presencia de fuerzas militares. Se considera que las infraestructuras locales no permiten establecer enlaces inalámbricos de ningún tipo, por lo que es necesario contar únicamente con medios propios para establecer todos los circuitos de comunicaciones.

Se dan dos casos de uso, uno consistente en un despliegue de contingente desde una plataforma naval, en la que permanece embarcado el

puesto de mando y desde donde se deben desplegar las estaciones base aéreas para dar cobertura de datos mediante relés, y un segundo caso, consistente en un despliegue completo de contingente militar, proyectado desde territorio nacional, que establece el puesto de mando en tierra y desde donde se dirigen todas las operaciones, incluido el despliegue de estaciones base.

Se deben identificar todos los sistemas disponibles para el C2 en cada caso de uso, así como los servicios que deberán alimentar, para en conjunción con los movimientos previstos, y definir el plan de despliegue óptimo.

Integración de las estaciones base aéreas

Para identificar la aplicabilidad es necesario estudiar una gran cantidad de factores: recursos disponibles, frecuencias de uso, alcance de los enlaces, potencia de transmisión, autonomía de drones, sistemas de alimentación, planes de recarga, perfil de misión, etc. El resultado debe ser una arquitectura robusta, flexible, escalable e interoperable. También se deben abordar diferentes desafíos, como los riesgos relacionados con la seguridad de las comunicaciones, el impacto de las condiciones meteorológicas, aspectos normativos en la gestión del espectro radioeléctrico y la aeronavegabilidad, gestión de enjambres de drones y, por encima de todo, la gestión de la energía.

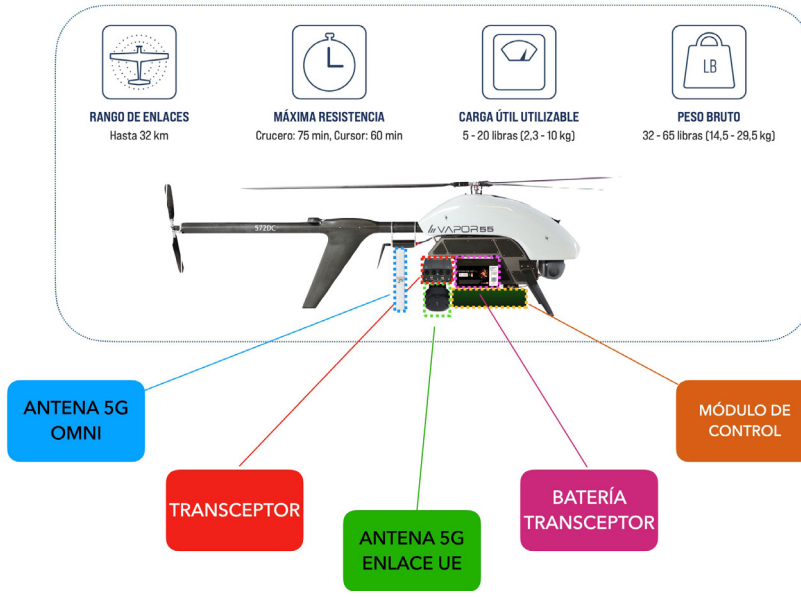


Figura 2. Configuración tipo de dron con módulo 5G

Un modelo de las características que se detallan en la figura 2, permitiría dar cobertura ubicua de datos de alta capacidad o establecer enlaces como relé para dar servicio a cualquier elemento de un contingente desplegado en cualquiera de los escenarios planteados. Con el equipamiento

incorporado podría establecer enlaces MIMO con haces *beamforming* en LoS con los elementos en tierra, utilizando la banda de ondas milimétricas del espectro 5G, al mismo tiempo que podría establecer enlaces de largo alcance con otros drones o con estaciones base en tierra, utilizando las bandas medias y baja de 5G.

3. Conclusiones

El empleo de estaciones base 5G aéreas mediante drones, supone una solución idónea como elemento complementario en la arquitectura de Mando y Control para los escenarios planteados, un sistema basado en estaciones base aéreas con capacidad 5G. Este modelo permite resolver las tres principales limitaciones de la arquitectura típica tradicional:

- Dependencia de sistemas satelitales o de infraestructuras de comunicaciones no propias o inseguras. Si bien se requerirá una pasarela en el puesto de mando para conectar la red a internet o a emplazamientos de red privada remotos, los elementos desplegados en el teatro no requerirán de ningún otro sistema para acceder a la red C2.
- Disponibilidad del servicio desde el primer momento del despliegue. Con este modelo no será necesario esperar a establecer enlaces satelitales o desplegar infraestructuras físicas en el terreno. El acceso a la red estará disponible en el instante en el que el dron sobrevuele la zona de cobertura.
- Dependencia de conexiones físicas. El puesto de mando avanzado tendrá conectividad directa de alta capacidad desde el momento en que comience su desembarco, incluso antes de desplegar sus medios sobre el terreno. Cualquiera de los elementos terrestres tendrá acceso a la red, independientemente de si se encuentra en una zona aislada, alejada o de difícil accesibilidad.

Respecto de las líneas futuras, existen aspectos que deben desarrollarse para optimizar el empleo de este tipo de estaciones base aéreas. La comunidad científica coincide en resaltar la necesidad de mejorar la autonomía de las aeronaves, bien con nuevas fuentes de energía o bien con optimización de las disponibles; además, se considera conveniente profundizar en la gestión automatizada de las mallas de drones, para conseguir un funcionamiento autónomo que garantice los canales óptimos de enlace; del mismo modo, se debe mantener el foco sobre la investigación de nuevas tecnologías que puedan incorporarse al modelo, para facilitar su escalabilidad.

Agradecimientos

Al director de mi trabajo de fin de máster, a los profesores del CUD de la Escuela Naval Militar, a mis compañeros de máster y de especialidad y a mi familia, por haberlo hecho posible.

Referencias

Błaszczyszyn, B. y Giovanidis, A. (2015). Optimal geographic caching in cellular networks. Proc. *IEEE Int. Conf. Commun. (ICC)*, p. 3358-3363.

Dhillon, H. S. y Andrews, J. G. (2014). Downlink rate distribution in heterogeneous cellular networks under generalized cell selection. *IEEE Wireless Commun*. 3(1): p. 42-45.

Ding, M. *et al.* (2016). Performance impact of LoS and NLoS transmissions in dense cellular networks. *IEEE Trans. Wireless Commun*. 15(3), p. 2365-2380.

España. (2021). Resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaría de Estado de Defensa. Estrategia de comunicaciones móviles de quinta generación.

Heath, W., Kountouris, M. y Bai, T. (2013). Modeling heterogeneous network interference using Poisson point processes. *IEEE Trans. Signal Process.* 61(16): p. 4114-4126.

Hellaoui, H. *et al.* (2018). Aerial control system for spectrum efficiency in UAV-to-cellular communications. *IEEE Communications Magazine*. 56(10): p. 108-113.

Sekander, S., Tabassum, H. y Hossain, E. (2017). *Multi-tier Drone Architecture for 5G/B5G Cellular Networks: Challenges, Trends, and Prospects*. arXiv. 2017; arXiv:1711.08407.

Sun, R. y Matolak, D. W. (2017). Air-ground channel characterization for unmanned aircraft systems—Part II: Hilly and mountainous settings. *IEEE Trans. Veh. Technol.* 66(3), p. 1913-1925.

Wang, H. *et al.* (2018). Resource allocation for energy harvesting-powered D2D communication underlaying UAV-assisted networks. *IEEE Transactions on Green Communications and Networking*. 2(1), p. 14-24.

Wu, H. (2018). On base station coordination in cache- and energy harvesting-enabled HetNets: A stochastic geometry study. *IEEE Trans. Commun.* 66(7), p. 3079-3091.

Yin, S., Tan, J. y Li, L. (2017). UAV-assisted cooperative communications with wireless information and power transfer [en línea]. Disponible en: https://arxiv.org/abs/1710.00174

Yu, P. S. (2016). Traffic offloading in heterogeneous networks with energy harvesting personal cells-network throughput and energy efficiency. *IEEE Trans. Wireless Commun.* 15(2), p. 1146-1161.

Zeng, Y., Zhang, R. y Lim, T. J. (2016). Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Communications Magazine*. 36-42; 54(5), p. 36-42.

Zhang, C. y Zhang, W. (2017). Spectrum sharing for drone networks. *IEEE Journal on Selected Areas in Communications*. 35(1), p. 136-144.

Redes de comunicaciones militares Intra-Teatro basadas en tecnología 5G mediante empleo de drones

Autor: Rafael López Lucendo
Director: José Pablo González Coma

Universidad de Vigo

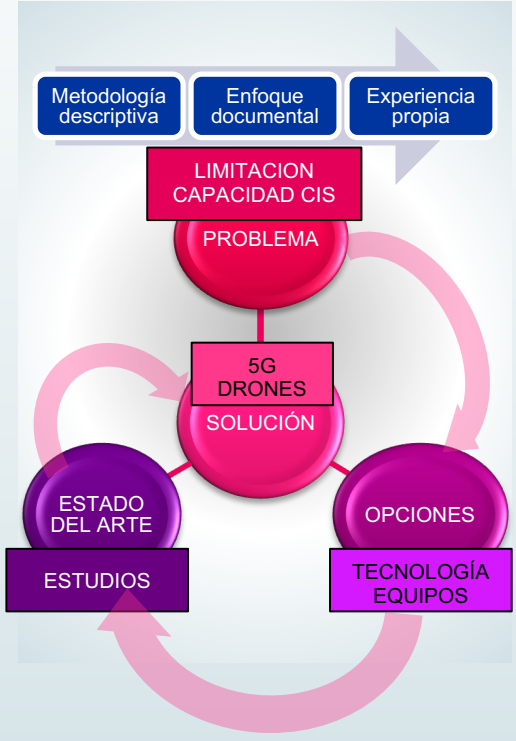
Introducción

NECESIDAD DE SOLUCIÓN PARA FACILITAR COBERTURA INALÁMBRICA DE ALTA CAPACIDAD PARA UN CONTINGENTE MILITAR EN OPERACIONES EXPEDICIONARIAS COMPLEMENTANDO LOS SISTEMAS DE TELECOMUNICACIONES MILITARES

Resultados

Estaciones base 5G aéreas en escenarios sin infraestructura de telecomunicaciones o con infraestructura insuficiente

Metodología



Conclusiones

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Propuesta de arquitectura para la red táctica permanente multi-dominio JRE nacional

Autor: José Luis Martínez Leyva (jmarley@fn.mde.es)
Directores: José González Coma (jose.gcoma@cud.uvigo.es) y Francisco Javier Rodríguez Martínez (franjrm@uvigo.es)

Resumen: – La Directiva 19/19 del Jefe del Estado Mayor de la Defensa (JEMAD), que marca las líneas generales para el desarrollo, evolución e interoperabilidad de la capacidad de enlace de datos tácticos (TDL) en las Fuerzas Armadas españolas, describe una variedad de tecnologías utilizadas por ciertas unidades militares, integradas en redes tácticas seguras y ultrarrápidas, mediante equipos radio específicos. En el marco de la transición de las denominadas TDL, Link16, implementado sobre la plataforma radio JTIDS/MIDS, es el protocolo de mayor capacidad utilizado en el ámbito de la OTAN, constituyéndose en ventaja tecnológica decisiva en el campo de batalla. Un protocolo que trabaja en la denominada banda Lx (UHF de 960 a 1215 MHz), limitando su alcance a la línea de vista (LOS) por tanto, en el ámbito estrictamente táctico. El *Joint Range Extension Protocol* (JREAP), permite extender más allá de la línea de vista (BLOS) la capacidad Link16, empleando enlaces vía satélite, terrestres o redes TCP/IP, superando así dicho ámbito táctico para presentarse en el estratégico-operacional.

Este trabajo tiene como objetivo fundamental realizar una propuesta de arquitectura para una red de tal naturaleza, basada en el despliegue de procesadores JRE, que sea distribuida, permanente y multi-dominio. Que permita a los mandos militares el seguimiento de las operaciones en curso por muy lejos que de estas se encuentren. De forma adicional, se propone un modelo basado en microservicios en el entorno limitado de la Red de Mando y Control de la Defensa (SC2N) para una explotación más eficiente de la información táctica allí producida.

Palabras clave: – Táctica, Link16, JRE, Operaciones, Satélite, Web-services, Microservicios

1. Introducción y estado del arte

Antecedentes históricos

Desde la antigüedad, el comandante de una fuerza ha tenido la necesidad de emplear los recursos de los que disponía con inteligencia y determinación para lograr la derrota del enemigo. Mucho antes de las comunicaciones por radio actuales, existieron otras muy distintas, basadas en mensajeros y algún tipo de señal simple.

Tras la Segunda Guerra Mundial, y sobre todo la guerra de Vietnam, las lecciones aprendidas sobre dichos conflictos, por parte de las fuerzas de los Estados Unidos y sus aliados, hacen pensar en la necesidad de impulsar el desarrollo de nuevas herramientas para el intercambio y difusión veloz de información táctica. Surge en ese momento la necesidad de desarrollar un sistema que permitiese, por un lado, conocer con exactitud, y en todo momento, la posición de las fuerzas propias, y, por otro, que permitiese el intercambio ultrarrápido y seguro de la información táctica disponible entre las diferentes unidades y centros de mando.

Contexto y motivación

La Directiva 19/19 del JEMAD (Jefe del Estado Mayor de la Defensa) [1], que marca las líneas generales para el desarrollo, evolución e interoperabilidad de la capacidad TDL en las Fuerzas Armadas, describe una variedad de tecnologías de enlace de datos tácticos que los mandos militares puede utilizar para llevar a cabo y/o supervisar las operaciones. En este sentido, Link16, descrito en el STANAG 5516, es el sistema/protocolo más importante y de mayor capacidad utilizado, hoy en día, por las naciones OTAN y aliadas. Se basa en la utilización de equipos radio especiales, sea el *Joint Tactical Inforrnation Distribution System* (JTIDS) o sea el *Multifunctional information Distribution System* (MIDS), integrados en las diferentes unidades.

Conviene precisar que en el contexto de este trabajo los datos o información táctica se refiere a la que procede de los sistemas de las plataformas de combate y, en particular, aquella información táctica proveniente de diferentes sensores, y que las tecnologías TDL que «engloba a aquellos procedentes de las plataformas de combate aéreas y de superficie (navales y terrestres), radar, sónar, sistemas de identificación amigo-enemigo, de guerra electrónica, de observación, y en general, de aquella información táctica procedente de diferentes sensores» [1] y que los TDL son el subconjunto de los datos o información proveniente de las determinadas «comunicaciones radio estándar que se rigen por una estructura de mensajes formateados y un uso compartido del ancho de banda respecto al tiempo» [1].

La capacidad TDL se materializa mediante el uso de equipos radio especiales y una serie de protocolos estandarizados internacionalmente que

realizan el intercambio de la información táctica obtenida de diferentes sensores. Dicho intercambio incluye texto planto y voz digitalizada, no así video. Cabe resaltar que la mayor parte de los sistemas/protocolos TDL pueden ser traducidos para ser interoperables entre sí, mediante la formalización del denominado *data forwarding*, sustentado en el STANAG 5616.

En virtud de la citada directiva, los TDL, formando parte de los Sistemas de Mando, Control y Comunicaciones (C3), tienen como objetivo fundamental la difusión e intercambio de información táctica (datos tácticos) entre las unidades desplegadas, para permitir optimizar las capacidades militares conjuntas.

Para lograr tal fin, el concepto de empleo conjunto de las TDL en la OTAN [2] establece que las TDL son la fuente de información en tiempo real principal que alimenta la *Common Operational Picture* (COP), producto que permite la visualización de la situación operativa común dentro de una operación militar, herramienta que da la agilidad necesaria al planeamiento y a la conducción de las operaciones.

En este sentido, en 2013, el Comandante del Mando de Operaciones (CMOPS) aprueba el concepto de empleo operativo de las TDL, estableciendo que «constituyen una herramienta esencial en las operaciones conjuntas pues permiten acceder a la información táctica en tiempo real y evaluar la situación actualizada» [3].

Por otra parte, el concepto *Federated Mission Network* (FMN) establece también [4] que «Estas Instrucciones para enlaces de datos brindan orientación sobre la implementación de la federación de servicios para respaldar el uso de mensajes TDL dentro de una Red de misión federada, utilizando específicamente JREAP-C», lo cual nos indica el camino a seguir para formalizar una arquitectura de la naturaleza que se propone en este trabajo en el marco de la SC2N que, en este sentido, conviene recalcar lo que supone SC2N como red integral y vertebradora: «que permite al JEMAD y a los jefes de Estado Mayor de los Ejércitos y la Armada, dentro sus competencias, definir, dirigir, organizar, planear, preparar, sostener, emplear y efectuar el seguimiento del empleo de la Fuerza Conjunta de manera eficaz y de forma precisa, segura y rápida», según cita la Directiva 02/2019 de JEMAD [5] que desarrolla e impulsa la SC2N.

Toda esta visión es fundamento de lo establecido en el documento de Requisitos de Estado Mayor (REM) «Migración de los Sistemas TDL de las FAS» aprobado por JEMAD, en 2020, apartado «3.1.1 Misión y Amenaza» [6], donde sienta la configuración en dos capas diferenciadas:

- Capa inferior: formada por TDLs que recogen la información de sensores de los sistemas de armas/combate en tiempo real.
- Capa superior: formada por los sistemas de Mando y Control de nivel operacional y estratégico militar que reciben la información de los TDLs y la presentan adecuadamente en tiempo útil.

2. Objetivos y alcance

El objeto del presente trabajo, teniendo en cuenta lo visto anteriormente, es concretar una propuesta de arquitectura de red/sistema distribuido de alto nivel, basada en el protocolo JRE, descrito en el STANAG 5518, que sea multidominio y tenga carácter permanente a nivel nacional.

De forma adicional, se presenta un enfoque desde la perspectiva de servicios que pueden proporcionarse en el entorno concreto de la SC2N. Dicha red/sistema tendrá la denominación genérica de red JRE nacional.

Es obvio, por otra parte, que la misión fundamental sea la de dar respuesta en el ámbito estratégico-operacional a la necesidad que tienen las FAS, tanto desde la perspectiva de los ejércitos por separado como de forma conjunta, a la eficaz explotación de la información táctica procedente de la ingente cantidad de datos que proporcionan los sensores de las unidades militares desplegadas tanto en territorio nacional como en el extranjero.

El alcance del presente trabajo se muestra en la tabla 1 siguiente:

Área	Autoridad
Conceptual	DLMC
Operativa	CMOPS / MACON-JFAC-AOC / DLMC
Técnica	CESTIC
Funcional	MACOM-JSVICA-CRC/ARS / MACOM-JFAC-AOC / DLMC / CESTIC
Seguridad	EMAD-CRIPTO/CCN

Tabla 1. Alcance por área/responsabilidad

Por ello, el GT JRE nacional liderado por el DLMC, creado al efecto, debe tomar la iniciativa y proponer primero una arquitectura que cubra los requisitos de los ejércitos e impulsar después su desarrollo, mediante un proyecto que cubra todas las necesidades, incluidas las instrucciones que regulen y de coordinen su explotación, gestión y administración. Este trabajo podría constituir la base de alto nivel para dichos trabajos.

3. Estado del arte

Actualmente, las FAS españolas explotan una diversidad de sistemas de intercambio y diseminación de información táctica, ya sea específicamente TDL o no, que de forma heterogénea han venido resolviendo tales necesidades. Al respecto hay que mencionar el Sistema de Gestión de Batalla BMS-LINCE, integrado en el Sistema de Mando y Control del Ejército de Tierra (SIMACET), que contribuyen a la conformación de la *Recognized Ground Picutre* (RGP) y Sistema de Información y de Vigilancia Integrado para el Conocimiento del Entorno Marítimo (SIVICEMAR) de la Armada, que hace lo propio en la conformación de la *Recognized Maritime Picutre* (RMP). Sin embargo, ambos sistemas no

implementan ningún protocolo TDL. El Ejército del Aire y del Espacio, por otro lado, cuenta con Sistema Integrado de Vigilancia Aeroespacial (SVICA), basado en el despliegue de varias estaciones radar en el territorio español, implementando diferentes TDL, como Link16, Link11 y Link11B, exclusivamente para la imagen de situación táctica aérea o *Recognized Air Picture* (RAP).

Teóricamente, dichas *pictures* deberían contribuir en su conjunto a la conformación de una COP conjunta, fuertemente enlazada con la denominada *Situational Awareness* (S-AWAR), o conciencia de la situación común, que integra múltiples fuentes de información, aparte de las TDL. Sin embargo, esto no ocurre así en la actualidad de una manera consistente, fiable y completa.

El esfuerzo común más importante llevado a cabo al efecto, son los Proyectos JRE y LINPRO (procesador TDL desarrollado por la empresa española TECNOBIT). La infraestructura resultante se compuso de diverso equipamiento y una configuración de enlaces de comunicaciones sobre la infraestructura de telecomunicaciones de la defensa (I3D), para una red UDP *multicast,* basada en JREAP. Buena solución de partida, pero rígida, semipermanente, *ad hoc*, sin ninguna norma que la regule y donde no existen ni roles ni responsabilidades asignados.

La figura 1 ilustra la situación de partida que contemplaron dichos proyectos, donde una operación *multilink* (a), que despliega unidades de muy diversa índole, aporta y disemina información táctica directamente desde el ámbito táctico para que sea mostrada en un mapa situacional (b) que otro mando o centro directivo, dentro del ámbito táctico, podrá visualizar y explotar.

En lo que respecta al enfoque hacia los servicios que se pretende, destacar los trabajos realizados en el ámbito del Grupo de Trabajo TDL Cat XMLS (XML Syndicate) de la OTAN, donde se han desarrollado varias propuestas de descripción y modelado de datos en formato *Extensible Markup Language* (XML) de los elementos de configuración de los distintos TDL. Conviene resaltar también, el uso actual que se realiza de herramientas específicas OTAN como el *Integrated Command and Control* (ICC), junto al *Networked Interoperable Real Time Information Services* (NIRIS), que dan cobertura parcial a las necesidades de intercambio flexible de información táctica, empleando el paradigma cliente-servidor, aunque exclusivamente en el entorno táctico hasta tanto no se desarrollen por completo los conceptos FMN en el ámbito de la SC2N.

4. Desarrollo

El paso lo marca la directiva de JEMAD [1], donde cita:

> «Por otra parte, la flexibilidad y distintas arquitecturas que ofrece el protocolo JREAP C requieren la determinación de una arquitectura única a implantar a nivel conjunto. Esta arquitectura al mismo tiempo deberá permitir la interoperabilidad con las

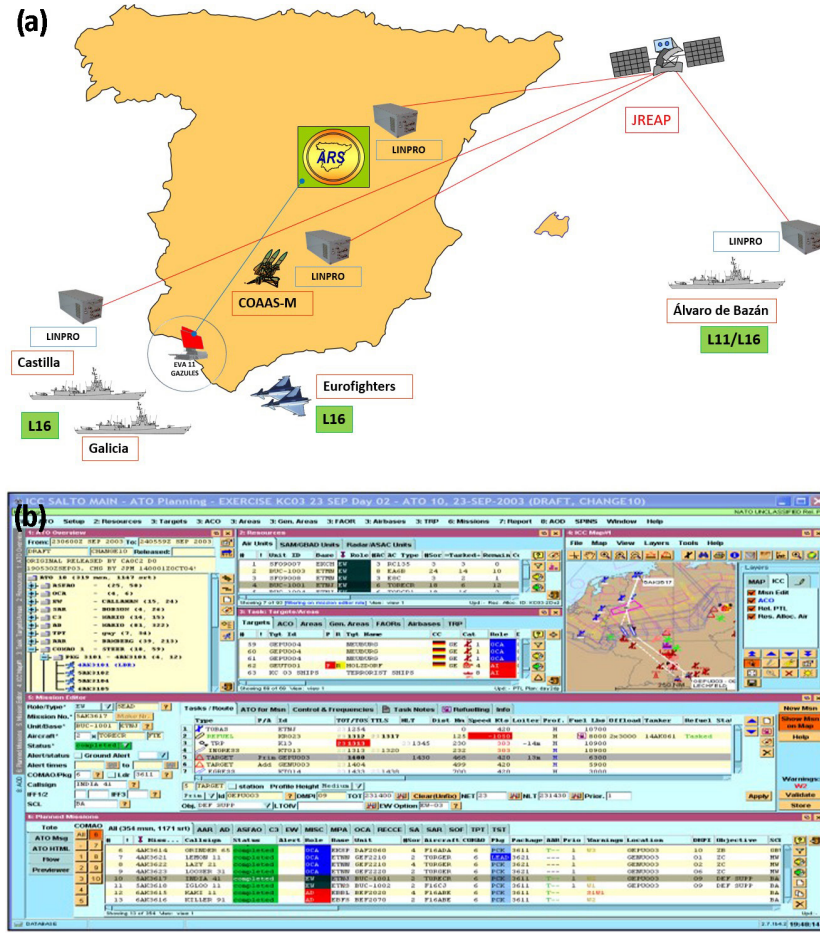


Figura 1. Operación multilink apoyada en JREAP/LINPRO (a). Imagen situacional mediante COP (b)

distintas agencias y organismos de la OTAN involucrados en la defensa aérea, y en términos conceptuales viene representada según el siguiente gráfico».

Para tal labor, partiendo de una visión y misión de la red JRE nacional, este trabajo propone un desarrollo iterativo enmarcado en una serie de etapas que resuelvan lo siguiente:

- Determinación de los elementos, actores de la organización y entidades físicas que conformarán la red JRE nacional, con sus roles y responsabilidades.
- Determinación de requisitos funcionales, operativos y técnicos.
- Sopesar alternativas.
- Visión general de la red JRE nacional, primero desde una perspectiva exclusiva de despliegue de los JRE processors y segundo desde una óptica integral que incluya el enfoque de servicios.

Visión y misión

Partiendo del liderazgo JEMAD, el sistema se propone, como referente que permita a los mandos militares, tanto del entorno táctico como del estratégico-operacional, explotar una imagen (*picture*) de varios niveles, enriquecida con la aportación de la información táctica que proviene de los TDL.

La misión de la red JRE nacional sería la de incrementar la capacidad de los TDL actuales (como Link16, Link22 y/o Link11), extendiendo su alcance a BLOS, por un lado mediante el despliegue de los JRE *Processors*, ofreciendo con un alto grado de calidad, disponibilidad, flexibilidad y detalle la información táctica disponible, por otro mediante el enfoque de servicios en el entorno concreto de la SC2N.

Para conseguirlo, la mayor autoridad estratégico-operacional de las FAS que es JEMAD, promulgando una norma al respecto, ha de lograr la implicación de todos los actores interesados en la consecución de las metas que plantea la red JRE nacional, incluso planteando colaboraciones estrechas, relaciones directas e integración de estructuras de forma temporal.

Elementos de la red JRE nacional

En la tabla 2 siguiente, se muestran los roles y responsabilidades correspondientes a los diferentes elementos, ya sean actores de la estructura orgánica de las FAS o entidades físicas que conforman la red JRE nacional:

Área	Autoridad	Responsabilidad	Rol JRE	Rol FMN
Conceptual	DLMC	Desarrolla	-	-
Operativa	CMOPS	Conducción/Dirección	JRE-NP	*Node*
Operativa	MACOM-JFAC-AOC	Coordina/Planea	JRE-NP	*Node*
Operativa	DLMC	Diseña/Custodia	-	-
Técnica	CESTIC	Gestiona/Administra	-	-
Funcional	MACOM-JSVICA-CRC/ARS	Ejecuta tareas ordinarias	JRE-NP	*HUB*
Funcional	MACOM-JFAC-AOC	Ejecuta tareas ordinarias	JRE-NP	*Node*
Funcional	DLMC	Ejecuta tareas ordinarias	JRE-NP	*Node*
Funcional	CESTIC	Apoyo ejecución tareas ordinarias	-	-
Seguridad	EMAD-CRIPTO/CCN	Monitorización	-	-
Usuario Táctico	Unidades y plataformas EA, ET y AR	Explotación	FJUG	
Usuario SC2N	Cuartes, Centros y Unidades	Explotación	JRE-NP	*Node*
Usuario HUB	Centros TDL	Gestión y explotación	JRE-NP	*HUB*

JRE-NP: JRE *network participant* (NP).
FJUG: *Dataforwarding Unit* (en este contexto entre Link16 y JREAP).
HUB: nodo central para la distribución y diseminación de información táctica.
Node: nodo integrado de la red JRE nacional integrado en la SC2N.

Tabla 2. Roles y responsabilidades de los elementos de la red JRE nacional

En la tabla 3 siguiente, se muestran los requisitos funcionales, operativos y técnicos que hay que tener en cuenta a la hora de desplegar la red JRE nacional propuesta:

	Funcionales	Operativos	Técnicos	
Tipo de flujo:	*Multicast* o *unicast*	OTL segmento JRE	Comunicaciones E y P	CESTIC
Protocolo:	TCP o UDP	OTL segmento JRE	Administración R y N	CESTIC
	Número de trazas		Comunicaciones D	Usuario
Filtro:	Local o remoto (estático o en tiempo de ejecución)	OTL segmento JRE	Config JRE *Processors*	Usuario
			Sistemas TDL	Usuario
			Redes TDL	Usuario
			Sistemas C2	Usuario

E: estática; P: permanente; R: roja; N: negra; D: desplegable.

Tabla 3. Requisitos funcionales, operativos y técnicos red JRE nacional

Respecto a la tabla anterior, hay que recalcar que una traza es la expresión genérica utilizada para la indicación unidades que han sido captadas mediante algún tipo de sensor, ya sean propias, remotas o mutuas, dependiendo de quién es el responsable de esta. En este sentido, una traza se referencia (datos de traza) mediante un código único *Track Number* (TN) o *Source Track Number* (STN) y tiene dos características fundamentales que son la identidad y la categoría (ver figura 2).

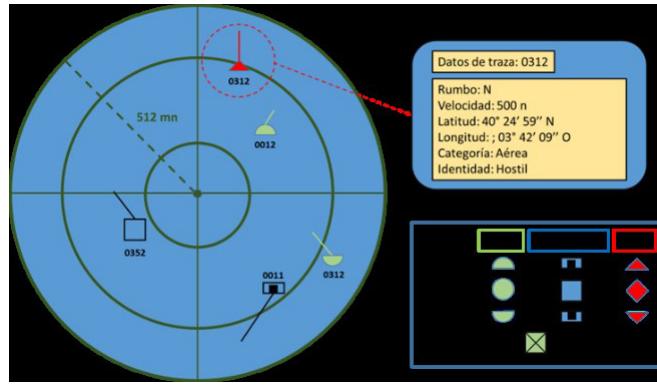


Figura 2. Imagen consola radar

Respecto a los filtros, que pueden ser definidos de forma local o remota, aplicables a las trazas mediante una acción del operador del JRE *processor*, tendríamos por categoría, identidad, geográficos, distancia (máxima y mínima), sectores (demoras y distancia), etc.

En la figura 3 siguiente, se presenta la arquitectura final objeto de este trabajo para la red JRE nacional, teniendo en cuenta el despliegue, exclusivamente nacional, de los JRE *Processors* necesarios y el despliegue de los elementos básicos del modelo de microservicios propuesto.

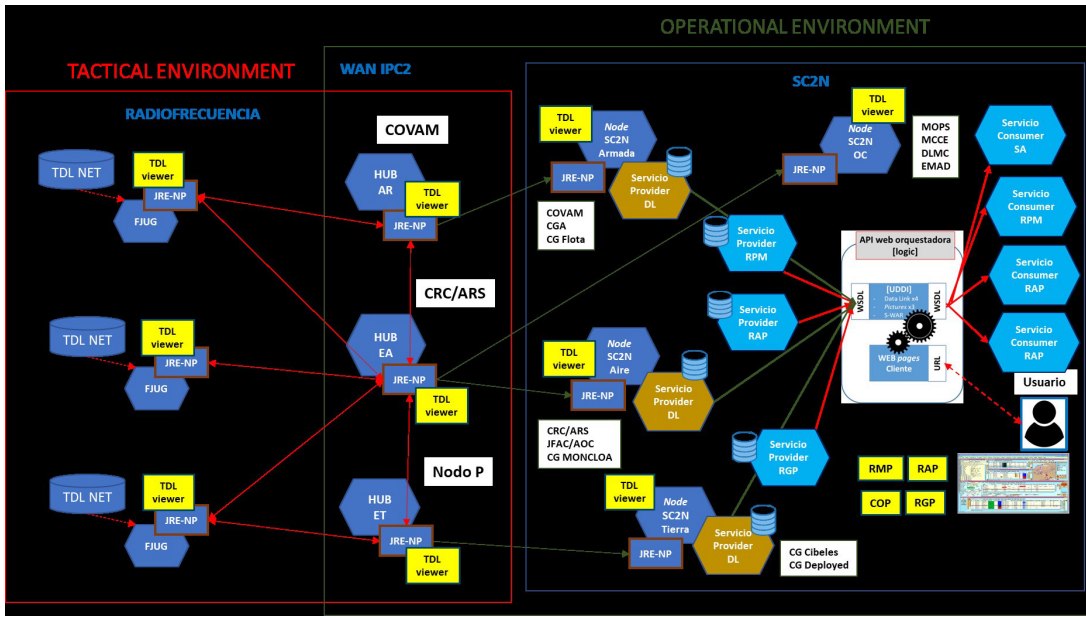


Figura 3. Arquitectura final propuesta para la red JRE nacional

El despliegue que se propone se circunscribe a los elementos señalados en el caso de uso 1, analizado en el cuerpo de la memoria del trabajo. Conviene señalar al respecto que el entorno específico estratégico-operacional se configura sobre la red IP subyacente de Mando y Control (WAN-IPC2), que a su vez se divide en múltiples dominios de seguridad, uno de los cuales es la SC2N, precisamente el lugar donde se despliega la parte correspondiente a la red JRE nacional y servicios asociados, en el entorno estratégico-operacional.

De acuerdo con las necesidades funcionales, se deben desarrollar las matrices de enlaces que determinen los flujos válidos, todos ellos caracterizados por un *link designator* único, así como con sus características (TCP, UDP *multicast* y UDP *unicast)*, entre los diferentes JRE *processors*, con su correspondiente dirección IP fija, así como con la configuración de las matrices de conexión (o CONMATRIX) específicas de cada uno de ellos. La materialización operativa de dichas necesidades funcionales se concretan en el documento OPTASKLINK, de acuerdo con la publicación APP-11, que regula el catálogo de mensajes OTAN [7], y se despliegan sobre la infraestructura de telecomunicaciones comunicaciones de la I3D, en múltiples dominios, de acuerdo con los requisitos técnicos correspondientes.

5. Resultados y discusión

Tras la validación y prueba efectuada mediante la herramienta EVALINKL16 de un escenario concreto ilustrativo, la conclusión principal es que se deben poner a prueba escenarios y casos de uso diversos, de

menor a mayor complejidad, para comprobar que la transmisión y recepción de mensajería Link16 y paquetes JRE se produce tal y como se espera.

6. Conclusiones

Al término de este trabajo los objetivos principales que se han cumplido son los siguientes:

- Se ha presentado una propuesta concreta de arquitectura distribuida de red/sistema de alto nivel basada en el protocolo JRE, multidominio y de naturaleza permanente.
- Se le ha dado a la propuesta un enfoque adicional hacia un el modelo basado en web-services o microservicios a implementar en el entorno de la SC2N, conforme al concepto FMN.
- La red/sistema propuesto permite dar respuesta a las necesidades que tienen las FAS, mandos y centros directivos del entrono estratégico-operacional, en relación con la explotación eficaz de la información táctica producida en el entorno táctico, propio de las operaciones militares.

7. Líneas futuras

En cuanto a las líneas principales a destacar:

- Desarrollo de un proyecto software completo que comprenda todas las tareas de análisis, diseño y codificación y pruebas de los web-services o microservicios asociados a la red JRE nacional.
- Despliegue completo de un laboratorio de pruebas de la infraestructura de red de JRE Processors, que incluya herramientas avanzadas como CSI, NIRIS y LINPRO.

Referencias

Allied Commander Operations, OTAN [30/05/2016] ACO Joint Concept of Employment for Tactical Data Links in NATO, ACO. (2016).

EMAD. Estado Mayor de la Defensa. (2013). Concepto de empleo de TDL en operaciones conuntas lideradas por el CMOPS.

—. (2019). Directiva 19/19 del JEMAD de líneas generales para el desarrollo, evolución e interoperabilidad de la capacidad de enlace de datos tácticos (TDL) en las FAS.

Ministerio de Defensa. (2019). *Directiva 02/2019 del JEMAD, Despliegue del Sistema de Mando y Control Nacional (SC2N).*

—. (2020). *GRUPLAN - JEMAD, Migración de los Sistemas TDL en las FAS.*

NATO. (2001). Standarization Agency, APP-11. *NATO message catalogue (OPTASKLINK).*

—. (2019). *Capability Planning Working Group (CPWG), FMN Spiral 4 Instructions and Service Instructions for Data Links*. Military Committee.

Propuesta de arquitectura para la red táctica permanente multi-dominio JRE nacional

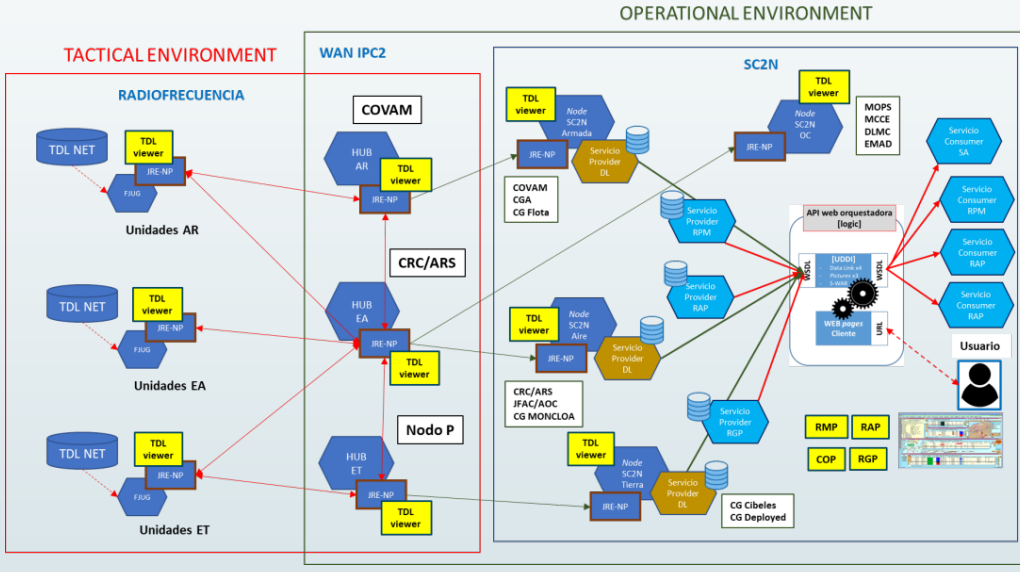
Autor: José Luis Martínez Leyva

Director/es: José González Coma, Francisco Javier Rodríguez Martínez

Universidad de Vigo

Contexto y motivación

La **Directiva 19/19 del Jefe del Estado Mayor de la Defensa (JEMAD)**, que marca las líneas generales para el desarrollo, evolución e interoperabilidad de la capacidad Tactical Data Link (TDL) en las Fuerzas Armadas, describe una variedad de **tecnologías de enlace de datos tácticos**, que los mandos militares utilizan para llevar a cabo y/o supervisar las operaciones. La ventaja tecnológica que ofrece a los ejércitos la capacidad **Link16**, se ve limitada a su uso en el ámbito estrictamente táctico. Para solucionar el "gap" que supone la presentación de información táctica procedente de las operaciones militares al **entorno estratégico-operacional**, surge el protocolo ***Joint Range Extension Protocol* (JREAP)**. De forma adicional, con arreglo al marco conceptual que marca el concepto FMN (*Federated Mission Network*), propio de la SC2N (Red de Mando y Control de las FAS), se propone un **modelo basado en servicios**.



Objetivos

1º Definir una **arquitectura** de alto nivel para una red basada en el despliegue de procesadores **JRE**, que sea **distribuida**, **permanente** y **multidominio**, y que permita a los mandos militares el seguimiento de las operaciones en curso por muy lejos que de éstas se encuentren.

2º Propuesta adicional hacia un modelo de servicios (**web-services o microservicios**) en la SC2N.

Conclusiones

El Sistema que se ha presentado permite dar respuesta a las necesidad que tienen los mandos y centros directivos del **entrono estratégico-operacional** en las FAS, al problema de la explotación eficaz de la **información** táctica producida en el **entorno táctico** "campo de batalla", propio de las operaciones militares.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Análisis de imágenes satelitales por técnicas de inteligencia artificial

Autor: José Antonio Muñoz Jiménez (jmunjim@mde.es)
Directores: Javier Vales Alonso (javier.vales@upct.es) y Francisco Troncoso Pastoriza (ftroncoso@cud.uvigo.es)

Resumen: – El objetivo principal de este trabajo de fin de máster es el desarrollo de un proyecto para automatizar el procesado de imágenes de satélite, ofreciendo un sistema capaz de obtener información de diferentes fuentes (tanto privadas como públicas) y procesar automáticamente dicha información para garantizar la detección temprana y eficaz, y posterior identificación de elementos relevantes para la Defensa.

Entre los elementos relevantes a detectar se encuentran los barcos de un tamaño suficiente, las estructuras, la propia línea de costa y los emplazamientos de artillería de costa. El hecho de proponer una lista corta de elementos relevantes no obsta que esta lista se pueda ampliar a otro tipo de elementos técnicamente detectables, pero esta inclusión en la lista llevaría a unas configuraciones de estructuras de detección potencialmente nuevas (adaptadas para la detección e identificación del elemento concreto) y al necesario entrenamiento dedicado en el procesado de estos nuevos elementos.

El objetivo del proyecto se plasmará en el desarrollo e implementación de una plataforma web de inteligencia geoespacial para Defensa. Esta plataforma estará basada en un conjunto de motores de inteligencia artificial que permitirán, por un lado, la colección, fusión y análisis de datos satelitales (imágenes ópticas y radar) procedentes de canales privados y fuentes abiertas y, por otro, la detección automática en las imágenes derivadas de los mismos, de «anomalías» u objetos cuya identificación resulte clave a la hora de tomar decisiones que puedan comprometer la seguridad tanto a nivel nacional como internacional.

Palabras clave: – Entrenamiento, Detección, Identificación, Automatización.

1. Introducción y objetivo

Introducción

Una de las fuentes de datos más importantes de información al mando son las fuentes satelitales, por lo que es de particular importancia la automatización de su explotación. Esta necesidad de procesar mucha información, de manera rápida y automática, justifica el objetivo último de este estudio.

La automatización de las estructuras de detección requiere el entrenamiento de estas mediante miles o millones de imágenes preprocesadas, para que los sistemas aprendan a detectar e identificar correctamente.

Conseguir los datos de entrenamiento y procesarlos (etiquetado) es muy laborioso, requiriendo un esfuerzo humano y técnico grande. El éxito de la tarea depende, en gran medida, de la cantidad y calidad del entrenamiento realizado, por eso el entrenamiento de las estructuras de detección es tan crítico. Contar previamente con estructuras pre-entrenadas para elementos similares, acorta drásticamente los tiempos de entrenamiento. Esta técnica se denomina *transfer learning* o transferencia del aprendizaje.

Objetivo

El objetivo principal de este trabajo de fin de máster es el análisis y desarrollo de un sistema para automatizar el procesado de información satelital, ofreciendo uno capaz de obtener información de diferentes fuentes de datos (tanto privadas como públicas) y procesar automáticamente la información para garantizar una eficaz detección temprana y posterior identificación de elementos relevantes para la Defensa. Entre estos se encuentran: barcos de tamaño suficiente, estructuras, línea de costa y emplazamientos de artillería de costa y antiaérea.

El proyecto conlleva el desarrollo e implementación de una plataforma web de inteligencia geoespacial para Defensa, con un conjunto de motores de inteligencia artificial que permitan, la colección, fusión y análisis de datos satelitales (ópticos y radar) y la detección automática, en las imágenes derivadas de los mismos, de anomalías u objetos relevantes para la seguridad, tanto nacional como internacional.

Una vez indicados los parámetros de búsqueda en la plataforma (zona a inspeccionar, tipo de acción u objeto a buscar), el sistema buscará, en esa área, por los canales disponibles. Con esa información, este fusionará y analizará los datos, extrayendo aquellos realmente relevantes.

Estos datos se procesarán mediante un motor de inteligencia artificial basado en redes neuronales profundas (*deep learning*) que buscará el objeto, elemento o anomalía que el usuario indicó inicialmente en su patrón de búsqueda.

Si el sistema identifica el objeto buscado, lanzará una alerta al usuario. El alcance final es disponer de un sistema operativo, entrenado para los casos de uso que se determinen de interés para el MINISDEF y preparado para su potencial despliegue en un entorno seguro, de manera que el *software* resultante esté preparado para ser instalado en la unidad operativa del MINISDEF que la Administración determine.

2. Desarrollo

Se parte de un estudio de la arquitectura general para posteriormente detallar los modelos de *deep learning* y se expone cómo estos módulos se estructuran y organizan para resolver los casos de uso del proyecto.

Análisis y diseño

La arquitectura lógica del sistema se basa en tres dispositivos con sus respectivas tareas asociadas: flujo de procesamiento de datos, sistema de almacenamiento y flujo de *deep learning*. También se incluyen partes ajenas al sistema como: PC del usuario, protocolo de comunicaciones y fuentes de datos satelitales incluidas en entorno *Cloud* a las que se accede para obtener las imágenes.

— Sistema flujo del procesamiento de datos

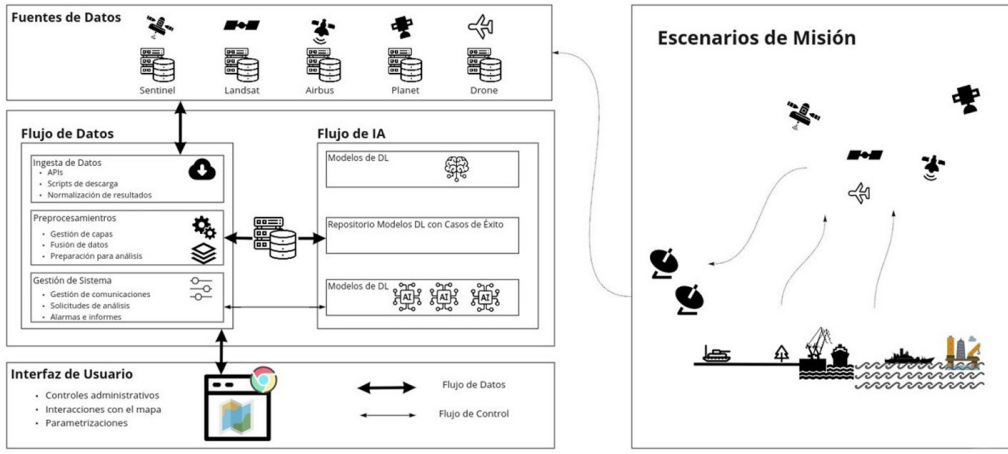
  Servidor que ejecuta los procesos de control principal del sistema, así como los de comunicación con las fuentes de datos satelitales, el cliente y el resto de sistemas.

— Sistema flujo de deep learning

  Servidor que ejecuta los procesos de análisis y entrenamiento para resolver con éxito los casos de uso expuestos.

— Sistema almacenamiento

  Servidor NAS para almacenamiento y protección de los datos satelitales.



Esquema arquitectura lógica del sistema

Modularización de los modelos

En esta sección se describen todos los modelos que se desplegarán en el sistema, especificando para cada uno, el tipo de datos de entrada y salida, y una o varias arquitecturas de modelos *deep learning* posibles, para ir conformando un modelo listo para ser desplegado.

En los diferentes modelos, usamos arquitecturas que comparten elementos entre los modelos. Estas arquitecturas se conocen como de aprendizaje multitarea.

Detección y segmentación de objetos y estructuras

El primer paso es la detección de los elementos de interés en las imágenes. Por tanto, es necesario entrenar un modelo para cada uno de los casos de uso.

Estos modelos tienen una primera parte (*backbone*) que toma las imágenes de entrada y los metadatos, extrayendo un mapa de características de las mismas, que luego es utilizado por cada una de las partes finales de los modelos correspondientes a los casos de uso.

Los casos de uso que requieran de una clasificación de barcos/estructuras toman el resultado de estas detecciones como *input* para clasificar los elementos de las imágenes

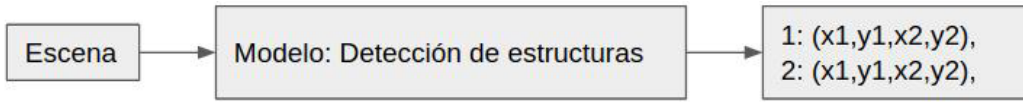
Modelo de detección de barcos (MM-1.1)

Este modelo compartirá el *backbone* común y detectará los buques que aparezcan en la imagen satelital. Se trata de un modelo básico para la resolución de los casos de uso y es, en gran parte, el primer paso necesario para analizar las imágenes.

Los datos de entrada a este modelo son imágenes satelitales + metadatos y los datos de salida son regiones de interés o *bounding boxes* que sitúan los barcos en la imagen. En definitiva, el *backbone* común para extraer las características y un módulo llamado «cabeza» propone las regiones de interés y devuelve la detección de los barcos (coordenadas de los *bounding boxes*).

Modelo de detección de estructuras (MM-1.2)

Similar al anterior, usa *backbone* común, el objetivo de este modelo es la detección de estructuras en una imagen. Los datos de salida corresponden a la localización en la imagen de las estructuras detectadas. Este modelo tiene arquitectura similar al modelo de detección de buques.



Modelo de segmentación de barcos (MM-1.3)

Para mayor resolución en las detecciones y mejor detección de cambios (salidas de puertos, construcciones, etc.), usamos modelos de segmentación semántica para complementar el análisis de las imágenes. Los datos de entrada del modelo son imágenes satelitales + metadatos y la salida son predicciones para los diferentes píxeles.

Al tener un modelo de segmentación de estructuras entrenado hacemos un seguimiento de determinadas zonas en busca de nuevos elementos, cambios graduales como la construcción de nuevas estructuras, etc.

Clasificación de barcos y estructuras

Los modelos de clasificación con un *backbone* común establecen la categoría de las imágenes generadas por los modelos de detección. Gran parte de los casos de uso implicará la categorización de los elementos de las imágenes.

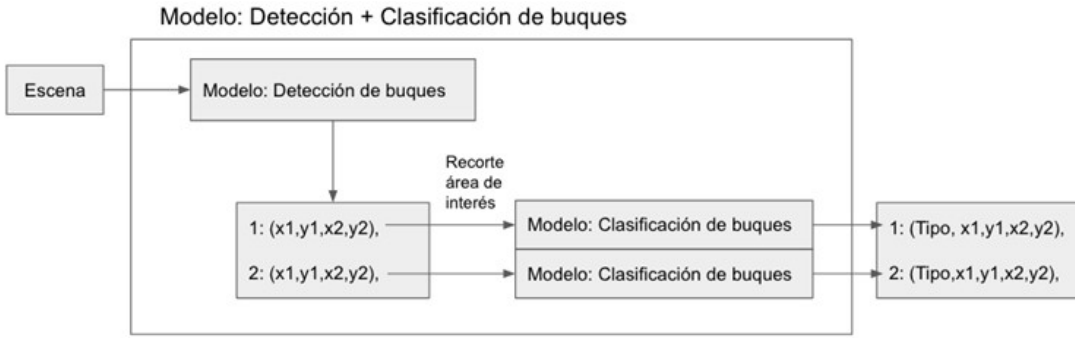
Modelo de clasificación de barcos (MM-2.1)

Input: imagen satelital (*Output* MM-1.1) + metadatos
Output: probabilidad del barco de la imagen de pertenecer a cada una de las clases

Los tipos de barcos que se desean identificar en una primera versión son los siguientes:

- Buques mercantes: carga general, Ro-Ro (transporte de carga rodada y/o de personas), transportador o ferry o pesqueros.
- Buques militares: portaaeronaves, submarinos, destructores, fragatas, corbetas, dragaminas, guardacostas o patrulleras.

Combinando ambos modelos (detección y clasificación de buques), al procesar automáticamente una imagen satelital, obtenemos la ubicación de los barcos detectados en la imagen (*RoIs, Region of Interest*) y la clasificación de dichos barcos.



Modelo de clasificación de estructuras (MM-2.2)

Input: imagen satelital + metadatos
Output: probabilidad del objeto de la imagen de pertenecer a cada una de las clases de estructuras

Para el modelo de clasificación de estructuras se usa una arquitectura estándar de clasificación como EfficientNet, ResNet, Inception, MobileNet, etc. Las clases en las que incluir las estructuras, podrán ser boyas, plataformas petroleras y/o aerogeneradores.

Modelo de clasificación de áreas de interés en imágenes radar (MM-2.3)

Input: imagen satelital de tipo radar + metadatos
Output: probabilidad de pertenecer a una clase predefinida

Para las imágenes radar elaboramos un modelo de clasificación de barco/no barco.

El modelo toma como entrada una imagen radar + metadatos y como salida predice la probabilidad de que exista un barco en la imagen.

Debido a la gran diferencia entre las imágenes radar y RGB, este modelo usa una red neuronal aparte de la de los modelos de clasificación para imágenes RGB, de arquitectura parecida, basada en EfficientNet, pero comparten el mismo *backbone*.

Modelo de detección de cambios (MM-3)

Input: par de imágenes satelitales
Output: máscara de los píxeles donde se considera que existen cambios sustanciales en la imagen

Se realiza un análisis de la escena mediante un modelo de segmentación semántica de entornos costeros, pudiendo ser distinto a los modelos de segmentación MM-1.3 y MM-1.4, con el objetivo de separar las clases a predecir y ganar precisión. Una vez segmentado el par de imágenes, se utiliza un modelo capaz de detectar cambios entre las dos máscaras de segmentación mediante análisis de imágenes del mismo lugar en distintos momentos en el tiempo.

Para segmentar las imágenes tomadas en distintos momentos, podemos utilizar los modelos de segmentación de barcos y estructuras definidos anteriormente.

Modelo de comparación de buques (MM-4)

Input: par de imágenes RGB
Output: probabilidad de que el buque sea el mismo

Este modelo se encarga de decir si un buque es similar a otro. Así, teniendo una base de datos de buques objetivos a buscar, se puede comparar y detectar si son parecidos o no. Para buques similares devuelve un valor cercano a uno, mientras que para buques diferentes devuelve valores cercanos a cero.

Este modelo se basa en arquitecturas de redes siamesas, donde se codifican los buques con la misma red y se comparan sus mapas de características para ver lo diferentes que son estos.

Identificador del modelo	Descripción
MM-1.1	Modelo de detección de barcos.
MM-1.2	Modelo de detección de estructuras.
MM-1.3	Modelo de segmentación de barcos.
MM-1.4	Modelo de segmentación de estructuras.
MM-2.1	Modelo de clasificación de barcos.
MM-2.2	Modelo de clasificación de estructuras.
MM-2.3	Modelo de clasificación de áreas de interés en imágenes radar.
MM-3	Modelo de segmentación de puertos y zonas costeras.
MM-4	Modelo de comparación de buques.

Tabla 1. Resumen modelos de red neuronal

3. Casos de uso

Aquí se detalla qué modelos de red neurona se usa en cada caso de uso y la denominación y explicación intuitiva de cada uno.

Caso de uso	Denominación del caso de uso	Modelo usado
CU-01	Reconocimiento de tipo de buque.	MM-1.1, MM-2.1
CU-02	Identificación de buque específico.	MM-1.1, MM-2.1
CU-03	Detección zonal de buques y alertado.	MM-1.1, MM-2.3
CU-04	Detección de buques abarloados en el mar.	MM-1.1
CU-05	Detección de estructuras.	MM-1.2, MM-2.2
CU-06	Seguimiento de trazas y obtención de histórico.	MM-1.1, MM-2.1
CU-07	Obtención de mapas de calor.	MM-1.1
CU-08	Alerta por salidas de puerto y fondeos.	MM-1.1, M-2.1
CU-09	Detección de cambios en puertos o línea de costa.	MM-3
CU-10	Detección emplazamientos artillería de costa o A/A.	MM-1.4, MM-2.2

Tabla 2. Casos de uso y modelos que intervienen en cada uno

4. Resultados y discusión

Pese a la tremenda evolución en el campo de la detección de objetos, la tecnología sigue siendo significativamente más primitiva que la visión humana y aún no puede abordar con eficacia los desafíos del mundo real. Los progresos en este campo son vertiginosos y mientras se escribe este artículo acontecen avances que determinan futuras líneas de investigación, no tenidas aquí en cuenta, que acercan aún más la visión artificial a la humana.

5. Conclusiones

Tras evaluar las diferentes estructuras de detección, se enumeran los factores clave que han surgido de los diferentes estudios y desarrollos dentro de la detección genérica de objetos basada en el aprendizaje profundo.

Estructuras de detección seleccionadas

— Cuando el coste computacional no es el factor limitante, los detectores de dos etapas generalmente producen precisiones de detección más altas que los de una etapa, porque su estructura es más flexible y adecuada para la clasificación basada en regiones. Los marcos más utilizados son Faster R-CNN, R-FCN y Mask R-CNN. En nuestro caso, se ha elegido este tipo de detectores casi de manera exclusiva, salvo en los casos que implicaban detección de cambios donde usamos estructuras basadas en redes siamesas.

— Las configuraciones de una etapa (e.g. YOLO y SSD) suelen tener un rendimiento mucho más bajo en la detección de objetos pequeños que las arquitecturas de dos etapas como Faster R-CNN y R-FCN, pero son competitivos en la detección de objetos grandes.

Mejora de la fiabilidad de la representación de objetos frente a circunstancias adversas

La variabilidad de las imágenes del mundo real (*e.g.* iluminación, posturas, deformaciones, desorden de fondo, oclusiones, desenfoque, resolución, ruido y distorsiones de cámara) son un desafío clave en el reconocimiento de objetos.

Procesamiento de entorno del objeto

Queda por explorar cómo incorporar información contextual de manera eficiente.

Propuestas de detección

Reducen significativamente los espacios de búsqueda en comparación con las propuestas de región.

Otros factores

Por ejemplo, aumento de datos, estrategias de entrenamiento novedosas, combinaciones de modelos de redes troncales, marcos de detección múltiples, incorporación de información de otras tareas, métodos para reducir el error de localización, etc.

6. Líneas futuras de investigación

En cuanto a los problemas que quedan por resolver y que marcan las tendencias futuras se prevén las siguientes direcciones de investigación:

— Aprendizaje de mundo abierto. Capacitar a los algoritmos para reconocer categorías de objetos fuera de su conjunto de datos de entrenamiento, para mejorar comportamiento en ambientes reales.

— Conseguir estructuras de detecciones mejores y más eficientes. Los detectores basados en regiones tienen mayor precisión, los de una etapa son generalmente más rápidos y simples. Los detectores de objetos dependen, en gran medida, de las redes troncales subyacentes que se han optimizado para clasificación de imágenes.

— Diseñar funciones de CNN compactas y eficientes. Las CNN tienen millones de parámetros, lo que requiere datos masivos, memoria y capacidad de cálculo para el entrenamiento. Se necesitan mayores esfuerzos en compactación de las redes (e.g. mediante uso compartido de fases o módulos) para aprovechar más la capacidad de cómputo.

- Búsqueda automática de arquitecturas neuronales mediante programas de diseño automático.
- Detección débilmente supervisada. Actualmente, se usan modelos supervisados por completo con datos etiquetados con cuadros delimitadores de objetos o máscaras de segmentación. Sería preciso diseñar CNNs que solo usen datos anotados débil o parcialmente.
- Detección de objetos con pocos o cero intentos. La capacidad de aprender de unos pocos ejemplos y la detección en pocos intentos es otro de los campos de mejora para el futuro. Otra línea de investigación es la mejora en el reconocimiento de objetos nunca vistos, entrenados o conocidos, por tanto, como intento «O».
- Detección de objetos en otras modalidades. La mayoría de los detectores usan imágenes fijas en 2D, la detección en otras modalidades puede es muy relevante para vehículos autónomos, vehículos aéreos no tripulados y robótica.
- Detección universal de objetos. Indentificar de cualquier clase de objeto, no solo aquellos en los que se ha especializado la red.

Referencias

Howard, A. G. (2017). MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. Disponible en: https://doi.org/10.48550/arXiv.1704.04861

Kaiming, H., *et al.* (2015). *Deep Residual Learning for Image Recognition.* Disponible en: https://arxiv.org/abs/1512.03385

Mingxing, T. y Quoc V, L. (2019). *EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks.* Disponible en: https://arxiv.org/abs/1905.11946

Szegedy, C. *et al.* (2015). Rethinking the Inception Architecture for Computer Vision. Disponible en: https://doi.org/10.48550/arXiv.1512.00567

Análisis de Imágenes Satelitales por técnicas de Inteligencia Artificial

Autor: José Antonio Muñoz Jiménez

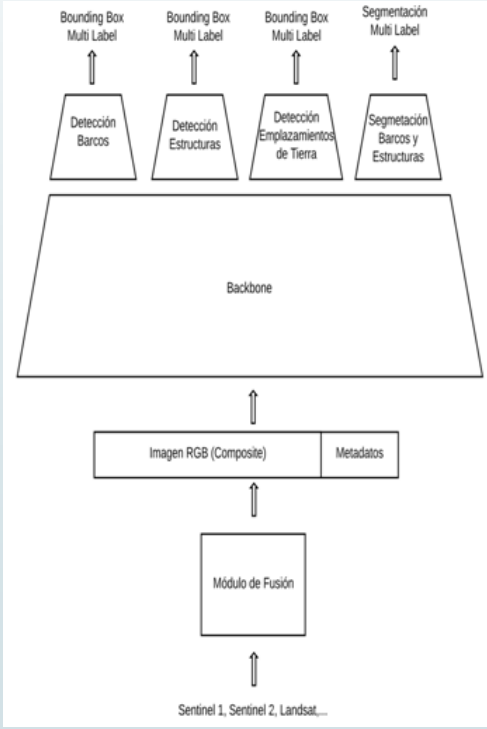
Director/es: Francisco Troncoso Pastoriza y Javier Vales Alonso

Universidad de Vigo

Introducción

El objetivo principal de este Trabajo Fin de Máster es el desarrollo de un sistema para automatizar el procesado de imágenes de satélite tomadas de diferentes fuentes (tanto privadas como públicas), mediante estructuras de detección basadas en Inteligencia Artificial materializadas en una plataforma web de Inteligencia geo-espacial para Defensa.

Metodología



Resultados

Conclusiones

El sistema resulta técnicamente viable, siendo todavía la tecnología más primitiva que la visión humana y sin poder abordar desafíos “reales”, que no conlleven un concienzudo entrenamiento de estructuras de detección dedicadas. Aún así, los progresos técnicos en IA son vertiginosos y con el crecimiento esperado de la capacidad de cálculo alcanzará cotas cada vez más cercanas a la visión humana. Con todo, el sistema resulta muy útil como herramienta de procesado automático de información para el mando.

Agradecimientos

A mi familia, especialmente a mi mujer y a mis hijos, que han sufrido el déficit de atención provocado por mi dedicación al Máster.

A mis compañeros, profesores y tutores por el apoyo, la buena relación mantenida en todo momento y el gran ambiente de compañerismo entre todos.

Plan de Renovación Tecnológica en el Ministerio de Defensa. Gestión de Activos TI

Autor: Raúl Jesús Richarte Reina (rrichart@et.mde.es)
Directores: Miguel Ángel Ares Tarrío (externo.miguelares@cud.uvigo.es) y Francisco Javier Rodríguez Rodríguez (jjavierrodriguez@cud.uvigo.es)

Resumen: – Publicada la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, se hace imprescindible, entre otras, acciones, coordinar los procesos de planeamiento y obtención de los recursos materiales de los sistemas de información y telecomunicaciones, con la finalidad de optimizar y racionalizar los recursos financieros y materiales CIS/TIC.

Esta Política se desarrolla con base en el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones (PECIS) que constituye la guía para la transición desde la situación existente en el momento de su aprobación a la situación final de implantación efectiva de las Capacidades CIS/TIC.

En consonancia con los objetivos del PECIS, este Trabajo de Fin de M*á*ster (TFM) se enfoca en el Planeamiento de la Renovación Tecnológica del Puesto de Trabajo Digital (PTD) del Ministerio de Defensa, englobando aspectos relevantes que alinearemos con el ciclo de *deming* en busca de un proceso de mejora continua.

En una primera fase, estableceremos las necesidades reales del Ministerio de Defensa, estableciendo una Plantilla Objetivo que nos sirva de referencia para completar una Renovación del Puesto de Trabajo Digital.

En la segunda fase, presentaremos la contratación, desde el punto de vista del Técnico CIS, resaltando la importancia de la compra pública para poder llevar a cabo la adquisición de los recursos informáticos que renovaran el parque informático del Ministerio de Defensa.

Por último, se sentarán las bases para automatizar un cuadro de mando que apoye la toma de decisiones de la Dirección del Gobierno TIC.

Palabras clave: – Política CIS/TIC, Renovación tecnológica, Puesto de trabajo digital, Plantilla Objetivo, Contratación, Control de activos TI.

1. Introducción

El Ministerio de Defensa, centrándose en la información como recurso estratégico sustentado por las TIC, estableció la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC) [1], cuyo control, seguimiento y desarrollo justifica el nacimiento del CESTIC como Gobierno TIC del Ministerio de Defensa.

Según esta política, CESTIC asumirá el planeamiento y obtención de los CIS/TIC, su control, organización, operación y mantenimiento, para el establecimiento y provisión de los servicios TIC, y se regirá por los principios, finalidad, ejes estratégicos y directrices de la presente política.

Para la consecución de la finalidad de la Política CIS/TIC surge el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS) [2] como un instrumento de planeamiento para el desarrollo de la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del MDEF (Política CIS/TIC).

En consonancia con los objetivos del PECIS OE 6.2:

- Racionalizar los recursos financieros y la estrategia de contratación en materia CIS/TIC y OE 6.3.
- Racionalizar los recursos materiales en materia CIS/TIC.

Se plasmará un procedimiento que permita esa racionalización de forma centralizada.

Con este TFM se pretende planear un procedimiento/guía para centralizar, racionalizar y homogenizar la adquisición de recursos TI del Puesto de Trabajo Digital (PTD) del Ministerio de Defensa y posteriormente llevar un control y supervisión que permita al Gobierno TI disponer de un Cuadro de Mando que le apoye en la toma de decisiones.

2. Objetivos

Los objetivos de este trabajo de fin de máster se pueden considerar como fases alineadas al ciclo de *deming*:

- Llevar a cabo un estudio con los datos históricos de los que disponemos para concluir unas necesidades reales que nos ayuden a planificar la renovación tecnológica de los recursos HW del Puesto de Trabajo Digital del Ministerio de Defensa.
- Presentar la compra pública y la contratación centralizada, desde una visión del Técnico TI, que facilite la adquisición y el planeamiento de costes como apoyo a la toma de decisiones.
- Plantear un procedimiento de control de activos TI.
- Establecer unas líneas futuras en busca de la mejora continua y la automatización de procesos de la Gestión de Activos TI.

3. Desarrollo

La antigüedad del parque informático y la eclosión de la transformación digital en todos los ámbitos de la sociedad hacen necesaria, más que nunca, una renovación tecnológica de los recursos informáticos del Ministerio de Defensa.

Las fases a seguir para conseguir la renovación tecnológica del Ministerio de Defensa serán las siguientes:

- Planeamiento: planeamiento de necesidades reales. En este punto esimportante diferenciar la necesidad real de lo que hay en inventario. La acumulación de equipos y la falta de control en la compra de estos ha provocado un aumento del parque informático que difiere en gran medida con las necesidades legítimas. Por ello será necesario realizar un estudio para dar con una Plantilla Objetivo de necesidades reales consensuada con los ámbitos interesados.
- Hacer: proceso de contratación que permita centralizar y homogeneizar el parque informático, facilitando su gestión posterior y contribuyendo a la transparencia, competencia de empresas y reducción de costes.
- Verificar: sistema de control de activos que facilite una gestión eficiente y eficaz de los recursos TI y alimentar un Cuadro de Mando Integral que permita al Gobierno TIC del Ministerio de Defensa tener la información necesaria para la toma de decisiones.
- Actuar: toma de decisiones y mejora continua.

Como vemos estas fases podemos alinearlas con el ciclo de *deming* o PDCA, el cual puede emplearse en cualquier proceso, de modo que la organización se encuentra siempre en un ciclo de mejora continua para implantar normas y aumentar la eficiencia.

Cuantas más repeticiones se hagan, mayor será la ganancia de calidad y mejor será la entrega al cliente, aumentando la ventaja competitiva.

Planeamiento de las necesidades reales

Se tiene la tendencia de solicitar mucho más de lo que se necesita, sobre todo, cuando se trabaja con dinero público. Esto conlleva consecuencias negativas para cualquier planeamiento, por un lado, no solo incrementa los gastos sobre un presupuesto limitado, sino que, además, dificulta una priorización adecuada que permita cubrir las necesidades globales de la organización.

Para el cálculo de las necesidades reales dentro del Ministerio de Defensa, entre otras cosas, necesitaremos definir:

- Las características y el equipamiento hardware que compondrá cada PTD en el segmento no clasificado de la I3D, aulas de enseñanza y hospitales.
- Una Plantilla Objetivo que indique el número de PTD que deben ser equipados por ámbitos de tal forma que permita su sostenibilidad en

función de los créditos históricamente disponibles y los previstos en el futuro.

— Un planeamiento de las adquisiciones anuales que permita una renovación de los recursos informáticos de manera homogénea en el tiempo.

Partiendo del estudio de datos como:

— Personal en plantilla en el Ministerio de Defensa en 2016 y 2022.

— Ordenadores contabilizados en 2016 por el cambio a Windows 10. Este hecho hizo comprender la necesidad de un inventariado y una Gestión de Activos TI más automatizada.

— Puestos existentes en aulas de enseñanza y hospitales procedentes de anuarios estadísticos.

Teniendo en cuenta las necesidades actuales del Ministerio de Defensa en cuanto a trabajo en movilidad para militares y trabajo a distancia para el funcionario civil, podemos establecer una Plantilla Objetivo que nos servirá referencia durante todo el proceso de Renovación Tecnológica para el ciclo 2022-26.

Perfiles *Hardware*	Renovación	Equipamiento
Genérico	Ocho años	PC sobremesa con uno o dos monitores (se promedia que un 25 % de los puestos con perfil genérico se configurarán con dos monitores).
Técnico	Ocho años	PC de sobremesa y dos monitores que cumplan con los requisitos solicitados (CPU de alto rendimiento, memorias\ tarjetas gráficas especiales, monitores de grandes dimensiones).
Movilidad	Cinco *años*	PC portátil para movilidad. Su puesto de trabajo habitual se complementará con un monitor, una *Docking Station*, un teclado y un ratón auxiliar para asimilarlo a un puesto de trabajo genérico
Autoridad	Cinco/ocho *años*	Se le dotará con el material de un puesto genérico de capacidades medias (ofimáticas) y un puesto *móvil para movilidad/teletrabajo sin complementos periféricos.*

Tabla 1. Definición de Perfiles PTD

Ámbito\Perfil	Genéricos	Técnicos	Móviles	Autoridad	Total
ÓRGANO CENTRAL	7.882	138	1.795	70	9.885
EMAD	1.540	172	379	56	2.147
EJÉRCITO DE TIERRA	29.188	800	5.000	112	35.100
ARMADA	8.412	351	2.900	37	11.700
EJÉRCITO DEL AIRE	10.781	375	1.300	44	12.500
UME	904	33	149	2	1.088
GUARDIA REAL	457	8	69	0	534
	59.164	1.877	11.592	321	72.954

Tabla 2. Plantilla Objetivo

Contratación

Se podría pensar que el proceso que engloba la contratación es una parte estanca de la organización gestionada por personal ajeno al mundo TIC. Nada más lejos de la realidad, la contratación moja de lleno todos aquellos departamentos que manejen presupuestos dentro de una organización, ya que la especificidad de las necesidades de muchos departamentos como el TI obliga a que los interesados generen documentos de muy diversos tipos para definir con exactitud lo que necesitan adquirir.

El CESTIC, gobierno TIC del Ministerio de Defensa, es el encargado de racionalizar los recursos financieros y la estrategia de contratación en materia CIS/TIC, es decir, no solo debe de llevar a cabo el planeamiento de los recursos de los Sistemas TIC, sino que además tiene que gestionar la contratación en todos sus aspectos.

Fases de la contratación:

— Preparación de la licitación. Fase muy activa del técnico TIC.

Figura 1. Inicio contratación [3]

— Licitación. Técnico TIC valora y propone adjudicatario.

Figura 2. Licitación [3]

— Adjudicación y formalización del contrato. Técnico TIC supervisará el cumplimiento del contrato.

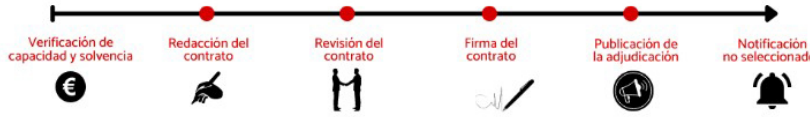


Figura 3. Control del contrato [3]

Control de activos

El control de inventario es una fase importantísima del ciclo, ya que será la base para sacar los datos/información necesaria para construir un Cuadro de Mando que sirva para la toma de decisiones.

La información mínima necesaria para hacer un seguimiento a la renovación tecnológica que se llevará a cabo hasta poseer alguna herramienta ITAM, se basa principalmente en las estadísticas de altas de equipos, bajas de equipos y la conexión de estos a la Red I3D del Ministerio de Defensa, a la cual abastecemos.

Con todos estos datos, y a través de herramientas ofimáticas, cruzaremos la información necesaria para el control y apoyo a la toma de decisiones.

Ejemplo:

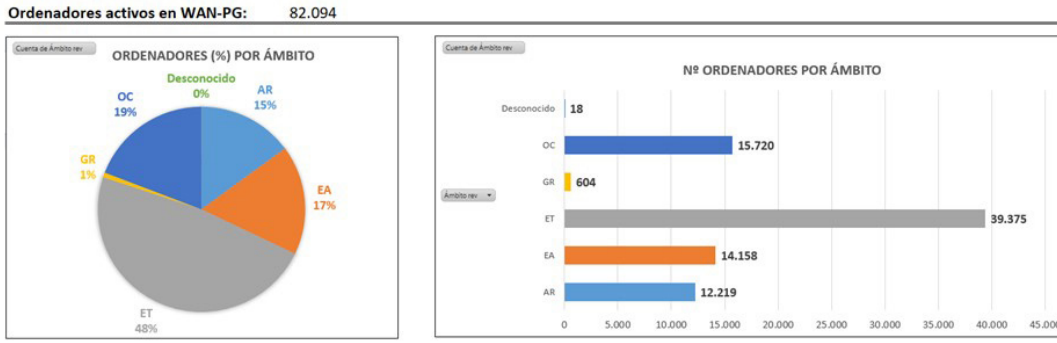


Figura 4. Ordenadores activos I3D no clasificada (WAN PG). Aquí podemos comprobar los ordenadores conectados a la WANPG, a finales 2022, que, comparados con la Plantilla Objetivo, reflejan un exceso de equipos para los cuales hay que buscar acciones correctoras

4. Resultados y discusión

Siguiendo las fases descritas en el desarrollo:

— Planeamiento de necesidades Reales. Hemos obtenido la Plantilla Objetivo que nos servirá de referencia para el cálculo de necesidades.

  El número total de PTDs a equipar es inferior a las necesidades manifestadas por los ámbitos, pero la experiencia de los últimos diez *años y la situación económica actual, y prevista en los próximos, no permite garantizar la reposición y dotación del hardware* y *software* en cantidades superiores.

— Hacer: proceso de contratación.

  Los procedimientos para contratar más idóneos para las necesidades de la renovación tecnológica, por cantidad y características del suministro, es el acuerdo marco. Es indiscutible que los acuerdos marcos otorgan ventajas, tanto a la Administración como a las empresas participantes, en cuanto a ofrecer un procedimiento que reduce costes, tiempo, dinero y garantiza contrataciones a largo plazo.

— Verificar: sistema de control de activos. Cuadro de Mando Integral que permita al Gobierno TIC del Ministerio de Defensa tener la información necesaria para la toma de decisiones.

  Las herramientas utilizadas para el control de activos son escasas y pobres comparadas con las herramientas de Gestión de Activos TI que ofrecen el mercado y fueron repasadas en el apartado del estado del arte.

5. Conclusiones

Todo lo realizado en el TFM:

— Estudios estadísticos para llegar al planeamiento de las necesidades reales, no de manera automatizada, pero si con cierto rigor en el apoyo en los datos históricos, concluyendo con una Plantilla Objetivo.

— Una Plantilla Objetivo que nos guiará en el proceso de contratación anual, permitiendo cubrir las necesidades programadas para los ámbitos que conforman el Ministerio de Defensa.

— Un control de inventario para todos los recursos puestos en manos del ministerio como base para un Cuadro de Mando que nos ayude a resaltar las acciones correctoras a llevar a cabo y toma de decisiones.

Y su aprobación por parte del Gobierno TIC para su ejecución, confirma que hemos conseguido los objetivos marcados en el TFM.

Hemos iniciado la renovación tecnológica propuesta al inicio del TFM, designado el mejor procedimiento para la contratación, conseguido acumular datos para sacar conclusiones y apoyar la toma de decisiones, pero lo más importante o concluyente del TFM es que estamos retrasados en aspectos de control de activos, con respecto al mercado actual.

Estamos obligados a mejorar y donde hay que centrarse para dicha mejora, es en la automatización de los procesos y, en nuestro caso, en la Gestión de Activos TI. Esta Gestión de Activos TI nos proporcionará la verdadera automatización de un Cuadro de Mando Integral como una herramienta de gestión para medir la situación y evolución de la renovación tecnológica desde una perspectiva general.

Figura 5. Ciclo PDCA del TFM

Referencias

España. (2015). Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. *BOE*. 10 diciembre 2015.

—. (2018). Instrucción 33/2018, de 6 de junio, del secretario de Estado de Defensa, por la que se aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. *BOD*. 7 junio 2018.

Tender Service Group. (s. f.). Pasos en un proceso de licitación pública. *Licitaciones.es*. Imagen Fase de Inicio. [Consulta:17 enero 2022]. Disponible en: https://www.licitaciones.es/service/noticias/proceso-licitacion-publica.

Plan de Renovación Tecnológica en el Ministerio de Defensa. Gestión de Activos TI

Autor: Raúl Jesús Richarte Reina
Director/es: Miguel Ángel Ares Tarrío y Francisco Javier Rodríguez Rodríguez

Introducción

Publicada la Política CIS/TIC del Ministerio de Defensa, desarrollada en base al Plan Estratégico CIS (PECIS) que constituye la guía implantación efectiva de las Capacidades CIS/TIC y de los distintos procesos y estructuras necesarios para su adecuado funcionamiento, y siguiendo los objetivos del Gobierno TIC (GESTIC) de este Ministerio, este Trabajo Fin de Master aborda un Planeamiento para la Renovación Tecnológica del Puesto de Trabajo Digital, siguiendo una serie de fases alineadas con el Ciclo de Deming, con el objetivo principal de impulsar la mejora continua en el planeamiento, contratación y control de activos del ámbito TIC.

Metodología

El planeamiento del Puesto de Trabajo Digital del Ministerio de Defensa englobará tres aspectos relevantes.

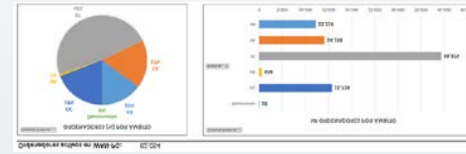
- En una primera fase, se establecen las necesidades reales de los ámbitos del Ministerio de Defensa, diseñando una "Plantilla Objetivo".
- En la segunda fase, se muestra la contratación pública desde el punto de vista del Técnico CIS.
- En la tercera fase, se presenta una forma de controlar/supervisar el recurso informático adquirido.
- Para culminar se automatiza un cuadro de mando que apoye la toma de decisiones de la Dirección del Gobierno TIC de la organización.

Resultados

Tras el estudio de los datos obtenidos de diferentes fuentes del Ministerio de Defensa, se han obtenido los resultados necesarios para ejecutar el Planeamiento de Renovación Tecnológica para el ciclo 2022-2026.

Para la ejecución final habrá que apoyarse en:

- La Plantilla Objetivo obtenida en base a las necesidades del Ministerio.
- Los procedimientos de Contratación Pública para la adquisición de los recursos previstos en la plantilla objetivo.
- Un Cuadro de Mando para Toma de decisiones en base a los datos generados de la compra y distribución de los activos a renovar.



Conclusiones

La aprobación por parte del Gobierno TIC del Ministerio de Defensa de los resultados contenidos en este TFM:

- Estudios estadísticos para llegar al planeamiento de las necesidades reales.
- La Plantilla Objetivo que nos guiará en el proceso de contratación anual permitiendo cubrir las necesidades programadas para el ciclo 2022-2026.
- Un Control de Inventario para todos los recursos puestos como base para un Cuadro de Mando que apoye la toma de decisiones.

Ello nos confirma la consecución de los objetivos marcados.

Tras dicha aprobación, estamos en la fase inicial de la Renovación Tecnológica necesaria en el Ministerio de Defensa y hemos preparado el primer escalón hacia una mejora en la automatización de los procesos. Particularizando en este trabajo, se han establecido las simientes para evolucionar en la Gestión de Activos TI.

Por último, indicamos unas líneas futuras a seguir que servirán de guía para continuar con la mejora en los procedimientos ahora establecidos.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Despliegue y aplicabilidad de una constelación de nanosatélites

Autor: Luis José Riesgo Juan (ljta1@hotmail.com)
Director: José María Núñez Ortuño (jnunez@cud.uvigo.es)

Resumen: – En los últimos años, el sector aeroespacial ha experimentado una importante evolución tecnológica, que se ve materializada con la puesta en órbita de satélites de mucho menor tamaño (nanosatélites), funcionando bien de manera individual, o conformando una constelación entre varios de este tipo. El coste de estas innovadoras soluciones es mucho menor (de un orden de magnitud de varias decenas o centenas de veces inferior respecto a un satélite convencional), lo que facilita la financiación de un mayor número de iniciativas tanto de empresas privadas como públicas (como los proyectos que dispone la empresa Marine Instruments o con los satélites Lume-1 desarrollados por la Universidad de Vigo, entre otros) e incluso se llevan a cabo hasta iniciativas de particulares.

El objetivo de este trabajo de fin de máster es presentar la composición de un nanosatélite, bajo el estándar de diseño normalizado que se denomina Cubesat. También se expone información de distintas aplicaciones que se consiguen cuando se ponen en órbita diferentes nanosatélites conformando una nanoconstelación.

Finalmente, se presenta un caso de uso que se basa en un estudio sobre la viabilidad para la realización del despliegue de una constelación de nanosatélites enfocado en monitorizar cualquier punto de interés de nuestro planeta. Se analizarán todos los aspectos que se desarrollan en la fase inicial (fase O) de una misión, tanto desde un aspecto técnico en el diseño del propio nanosatélite, como en aspectos que suponen la gestión e implementación del proyecto (planificación temporal, costes del proyecto).

Para llevar a cabo este estudio se ha una utilizado una de las herramientas comerciales más avanzadas para el diseño y simulación de la constelación junto a las estaciones terrestres y puntos de interés con los que se han hecho sus análisis.

Palabras clave: – Nanosatélite, Cubesat, Constelación, Teledetección, STK.

1. Introducción

En los últimos años, el sector aeroespacial ha experimentado una destacable evolución tecnológica. Este hecho se ve reflejado en la puesta de número, cada vez un mayor, de satélites de menor tamaño y con un más altas de funcionalidades que las que se disponían con los primeros satélites de la era espacial. Asimismo, el coste de estas innovadoras soluciones es mucho menor que en sus orígenes, lo que propicia un amplio desarrollo por parte de los principales países desarrollados del mundo, donde España también está llevando a cabo una labor destacable en este sector.

En los últimos veinte años han aparecido un mayor uso de los satélites de menor tamaño estandarizados bajo el concepto de los Cubesats [1], y que se denominan nanosatélites [2]. Este tipo de satélites se puede poner en órbita bien de manera individual o conformando una constelación de nanosatélites.

Estas constelaciones, además de ofrecer redundancia y robustez, constituyen un sistema flexible para el que los conceptos de obsolescencia o vida útil ya no constituyen una limitación. Por su propia naturaleza, los nanosatélites de una constelación se van renovando con regularidad por lo que el sistema y todos sus componentes se encuentran actualizados por completo, permitiendo ofrecer el mejor servicio tecnológicamente posible.

Este TFM presenta la composición de los diferentes subsistemas de un nanosatélite, según la definición que marca la normalización ideada del desarrollo de un Cubesat. El componente principal que determina las funcionalidades de una misión lo constituye su payload o carga útil, que llevan instalados los nanosatélites. Este subsistema, junto con el despliegue en órbita de otros satélites conformando una constelación, es lo que determina una gran variedad de aplicaciones en distintos sectores industriales, y que han sido revisados para cada uno de estos ámbitos en el presente trabajo.

En la parte final de este trabajo, se presenta una propuesta de anteproyecto en uno de estos ámbitos de aplicación, demostrándose su viabilidad de realización y exponiéndose los beneficios que se pueden obtener con este tipo de soluciones aeroespaciales.

2. Desarrollo

Tras realizar un amplio análisis del estado del arte que permite observar la evolución de la era espacial en su corta, pero intensa trayectoria, así como la tipología de satélites en sus diferentes tipos de órbitas, se introduce en detalle en presentar la composición detallada de un nanosatélite genérico bajo la concepción normalizada, siguiendo el concepto definido para los Cubesats.

Asimismo, se presenta la interrelación e interfaces de un nanosatélite con las partes que constituyen en la arquitectura de un sistema espacial,

bien de manera sencilla en una misión con una única nave o misiones formadas por varias aeronaves dando forma a una constelación. En este último escenario, se ha realizado un análisis completo de distintos usos y aplicaciones que actualmente se están llevando a cabo.

Se han abordado también algunas consideraciones necesarias para poder llevar a cabo la realización de una misión, y se finaliza este trabajo con la presentación de una propuesta de una constelación de nanosatélites para poder llevar a cabo la observación óptica la de Tierra.

Composición de un Cubesat

Los principales subsistemas que definen un Cubesat son los siguientes [3]:

- Payload o carga útil, componente que realiza las principales funciones de la misión particular establecida.
- Plataforma, equipamiento encargado de soportar la carga útil de la misión y que, a su vez, está compuesto por los siguientes módulos o componentes:
  - Módulo de control de la altitud y órbita - *Attitude and Determination Control Subsystem* (ADCS) o *Attitude and Orbital Control Subsystem* (AOCS).
  - Propulsion (PROP).
  - Mecanismos y estructura (MEC).
  - Subsistema de control térmico (TH).
  - Subsistema de energía eléctrica o *Electrical Power Systems* (EPS).
  - Comunicaciones: Telemetría, Seguimiento y Comunicaciones (TTC).

Arquitectura de una misión espacial

A alto nivel, una misión espacial consta de los siguientes tres segmentos interrelacionados entre sí [4]:

- Segmento de tierra: proporciona el enlace con los satélites. Por un lado, recibe la información de telemetría, los datos científicos de la misión generados en el payload. Por otra parte, envía los telecomandos para ejecutar operaciones de la plataforma y de la misión el payload.
- Segmento espacial: genera los planes de operación, controla la nave espacial, de acuerdo con los planes de operación, y obtiene los datos solicitados por el usuario.
- Segmento de usuario: recibe las solicitudes de los usuarios y les distribuye los datos científicos del payload.

Para comunicarse con los nanosatélites generalmente operan en distintas bandas de frecuencias, que se presentan, si las bandas VHF, UHF, L o banda S, las más extendidas en su uso.

Es muy importante la interrelación y visibilidad que deban tener los satélites con la estación terrestre, que en algunos casos corresponde con más de una estación terrestre, bajo el concepto de Red de Estaciones Terrestres Distribuidas (DGSN).

Dependiendo de la misión, también los propios nanosatélites tienen la opción de poder tener comunicación entre ellos (comunicaciones intersatelitales, ISL).

Aplicabilidades de las constelaciones de satélites

La funcionalidad básica de la misión de una constelación viene determinada principalmente por la carga útil que lleven instaladas las aeronaves o el tipo de plano orbital en el que transitan. Se han podido ver las grandes ventajas y versatilidad que propician para los nanosatélites transitar en órbitas de tipo LEO, y dentro de estas en un tipo de órbitas específicas que son las de tipo SSO [5].

De manera agrupada, las principales aplicaciones que una constelación de satélites puede disponer son las siguientes:

- Observación de la Tierra: de gran versatilidad y variedad de usos en misiones que permiten, por ejemplo, realizar labores de teledetección y analizar el medioambiente y hábitat de la Tierra [6]. Otros ámbitos de relevante utilidad son para defensa o análisis de intereses estratégicos de una nación.
- IoT o M2M, permitiendo una gran conectividad mundial con internet (IoT). A través de una red de nanosatélites interconectados en órbita [7][8] se puede llevar a cabo comunicaciones en zonas sin cobertura terrestre u oceánica, donde, adicionalmente, se están desplegando una gran de cantidad de objetos con sensores que transmiten información a través de, las cada vez mayores y más evolucionadas, redes de comunicaciones y servidores. Las rápidas conexiones y servicios permiten conectar distintas máquinas (M2M) u objetos de manera más eficiente.
- Geolocalizaciones y logística, se puede llevar a cabo la gestión de flotas de vehículos, aviones o barcos, entre otros, desde el espacio, incluso en zonas sin cobertura terrestre, y tener una visión global de manera prácticamente instantánea [9][10][11].
- Usos científicos, realización de pruebas e investigaciones de diversa índole.
- Usos militares [12], ampliando el espectro de comunicaciones militares surgen nuevos conceptos como, IoMT (Internet of Military Things) que incluye sensores, dispositivos portátiles, municiones, armas inteligentes, IoBT (Internet of Military Things), o combat cloud, entre otros.

Constelación IMSAT

Se presenta y desarrolla el análisis de la misión de una constelación de nanosatélites para la observación con cámaras ópticas de la Tierra. Se han partido de unos requerimientos para cubrir unas necesidades, entre ellas garantizar un número de visitas diarias a cualquier zona de interés, se ha realizado un estudio y dimensionamiento de la constelación que se ha denominado IMSAT. En este caso, estará constituida por doce satélites dispuestos en tres planos orbitales según una configuración definida mediante el esquema de Walker (Delta 97, 4º:12/3/1). Para ello, se han realizado distintas simulaciones con el programa STK Systems Tool Kit [13] (anteriormente Satellite Tool Kit). Con esta aplicación se ha podido comprobar no solo los tiempos de paso por cada zona de interés para su captación óptica, sino también con las estaciones terrestres propuestas que para este proyecto son dos, una situada en la actual estación del INTA en Torrejón de Ardoz y la otra en la estación de Maspalomas. También ha permitido simular en función de diferentes pesos y alturas orbitales su tiempo de vida.

Para esta misión se ha planteado en órbita LEO a 550 km de altitud, que junto a un diseño planteado en estructura Cubesat de 6U, permite un ciclo de vida estimado de unos cuatro años para cada nanosatélite. Se ha podido comprobar con STK la gran potencia de simulación que tiene para comprobar otros parámetros de vuelo de interés como son las comunicaciones mediante diferentes antenas planteadas y que para este caso se ha propuesto para transmisión en banda S, condiciones de temperatura, radiaciones, etc.

Adicionalmente, con las características requeridas se han podido decidir y seleccionar los principales componentes de los distintos subsistemas

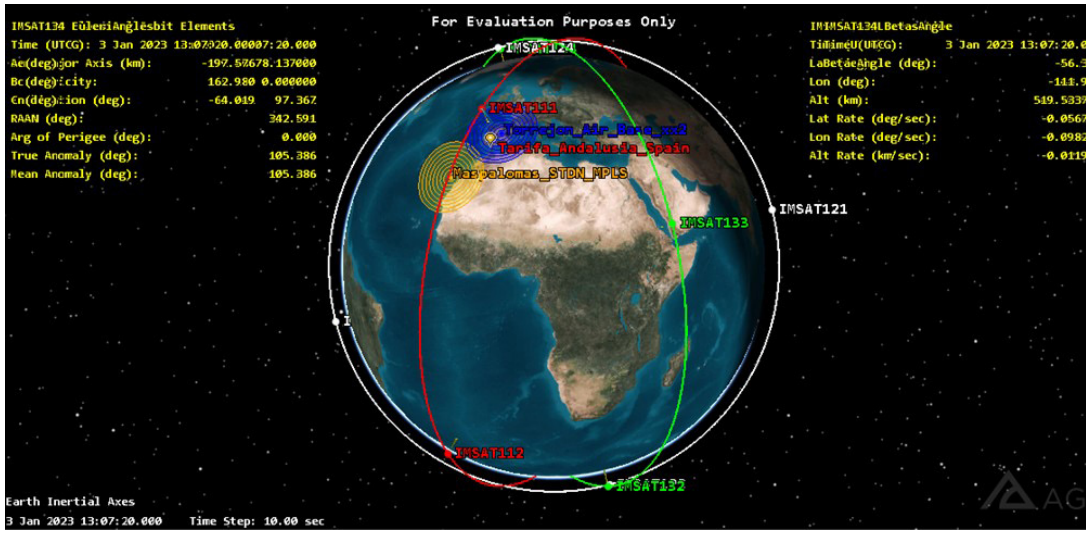


Figura 1. Posibles escenarios para una internet interestelar (extraído de [5])

de los nanosatélites. Sin lugar a duda, el más destacado de estos componentes es la carga útil o *payload*, que es el que determina la funcionalidad y aplicación del proyecto espacial. Por este motivo, se ha seleccionado una cámara ISIM-90 de la empresa SATLANTIS [14], de reducido tamaño y peso (4 kg) que puede instalarse en una estructura 6U sobre la que se montarán el resto de subsistemas y cuyo peso total, de cada nanosatélit,e será de poco más de 8 kg. Este tipo de cámara permitirá tomar imágenes ópticas de muy baja resolución (1,65 metros).

En paralelo al estudio del peso de la nave, se ha tenido que seleccionar los adecuados componentes que permitan garantizar su alimentación en vuelo. Para ello se han seleccionado tras ponderar el balance energético del consumo total que requerirá (48,28 W) con la energía proporcionada por cuatro paneles solares seleccionados para el tamaño 6U del satélite y que suministrarán en media unos 51,47 W, teniendo en cuenta el tiempo estimado de exposición solar con la inclinación de la órbita determinada. Mientras la nave no está en exposición a la luz del solar, se seguirá alimentando con un *array* de baterías recargables en cada giro con parte de la energía que se obtendrá de los paneles solares.

Siguiendo los estándares de realización de este proyecto creados por la Cooperación Europea para la Estandarización del Espacio (ECSS), desglosado en siete fases, se tiene planificado poner en órbita el primer nanosatélite a un año y medio del inicio del proyecto, y tener desplegado la misión completa de doce satélites tras dos años de proyecto. De este modo, si el proyecto se iniciara en enero de 2024, podría tener desplegado los primeros nanosatélites entre junio de 2025 y enero de 2026.

Teniendo en cuenta la planificación del proyecto con sus recursos, tanto materiales como de personas implicadas en su realización, se ha cuantificado un coste total de unos 14.255.000 € en sus primeros cinco años de la misión, con un coste estimado anual de mantenimiento de 3.397.360 € (3.056.400 € de CAPEX en la renovación anual de tres satélites y 340.960 € de OPEX dedicados a su mantenimiento y operación).

3. Resultados y discusión

Se ha podido constatar en este trabajo que los costes de una constelación con pequeños satélites en órbita LEO, como la planteada, son muy inferiores a los que implicaba su realización a los proyectos que se realizaban en el pasado y que culminaban con el lanzamiento de satélites de mucho mayor tamaño y peso en órbitas geoestacionarias.

En el estudio, confección y configuración de la constelación IMSAT que se ha presentado, se ha podido también comprobar que esta solución mejora sustancialmente la misión inicial que se inició en 2007 con INGENIO [15], y que no dio a luz en 2020 como se tenía previsto.

La tabla 1 resume las principales mejoras que se obtiene mediante la misión IMSAT, comparándola con la misión INGENIO. De este modo y de una manera sencilla, se puede apreciar que IMSAT es un proyecto mucho más económico, que asume menos riesgos para su realización y tiene una mayor versatilidad y flexibilidad de evolución futura, establecido por un diseño diferente, modular y mucho más sencillo de cada satélite que compone la constelación.

Aunque en este trabajo se ha comprobado los grandes beneficios y múltiples ventajas que se pueden llevar a cabo con constelaciones de nanosatélites, también hay otros tipos de proyectos que, por la magnitud de sus requerimientos, tal vez deban implementarse con otros tipos de satélites de mayor tamaño, o en su caso buscarse alguna solución tecnológica alternativa para poder llevarlos a cabo de manera viable. Este es el caso, por ejemplo, del programa de conectividad segura de la Unión Europea para el periodo 2023-2027 [20], o de proyectos actualmente en curso como las constelaciones Starlink [7] u Oneweb cuyos objetivos son conseguir dar una capacidad de telecomunicaciones con cobertura a nivel mundial.

Misión	Ingenio	IMSAT
Coste	Muy Alto 200 M €	Medio 14 M €
Despliegue	Plazos largos trece años (2007-2020)	Plazos cortos dos años (2024-2025)
Riesgo	Muy Alto Misión fallida	Bajo/Medio Equirepartida por cada nanosatélite de la constelación
Peso	700 kg/sat.	8 kg/sat.
Diseño	Complejo	Sencillo
Cobertura	Parcial Limitada por su órbita GEO	Global Facilitada por su órbita LEO
Revisitas	Limitada	Dos imágenes diarias/punto de interés Ampliable con más nanosatélites
Capacidad (estimada)	Menor Cien imágenes/diarias	Superior 1.440 imágenes/diarias
Resolución Óptica	10 m Fija	1,65 m Renovable con nuevas y avanzadas cámaras
Tecnología	Fija Definida al inicio de la misión	Flexible Renovable en nuevos nanosatélites
Sostenibilidad	Basura Espacial Mayor dificultad y costo su eliminación por su gran tamaño	Ecológica Mejor eliminación por su menor tamaño

Tabla 1. Comparativa entre las misiones INGENIO e IMSAT

4. Conclusiones

La tendencia actual en el mundo aeroespacial es a la realización de proyectos y misiones con pequeños sistemas de satélites (generalmente micro o nano) distribuidos y descentralizados de manera uniforme en uno o más planos orbitales y constituyéndose en constelaciones.

Las constelaciones de nanosatélites dan lugar a una gran variedad aplicaciones, que se han detallado en este TFM, con costes totales muy reducidos frente a los primigenios proyectos espaciales que se realizaban con enormes satélites.

Además de la reducción en costes, se han podido comprobar que se obtienen otras mejoras con este tipo de misiones con un menor riesgo de realización y mayor flexibilidad y adaptación en tiempo a los cambios y modernizaciones tecnológicas que se vayan requiriendo.

De manera sencilla se ha propuesto la implementación de una misión con una constelación de doce nanosatélites que permitiría a España reemplazar el proyecto que se pretendió abordar con la misión fallida INGENIO.

Si bien es cierto que se ha comprobado que, por envergadura de las necesidades, no toda solución se puede resolver con satélites del tamaño nano, como se ha desarrollado principalmente en este trabajo, si se puede plantear su evolución y desarrollo con otros tipos de constelaciones de satélites de mayor tamaño, o mediante una solución combinada con satélites de diferentes tamaños e interconectados entre sí.

Agradecimientos

En primer lugar, quiero agradecer a las personas que más cerco tengo y que me han apoyado durante la realización de este máster. A mi hijo Raúl, por estar siempre conmigo, además de haberme apoyado de manera especial cuando fue necesario en un par de momentos concretos en los que tuvo que declarar y supo defenderme durante la realización de este máster. A mis padres, por estar ahí y, sobre todo, por haberse podido hacer cargo de la atención de mi hijo cuando tuve que abordar la parte presencial en Marín. Y a mi pareja, por todo su apoyo, cariño y paciencia con el tiempo que le he quitado para poder dárselo a este curso.

Quiero también agradecer el apoyo de mi tutor, José María Núñez Ortuño, que gracias a su tutoría y apoyo incondicional me ha permitido desarrollar de manera satisfactoria este trabajo. Además, me facilitó el contacto directo con Fernando Aguado Agelet, experto en la materia que se ha tratado en este TFM. Ambas personas, pese a tener sus agendas muy ocupadas, fruto de la demanda que les requiere su buen trabajo y profesionalidad, se han volcado mucho conmigo, con absoluta disponibilidad, facilitándome todo lo que necesitaba para poder aprender mucho en el tema que se ha trabajado. Gracias a sus muy adecuados consejos, comentarios e indicaciones he podido realizar este trabajo.

Por último, quiero mencionar a todos los profesores y asociados, así como a todos mis compañeros, con los que he podido compartir de manera muy agradable la realización de este máster y aprender las últimas novedades de este dinámico mundo TIC y su gestión.

Referencias

Aerospacetech. *Curso de Ingeniería de Diseño de una misión y sistemas de un Satélite* [en línea]. [Consulta: 15 de septiembre 2022]. Disponible en: moodle.aerospacetech.org/pluginfile.php/1465/mod_resource/content/2/20200903_Master_Satellites_Platform_Cubesats_examples.pdf.

Alen space. (s. f.). Más de 15 años de proyectos exitosos. En: Casos de éxito de Alen Space [en línea]. Disponible en: alen.space/es/casos-de-exito/

Ansys Company. Disponible en: www.agi.com

Asher Space Research Institute. (s. f.). *Proyecto Adelis -Samson* [en línea]. Disponible en asri.institute/space-missions/adelis-samson/

Carvalho, R., Estela, J. y Langer, M. (eds.) (2020). *Nanosatellites. Space and Ground Technologies. Operations and Economics*. Wiley.

Çelikbilek, K. *et al.* (2022). *Survey on Optimization Methods for LEO-Satellite-Based Networks with Applications in Future Autonomous Transportation* [en línea]. Disponible en: //www.ncbi.nlm.nih.gov/pmc/articles/PMC8877282/

Comisión Europea. (2022). *Reglamento. Programa de conectividad segura de la Unión para el periodo 2023-2027*.

Solution for Cubesats [en línea].

Flightradar24. *Live Air Traffic* [en línea]. Disponible en: www.flightradar24.com.

Pérez Martínez, F. (2022). Tecnologías para la Defensa. *BIT de COIT*. Vol. 224, n.º 41.

Plass, S., Clazzer, F. y Bekkadal, F. (2015). *Current Situation and Future Innovations in Arctic Communications* [en línea]. [Consulta: 15 de diciembre de 2022]. Disponible en: https://www.researchgate.net/publication/283042184_Current_Situation_and_Future_Innovations_in_Arctic_Communications

Sateliot. Disponible en: www.sateliot.space/en/

Sener. *SEOSAT/INGENIO. Satélite Español de Observación de la Tierra* [en línea]. Disponible en: www.aeroespacial.sener/productos/seosat-ingenio-satelite-espanol-de-observacion-de-la-tierra

Satlantis. Disponible en: www.satlantis.com

Startical. Disponible en: www.startical.com/

Starlink. Disponible en: www.starlink.com.

Twiggs, B. (2021). *CUBESAT HANDBOOK From Mission Designs to Operations*.

Título del Trabajo Fin de Máster

Autor: Luis José Riesgo Juan
Director/es: José María Núñez Ortuño

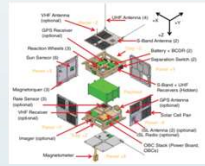
Introducción

En los últimos años, se está fomentando la puesta en órbita de satélites más pequeños o **nanosatélites**, de manera individual o conformando **constelaciones**. Este tipo de satélites se construyen según el estándar definido para **Cubesats**.
Se exponen también una amplia variedad de **aplicaciones** que este tipo de misiones permite.
Se presenta una **propuesta práctica** para la implementación de una constelación de satélites enfocado al campo de la teledetección mediante observación óptica de la Tierra, comparando las ventajas de esta solución frente a otro proyecto del pasado que se diseñó con un satélite de gran tamaño.

Metodología

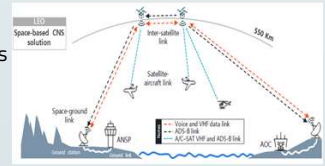
✓ **Nanosatélite:**

Estándar Cubesat



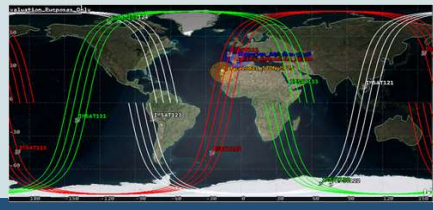
✓ **Aplicabilidad de las constelaciones** de satélites:

- Teledetección
- IoT/M2M
- Gestión de flotas
- Científicas
- Militares: IoMT, IoBT, Cloud



✓ **Constelación IMSAT:**

- Análisis y viabilidad del proyecto
- Simulador STK
- Carga útil ó payload: cámara óptica



Resultados

MISIÓN	IMSAT
Coste	14 M€
Despliegue	2 años
Riesgo	Bajo/Medio
Peso	8 kg/sat.
Diseño	Sencillo (Cubesat)
Cobertura	Global (LEO)
Revisitas	2+ imgs. diarias
Capacidad	1.440+ imgs. diarias
Óptica	1,65+ metros
Tecnología	Flexible
Sostenibilidad	Ecológica

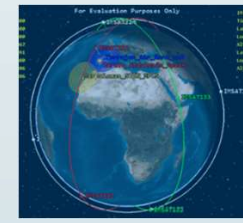
12

Conclusiones

✓ Tendencia actual hacia misiones con **nanosatélites** individuales o conformando una **constelación**.

✓ Resultan ser proyectos con un coste muy inferior a las misiones del pasado, y con muchas más **grandes ventajas** expuestas en este TFM.

✓ El **futuro** de este tipo de misiones es amplio con gran variedad de aplicaciones, algunas en curso y muchas otras están por descubrir, fruto de la gran flexibilidad y **versatilidad** que ofrecen.



Agradecimientos

✓ A mi hijo Raúl, mis padres y mi pareja.
✓ A mi tutor José María Núñez Ortuño, y a Fernando Aguado Agelet gran experto en la materia de este TFM, ambos por su tiempo y dedicación.
✓ A todos los profesores y personal asociado de la CUD, así como a mis compañeros de Máster.

Las comunicaciones en el espacio profundo. Hacia una internet interestelar

Autor: Mauricio Rodrigo Madrigal (mauricio.rodrigo@mde.es)
Director: José María Núñez Ortuño (jnunez@cud.uvigo.es)

Resumen: – En este TFM se aborda, en primera instancia, el estudio de los sistemas que se utilizan para establecer comunicaciones entre naves espaciales y sondas que navegan por el espacio profundo y la Tierra. Como es lógico, la variedad de sistemas y tecnología que se encuentra desarrollada desde los inicios hacia la década de los sesenta del siglo pasado (alguna de la cual todavía se encuentra activa por ser de utilidad) es muy amplia. Por ello, en el marco de este trabajo se desarrollarán las líneas generales de estos enlaces que son comunes a todas las misiones espaciales y que conforman lo que se conoce como Red del Espacio Profundo (DSN), haciendo hincapié en la tecnología propia de este tipo de sistemas tan específico.

La DSN es el germen que ha dado lugar al estudio de la futura implantación de una internet interestelar, esto es, la posibilidad de trasladar la internet terrestre que todos conocemos y utilizamos diariamente al espacio profundo. Por la magnitud de las distancias que hay que considerar, de hasta miles de millones de kilómetros, la internet interestelar tendrá que luchar contra parámetros que aquí en la Tierra no se plantean como puede ser el de las grandes latencias. Para este fin, se desarrollará un escenario especial de aplicación para una arquitectura destinada a ofrecer su servicio en el espacio, basada en las Redes Tolerantes a Demoras.

En la parte final de este TFM, el autor da un golpe de timón para cambiar radicalmente de escenario, volviendo a poner los pies en la Tierra. Se trata de una aplicación de lo anterior a un campo práctico en las Fuerzas Armadas y más en concreto en la Armada: las comunicaciones submarinas. Salvando las distancias conceptuales, el autor ha encontrado una similitud entre los medios espacial y submarino en cuanto a la dificultad que plantean para establecerse comunicaciones en cada uno de ellos. Con base en esto, traslada los estudios y desarrollos de la futura implantación de una internet interestelar hacia una próxima aplicación en las comunicaciones de los submarinos de la Armada, claro está, con sus correspondientes adaptaciones.

Palabras clave: – DSN, Internet, Latencia, Armada, Submarino.

1. Introducción

¿Qué es el espacio profundo? Se entenderá por espacio profundo aquel que se extiende desde más allá del sistema Tierra-Luna hasta el infinito. Desde el momento del lanzamiento, la única conexión que existe entre una nave espacial y la Tierra es el sistema de comunicaciones que se establece entre ambos elementos.

Para el establecimiento de este tipo de comunicaciones, la NASA cuenta con la Red de Espacio Profundo (DSN), que está configurada por tres grandes centros distribuidos 120º alrededor del globo terráqueo [1]. De esta forma, antes de que una nave espacial desaparezca por el horizonte en uno de los tres complejos de la DSN, ya hay otro de ellos que la tiene visible y toma el relevo de sus comunicaciones. Cada uno de los tres complejos que forman la DSN tiene un campo de antenas de gran tamaño, siendo las de 34 m y 70 m de diámetro las más utilizadas. Estas permiten la comunicación vía radio entre las naves espaciales y la Tierra y cuentan con receptores ultrasensibles que son capaces de detectar las señales de radio extremadamente débiles que emiten las naves espaciales. Además, se utilizan técnicas de criogenia (alrededor de 4º K) gracias a las que se reduce, de manera significativa, la temperatura de ruido de funcionamiento de los sistemas receptores [2].

Las funciones que básicamente se realizan en los complejos de la DSN son: telemetría (datos científicos, imágenes) en sentido nave-Tierra, mando (control de la nave, por ejemplo, cambio de ruta de vuelo) en sentido Tierra-nave y seguimiento (situación y velocidad de la nave) en sentido nave- Tierra. Las bandas de frecuencia utilizadas para las comunicaciones espaciales son: banda S, X, K y Ka [3].

La cantidad de misiones espaciales que hay operativas hoy en día es elevada y su número se va incrementando progresivamente, por lo que las arquitecturas de comunicaciones que les dan servicio son cada vez serán más demandantes. El escenario actual en el que se establece un único enlace de datos entre el centro de control en tierra y la nave espacial, en un futuro se dibuja como otro tipo de arquitectura en el que se contemplan múltiples nodos que no solo se comunican entre el espacio y la Tierra, sino que también podrán establecer comunicaciones entre los sistemas que se encuentren en el espacio.

Se plantea, por lo tanto, la creación de una red de comunicaciones que, a semejanza de la actual internet, ofrezca un servicio en el espacio en lo que se ha denominado en este TFM: internet interestelar que tendrá su base conceptual en las Redes Tolerantes a Demoras (DTN). Estas fueron concebidas para, entre otras cosas, salvar las enormes distancias que separan sus nodos (elevadas latencias) y las interrupciones que debido al escenario espacial sufren las comunicaciones. Con las DTN se pretende crear una infraestructura espacial confiable que dé una respuesta operativa a las necesidades de comunicaciones que los nuevos tiempos demandan.

2. Desarrollo

Las redes tolerantes a demoras (DTN), son, por tanto, la arquitectura en la que se fundamenta el desarrollo de la internet interestelar planteada en este TFM. La DTN consiste en una red de subredes independientes en las que no existe un canal único de comunicación entre origen y destino. Deben aprovecharse los contactos ocasionales entre nodos para realizar la transferencia de datos, haciendo progresar así los mensajes desde la *host* fuente hasta el sumidero.

En este tipo de redes ocasionales se evita la pérdida de datos por falta de conectividad entre nodos mediante el almacenamiento de estoss en discos duros que tendrán instalados los nodos y que les permitirán acopiar la información de manera indefinida hasta que se produzca la ocasión del contacto con otro nodo y le sean transferidos los datos [4].

Las transacciones de datos en estas redes son posibles gracias a la existencia del protocolo Bundle que se encarga de empaquetar toda la información en una sola entidad (denominada *bundle*) y transmitirla a través de la DTN. El protocolo Bundle permite la interoperabilidad entre redes que son heterogéneas.

Los posibles escenarios básicos que se tendrán que considerar a la hora de establecer una internet espacial se han reseñado en la figura 1. Basándose en estos, podrán irse construyendo el resto de posibles casos futuros, como si se tratase de ir montando piezas en un puzle.

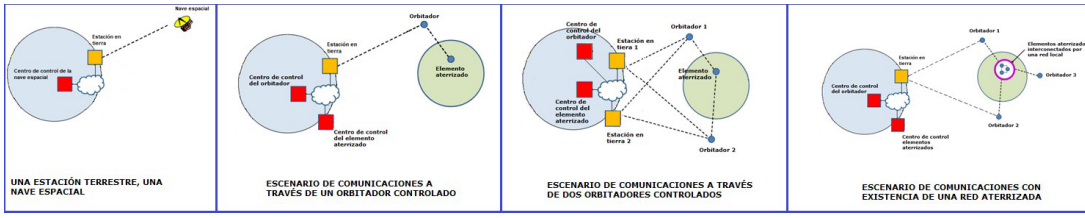


Figura 1. Posibles escenarios para una internet interestelar (extraído de [5])

A efectos prácticos, el autor propone un modelo/prototipo de cómo sería la arquitectura a implementar en el ejemplo práctico de que un astronauta en misión recibiese un correo electrónico desde su domicilio en la Tierra.

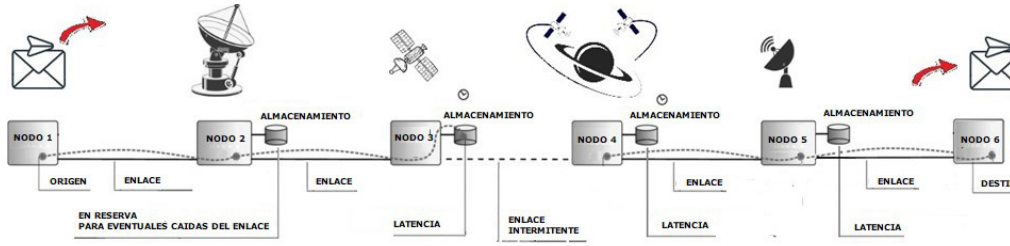


Figura 2. Arquitectura prototipo propuesta para envío de un mensaje por internet interestelar

En la arquitectura prototipo planteada en la figura 2 se involucran de manera directa seis nodos. El protocolo de enrutado para este modelo será un esquema de enrutamiento ilimitado donde no se habrá definido con antelación un número determinado de réplicas para un mensaje.

Para proceder a la transferencia de los mensajes en la red, se ha considerado usar el protocolo conocido como «rap de burbujas». Según este, todos los nodos pertenecerán a una única comunidad global y dentro de esta los nodos pertenecerán a comunidades locales diferentes. El reenvío de mensajes se hará de forma que, al principio los nodos reenviarán los mensajes a otros nodos que se encuentren en la comunidad global; esto se hará así hasta que el mensaje alcance un nodo que pertenezca a la misma comunidad local que el de destino, a partir de este punto el reenvío de mensajes ya se hará dentro de la propia comunidad local hasta que se alcance el destinatario [6].

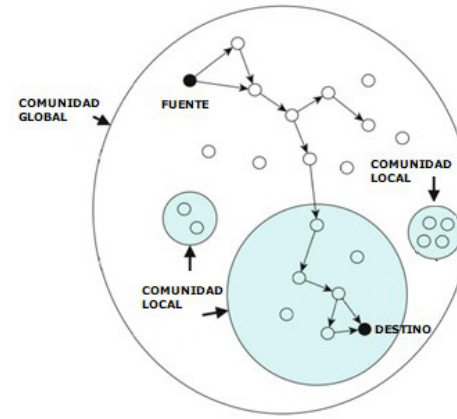


Figura 3. Descripción gráfica del protocolo «rap de burbujas» (extraído de [6])

Para fomentar la cooperación entre nodos, en esta arquitectura se utilizará el sistema de incentivos conocido como «reputación» [6].

Los beneficios que se obtendrán con la instalación de esta nueva arquitectura espacial de comunicaciones serán:

- Preservar la integridad de los datos, salvando los problemas de latencia.
- Reorganizar rutas futuras en la red, aunque en ese momento no estén disponibles, lo cual permite anticiparse a posibles pérdidas de enlace.
- Aumentar la velocidad de recepción de los datos que nos llegan a la Tierra desde las naves espaciales o sondas (downlink).
- La existencia de nodos intermedios y orbitadores permitirá una reducción de potencia muy considerable en las comunicaciones con respecto al actual sistema de enlace directo entre la Tierra y la misión espacial.

El autor no ha querido concluir el desarrollo del prototipo de una red de comunicaciones para su implementación en un entorno hostil (que en resumidas cuentas se podría sintetizar en esto) sin llevar también esta solución, además del entorno espacial, a una aplicación dentro del ámbito del Ministerio de Defensa: la Armada.

En principio la Armada, que desde siempre y por su particular idiosincrasia ha volcado gran parte de sus esfuerzos en el desarrollo de sus sistemas de comunicaciones, «ojos y oídos de sus unidades» desplazadas y

navegando a través de mares y océanos sin ningún otro punto de apoyo en muchas millas a la redonda, presenta *a priori*, una candidatura fuerte para ser usuaria de redes DTN.

Es por este motivo por lo que para encarar el tramo final de este TFM se va a (nunca mejor dicho) dar un fuerte golpe de timón para pasar del espacio profundo al «océano profundo». Se procederá a elaborar un prototipo de red con el que mejorar las actuales condiciones de comunicación con las que trabajan los submarinos de la Armada.

Actualmente, las comunicaciones submarinas militares se hacen vía radio (HF) o vía satélite militar, teniendo que salir a la superficie para establecer un enlace completo (emitir y recibir) con el consiguiente riesgo que para la discreción y seguridad de estas unidades implica.

En sus condiciones de trabajo, las comunicaciones submarinas se ven afectadas por los siguientes puntos:

- Cortes en el enlace de comunicaciones por necesidades operativas de la unidad (inmersiones).
- Cortes en el enlace de comunicaciones por condiciones atmosféricas, distancias de radiodifusión, estabilidad antena satélite, etc.
- Necesidad de retransmisión de los datos debido a cualquiera de los dos puntos anteriores.
- Necesidad de retransmisión de los datos porque uno de los nodos implicados en la arquitectura de la red que da servicio a la unidad no ha realizado el reenvío del mensaje.
- Que no exista comunicación con el submarino durante un periodo de tiempo prolongado de inmersión.

Una vez recopilados los problemas más importantes que rodean a las comunicaciones de los submarinos se puede observar que las redes DTN, que dan respuesta al futuro desarrollo de una internet interestelar, ofrecen también una solución a las comunicaciones submarinas en su ambiente de trabajo.

Como resultado de lo anterior, se establece que las redes ocasionales o redes DTN presentarán la solución práctica que como resultado de este TFM se propondrá para el establecimiento de una red de transporte dirigida a las comunicaciones de los submarinos de la Armada como mejora de las dos opciones antes expuestas, radio y satélite, y que son las que actualmente se utilizan.

El único hándicap es cómo conseguir efectuar, de forma novedosa, algún tipo de comunicación debajo del agua. En este sentido y aprovechando el desarrollo de una nueva tecnología que permite establecer comunicaciones submarinas vía láser [7], se instalarán dispositivos transceptores alrededor de todo el casco del submarino, según figura 4.

El concepto de internet interestelar desarrollado en este mismo trabajo se ha aplicado al montaje de una red DTN submarina. En ella se establecerá un ecosistema de nodos multidisciplinares para favorecer las transacciones de datos con la nave y facilitar sus comunicaciones sin necesidad de que tenga que subir a la superficie y poner en peligro su discreción.

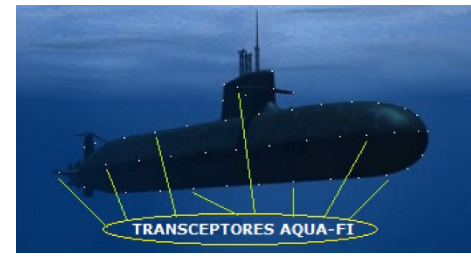


Figura 4. Prototipo de disposición de transceptores Aqua-Fi en un submarino de la Armada

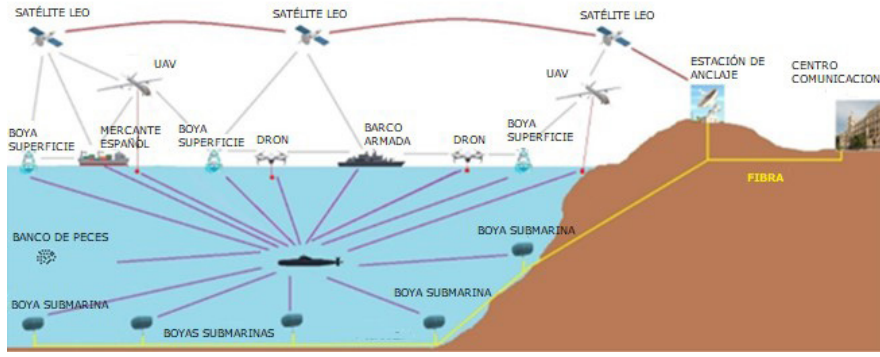


Figura 5. Modelo de red propuesto como solución para comunicaciones submarinas en la Armada

Para este prototipo, se elegirá un protocolo de enrutamiento denominado «epidemia». En este, un nodo que tiene un mensaje se considerará que es un nodo infectado. En el momento en el que un nodo infectado contacta con otro nodo que no tiene ese mensaje y, por lo tanto, no está infectado, el nodo infectado transmite el mensaje al segundo nodo y lo infecta... esta cadena transcurre así sucesivamente; infectando nodos hasta que en la red ya hay múltiples nodos infectados y el mensaje termina por llegar a su destino [6].

En este caso, y para lograr el objetivo de máxima cooperación entre nodos, el autor ha considerado utilizar un incentivo de «crédito» [6] que consiste en realizar pagos en forma de moneda virtual a los nodos cuando han participado en el reenvío de mensajes.

3. Conclusiones

El estudio de cómo realiza la NASA en la actualidad las comunicaciones en el espacio profundo gracias a su DSN, ha permitido comprender la necesidad de implementar un nuevo modelo de red de comunicaciones semejante a la que tenemos en la Tierra (internet).

Diversos problemas identificados en el medio espacial (elevadas latencias, cortes de servicio, etc.) han supuesto un hándicap a superar para poder modelar una solución viable. En este sentido, las DTN, dan respuesta a las preguntas encontradas y se erigen en un modelo real sobre el que plantear la arquitectura buscada para hacer real una futura internet interestelar.

En la búsqueda de una aplicación para la Armada a esta solución espacial encontrada, el autor ha identificado el medio submarino como equivalente al espacial en cuanto a que ambos representan un medio hostil para las unidades que lo transitan (unidades espaciales y submarinos, respectivamente para cada uno de los medios) y que, por tanto, tienen grandes problemas de comunicaciones actuamente. En este sentido, se ha modelado un nuevo escenario basado en las redes ocasionales, para dar una solución a las comunicaciones submarinas de la Armada.

Agradecimientos

Quiero expresar mi agradecimiento a mi familia, por su constante apoyo, a mi director José María Núñez Ortuño y el resto del personal docente del CUD de Marín. Al CN Díaz - Pache Mackinlay. Al director y resto de personal del Complejo de Comunicaciones en el Espacio Profundo de la NASA en Madrid por su inestimable ayuda. A la Armada a la que tanto debo. A Don Bosco...que guía mis pasos.

Referencias

Misra, S. (2016). *Opportunistic Mobile Networks*, Editorial Springer.

Nasa. Web Jet Propulsion Laboratory. (s. f.). *Red de Espacio Profundo* [en línea]. Disponible en: https://www.jpl.nasa.gov/missions/dsn. [Consulta: 29 junio 2022].

Páez Bencomo, M. I. (2013). Análisis y Evaluación de Prestaciones de Protocolos de Encaminamiento en Redes Tolerantes al Retardo [trabajo de fin de máster]. Director, Manuel Álvarez-Campana Fernández-Corredor. Madrid, Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros de Telecomunicación. Disponible en: https://www.dit.upm.es/~posgrado/doc/TFM/TFMs2012-2013/TFM_Maria_Irene_Paez_2013.pdf [Consulta: 10 octubre 2022].

Pérez, E. (2020). Aqua-Fi: crean el primer «Wi-Fi submarino» mediante LEDs y láseres para poder enviar información inalámbricamente bajo el agua [En línea]. *Xataka*. Disponible en: https://www.xataka.com/investigacion/aqua-fi-crean-wi-fi-submarino-mediante-leds-laseres-para-poder-enviar-informacion-inalambricamente-agua. [Último acceso 03 noviembre 2022].

Reid, M. S. (2008). *Low-Noise Systems in the Deep Space Network*. Jet Propulsion Laboratory California Institute of Technology. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://descanso.jpl.nasa.gov/monograph/series10/Reid_DESCANSO_sml-110804.pdf

The Consultative Committee for Space Data Systems. (2010), *Rationale, Scenarios, and Requirements for DTN in Space*. Space Operations Mission Directorate NASA Headquarters Washington.

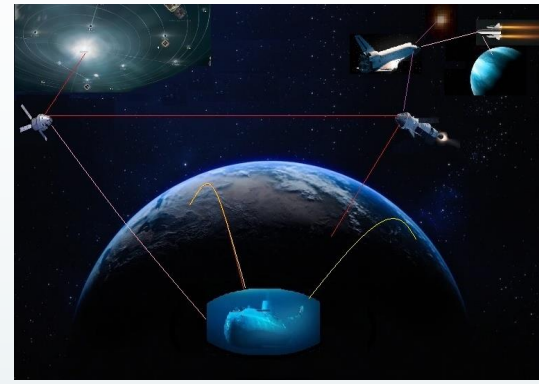
Yuen, J. H. (1982). *Deep Space Telecommunications Systems Engineering*. Jet Propulsion Laboratory California Institute of Technology. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://descanso.jpl.nasa.gov/dstse/DSTSE.pdf

Las comunicaciones en el espacio profundo. Hacia una Internet interestelar

Autor: Mauricio Rodrigo Madrigal
Director: José María Núñez Ortuño

SINOPSIS

Para el hombre, la exploración del universo no tiene límites, más allá de los límites tecnológicos. Las sondas y naves espaciales nos envían información de lo que están viendo y para eso es necesario contar con una potente red de comunicaciones como es la Red del Espacio Profundo de la NASA. ¿Cómo es posible comunicarse con una astronave a más de 23.000 millones de Km de la Tierra?
Actualmente, el desarrollo y proliferación de las misiones espaciales demandan comunicaciones similares a las terrestres donde las barreras que suponen las hostilidades propias del medio espacial como las elevadas latencias o las interrupciones de servicio, se superen y se pueda llegar a trabajar con una gran red de redes: Internet interestelar.



Aplicación en el campo de las comunicaciones submarinas de la Armada

Se ha aprovechado la necesidad de desarrollar una nueva arquitectura de comunicaciones en un entorno tan adverso como el espacio, para dar un golpe de timón y asemejar este escenario al de las comunicaciones submarinas en la Armada. Con este ánimo, se ha planificado una nueva solución que permitirá establecer una red submarina de comunicaciones en aras de mejorar las condiciones actuales de este tipo de unidades

Agradecimientos

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2022/2023

Cobertura 5G para la integración de las radios tácticas SDR

Autor: Luis Rojo Pinilla (lrojpin@gmail.com, lrojopin@et.mde.es)
Director: Miguel Rodelgo Lacruz (mrodelgo@cud.uvigo.es)

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

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

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

1. Introducción

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

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

Cabe destacar que este trabajo no es una solución única, es una propuesta, debido a que hay que tener en cuenta los distintos entornos operativos en que se pueden ver inmersos nuestras unidades. Ya que no es lo mismo su utilización en los distintos medios como mar, tierra o aire, y en las circunstancias donde se desarrollan las operaciones, por ejemplo, diferente manera de desplegar los medios CIS en una operación convencional, en un combate híbrido, en zona de operaciones, desembarcos paracaidistas, operaciones en ambientes confinados, etc.

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

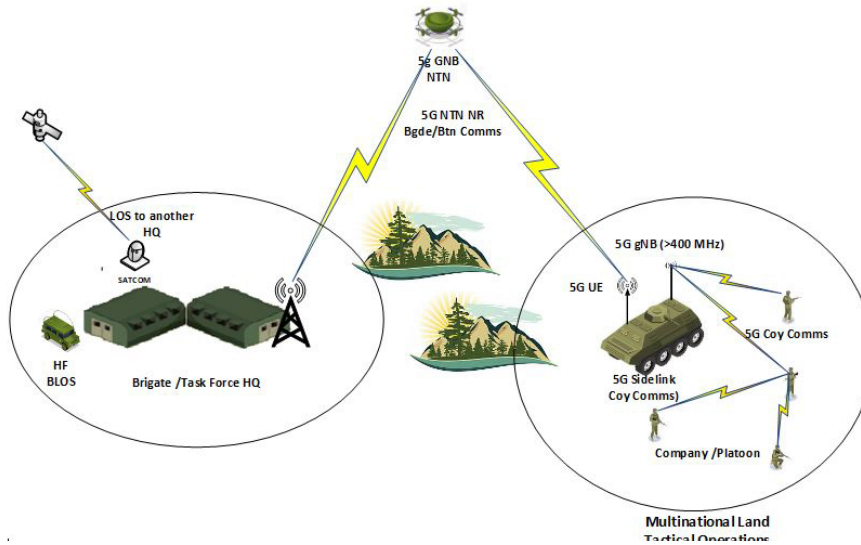


Figura 1. Empleo del 5G en PC desplegables (nivel brigada y grupo táctico). Fuente: diseño propio

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

Para desarrollar un proyecto fiable y siguiendo la documentación de referencia que han determinado el MINISDEF y la OTAN para la implantación de la tecnología 5G en los CIS de las Fuerzas Armadas, así como el seguimiento de las normativas y restricciones que limitan su uso, se hará un estudio de Gestión de Procesos de Negocio (BPM-Business Process Management), empleando la herramienta Bizagi y una planificación del proyecto, utilizado la herramienta Project2013.

Es importante tener en cuenta que este proyecto es solo una propuesta particular que puede coincidir con los proyectos que se puedan presentar por los distintos grupos de trabajo tanto del 5G como para las SDR designados por Defensa para este fin.

2. Objetivos

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

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

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

Por *último,* implementar los requisitos de seguridad necesarios para que las comunicaciones sean fiables y siempre siguiendo la arquitectura objeto y de la documentación de referencia que marca en Ministerio de Defensa.

3. Desarrollo

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

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

Adquisición de las SDR

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

Adquisición de equipos con tecnología 5G

- CORE 5G de telecomunicaciones en propiedad, con el fin de gestionar y administrar la propia red de telecomunicaciones en los puestos de mando desplegables, con capacidad de acceso a la I3D, mediante la capacidad que les proporcionaría las radios TACSAT (Terminales Satélite Tácticos). Securización de la red, control de acceso total sobre los usuarios. Establece una conectividad confiable y segura a la red para los usuarios finales y proporciona acceso a sus servicios, independientemente si hay o no proveedor de servicios.
- Integración a la «Nube de Combate» [5], entendiendo como nube de combate

  «La aplicación de una solución tecnológica avanzada a las capacidades militares que habilita su empleo, especialmente el mando y control, en el multidominio y que permite mediante la captura , procesamiento y distribución de datos, incluidos los que proporcionan sensores y sistemas e intercambio de información de datos, así como la prestación de servicios, que cada usuario, plataforma o nodo autorizado contribuya y reciba información esencial a tiempo para que sea capaz de utilizarla para la toma de decisiones y la ejecución de operaciones militares dentro de un espacio de batalla».
- Aumento notable de la capacidad de transmisión de datos, incremento del ancho de banda, acceso a sensores con garantías de recibir información en tiempo real, disminución de latencia, etc.
- Otro concepto que hay que tener en cuenta en la tecnología 5G, que permite la segmentación de redes, referido al empleo inteligente de secciones del espectro según las necesidades específicas del dispositivo o la aplicación en cuestión.
- Tiene la capacidad de verificación del rendimiento de diversos elementos virtuales de las redes 5G en el mundo real, se puede ampliar realizando pruebas y validando diversos casos prácticos de segmentación de redes en el entorno del laboratorio.

Implantación de Redes Definidas por *Software*. SDN

- Capacita a los usuarios finales (combatientes) para que puedan hacer uso de las redes de forma remota, segura, fácil y productiva, dándoles mayor capacidad de recursos para ejercer el Mando y Control de sus unidades. La SDN permiten conectar cualquier dispositivo o usuario a un sin límite de aplicación, sin importar lugar, ya sea en la nube, en el perímetro o en el centro de datos, con análisis y seguridad de red profundos.
- Se simplifican las implementaciones de nodos y sitios remotos con la visibilidad, agilidad y escalabilidad globales de la WAN, a través de una plataforma automatizada.
- La seguridad de la nube de la SDN se logra mediante la segmentación integral y funciones de red virtual (VNF) de seguridad, a través de la plataforma SDN. La SDN combina los servicios de seguridad y Edge Compute en una sola plataforma, controlado desde una sola interfaz de usuario, lo que permite que los usuarios y organizaciones se conecten de forma segura a múltiples nubes sin consumir recursos de los centros de datos. Además, garantiza la calidad de las aplicaciones, llevando el tráfico directamente a la nube y a las aplicaciones SaaS sin backhaul a través del centro de datos tradicional.

Capacidad de acreditación de la red, hasta difusión limitada

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

Viabilidad del proyecto

- Este proyecto se adapta a la normativa para la implantación del 5G en el ámbito del MINISDEF.
- El Proyecto está alineado con la Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones del CESTIC del Ministerio de Defensa.
- Respecto al presupuesto económico que se ha puesto como ejemplo, es importante hacer un inciso, ya que no está documentado por GEC (Grupo de Evaluación y Coste) ni por otro organismo competente en la materia, esta valoración no tiene soporte legal. En todo caso si se acepta esta cantidad, de unos 5.000.000 €, sería viable en el ámbito de MINISDEF.

4. Líneas futuras

Implantación del 5G, en redes y servicios del MINISDEF

La 5G es una tecnología de redes de comunicaciones de quinta generación que ofrece una mayor velocidad, capacidad y conectividad que las tecnologías de comunicaciones anteriores. Esto tendrá un gran impacto en la mejora de la eficacia de las comunicaciones en las operaciones militares, desarrollo de nuevas aplicaciones y tecnologías para inteligencia, vigilancia y defensa. Sin embargo, también existen preocupaciones sobre la seguridad de la tecnología debido a posibles ataques y espionaje, como consecuencia el MINISDEF ha desarrollado la «Resolución 07/08135/21 [3], de 17 de mayo de 2021, de la Secretaría de Estado de Defensa, por la que se establece la Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa», donde especifica que los desarrollos y definiciones de los proyectos se adaptaran a la evolución del contexto tecnológico y normativo que afecte al empleo de redes y servicios 5G, sobre todo en su seguridad en operaciones.

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

Seguridad del 5G [8][9]

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

El investigador principal Félix Arteaga, perteneciente al Real Instituto Elcano, en su artículo «Las medidas de la UE para proteger las redes 5G (EU Toolbox): se dice el pecado, pero no el pecador» [4], identifica los siguientes escenarios y los riesgos que se presentan.

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

Escenarios	Categorías de Riesgos (R)
Medidas de seguridad insuficientes	R1 desconfiguración de las redes
Cadena de suministros	R3 baja calidad de los productos
Modus operandi de los actores detrás de los riesgos (amenazas)	R7 disrupción relevante de las infraestructuras o servicios críticos
Interferencia entre redes y otros sistemas críticos	R8 fallo masivo de las redes debido a la falta de electricidad o de los sistemas de apoyo
Dispositivos de los usuarios finales	R9 alteración de los dispositivos lono

Tabla 1. Escenarios y categorías sobre riesgos principales en las redes 5G. *EU Coordinated Risk Assessment Report* [9]

Adquisición de CORE 5G

Las funciones básicas de la red 5G, en general, se consideran críticas. En efecto, afectar a la red central puede comprometer potencialmente la confidencialidad, disponibilidad e integridad de todos los servicios de red.

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

Desarrollo 5G *Non-Public Networks* [1]

Esta capacidad permitiría la implementación de 5G *Non-Public Networks* (NPN-Red no pública de 5G) [1], que permitiría a las unidades, tanto de nivel táctico como operacional, tener su propia red de datos, que, además, posibilitaría el acceso a la red pública o ISP, mediante la instalación de su correspondiente DMZ. Como se muestra en la figura 2, la única vía de comunicación entre NPN y la red pública es a través de la DMZ.

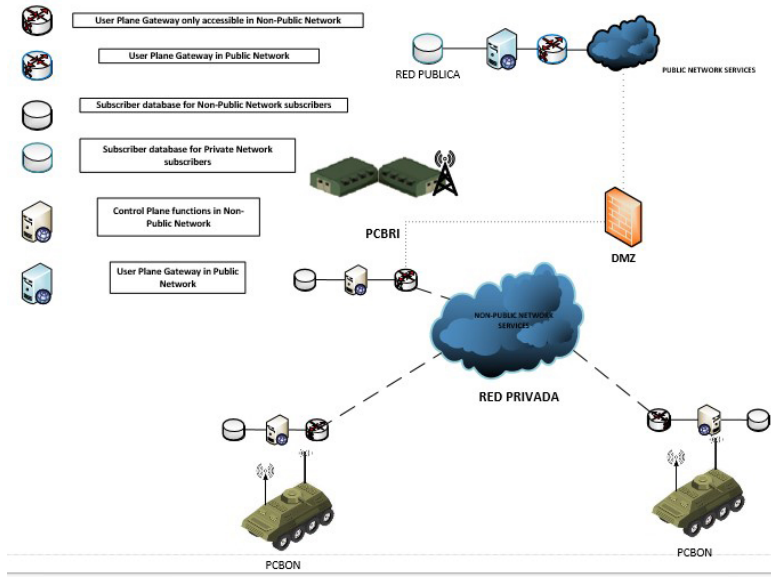


Figura 2. NPN. Non-Public Network. Fuente: diseño propio

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

Implantación SDN

La arquitectura de una red definida por *software* introduce un increíble potencial que sus controladores están basados en *software* y los interfaces de programación de aplicaciones (API), de innovación en el uso de la red.

La red definida por *software* proporciona una nueva forma de controlar el enrutamiento de los paquetes de datos, a través de un servidor centralizado. La combinación de la vista global de la red y la programabilidad de la red respalda el proceso de recopilación de inteligencia de los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) existentes, seguido de la reprogramación y el análisis centralizado de la red. En la STIC 140 [2], se explica los requisitos que debe cumplir.

Equipación de SDR para las FAS

La DGAM y MALE [6], han realizado ambos expedientes para la adquisición de SDR para el combatiente y se lo han adjudicado a la UTE Telefónica y Aicox. Por otro lado, la JCISAT del ET, en 2021 ha realizado «Pruebas de la radio SDR para Batallón» [7], de las SDR TGOR-V de Tecnobit-Grupo Odesia.

La adquisición de estos tipos de radios, siguen las especificaciones marcadas en el proyecto, a continuación, se expone todas las especificaciones técnicas de la radio presentada por Tecnobit [7].

«La radio TGOR trabaja con un ancho de banda de hasta 100 Mbps, en la banda VHF, UHF y la banda L, realiza asignación dinámica del espectro, permite la recepción multicanal, y la priorización de comunicaciones simultáneas [...]»

> «Como dos de sus características más destacables podríamos mencionar su carácter de radio cognitiva, gracias a su capacidad de análisis del espectro electromagnético y de detección de posibles perturbadores (jammers)». «Además permite también la utilización de una Red Móvil Ad-Hoc (MANET) para que cada uno de los nodos / radios puedan comunicarse entre sí».

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

5. Resultados y discusión

En consonancia con el proyecto presentado, ya existen equipos SDR adquiridos por las FAS y está en estudio la optención de equipos que tienen capacidad cognitiva para gestionar la forma de onda específica que pueda integrarse con las frecuencias utilizas en 5G.

Existen estándares de la 3GPP desarrollados para 5G, que permiten la creación de una NPN, para uso único, por lo que se aumentaría la seguridad al estar controlado el acceso libre a las redes públicas.

El CCN, ya ha definido mediante la STIC 149 «Redes Definidas por Software» y STIC 499. «Arquitectura de Seguridad en la Cloud», como sería el acceso tanto a la nube como a la implementación de SDN.

6. Conclusiones

Una vez realizado un estudio de viabilidad y de planificación del proyecto, se puede sacar la conclusión, teniendo en cuenta tanto la Normalización Técnica sobre regulación y estandarización de 3GPP, respecto a la tecnología 5G, como las especificaciones de seguridad marcadas por el CCN para su implementación como red de acceso a los CIS desplegables del ET y su integración a la I3D, es posible su implementación.

Hay que destacar la importancia que tiene la capacidad de gestión del espectro de los modelos de SDR (algunos con capacidad cognitiva), presentado por las empresas, esto nos abre aún más el camino para conseguir que mediante la configuración de la forma de onda que definan las frecuencias asignadas para el 5G, sea posible que estos equipos puedan integrarse. No hay que olvidar que tienen la capacidad de ser interoperables con GESCOMET (Gestor de Comunicaciones del ET), permitiendo la interoperabilidad entre equipos legados como pueden ser las radios tácticas de VHF PR4G.

También hay que hacer mención, que un proyecto cuya financiación es de aproximadamente 5.000.000 €, no puede ser impedimento insalvable para las capacidades de Mando y Control que ofrece estas tecnologías, proporcionando la hiperconexión de todos los sistemas CIS, permitiendo un entorno multidominio definido como «Nube de Combate».

Agradecimientos

Agradezco y dedico este trabajo de fin de máster a mi familia y, en especial a mi mujer, Rosa, por el apoyo y la paciencia que ha tenido, soportando toda la carga familiar durante el desarrollo de este máster.

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

Sin olvidar a los profesores del CUD y compañeros del máster, por los conocimientos adquiridos con su ayuda.

Referencias

5G Alliance for Connected Industries and Automation. (2019). *5G Non-Public Networks (5GACIA).* Disponible en: https://5g-acia.org/wp-content/uploads/2021/04/WP_5G_NPN_2019_01.pdf

Arteaga, F. (2020). Las medidas de la UE para proteger las redes 5G (EU Toolbox): se dice el pecado, pero no el pecador. *Elcano, F. A.-R.* Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari17-2020-arteaga-medidas-ue-para-proteger-redes-5g-eu-toolbox-se-dice-pecado-pero-no-pecador.pdf

CENTRO CRIPTOLÓGICO NACIONAL. (2021). *CNN STIC 140. REDES DEFINIDAS POR SOFTWARE*. Recuperado en diciembre de 2022.

DEFENSA, (2021). *Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa.*

Defensa.com. (2020). *Telefónica y Aicox suministrarán radios del combatiente a Defensa por 6,6 millones* [en línea]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3124895/telefonica-aicox-suministraran-radios-combatiente-defensa-66-millones

—. (2021). *El Ejército de Tierra evalúa las radios vehiculares SDR TGOR-V que podrían equipar el VCR 8x8* [en línea]. Disponible en: https://www.defensa.com/espana/ejercito-tierra-evalua-radios-vehiculares-sdr-tgor-v-podrian-vcr

EMAD. (2022). *Visión del JEMAD de la «Nube de Combate». 04 de enero de 2023*

Kaspersky (2019). ¿Es peligrosa la tecnología 5G? - Ventajas y desventajas de la red 5G. Disponible en: https://latam.kaspersky.com/resource-center/threats/5g-pros-and-cons

NIS COOPERATION CROUP EU. (2019). *EU coordinated risk assessment of the cybersecurity of 5G networks.*

Cobertura 5G para la integración de las radios tácticas SDR

Autor: Luis Rojo Pinilla
Director: Miguel Rodelgo Lacruz.
Universidad de Vigo

Introducción

Este trabajo tiene como fin plantear soluciones para poder utilizar la tecnología 5G en las FAS, para la integración con los sistemas de radio tácticos definidos por software.
Para esto se hace referencia, a la Arquitectura de Referencia definida por el Ministerio de Defensa, la Estrategia de la utilización de la nube y de la utilización de la tecnología 5G, definida en distintas resoluciones por MINISDEF en entornos operativos.

Metodología

1. Se sigue lo marcado por el MINISDEF en las siguientes resoluciones:

"**Estrategia de Explotación de la Nube en el Ministerio**".
Se aplican los siguientes puntos:

- Necesidad operativa.
- Objetivos esperados y plazos previstos de inicio y consecución.
- Dominio/s de aplicación, escenario/s de referencia y opción de despliegue y uso más adecuada.
- Matriz de responsabilidades (RASCI) .
- Interdependencia con proyectos de desarrollo del PECIS.
- Recursos implicados (humanos, materiales, financieros y formativos).

"**Estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa"**

- Definir las **líneas de actuación** para la consecución de los objetivos de la Estrategia. Se coordinará con los Planes de Acción de desarrollo del Plan Estratégico CIS del Ministerio (PECIS).
- Identificar las áreas de aplicación de **esta tecnología para el Ministerio de Defensa** y su alineación con las Capacidades Militares .

2. Planificación y gestión del proyecto.

Resultados

- Identificadas las capacidades militares y las necesidad operativa con la que se relaciona este proyecto.
- Propuesta de arquitecturas que dan cumplimiento de las especificaciones de seguridad CCN.
- Estudio de viabilidad del proyecto.

Conclusiones

- En este trabajo se puede sacar como conclusión principal que el proyecto es viable tanto técnicamente como con respecto a la legislación que regula la utilización del 5G y la Nube para su implementación en el MINIDEF.
- Es importante señalar , que la utilización de esta tecnología permitiría a las CIS desplegables, dar un gran salto cualitativo respecto a las capacidades operativas que ofrece. Dando la posibilidad de proporcionar la hiperconexion de todos los sistemas, permitiendo un entorno multidominio definido como "Nube de Combate".

Agradecimientos

Agradezco y dedico este Trabajo Fin de Master a mi familia y en especial a mi mujer Rosa, por el apoyo, paciencia que ha tenido soportando toda las cargas familiares durante el desarrollo de este Master.
También quiero hacer mención para agradecer el apoyo que me han proporcionada mis mandos y compañeros durante estos meses.
Y sin olvidar a los profesores del CUD y compañeros del MASTER, por los conocimientos adquiridos con su ayuda.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL