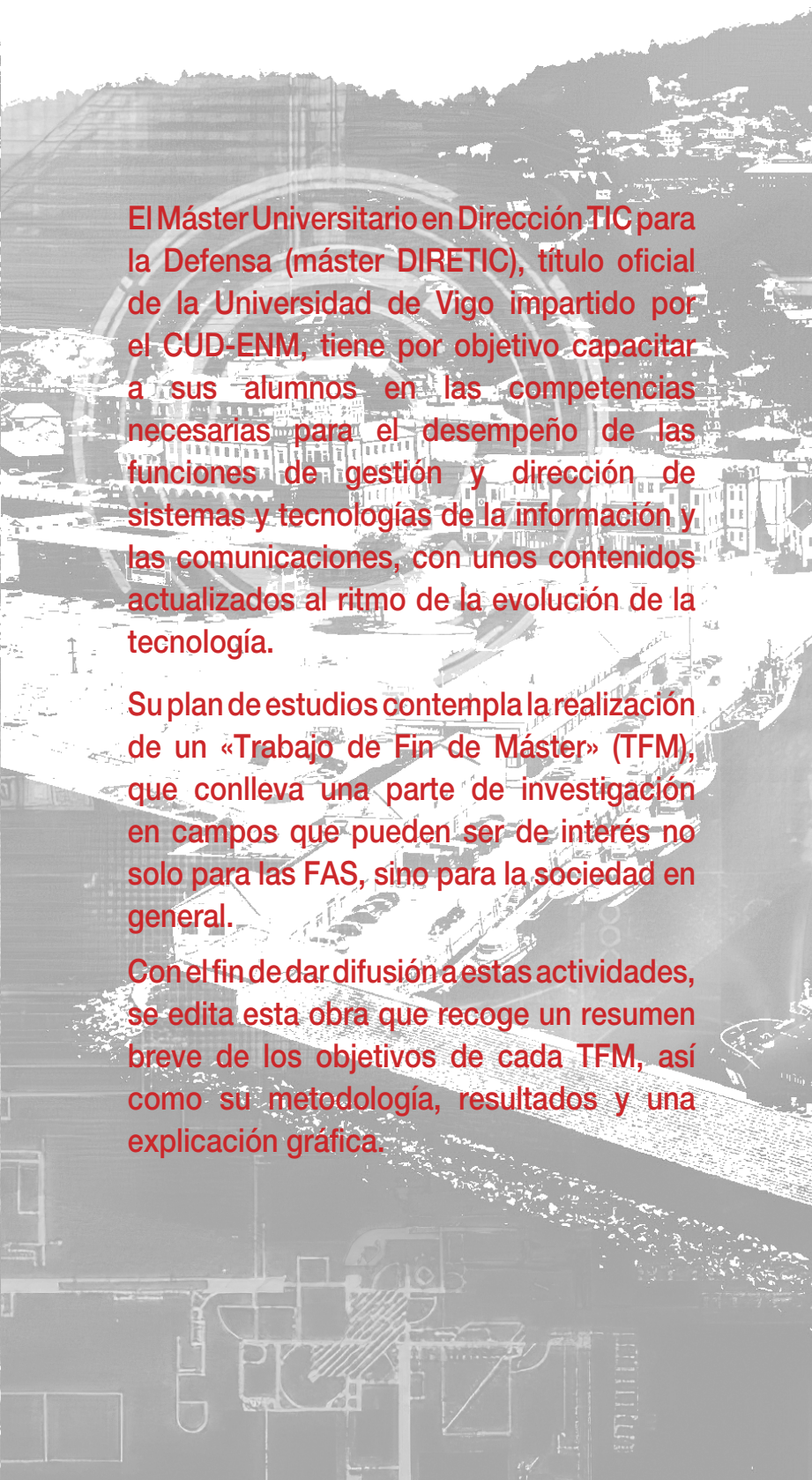
Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2023-2024

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 2023-2024

RESÚMENES EXTENDIDOS

Centro Universitario de la Defensa en la Escuela Naval Militar

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
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

© Autores y editor, 2024

NIPO 083-24-293-0 (edición impresa)
ISBN 978-84-9091-978-1 (edición impresa)

NIPO 083-24-297-2 (edición en línea)

Depósito legal M 2072-2025
Fecha de edición: enero de 2025
Maqueta e imprime: Imprenta Ministerio de Defensa

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad de los autores de la misma.
Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del copyright ©.

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 la citada universidad, pero el propio Real Decreto contempla que se puedan impartir enseñanzas de posgrado, en las modalidades de máster y doctorado.

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[1]), asignada al

[1] Un crédito ECTS (Sistema Europeo de Transferencia y Acumulación de Créditos) equivale a aproximadamente 25-30 horas de trabajo del estudiante.

CUD-ENM en forma de máster, más un periodo de prácticas presenciales (6 ECTS), cuya responsabilidad recae en el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (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 produjo el egreso de la primera promoción de este máster.

El plan de estudios del máster DIRETIC contempla la realización de un Trabajo 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 2023-2024, 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 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

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/123456789/518

Índice de contenidos

Índice por autores

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de Información

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de Información

Seguridad en Sistemas de Control Industrial Embarcados

Autor: Abad Barral, Fernando (fabadbarral@gmail.com)
Director: González Coma, José (jose.gcoma@cud.uvigo.es)

Resumen – Cada vez con mayor frecuencia los sistemas industriales de cualquier organización o nación se ven involucrados en un incidente de seguridad. Son sistemas robustos caracterizados por su fiabilidad a lo largo del tiempo y que no han sido sometidos a una política de seguridad definida. En concreto, en muchos casos, los administradores de este tipo de sistemas confían en su completo aislamiento para no aplicar ninguna medida que mejore su seguridad, como puede ser la actualización de su *software*.

Sin embargo, la transformación digital está ofreciendo soluciones para mejorar las capacidades digitales de los procesos y gestionar los datos de este tipo de infraestructuras. El principal hándicap de estas soluciones es que están directamente relacionadas con servicios de tecnología de la información habituales y suponen una verdadera amenaza para cualquier instalación industrial. Ello implica que su superficie de exposición se incremente exponencialmente y entre en juego la evaluación de un análisis de riesgos para determinar cuantitativa y cualitativamente las consecuencias que puede suponer el empleo de terceras tecnologías expuestas al exterior.

El presente trabajo pretender abordar la seguridad de sistemas industriales específicos que están embarcados en buques. Estos sistemas, por su relevancia, juegan un papel fundamental en la correcta operatividad del buque y la seguridad de la dotación. En la primera parte de este trabajo se realiza una introducción a los sistemas de control industrial y sus principales componentes. En el segundo punto se explican las particularidades de los sistemas industriales y, más en concreto, sus tipos de comunicaciones y protocolos. En la tercera parte se explica la infraestructura física desplegada con dispositivos del fabricante Siemens, simulando ciertos sistemas y servicios de una infraestructura industrial de un buque. Tras ello, se realiza una auditoría de la infraestructura, detallando los diferentes métodos empleados y las herramientas utilizadas para evaluar su seguridad. Finalmente, en la última parte del trabajo, se propone una estrategia basada en la defensa en profundidad para mejorar la seguridad de

este tipo de entornos, de tal manera que se posicione como un marco de referencia para su protección durante todo su ciclo de vida.

Palabras clave – Ciberseguridad, Sistemas de Control Industrial, ICS CyberSecurity, ICS and PLC Pentesting, ICS Defense In Depth.

1. Introducción

Los actuales buques de la Armada española se enfrentan a diario a operaciones de una amplia variedad a lo largo de todo el panorama internacional y de diferente índole. Entre sus diferentes funciones se encuentran la de garantizar la seguridad nacional desde y en la mar, y apoyar a otras organizaciones en el mantenimiento de la paz mundial. Para ello, los buques cuentan con sistemas específicos para llevar a cabo sus misiones, sostenidos por una compleja infraestructura naval y de telecomunicaciones.

Dada la envergadura de tal infraestructura, la superficie de exposición ante cualquier amenaza es, como mínimo, considerable. Otras unidades se limitan a un número, sino solo una, limitado de redes en sus destacamentos. Por el contrario, un buque despliega todo tipo de redes y sistemas, tanto TI (Tecnología de la Información) como TO (Tecnología de Operación), para ser autónomo y poder llevar a cabo todo tipo de operaciones en la mar. A esto hay que sumarle la digitalización que se está produciendo y que da como resultado una capa empresarial y de producción más conectada.

Debido al mundo actual cambiante y lleno de incertidumbre, en el que las amenazas son cada vez más sofisticadas, innovadoras y específicas, los buques necesitan mejorar la seguridad en sus redes y sistemas con el fin de garantizar los tres ejes de la seguridad de la información: confidencialidad, integridad y disponibilidad. Además, esto toma mayor importancia desde dos puntos de vista. El primero, operativo y ligado al nivel de clasificación de la información que se maneja y que es vital para el buen desempeño de la misión. Por otro lado, el del correcto funcionamiento de la infraestructura naval y de la seguridad de la dotación, también denominado *safety* y directamente relacionado con los sistemas TO.

En los últimos años se ha mejorado la seguridad de los sistemas TI en todas las unidades, implementando unas políticas de seguridad bien definidas. Sin embargo, a pesar de que la industria y las necesidades tecnológicas han seguido evolucionando vertiginosamente a lo largo de las últimas décadas, no se ha hecho el mismo hincapié en la seguridad de los sistemas de tipo industrial. La Armada 4.0 tiende a mejorar los procesos logísticos y anticiparse de manera preventiva a los posibles defectos que se puedan originar en los elementos mecánicos de un buque e, incluso, poder actuar en remoto para realizar una asistencia crítica que repare un elemento concreto. Sin embargo, aunque se ha evolucionado en este sentido, no se ha hecho al mismo nivel en lo relativo a seguridad de la información, y en concreto, en los sistemas industriales embarcados.

Las redes industriales tienen requerimientos críticos que necesitan ser abordados. Su alta disponibilidad hace que sea una de sus prioridades como componente de la seguridad de un sistema de este tipo. De hecho, a diferencia de un sistema de información, en este tipo de sistemas es el primer eje fundamental de la ciberseguridad industrial, por delante de la

confidencialidad o la integridad. Otra característica de este tipo de sistemas es su robustez, que hacen que estén diseñados para hacer frente a entornos con condiciones físicas concretas y que hacen que sus ciclos de vida sean largos. Por lo general, llevan a cabo procesos deterministas en los que realizando un seguimiento se puede llegar a conocer sus parámetros y variables. Por último, hay que destacar su mantenimiento y diagnóstico como otro de los requerimientos críticos de este tipo de sistemas. No se conoce un mantenimiento como el que se plantea en sistemas de información y en este caso, los mantenimientos suelen ser programados y con una frecuencia determinada. Además, antes de realizar cualquier actualización se prueba en entornos de preproducción y se procede a su validación para garantizar su correcta funcionalidad antes de entrar en producción.

Por todo ello, se ve la necesidad de iniciar este proceso de mejorar los controles sobre los sistemas de tipo industrial embarcados en la flota actual. Son sistemas relativos al control de armas de combate y de la plataforma naval, que se encargan de gestionar el gobierno de la navegación, planta eléctrica o el direccionamiento de un misil, entre otros. Todo ello no supone una simple superficie de exposición más a ser atacada, si no que puede tener graves consecuencias sobre la dotación.

Ante esta situación y debido a que aún no se ha investigado nada al respecto, el panorama se prevé complejo y delicado. Este tipo de sistemas son sistemas específicos diseñados por diferentes empresas que colaboraron en su momento en la fase de diseño y construcción del buque, pero que en ningún momento tuvieron presente la premisa *security by design*. Por ello, es difícil poder llevar a cabo ciertas directrices sin tener un entorno de preproducción en el que poder ampliar conocimiento y depurar las acciones a realizar para mejorar la seguridad de estos sistemas y, más en concreto, su disponibilidad ante un ciberataque.

Definitivamente, los sistemas industriales son diferentes respecto a los sistemas de información. Llevar a cabo una auditoría de seguridad sobre estos sistemas requiere un enfoque totalmente diferente, sobre todo debido a que cualquier consecuencia sobre estos sistemas tiene unas implicaciones físicas. Asimismo, estos sistemas también usan tecnología y protocolos propios del sector que son particulares y que requieren conocimiento apropiado para poder abordarlos.

Por todo ello, se ve necesario poder contar con una infraestructura adecuada para poder mejorar las capacidades de ciberseguridad en sistemas industriales encaminadas a conocer en profundidad las particularidades de este tipo de sistemas y llevar a cabo pruebas en un entorno controlado, en el que desplegar soluciones de seguridad específicas para su control, mantenimiento y protección.

El presente trabajo está orientado a construir una infraestructura de un sistema de control industrial que se asemeje, en cierta medida, a los

posibles servicios de los que dispone un buque a bordo. A partir de ahí, las conclusiones se pueden extrapolar a un sistema industrial real, ya que en muchos casos la tecnología es similar o, lo que es peor, incluso bastante más obsoleta. Con dicho objetivo, la primera y segunda parte del proyecto están orientadas a explicar las características de un sistema industrial, sus componentes y sus particularidades tecnológicas en términos *software* y sus protocolos específicos. La tercera parte detalla la infraestructura física desplegada en un laboratorio de pruebas del Mando Conjunto del Ciberespacio (MCCE), explicando la arquitectura desplegada, componentes, funciones y lógica implementada. En la cuarta parte se aborda una auditoría de seguridad para poner en valor la necesidad de aplicar unas adecuadas políticas de seguridad a todos los niveles (administrativos, físicos y técnicos) y se documenta el procedimiento seguido y las vulnerabilidades descubiertas. El quinto apartado se destina a realizar una valoración exhaustiva de las deficiencias encontradas en el sistema y se propone un marco de referencia para llevar a cabo una defensa en profundidad. Finalmente, se exponen las conclusiones finales y posibles acciones de investigación futuras.

2. Desarrollo

Actualmente los sistemas industriales de control y automatización desempeñan funciones fundamentales en la industria. Son sistemas que por sus características están relacionados con el control de procesos industriales en sectores tales como el energético, farmacéutico, logístico, automovilístico y, en general, cualquier ámbito en el que se manejan y controlen señales de tipo físico. Estos sistemas, a diferencia de los sistemas de tecnología de la información convencional, están diseñados para poder soportar unas condiciones diferentes y más exigentes. Se trata de escenarios en los que estos tipos de sistemas están expuestos a variables físicas que ponen al límite los elementos *hardware* de la infraestructura.

Todo sistema industrial está formado por una serie de componentes específicos para este tipo de sistemas. Los posibles dispositivos que pueden existir en este tipo de instalaciones y que, por tanto, son susceptibles de ser analizados, monitorizados, controlados y auditados, son los sistemas SCADA, los sistemas de control distribuido (DCS), los Remote Terminal Unit (RTU), los Programmable Logic Controller (PLC) y los Human Machine Interface (HMI).

Controladores, dispositivos, sensores y actuadores comparten información y datos en tiempo real para acometer sus funciones dentro de la red de automatización industrial. Para llevar a cabo dicha comunicación, estos dispositivos emplean protocolos específicos basados en *ethernet* industrial como EtherNet/IP, ModBus TCP o Profinet. Hacia el año 2004 se consiguió que algunos buses de campo con base *ethernet* fueran introducidos por el IEC (International Electrotechnical Commision) para que pudieran convivir con protocolos *ethernet* no diseñados para dar respuesta

en tiempo real, de tal manera que se facilitase la integración vertical con esos protocolos de campo. La desventaja de todo esto es el incremento de los vectores de ataque que pueden ser empleados para explotar una vulnerabilidad debido a esta estandarización. Porque, al fin y al cabo, aquellos ataques que eran efectivos en redes IT, ahora también pueden ser extrapolables de alguna manera a redes OT.

Dada la importancia de los protocolos de comunicación, en el trabajo se estudia en detalle el protocolo Profinet, base de las comunicaciones de los dispositivos del fabricante Siemens. Al respecto, se ve conveniente estudiar los protocolos de nivel de enlace de datos Discovery and basic Configuration Protocol (DCP) y el protocolo Link Layer Discovery Protocol (LLDP). También se estudia en detalle el protocolo de comunicación S7Comm específico, implementado por Siemens para sus dispositivos.

Parte de este trabajo se destina a explicar la infraestructura desplegada como entorno de preproducción, simulando varios sistemas de un buque. Disponer de un entorno de preproducción es esencial para poder conocer en profundidad la tecnología, concienciar al personal y realizar acciones formativas donde no exista ningún riesgo para la dotación de un buque. Asimismo, el entorno de pruebas es la infraestructura adecuada para poder llevar a cabo auditorías de seguridad en las que validar los controles de seguridad de los sistemas y conocer las diferentes opciones que ofrecen los fabricantes para hacer frente a las vulnerabilidades descubiertas.

El entorno de pruebas desarrollado pretende simular el sistema de control integrado y el sistema de control de la propulsión de un buque utilizando componentes del fabricante Siemens. Para ello, se despliega una arquitectura de red en anillo redundante utilizando componentes del fabricante Siemens. En la figura 1 se muestran los diferentes componentes y su segmentación en función del sistema. El sistema de control integrado cuenta con un PLC Simatic S7 1516 destinado al control de todos los dispositivos de la red y a ejecutar la lógica de programación establecida. Este autómata también ofrece funciones de monitorización, diagnosis del funcionamiento del sistema y bloques implementados con librerías específicas

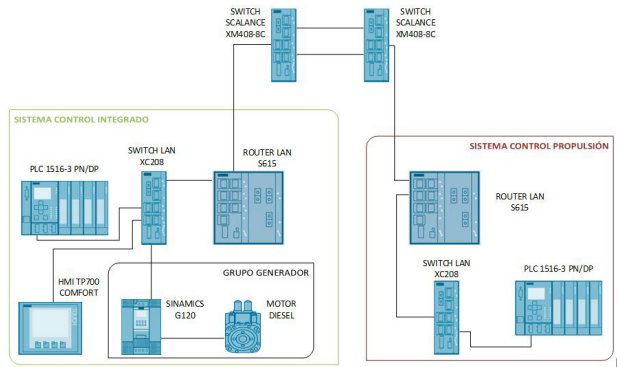


Figura 1. Arquitectura de red del entorno de pruebas del laboratorio

para su comunicación con otros controladores, en este caso, con el controlador del sistema de propulsión. Otro de los elementos de este segmento de red es el variador de frecuencia Sinamics G120 y su motor, que es controlado por el PLC y que actúa en función de las órdenes que recibe mediante un telegrama de comunicación específico. Este motor tiene la finalidad de simular el motor diésel generador de un buque.

Finalmente, el HMI TP700 Comfort presenta una interfaz de usuario para que el operario o el ingeniero puedan monitorizar el estado de los diferentes dispositivos de la infraestructura e interactuar con ellos, pudiendo activarlos y desactivarlos e incluso leer variables físicas como la potencia, la corriente o la tensión. Dispone de un menú desde el cual el operador puede acceder a diferentes pantallas de control, como puede ser la de la cámara de control de máquinas (figura 2) o la de los sistemas de apoyo a la misión.

Figura 2. Panel de control de la cámara de control de máquinas del HMI

Por otro lado, el sistema de control de la propulsión se encarga del control y monitorización de los motores de estribor y babor del buque. Estos motores son activados mediante las señales digitales del autómata del sistema de control de la propulsión, tal y como se detalla en el esquema de la figura 1 de la arquitectura de red del sistema industrial desplegado en este trabajo. Finalmente, en la siguiente figura se muestra la infraestructura completa desplegada en el laboratorio.

Figura 3. Sistema control integrado y sistema control de la propulsión desplegados en el laboratorio

3. Resultados y discusión

Se lleva a cabo una auditoría de seguridad de caja blanca asumiendo que el atacante se encuentra dentro de la red interna. La auditoría consistió en cuatro fases: fase de reconocimiento, fase de enumeración, fase de análisis de vulnerabilidades, fase de explotación y fase de elaboración de informes.

En la fase de reconocimiento se recabó información en fuentes abiertas de la infraestructura y de los sistemas. La fase de enumeración permitió disponer de información de los dispositivos y su direccionamiento en la red con los que poder estudiar sus vulnerabilidades. Se emplearon técnicas a nivel de capa dos y tres del modelo de referencia OSI (Open Systems Interconnection), demostrando que es posible interactuar con los dispositivos de la red y acceder a información de su configuración, bloques de programación o direccionamiento. Se emplearon técnicas específicas para entornos industriales y se programaron *scripts* utilizando librerías como Snap7. En la figura 4 se muestra una de las respuestas obtenidas al enumerar el PLC del sistema de control integrado.

En la fase de análisis de vulnerabilidades se utilizaron herramientas comerciales para tener una visión de las posibles vulnerabilidades que tenía el sistema de control. En el trabajo se exponen las herramientas utilizadas. Por otro lado, en la fase de explotación, con la ayuda de la información recopilada en las fases anteriores, se ejecutaron diferentes pruebas para validar la seguridad de la infraestructura.

```
┌──(root㉿kali)-[/home/kali/Python_Scripts/ICS]
└─# python Scan_Siemens_PLC.py --ip 10.20.101.2

Scanning Siemens S7 PLC ... Please wait


PLC IP: 10.20.101.2

CONNECTION STATUS(T/F): True

CATALOG:

 Basic Hardware: b'6ES7 516-3AN01-0AB0 '
 Version1: 2.2.1

CPU INFORMATION:

 Module Type: b'CPU 1516-3 PN/DP'
 Serial Number: b'S C-K7T633042018'
 Name: b'S71500/ET200MP station_1'
 Copyright: b'Original Siemens Equipment'
 Module Name: b'PLC_CONTROL_INTEGRADO'

CPU STATE: S7CpuStatusRun

COMMUNICATION PROCESSOR INFORMATION:

 Max Pdu length: 0
 Max Connecions: 0
 Max Mpi Rate: 0
 Max Bus Rate: 0

*****C0MPL3T3D*****
```

Figura 4. Información obtenida de un PLC Siemens mediante la librería Snap7

Se espiaron las comunicaciones para comprobar si existía algún método de cifrado y se verificó que todos los paquetes eran transmitidos en claro, sin ninguna protección. Mediante Scapy se pudieron diseccionar los paquetes en los que se podía identificar la información transmitida entre dispositivos. Estos paquetes fueron utilizados en otros ataques para suplantar la identidad de un dispositivo de la red o simplemente para que pasasen desapercibidos.

Otro de los ataques consistió en verificar la protección de los dispositivos ante la posibilidad de cambiar datos de proceso. Se logró modificar un bloque de datos del PLC del sistema de control integrado, consiguiendo detener el motor de babor del sistema de control de la propulsión.

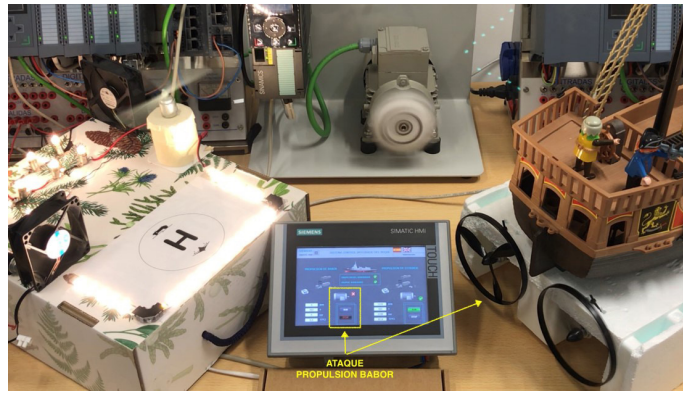


Figura 5. Pérdida de control sobre el motor de propulsión de babor

También se probó a realizar un cambio de nombre de dispositivo mediante el *crafteado* de paquetes DCP *ad hoc*. Se comprobó que se perdió la comunicación entre el PLC y el variador de frecuencia. Finalmente, se llevó a cabo un ataque para verificar como los PLC realizaban la gestión de interrupciones ante una anomalía en su funcionamiento. Para ello, se desarrolló un programa en Python para generar tráfico inusual de diferentes tipos, suplantando la identidad de alguno de los dispositivos de la red. Este tráfico consiguió aumentar el tiempo de ciclo de ejecución del PLC, ejecutándose la subrutina asociada al OB 80 encargada de manejar los errores de tiempo de ciclo.

Todas las pruebas pusieron de manifiesto las vulnerabilidades encontradas en la infraestructura y, por tanto, la necesidad de llevar a cabo una estrategia de seguridad para este tipo de sistemas.

4. Conclusiones

Como resultado de la auditoría de seguridad, se plantea una serie de medidas de seguridad teniendo en cuenta la normativa de referencia para los sistemas de control industrial y guías de ámbito nacional publicadas por el INCIBE.

Al respecto, se hace hincapié en la necesidad de conocer en profundidad la tecnología de la infraestructura, en este caso Siemens, para poder abordar soluciones de seguridad basadas en sus funciones nativas. De esta manera, se exponen soluciones específicas para el PLC Simatic S7-1500 y para el HMI TP700 Comfort.

En cuanto al PLC, se detallan medidas de tipo físicas, de protección de bloques, de nivel de acceso al PLC, de gestión de interrupciones, el uso de protocolos de comunicación seguros y su codificación segura basada en la filosofía *DevSecOps*. También se definieron medidas concretas para una conexión segura del HMI, la gestión de usuarios basada en grupos y permisos, y la creación de *logs* mediante *scripts* en Visual Basic que pudieran capturar información de interés de la interfaz.

Finalmente, se proponen posibles acciones de investigación futuras.

Referencias

Abad Barral, F. (2024). *POC Sistema Control Integrado y Sistema de Propulsión*. [Consulta: enero 2024]. Disponible en: https://youtu.be/iAbOH-LZCr4

Abad Barral, F. (2024). *POC Reconocimiento PLC Sistema Control Integrado*. [Consulta: enero 2024]. Disponible en: https://youtu.be/T6lS27RyiNI

Abad Barral, F. (2024). *POC Control de Usuarios en HMI TP700 Comfort de Siemens*. [Consulta: enero 2024]. Disponible en: https://youtu.be/zxLmgDenQZ0

Abad Barral, F. (2024). *POC Ataque motor de babor del Sistema de Propulsión*. [Consulta: enero 2024]. Disponible en: https://youtu.be/KR48Tmc-_Ys

Seguridad en Sistemas de Control Industrial Embarcados

Autor: Fernando Abad Barral
Director: José González Coma
Universidad de Vigo

Introducción

Los sistemas de control industriales (ICS) son vulnerables a ataques informáticos, y no han sido sometidos a una política de seguridad definida.

La transformación digital de la industria supone una amenaza para cualquier instalación industrial.

En este trabajo se simulan los ICS de un buque, los tipos de comunicaciones y protocolos, y la infraestructura física con dispositivos de Siemens.

Se realiza una auditoría de seguridad.

Se proponen unas medidas de seguridad basadas en el principio de defensa en profundidad para su protección durante todo el ciclo de vida.

Metodología

Configuración de dispositivos usando TIA Portal V15.1, StartDrive Advanced para variador de frecuencia Sinamics G120, y librerías especificas para las comunicaciones.

Desarrollo de un entorno de pruebas implementando el sistemas de control integrado y el sistema de control de la propulsión de un buque.

Conclusiones

La auditoría de seguridad demostró las diferentes vulnerabilidades de un sistema ICS.

Se establecen unas medidas de seguridad basadas en sus funciones nativas y en la normativa de referencia.

Agradecimientos

Al MCCE por darme la oportunidad de utilizar el laboratorio de Infraestructuras Críticas, en especial al CAP. D. Santiago Bueno Martínez.

A Marta Serrano, por tu apoyo y comprensión.

A mi hijo y mi inspiración, Pablo.

Despliegue de auditoría continua en sistemas de información en el Ministerio de Defensa

Autor: Carrasco Santiago, Rafael (rcarsan@ea.mde.es)
Director: Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – Las sociedades actuales basan su funcionamiento en la utilización de tecnologías: sistemas de información y comunicaciones que forman parte de la extensa y compleja red que interconecta Estados, administraciones, empresas, organizaciones y ciudadanos. Y todo ello a nivel mundial.

Cada vez hay un mayor número de dispositivos que acceden a recursos que están conectados a numerosas redes: desde sensores, ordenadores, sistemas, etc., llegando a la relativamente nueva internet de las cosas (IoT).

Y esta tendencia, lejos de estabilizarse, va a seguir creciendo de manera exponencial en los próximos años. La implementación de nuevos protocolos de comunicaciones que permiten identificar mediante la asignación de «nombres» a cada uno de los dispositivos va a favorecer aún más este auge.

Todo ello lleva a un alarmante aumento de la superficie de exposición y, por ende, de los riesgos y la probabilidad de sufrir ataques de la más diversa índole y con diferentes intenciones y objetivos, desde los puramente económicos hasta otros de tipo social, político, etc.

La situación que se plantea, si bien es compleja y llena de variables que afectan de manera directa a la seguridad con la que disponemos esos activos, no está exenta de otras ayudas que permitan, si bien no garantizar la utopía de la seguridad total, minimizar el impacto que un ciberataque podría tener sobre nuestros sistemas.

Conociendo nuestros sistemas –su estado, fortaleza, debilidades– podremos destinar los recursos que consideremos necesarios con el fin de reducir su superficie de exposición y las vulnerabilidades a las que están expuestos, así como mitigar los riesgos que produciría un potencial ataque.

Y esto es posible conseguirlo trabajando de una manera proactiva, analizando y corrigiendo de una forma sistemática y continua cada uno de los componentes que forman nuestros sistemas, adiestrando al personal que los administra para que obre en consecuencia, implementando cada una de las acciones que ofrezcan los resultados de una auditoría continua como parte de su trabajo cotidiano.

Palabras clave – Auditorías de seguridad CIS, Sistemas de información, Ciberseguridad, Vulnerabilidades, Ministerio de Defensa.

Los informes del estado de la ciberseguridad en España elaborados por organismos como el Instituto Nacional de Ciberseguridad (INCIBE) o el Centro Criptológico Nacional (CCN) demuestran que estamos expuestos de manera continua a ciberataques que, sin entrar en el detalle del propósito de los mismos –económicos, desinformación, exfiltración de información, etc.–, supone perder el control de nuestros activos que, en el caso del Ministerio de Defensa, podrían llegar a comprometer incluso la seguridad nacional.

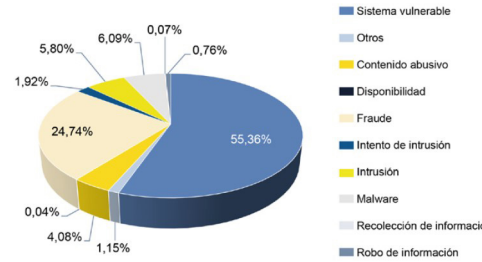


Figura 1. Porcentaje y tipología de incidentes gestionados por INCIBE-CERT en 2022

Los resultados de esos informes revelan que, un porcentaje elevado de los ataques que se reciben –más del 55 % en el año 2022, tal y como se refleja en la figura 1 del informe del INCIBE-CERT[1]– son debidos a vulnerabilidades existentes en los sistemas que soportan el manejo de la información, así como a fallos en el cumplimiento de las guías de bastionado y securización de los mismos.

Además, debe tenerse en cuenta que el nivel de peligrosidad de cada una de las vulnerabilidades que se detecte no es siempre el mismo, como puede verse en la figura 2, extraída del informe de ciberseguridad del CERT de Defensa –ESPDEF–, lo que puede permitir priorizar las acciones de corrección atendiendo a este criterio de criticidad.

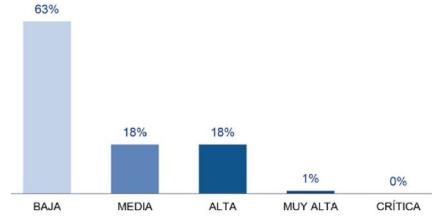


Figura 2. Peligrosidad de los incidentes gestionados por el ESPDEF-CERT en 2022

Ante esta situación, se hace evidente y se considera necesaria la implementación de herramientas que provean de la información suficiente sobre el estado de seguridad en el que se encuentra los diferentes elementos que

[1] CERT: Computer Emergency Response Team (equipo de personas dedicado a prevenir, detectar y responder de manera eficaz ante incidentes de ciberseguridad).

conforman cada uno de los sistemas que utiliza el Ministerio de Defensa, siendo este el motivo de la realización de este TFM.

En este sentido, en el TFM se presenta una serie de herramientas que están enfocadas en el análisis de las vulnerabilidades que tienen los sistemas y redes que escaneen, centrándose en una de ellas, el *software* Tenable Nessus, dado que proporciona un análisis más completo y exhaustivo. Además, esta herramienta permite la generación de diferentes tipos de informes, en los que se muestran tanto las vulnerabilidades detectadas con los escaneos como la criticidad que tienen cada una de ellas. En el trabajo se incluye igualmente un detalle de la instalación, así como de la configuración elegida para la realización de las pruebas, teniendo en cuenta que los anchos de banda en los que van a tener que ejecutarse los escaneos, pueden no tener la suficiente capacidad como para coexistir con otros servicios que estén en ejecución. Este caso podría ser el de un destacamento de las Fuerzas Armadas que opera fuera de territorio nacional y cuya capa de transporte y conectividad le viene proporcionada por un terminal satélite desplegable que, generalmente, va a proporcionar un ancho de banda reducido y que deberá ser usado por todos los sistemas que tenga desplegados, lo que va a obligar a dimensionar y establecer calidad de servicios para aquellas tareas que o bien se consideren críticas o bien se consideren prioritarias.

Figura 3. Logotipo del fabricante Tenable

Figura 4. Herramienta Nessus

Por otro lado, se analizará la solución ANA-CLARA proporcionada por el CCN, que permite comprobar el grado de cumplimiento con el que están configurados los sistemas. A la hora de instalar y configurar un sistema operativo del tipo que sea, tanto en servidores como en clientes, es necesario securizarlo y bastionarlo de la manera oportuna, siendo requisito imprescindible saber si va a estar incluido en algún sistema que va a manejar información clasificada. Para tal fin, el CCN ofrece diferentes guías de configuración segura –CCN-STIC– que, mediante *scripts* y otras directrices, permiten al administrador del sistema el establecimiento de parámetros que ajusten y afinen la instalación tanto del *software* en las máquinas como de cada uno de los elementos de *hardware* que se utilicen.

Figura 5. Logotipo de las soluciones del CCN-ANA

Figura 6. CLARA

La utilización conjunta del *software* indicado en los dos párrafos anteriores, Tenable Nessus y ANA-CLARA, proporciona una visión general del estado de ciberseguridad en el que se encuentran las TIC de la organización objeto de análisis. La generación de informes de las soluciones citadas, ofrecerá al personal responsable de la seguridad y al de la administración

de los sistemas la posibilidad de tomar las acciones conducentes a depurar los fallos mediante la actualización del *software* y *firmware* de los equipos, así como a aplicar correctamente las guías de seguridad que correspondan. Por otra parte, la dirección de la organización, a tenor de la información proporcionada por las herramientas comentadas, estará en condiciones de dimensionar y adecuar la toma de decisiones que corresponda, asignando o detrayendo recursos para mantener o aumentar la seguridad de sus sistemas.

La elección de utilización de la herramienta Tenable Nessus para el análisis de vulnerabilidades, aunque existen otras muchas opciones en el mercado, algunas de ellas incluidas en el TFM, se justifica por dos motivos principales: la enorme cantidad de *plugins* que ofrece –más de ciento treinta mil–, así como por el soporte que proporciona el fabricante de la herramienta, tanto para las actualizaciones del propio *software*, como para el desarrollo de soluciones *ad hoc* si fuera el caso. Además, en el caso del Ministerio de Defensa, en el que la instalación *on premise* se puede llegar a considerar como determinante o la única opción para la adopción de uno u otro *software* por el motivo antes citado de la existencia y manejo de información clasificada, la solución Tenable Nessus es la más válida. En este sentido, debe señalarse que para que un sistema pueda manejar información clasificada requiere de una acreditación por la autoridad correspondiente, exigiéndose como uno de los requisitos que el *software* instalado esté soportado por un fabricante.

En el caso del análisis de cumplimiento, la herramienta que se ha empleado es la que ofrece el CCN a través de la solución ANA-CLARA. La implementación de esta herramienta permite, al igual que en el caso de Tenable Nessus, una instalación *on premise* que, como se ha comentado anteriormente, se considera relevante a la hora de decidir su instalación en redes y sistemas que van a manejar información clasificada. El proceso de instalación y configuración, con las particularidades mencionadas en cuanto a anchos de banda se refiere, así como la realización de diversas pruebas de escaneo, también han sido realizadas y comentadas en la memoria del trabajo.

Una vez decididas las herramientas a implementar, se hace preciso elaborar un documento para la contratación del *software*. En el apartado de valoración económica de ambas herramientas, Tenable Nessus y ANA-CLARA, hay que diferenciar entre el *software* comercial de Tenable, que requiere de una licitación a través de acuerdos marco o publicación en el Portal de Contratos de la Administración Pública, del que se muestra una captura de la barra de navegación en la figura 3, debiendo elaborar los correspondientes pliegos de prescripciones técnicas (PPT) y pliegos de condiciones administrativas particulares (PCAP), y la de la solución ANA-CLARA, cuyo utilización es gratuita para los diferentes organismos de la Administración General del Estado.

Figura 7. Captura de pantalla de la barra de navegación de la Plataforma de Contratación del Sector Público

Con los resultados que arrojan las herramientas seleccionadas, que además vienen priorizados en función de la criticidad de las vulnerabilidades halladas, se podrán tomar las acciones oportunas conducentes a corregir las desviaciones que mitiguen los riesgos que pueda provocar el tener sistemas vulnerables o indebidamente securizados, todo ello de acuerdo con las directrices del responsable de seguridad correspondiente de cada uno de los sistemas.

Como finalización al trabajo, se establece una serie de consideraciones sobre líneas futuras de evolución de un sistema de auditoría continua, en el que, a través de cuadros de mando o *dashboards*, integren los resultados de otras herramientas y soluciones de ciberseguridad como EDR (Endpoint Detection Response), IDS (Intrusion Detection System), SIEM (Security Information and Event Management), antivirus y otras. Este aglomerado de información en una sola herramienta de gestión de información o cuadro de mando ofrecerá una visión más amplia y completa del estado de ciberseguridad de los sistemas, permitiendo controlar la evolución de los mismos a lo largo del tiempo, como puede verse en la figura 8, en la que se incluye, a modo de ejemplo, la evolución de los incidentes, su estado y el tiempo medio de resolución mensual de los mismos. Obviamente, este cuadro de mando podrá configurarse con las informaciones que ofrezcan las diferentes soluciones que implementemos en cada uno de nuestros sistemas.

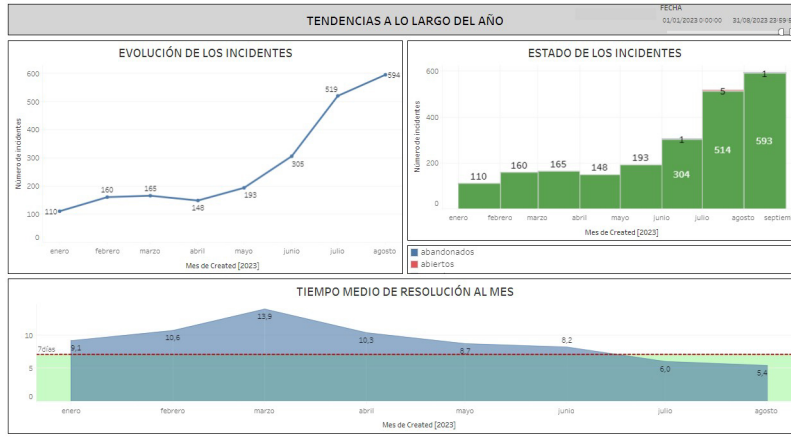


Figura 8. Tendencias de incidentes

Referencias

Balance de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE) 2022.

Guías CCN-STIC del Centro Criptológico Nacional. (Diciembre de 2023). Disponible en: https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es

Informe Anual de Seguridad Nacional 2022. Catálogo de publicaciones de la Administración General del Estado. (Diciembre de 2023). Disponible en: https://cpage.mpr.gob.es

Ley 9/2017 de 8 de noviembre de Contratos del Sector Público.

National Institute of Standards and Technology (NIST). (Diciembre de 2023). Disponible en: https://www.nist.gov/

Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Solución ANA-CLARA del CCN. Disponible en: https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/7540-ana-el-nuevo-sistema-de-auditoria-continua-del-ccn-cert [Consulta: noviembre de 2023].

Tenable Nessus. Disponible en: https://es-la.tenable.com/products/nessus [Consulta: noviembre de 2023].

Despliegue de auditoría continua en sistemas de información en el Ministerio de Defensa

Autor: Rafael Carrasco Santiago
Director: Francisco Javier Rodríguez Rodríguez

Introducción

La utilización de sistemas interconectados y que intercambian información es cada vez mayor. El uso de tecnologías que favorecen y posibilitan esas capacidades no deja de aumentar. Y el Ministerio de Defensa no es ajeno a ello, uniéndose además el hecho de que maneja información clasificada en muchos de sus sistemas.

La existencia de vulnerabilidades en los elementos que componen cada uno de esos sistemas, aumenta su superficie de exposición, posibilitando que un ciberatacante pueda lograr acceder a los mismos y a la información que albergan.

Metodología

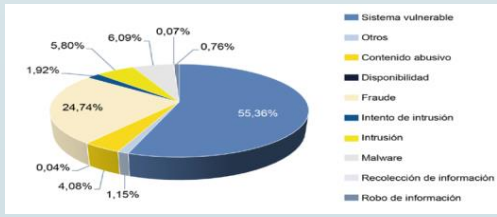
Para la realización del TFM se ha efectuado un análisis de informes de ciberseguridad de organismos como INCIBE o CCN.

Se han buscado herramientas que proporcionen información sobre el estado de seguridad de sistemas de información y que además permita su instalación como una solución *on premise*.

De las diferentes opciones de software evaluado, se ha elegido la que provee el fabricante Tenable Nessus, al considerarse la más completa y la que ofrece resultados e informes más válidos para el escaneo de vulnerabilidades.

Se proporciona igualmente información tanto de su uso e instalación, como de su valoración económica para iniciar un posible proceso de adquisición en la Administración Pública.

Respecto al análisis de cumplimiento, la herramienta analizada es la que ofrece el Centro Criptológico Nacional: ANA-CLARA, de uso gratuito para la Administración.



Resultados

La herramienta Tenable Nessus y las soluciones ANA y CLARA del Centro Criptológico Nacional, han facilitado la información necesaria del estado de los sistemas en los que se han ejecutado, obteniéndose una imagen fiel de la ciberseguridad de los mismos.

Conclusiones

Se determina que la necesidad de disponer de un sistema de herramientas que provea de información sobre estado de seguridad de nuestros sistemas no debe ser una opción. Se requiere de un análisis continuo de las vulnerabilidades y las brechas de seguridad de cada uno de los componentes hardware y software que conforman nuestros sistemas, permitiendo reducir la superficie de exposición y asignar los recursos necesarios para corregir las deficiencias que se obtengan con los análisis de auditoría continua.

Agradecimientos

A mis compañeros del Grupo de Auditorías del Mando Conjunto del Ciberespacio

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Irrupción de la inteligencia artificial en el Ministerio de Defensa, primeros casos de uso

Autor: Cuartero Lorenzo, Francisco (fcuarterol@fn.mde.es)
Directores: Fernández García, Norberto y Fernández Gavilanes, Milagros
(norberto@cud.uvigo.es / mfgavilanes@cud.uvigo.es)

Resumen – La inteligencia artificial es considerada la más transcendente de las tecnologías emergentes. En el campo militar, está siendo contemplada en todas las estrategias de defensa de nuestro siglo, llegando a manifestarse que la geopolítica estará marcada por los países que consigan dominarla. La evolución del escenario estratégico militar está sustituyendo el concepto clásico de operaciones conjuntas por el de operaciones multidominio. Este tipo de operaciones estará caracterizado por una masiva sensorización del campo de batalla y un volumen de información desbordante que superará las capacidades humanas de gestión. El Ministerio de Defensa de España, al igual que otras potencias militares y las organizaciones internacionales de seguridad y defensa consideran que las aplicaciones de la inteligencia artificial podrían suponer la clave de la superioridad en el combate y de la interoperabilidad y, a su vez, una oportunidad para establecer una brecha tecnológica frente a los posibles adversarios.

La transversalidad de la inteligencia artificial hace que su aplicabilidad alcance todo el espectro de actividades que se realizan en la sociedad en general y en las Fuerzas Armadas en particular. Este trabajo, guiado por la Estrategia de desarrollo, implantación y uso de la inteligencia artificial en el Ministerio de Defensa, de la Secretaria de Estado de Defensa, pretende hacer un recorrido por la aplicabilidad de esta tecnología en los casos de uso concretos documentados en el Ministerio de Defensa, así como otros que se estiman aplicables. Los casos de uso se presentan agrupados en las categorías reflejadas en dicha Estrategia, según el area de actividad en que repercutirán incluyendo tanto la operativa, como la administrativa o de apoyo.

Palabras clave – Inteligencia artificial, Multidominio, Defensa, Innovación, Aprendizaje automático.

1. Introducción

La última *Estrategia de Seguridad Nacional de 2021* es el documento que pretende configurar el marco político estratégico de la Política de Seguridad Nacional. Este documento incluye numerosas referencias a la inteligencia artificial entre las que destacan:

En el capítulo 3 dedicado a los «Riesgos y Amenazas» se lee:

> La superficie de confrontación geopolítica encuentra áreas de intersección con la tecnología y la economía, dibujando así un mapa de riesgos más complejos y muy interrelacionados. Adicionalmente, amenazas derivadas del uso de tecnologías de nueva generación, como la Inteligencia Artificial o el acceso al espacio ultraterrestre, añaden complejidad y dificultan la protección de los derechos individuales ante un eventual uso malicioso.

En el capítulo cuatro, titulado «Planeamiento Estratégico Integrado», se menciona el uso a favor: «[...] En particular es necesario tomar conciencia del potencial estratégico de la Inteligencia Artificial y la importancia de esta tecnología como puntal de la Seguridad Nacional». Ese potencial señalado en 2021 ya empieza a ser tangible en 2023.

El jefe del Estado Mayor de la Defensa tiene la tarea de definir el marco estratégico militar y en su doctrina recoge que: «Las Fuerzas Armadas tienen que acceder a las nuevas tecnologías emergentes y disruptivas, como la Inteligencia Artificial, cuyo desarrollo puede suponer la clave de la superioridad en el combate y de la interoperabilidad». Queda por tanto demostrado el interés que la inteligencia artificial ha despertado en el contexto de la seguridad y defensa en general y del Ministerio de Defensa de España en particular. Este trabajo pretende elaborar una recopilación ordenada de las iniciativas emprendidas para su incorporación transversal a múltiples áreas de actividad, desde lo puramente administrativo hasta sus aplicaciones en el campo de batalla.

El autor, como oficial de Estado Mayor destinado en el Área de Planes y Políticas de la Dirección General CESTIC, es conocedor de las expectativas y ambiciones que ha despertado en el Ministerio de Defensa la que ha denominado «irrupción de la inteligencia artificial» y espera que este trabajo ofrezca una visión global sobre su aplicabilidad en este entorno.

2. Desarrollo del TFM

La parte de desarrollo del trabajo se estructura en tres capítulos:

- Capítulo 2. Estado del arte, que profundiza en los posibles usos de la inteligencia artificial en aplicaciones militares.
- Capítulo 3. Dedicado a los casos de uso específicos identificados, agrupados según las categorías señaladas en la Estrategia de desa-

rrollo, implantación y uso de la inteligencia artificial en el Ministerio de Defensa.

— Capítulo 4. En este se recogen las conclusiones del trabajo y se plantean posibles líneas futuras de actuación para el Ministerio de Defensa.

2.1 Inteligencia artificial y era digital

El uso militar de la IA plantea interrogantes específicos. Uno de estos interrogantes son los posibles conflictos éticos que el uso de esta tecnología pueda conllevar, pero no es el único. Existen otros de gran importancia, como el origen de los datos, la mitigación del sesgo, el alcance de los algoritmos y su entrenamiento, por citar algunos. El Ministerio de Defensa ha elaborado una Estrategia para guiar la integración de esta tecnología. Publicada en 2023, dicha Estrategia tiene por finalidad establecer la base para el desarrollo, implantación y uso de soluciones de inteligencia artificial en el Ministerio de Defensa, que permitan incrementar la eficacia en las misiones y cometidos del departamento.

Por su parte, la Organización del Tratado del Atlántico Norte (OTAN) ha reconocido a la IA como una de las EDT que pueden potenciar las capacidades de la Alianza y apoyar el desarrollo de sus misiones. En ese orden de cosas, en octubre de 2021, los ministros de Defensa de la OTAN aprobaron la *Estrategia de la Alianza en esta materia (NATO's Artificial Intelligence Strategy)*.

2.2 ¿Cuál va a ser el «futuro» cercano del campo de batalla?

Desde el punto de vista militar, es importante visualizar las características del espacio de batalla futuro y el papel que jugará la IA. Volviendo al mencionado documento de la OTAN, el *Science & Technology Trends 2023-2043* establece que el concepto I2D2 (inteligente, interconectado, descentralizado y digital) seguirá vigente las próximas décadas (figura 1) y definirá el avance de las tecnologías militares. Las tecnologías militares existentes se fusionarán con las EDT para crear nuevas formas y medios de participar en los conflictos.

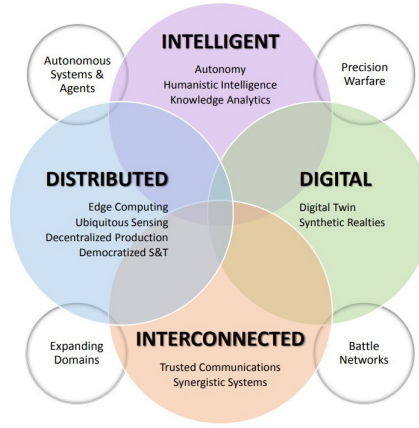


Figura 1. Concepto I2D2. Fuente: STO Tech Trends Report NATO

2.3 Referencias en el entorno del Ministerio de Defensa

Se ha estudiado el entorno del MDEF, con atención especial a las siguientes referencias:

- La *Agenda España Digital 2025/2026*.
- La *Estrategia Nacional de Inteligencia Artificial ENIA*.
- La *NATO's Artificial Intelligence Strategy*.
- El *Libro Blanco sobre la IA de la Unión Europea*.
- El *Reglamento de IA de la Unión Europea* (borrador).

Y también se han estudiado las estrategias de IA militares publicadas por el Departamento de Defensa de los Estados Unidos, por el Ministerio de Defensa del Reino unido y la estrategia estatal de IA de China.

A continuación se han descrito los puntos más importantes de la Estrategia de desarrollo, implantación y uso de la IA, publicada en julio de 2023 por la Secretaría de Estado de Defensa en el marco de la Transformación Digital del departamento, analizando su oportunidad y contenido.

Por su actualidad, se incluye un apartado relativo a la influencia que está teniendo la IA en el conflicto entre Ucrania y Rusia.

2.4 Categorías y clasificación de la IA y definiciones

Con vistas a poder clasificar las diferentes técnicas de IA disponibles se ha añadido un apartado de clasificación y definiciones, tomando como base las mostradas en la figura 2.

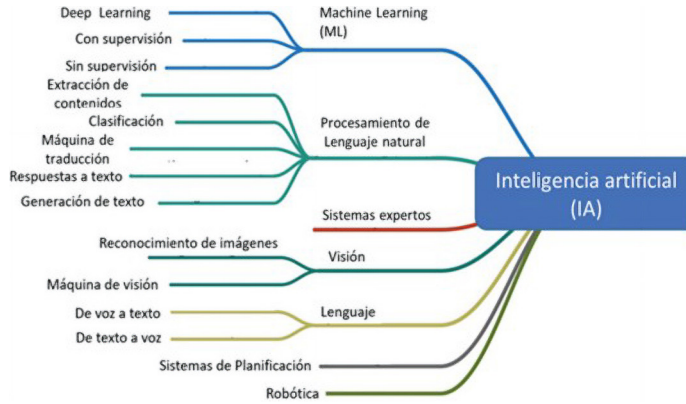


Figura 2. Tecnologías usadas en sistemas de IA. Fuente: IEEE

3. Casos de uso militar de IA

Para estudiar los casos de uso potenciales o en desarrollo en el MDEF, se tomará como referencia los recogidos en el apartado undécimo de la estrategia de 2023. Son los recogidos en la tabla 1.

Estrategia MDEF	NATO's Artificial Intelligence Strategy
Movilidad militar	Military Mobility Capability
Inteligencia	Intelligence
Guerra electrónica	-
Autonomía en sistemas no tripulados	-
Apoyo logístico y alistamiento operativo	Logistics Support & Operational Readiness
Conocimiento y vigilancia del entorno	Information Environment Assessment
Ciberdefensa	Cyber Defence and influence
Apoyo a la toma de decisiones	Assisted Decision-Making
Análisis geoespacial, meteorológico y oceanográfico	AI for climate analysis
Gestión de la información y CIS/TIC	-
Talento y formación	-

Tabla 1. Categorías de casos de uso militar de la IA ESP-OTAN

A continuación se analizan diversos casos de uso en producción o desarrollo en el MDEF o en otras organizaciones, entre los que se destacan a modo de ejemplo los siguientes por su madurez o por su nivel de innovación:

Proyecto ARCO. Aplicación robótica de un convoy operativo: este proyecto tiene como objetivo lograr el control a distancia del primer vehículo de un convoy militar en zona de operaciones para reducir riesgos de IED u otras amenazas. Se pretendía hacer un demostrador funcional capaz de operar en entornos de operaciones militares, y de superar situaciones de GNSS denegado o con comunicaciones degradadas.

Proyecto de reconocimiento de imágenes y asistencia a reacciones tácticas: desde el Centro de IA de la Armada (CIA 2) se está trabajando en el SEDA II, proyecto que incorpora IA para el procesado de imágenes procedentes de diferentes sistemas optrónicos. Se lleva a cabo en colaboración con NAVANTIA (SEPI), en el marco de los proyectos QuickWin de IA para el desarrollo de un modelo cuya implementación permitiría a los sistemas de vigilancia optrónicos (SVO) la detección y clasificación de unidades de superficie, aeronaves y misiles.

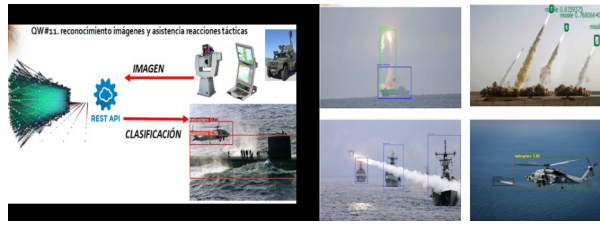


Figura 3. Proyecto SEDA. Fuente: CIA2

Mantenimiento predictivo en la Armada: según recoge la *Revista General de Marina,* «Tras el establecimiento del CESADAR en 2011 como Centro de Supervisión y Análisis de Datos de la Armada, se han

sucedido diversos hitos en la evolución de sus capacidades. Durante los primeros años, la capacidad de análisis de datos en el centro fue muy limitada y se basaba en análisis visual de variables». Y en 2017, «[...] se reafirmó la necesidad de ser capaces de aplicar modelos de IA sobre nuestros datos y adaptar la capacidad de análisis a las nuevas tecnologías y modelos inteligentes. La IA cobraba más importancia y era un objetivo prioritario como capacidad para ser adquirida».

La Armada no ha dejado de invertir personal y recursos para avanzar en esta línea. Ya iniciada la segunda década del siglo, el sistema SOPRENE está totalmente incorporado a la actividad de buques y arsenales de apoyo. Está constituido por varias herramientas específicas en función del usuario, localización y misión. Actualmente y en formato de demostrador tecnológico, la evolución a MAPRE (Mantenimiento Predictivo) busca la predicción y clasificación de anomalías. MAPRE incorpora técnicas de IA, es entrenado en tierra y ejecutado a bordo.

4. Conclusiones

4.1. Sobre la aplicabilidad de la IA

La IA no es una tecnología más, su relevancia geopolítica hace que vaya apareciendo en la agenda de todos los Estados y organizaciones internacionales de seguridad y defensa. Especialmente en el campo de lo militar, está llamada a ser la tecnología que ofrezca mayor desarrollo tanto para hacer uso de ella a favor como para negarle su uso al adversario.

La guerra de Ucrania ha demostrado que las aplicaciones de IA son útiles en situaciones de combate abierto. Estas aplicaciones de vertiginoso desarrollo han contribuido a equilibrar un conflicto inicialmente muy desigual entre los contendientes.

El Ministerio de Defensa de España mantiene visibilidad sobre iniciativas relacionadas con la IA en la Administración General del Estado, de donde obtiene aprendizaje y recursos. También permanece atento a las iniciativas de las organizaciones de seguridad y defensa OTAN, y de la UE. España participa activamente en los foros OTAN para buscar la coherencia y la cooperación con los aliados en esta materia con beneficio mutuo.

Los posibles conflictos éticos que acompañan a esta tecnología no deben ser, en el estado de madurez que nos encontramos, la principal preocupación para su empleo militar. Todavía estamos lejos de disponer de SALAS (Sistemas de Armas Letales Autónomos). De momento, lo recomendable es seguir avanzando en el conocimiento de la tecnología y participar en los foros donde se desarrolla la normativa. En la gran mayoría de aplicaciones que se han estudiado y las presumibles en los próximos años, la principal preocupación será asegurar, eso sí, que las aplicaciones respetan los derechos individuales de las personas, en cuanto a privacidad, imagen,

honorabilidad y, en general, todo los relacionados con la protección de datos personales.

4.2 Sobre la Estrategia de IA del MDEF

Estamos a tiempo de subirnos al tren de la IA. La Estrategia de IA del MDEF es una base normativa útil e indispensable para iniciar un desarrollo coordinado de aplicaciones de IA en el departamento y no caer en una dispersión de recursos, siempre escasos, y conocimiento.

Los Ámbitos del MDEF, coordinados desde la Secretaría de Estado por la DG CESTIC y por la DGAM, están diseñando e implantando soluciones concretas que dan respuesta a necesidades del MDEF, empleando IA de acuerdo con los principios de uso responsable recogidos en la Estrategia.

La DG CESTIC está preparando la I3D (Infraestructura Integral de Información para la Defensa), para poder soportar la demanda que traerán consigo las aplicaciones de IA. Al mismo tiempo, todo el MDEF avanza en la necesaria gobernanza del dato, cuestión en la que está poniendo especial énfasis el CIO del MDEF, sin la cual no se podrá aprovechar toda la potencialidad de la IA. No tendremos datos para entrenar los modelos.

El MDEF tiene una capacidad de innovación limitada, en el campo de las TIC y en todos los demás que cada vez tienen más componente digital. Es totalmente necesario apoyarse en el tejido industrial y en la universidad para emprender proyectos de IA con una cierta viabilidad. Experiencias como la del programa Coincidente muestran el camino, el uso dual de la IA es evidente.

4.3 Sobre los casos de uso de IA

En los últimos años se ha escrito mucho sobre IA y su aplicabilidad militar, pero la gran mayoría de las veces en genérico. Se considera recomendable comenzar a tratar cada una de las técnicas por separado, pues existen diferentes técnicas que se van ramificando conforme avanza la ciencia. El MDEF necesitará expertos en *machine learning*, en redes neuronales o en visión artificial y es imposible dominar todos los campos.

	Categoría caso de uso	Madurez	Potencial
1	Movilidad militar	Inicial	Medio
2	Inteligencia	Medio	Alto
3	Guerra electrónica	Inicial	Alto
4	Autonomía en sistemas no tripulados	Inicial	Alto
5	Apoyo logístico y alistamiento operativo	Avanzado	Alto
6	Conocimiento y vigilancia del entorno	Inicial	Alto
7	Ciberdefensa	Avanzado	Muy alto
8	Apoyo a la toma de decisiones	Inicial	Muy alto
9	Análisis geoespacial, meteorológico y oceanográfico	Medio	Medio

	Categoría caso de uso	Madurez	Potencial
10	Gestión de la información y CIS/TIC	Inicial	Alto
11	Talento y formación	Inicial	Medio

Nota: entre las once categorías de casos de uso señaladas en la Estrategia se han observado diferentes grados de desarrollo de los proyectos asociados a cada una de ellas. La tabla refleja, a juicio del autor, la madurez alcanzada y el potencial de empleo de la IA que se estima en cada categoría en función del conocimiento de iniciativas en otros estados y organizaciones.

Tabla 2. Valoración categorías IA

Los resultados obtenidos en las aplicaciones de ML y DL para apoyar la función logística y el alistamiento operativo deben servir de guía para el resto de aplicaciones. Estos desarrollos han demostrado que, aunque el camino es largo, los resultados obtenidos producen un aumento significativo de las capacidades y un mejor empleo de los recursos disponibles.

En el caso de las herramientas de ciberdefensa, podríamos decir que el empleo de la IA es irrenunciable en un entorno donde las capacidades humanas se ven claramente superadas por la velocidad de los acontecimientos y el volumen de información a analizar.

4.4 Líneas futuras

Se recomienda que el MDEF persevere en el desarrollo de la Estrategia iniciada en 2023, fortaleciendo sus infraestructuras y promoviendo el gobierno del dato en todo el departamento para permitir el entrenamiento de los modelos de IA.

El MDEF debe adquirir conocimiento experto en IA y fomentar la creación prevista de la Red de Centros de Referencia para el seguimiento técnico de proyectos de IA, la compartición de resultados de estos proyectos y el establecimiento de entornos de experimentación.

Se considera urgente comenzar a desarrollar herramientas de apoyo a la toma de decisión, especialmente en el planeamiento operativo, donde se estima un altísimo potencial.

El proyecto de Gemelo Digital para la F-110 merece ser seguido con atención por su potencial. Nuestro primer gemelo digital representa un ambicioso proyecto extrapolable a otras plataformas terrestres o aéreas.

Respecto a los proyectos piloto y demostradores tecnológicos que se han considerado viables en su fase inicial, es muy conveniente convertirlos en proyectos o programas con financiación propia, pues en caso contrario no se conseguirá dar el salto a producción que justifique el esfuerzo investigador realizado.

La colaboración con universidad y empresas del sector es imprescindible para alcanzar los objetivos planteados en materia de IA, por lo que deberán mantenerse y reforzarse los acuerdos y convenios asumidos por el MDEF para impulsar la aplicación de esta tecnología.

Referencias

Blank, S. (2020). Teaching Technology, Innovation, and Modern War at Stanford, Part 5: Autonomy and Defense in the Twenty-first Century.

Caride, V. M. (2023). Reflexiones sobre el nuevo entorno operacional multidominio. *Revista Ejército,* n.º 987.

Departamento de Seguridad Nacional. (2021). *Estrategia de Seguridad Nacional 2021.*

DGAM. Estrategia de tecnología e innovación para la Defensa. ETID 2020.

Estado Mayor de la Defensa. (2021). Concepto de empleo de las Fuerzas Armadas 2021.

Gobierno de España. (2022). *España digital 2026.*

León, G. (2023). El papel dual de la inteligencia artificial en una era de conflictos híbridos.

Ministerio de Asuntos Económicos y Transformación Digital. (2020). *Estrategia Nacional de Inteligencia Artificial (ENIA).*

Ministerio de Defensa. (2015, 3 diciembre). Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

Ministerio de Defensa. (2023, 6 julio). Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el MDEF.

NATO. (2019). NATO's Artificial Intelligence Strategy.

NATO. (2023). Science & Technology Trends.

NATO Science & Technology Organizatión. (2020). Science & Technology Trends.

Pedreño, A y Moreno, L. (2020). Europa frente a EEUU y China. Prevenir el declive en la era de la Inteligencia Artificial.

Unión Europea. (2020). Libro Blanco sobre la Inteligencia Artificial.

US Department of Defense. (2018). Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity.

Irrupción de la Inteligencia Artificial en el Ministerio de Defensa, primeros casos de uso.

Autor: Francisco, Quartero, Lorenzo

Director/es: Norberto Fernández García y Milagros Fernández Gavilanes

Universidad de Vigo

Introducción

La IA es considerada la más transcendente de las tecnologías emergentes. En el campo militar está siendo contemplada en todas las estrategias de defensa de nuestro siglo llegando a manifestarse que la geopolítica estará marcada por los países que consigan dominarla. El Ministerio de Defensa de España considera que las aplicaciones de la Inteligencia Artificial podrían suponer la clave de la superioridad en el combate y de la interoperabilidad y, a su vez, una oportunidad para establecer una brecha tecnológica frente a los posibles adversarios. Este trabajo pretende hacer un recorrido por la aplicabilidad de esta tecnología en los casos de uso concretos documentados en el MDEF.

Metodología

Este trabajo seguirá una metodología cualitativa basada en la revisión bibliográfica. Se han analizado los documentos relevantes sobre la materia publicados por instituciones académicas de primer nivel y fuentes oficiales del Ministerio de Defensa.

Para recopilar información sobre casos de uso concretos, actualmente en desarrollo, el autor recurrió a las fuentes primarias responsables de proyectos que incluyen Inteligencia Artificial en el Ministerio de Defensa y su entorno.

El estudio se complementa con documentación procedente de las Organizaciones Internacionales de Seguridad y Defensa (OTAN y UE), y de otras fuentes militares internacionales publicadas por potencias extranjeras relevantes en el ámbito militar y de la seguridad.

Resultados

Añada su información, imágenes, y gráficos en esta sección

Categoría caso de uso	Madurez
Movilidad militar	Inicial
Inteligencia	Medio
Guerra electrónica	Inicial
Autonomía	Inicial
Apoyo logístico	Avanzado
Conocimiento del entorno	Inicial
Ciberdefensa	Avanzado
Apoyo a la toma de decisiones	Inicial
Análisis meteorológico	Medio
Gestión CIS/TIC	Inicial
Talento y formación	Inicial

Conclusiones

Estamos a tiempo de subirnos al tren de la IA, la Estrategia de IA del MDEF es una base normativa útil e indispensable para iniciar un desarrollo coordinado de aplicaciones de IA en el Departamento y no caer en una dispersión de recursos, siempre escasos, y conocimiento.

Los Ámbitos del MDEF, coordinados desde la Secretaría de Estado por la DG CESTIC y por la DGAM, están diseñando e implantando soluciones concretas que dan respuesta a necesidades del MDEF empleando IA de acuerdo a los principios de uso responsable recogidos en la Estrategia. Claramente esto es solo el principio, llegar a tener una red de centros de excelencia y cubrir todos los casos de uso señalados y los nuevos que surjan, ha de ser una ambición del MDEF que además contribuya al crecimiento de la industria nacional del sector tecnológico.

Agradecimientos

A los tutores de este trabajo, Norberto Fernández García y Milagros Fernández Gavilanes por su apoyo durante la elaboración de este TFM.

Perturbación de GPS en cazaminas clase Segura

Autor: Fernández de León, Miguel Rafael (mferleo@fn.mde.es)
Directores: Núñez Ortuño, José María y Troncoso Pastoriza, Francisco Manuel (jnunez@cud.uvigo.es / ftroncoso@cud.uvigo.es)

Resumen – El TFM se enfoca en los buques de guerra clase Segura de la Armada española, dedicados a la detección, identificación y neutralización de minas marinas. Estos buques son clave para la seguridad marítima, operando cerca de costas, puertos, zonas de pesca y canales angostos, donde las minas marinas son un riesgo significativo. Es crucial que mantengan una posición precisa, especialmente en zonas con riesgo de minas o de poca profundidad.

Se abordan aspectos relevantes de los sistemas de posicionamiento global (GPS) en estos buques, analizando en detalle los equipos GPS y los ataques de perturbación GPS más comunes que afectan su funcionamiento. Se analizan ejercicios de perturbación de GPS realizados en estos buques para entender mejor los riesgos y vulnerabilidades asociados a las perturbaciones en los sistemas GPS.

Un aspecto crucial es la investigación de métodos para mitigar interferencias en el GPS con la tecnología actual. En caso de que el GPS haya sido degradado, se estudian técnicas existentes y se exploran alternativas para que los buques mantengan su posición y continúen con operaciones de medidas contra minas.

Finalmente se busca responder a una pregunta esencial: ¿es posible continuar con las operaciones de medidas contra minas tras un ataque de perturbación del GPS usando la tecnología actual? La respuesta a esta pregunta es crucial, ya que una interrupción en la navegación y operación de estos buques en zonas minadas podría tener consecuencias desastrosas, tanto táctica como operativamente. En este sentido, se evalúa la viabilidad de seguir con estas misiones críticas o, si fuera necesario, retirarse de la zona minada de forma segura.

Palabras clave – GPS, Perturbación, Cazaminas, Operaciones, Tecnología.

1. Introducción

Los cazaminas de la clase Segura (figura 1) pertenecientes a la Armada española, que incluyen al Segura, Sella, Tambre, Turia, Duero y Tajo, son buques específicamente diseñados y construidos con características únicas que les permiten operar eficientemente en áreas de poca profundidad y muy cercanas a la costa. Esta particularidad en su diseño los hace idóneos para tareas en estas zonas específicas.

La misión principal de estos cazaminas, como se detalla en la Instrucción Permanente de Organización de la Flota, IPO FLOTA 0327/201 es: «Prepararse y llevar a cabo misiones relacionadas con la libertad de acción en el ámbito de la Guerra de minas y en cualquier área geográfica, incluyendo teatros litorales y escenarios costeros alejados del territorio nacional integrado en una Fuerza Naval y contribuir, en su caso, al resto de capacidades de la Fuerza de Acción Marítima».

Figura 1. Cazaminas clase Segura

Basado en la definición de la misión propuesta, resulta claro que es esencial para este tipo de plataformas tener un conocimiento constante y preciso de su posición. Esta necesidad se debe a los riesgos inherentes de navegar en áreas cercanas a la costa, donde la profundidad del agua es limitada. Los riesgos se magnifican significativamente en el caso de que estas áreas también estén afectadas por la presencia de minas.

Por lo tanto, la capacidad de determinar la posición exacta en todo momento es crucial para la operación segura y efectiva de la plataforma, especialmente en entornos potencialmente peligrosos o comprometidos. La precisión en la localización no es solo una cuestión de navegación eficiente, sino una medida crítica de seguridad, considerando los desafíos adicionales que presentan las zonas minadas.

Con el auge reciente de ataques a sistemas de posicionamiento global (GPS), que cada vez son más avanzados y precisos, los modelos de GPS que se llevan a bordo de los cazaminas y la necesidad de conocer perfectamente la posición para realizar las misiones de estos buques. En este contexto, surge la pregunta: ¿es posible, con la ayuda de la tecnología actual, continuar los cazaminas con operaciones de medidas contra minas,

en el teatro de operaciones ante un ataque de perturbación de GPS o deben abandonar la zona de operaciones y cancelar la misión?

2. Desarrollo

2.1 Operaciones de los cazaminas

Para entrar en contexto, es necesario conocer el tipo de misiones que realizan los cazaminas, en las que se observa la importancia de conocer la posición GPS en todo momento.

- Operaciones de Medidas Contra Minas (MCM): incluyen el reconocimiento, exploración y limpieza de minas en zonas minadas para proteger territorios o impedir el movimiento del enemigo. Se suelen utilizar dos tipos de minas: de fondo y de orinque; ambas se fondean en zonas de poca profundidad. Estas operaciones son críticas y requieren una precisión en la posición del cazaminas extrema.

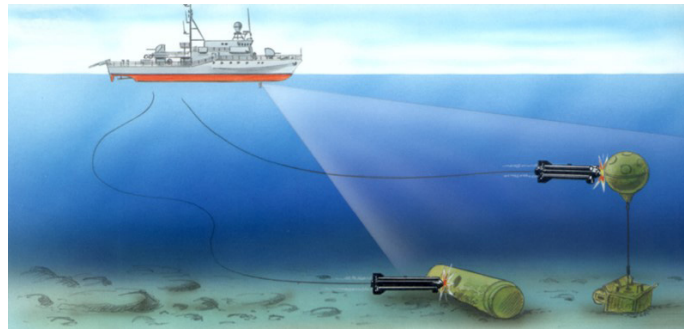


Figura 2. Operaciones MCM

- Operaciones de vigilancia de rutas (*route survey*): consisten en la vigilancia y protección marítima, especialmente en áreas de acceso a puertos. Incluyen el sondeo submarino y la recopilación de información medioambiental, siendo esenciales para la seguridad de las zonas portuarias.
- Operaciones anfibias: apoyan a las fuerzas anfibias en desembarcos militares, realizando el reconocimiento del fondo marino para identificar áreas óptimas para el desembarco.
- Otras operaciones: incluyen ejercicios nacionales e internacionales, participación en agrupaciones internacionales, presencia naval y colaboraciones con organismos civiles.

2.2 Tipos de GPS en cazaminas

Se describen los sistemas GPS de los cazaminas con detalles sobre su precisión, tecnología, durabilidad, funcionalidades, facilidad de uso y soporte. Se realiza una comparativa de estos sistemas, destacando que cada uno tiene aplicaciones específicas y ventajas únicas.

2.3 Tipos de perturbación GPS

Los tipos de perturbación se dividen en interferencias intencionadas, destacando técnicas como el *jamming* y el *spoofing,* y en interferencias no intencionadas, que serán mencionadas brevemente por su relevancia informativa.

- *Jamming* (obstrucción): consiste en la obstrucción deliberada de las señales GPS mediante señales de radiofrecuencia. Los *jammers* varían en potencia y pueden ser utilizados con fines ilícitos, como evitar el seguimiento o perturbar operaciones militares.
- *Spoofing* (suplantación): envía señales falsas a los receptores GPS, engañándolos sobre su ubicación real. Es particularmente peligroso, ya que puede causar errores de navegación sin que el usuario se dé cuenta.
- Otras perturbaciones: incluyen reflexión de señales (*multipath*), obstrucciones atmosféricas y problemas con la constelación de satélites. Todas ellas se tratan de interferencias no intencionadas.

2.4 Riesgos de perturbar el GPS

Se enfatizan los riesgos de la navegación con un GPS degradado, las dificultades en las operaciones MCM, problemas de coordinación con otros buques y desafíos en la navegación bajo condiciones meteorológicas adversas cuando el GPS es perturbado.

2.5 Medidas para mitigar ataques al GPS

A continuación se describen diferentes medidas y técnicas para mitigar los ataques de perturbación al GPS. En caso de que estas medidas fueran efectivas en los cazaminas, significaría que el GPS no estaría afectado ante un ataque de GPS y los cazaminas podrían continuar con las operaciones MCM.

- Antenas *antijamming*: se destaca la importancia de las antenas *antijamming* que utilizan tecnologías avanzadas como la formación de haces digitales y la información TLE de NORAD para combatir las interferencias. La antena GAJT-710ML (figura 3) es un ejemplo práctico que demuestra cómo estas tecnologías pueden integrarse en los sistemas existentes de los cazaminas para mejorar la resistencia frente a *jamming* y *spoofing*. La selectividad espacial y la inmunidad al ruido mejorada son aspectos clave de estas antenas.

Figura 3. Antena antijamming

- Detección y filtrado de señales: existen en desarrollo algoritmos avanzados para detectar y filtrar señales interferentes. Utilizando técnicas de procesamiento de señales y análisis espectral, junto con el aprendizaje automático, estos algoritmos pueden identificar eficazmente las señales anómalas y proteger los sistemas GPS. La implementación de estos algoritmos permitiría una evaluación continua de la autenticidad de las señales GPS, mejorando significativamente la seguridad y confiabilidad del sistema de navegación.
- Protección de GPS mediante redes neuronales: la introducción de redes neuronales, como la NARX NN, en el campo de la navegación GPS ofrece una vía prometedora para mitigar los efectos del *spoofing*. Estas redes son capaces de aprender y adaptarse a patrones de señales, lo que les permite identificar desviaciones de las normas y responder en consecuencia. Su eficacia en la mitigación de ataques de *spoofing* es notable, y su aplicación podría revolucionar la seguridad del GPS en operaciones críticas.
- Criptografía: se explora la posibilidad de implementar la criptografía en las señales GPS para protegerlas contra ataques de *spoofing*. La criptografía simétrica y asimétrica ofrece diferentes ventajas y desafíos. La simétrica proporciona una fuerte resistencia a los ataques, pero presenta dificultades en la distribución de claves. Por otro lado, la criptografía asimétrica facilita la distribución de claves, pero requiere más recursos computacionales. Ambas técnicas proporcionan un nivel adicional de seguridad para las señales GPS.
- Redundancia y diversidad de señales: esta estrategia implica el uso de varios sistemas de navegación satelital para proporcionar redundancia. En caso de interferencia en un sistema, el dispositivo puede cambiar a otro, asegurando la continuidad y precisión de la navegación. Esta diversificación aporta una seguridad adicional contra fallos o interferencias en cualquier sistema individual.

2.6 Medidas para mantener operaciones MCM

En caso de que no sea posible mitigar los ataques a los GPS de los cazaminas y estos queden degradados, es fundamental buscar una alternativa para intentar mantener la posición y poder continuar con las operaciones MCM, utilizando la tecnología actual.

- Sistemas de navegación inercial: son una opción viable cuando el GPS falla, proporcionando datos de navegación independientes. Aunque su precisión disminuye con el tiempo, son útiles para maniobras a corto plazo, como la evacuación segura de una zona minada, pero no para continuar realizando operaciones MCM.
- Sistema eLoran: se presenta como una alternativa robusta al GPS, especialmente eficaz contra interferencias. Aunque su precisión no es tan alta como la del GPS, su robustez y fiabilidad lo hacen

valioso para la navegación en situaciones críticas. Las señales de radio de baja frecuencia de eLoran ofrecen una cobertura efectiva y son menos susceptibles a interferencias, lo que lo convierte en una opción segura para la navegación y sincronización de tiempo en situaciones donde la integridad de la señal es crucial. Sin embargo, su precisión en decenas de metros puede no ser suficiente para realizar operaciones MCM.

— Triangulación 5G: la posibilidad de usar la tecnología 5G para la localización precisa de buques representa un avance significativo. La capacidad de las antenas MIMO para una orientación precisa de la señal, combinada con la alta capacidad de transmisión de datos y baja latencia de 5G, ofrece un potencial considerable para la localización en el mar. Sin embargo, los desafíos de cobertura y penetración de la señal en entornos marítimos, junto con el alto costo y complejidad técnica de implementar redes 5G a gran escala, representan obstáculos significativos para utilizar esta técnica para mantener la posición y continuar con operaciones MCM.

3. Conclusiones

Ante la creciente amenaza de ataques de perturbación GPS y las limitaciones que ofrecen ante un ataque de perturbación, los GPS de los cazaminas, como se ha visto a lo largo del trabajo, es imperativo que se realicen esfuerzos para modernizar y mitigar estos posibles ataques para salvaguardar la integridad y disponibilidad de los sistemas GPS que son de vital importancia. Esta modernización incluye las técnicas descritas en apartados anteriores, como adopción de protocolos de encriptación, antenas *antijamming*, detección y filtrado de señales, protección de GPS mediante redes neuronales o redundancia de señales. Todas ellas son medidas aplicables, excepto probablemente, las antenas *antijamming* por su elevado coste.

En relación con la hipótesis de este estudio –¿es posible, con la ayuda de la tecnología actual, continuar los cazaminas con operaciones de medidas contra minas, en el teatro de operaciones ante un ataque de perturbación de GPS, o deben de abandonar la zona de operaciones y cancelar la misión?– la repuesta es que sí es posible, utilizando una combinación de las técnicas descritas, para evitar prácticamente al 100 % un ataque de perturbación GPS y poder continuar con la misión. Pero en caso de que se produzca una degradación de la señal, con las técnicas actuales estudiadas, como la navegación inercial, la triangulación 5G o la navegación mediante el sistema eLoran, no sería posible continuar con las operaciones MCM en la zona minada, debido a que la precisión que nos ofrecen estas técnicas no es suficiente para garantizar la seguridad de la plataforma, por lo que debería cancelarse la misión. Aunque cabe destacar que las técnicas de navegación inercial y de navegación

con el sistema eLoran sí garantizarían una salida segura de la zona de operaciones.

Por otro lado, los procedimientos operativos de los cazaminas están obsoletos y no recogen ninguna medida ni de mitigación ni de medio alternativo de mantenimiento de posición en caso de que el GPS este degradado, por lo que se propone la actualización de dichos procedimientos con las técnicas descritas.

Por último, al no ser posible con las técnicas estudiadas mantener las operaciones de medidas contra minas en caso de ser efectiva la perturbación del GPS, se plantea la opción como línea futura de modificar el procedimiento de ejecución de operaciones MCM, evitando la entrada directa del cazaminas en áreas minadas y delegando esta labor a vehículos submarinos autónomos. Esto disminuiría significativamente los peligros asociados a la navegación en campos minados para la tripulación del buque y, además, evitaría los inconvenientes asociados a la perturbación del GPS en zona de minas al operar desde una zona segura.

Referencias

Armada española. 2001. Instrucción Permanente de Organización de la Flota: IPO FLOTA 0327/2001.

Rivero Díez, V. (2020). *Spoofing* y *jamming* en los GNSS. *Incibe-cert*. Disponible en: https://www.incibe.es/incibe-cert/blog/spoofing-y-jamming-los-gnss

NovAtel. (s.f.). GAJT-410ML Anti-Jam Antenna. *Hexagon*. Disponible en: https://novatel.com/products/anti-jam-antenna-systems-gajt/gajt-410ml-anti-jam-antenna

Demir, M. Ö., Kurt, G. K. y Pusane, A. E. (2023). A Pseudorange-Based GPS Spoofing Detection Using Hyperbola Equations. *IEEE Transactions on Vehicular Technology,* 72(8). Disponible en: https://ieeexplore.ieee.org/document/10068811

Tohidi, S. y Mosavi, M. R. (2023). A Non-linear Autoregressive Exogenous Neural Network-based Predictor for Protecting the GPS Receiver's Tracking Loop from the Spoofing Attack. DOI: 10.21203/rs.3.rs-2657692/v1.

Bybit Learn. (2021). What is Public Keys and Private Keys in Cryptography and How it Works. Disponible en: https://learn.bybit.com/es/blockchain/what-is-public-keys-and-private-keys-in-cryptography-and-how-it-works/

Maloy Smith, G. (2023). ¿Qué es un sistema de navegación inercial? *Dewesoft*. Disponible en: https://dewesoft.com/es/blog/que-es-un-sistema-de-navegacion-inercial

Ofcom. (2023). Enhanced Long-Range Navigation (eLoran). Disponible en: https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/enhanced-long-range-navigation

Cheng. E. (2021). 5G Indoor Positioning. *Pointr*. Disponible en: https://www.pointr.tech/blog/5g-indoor-positioning

Telecom Review. (2020). Emerging 5G Use Cases for the Maritime Industry. Disponible en: https://www.telecomreview.com/articles/reports-and-coverage/4073-emerging-5g-use-cases-for-the-maritime-industry

PERTURBACIÓN DE GPS EN CAZAMINAS CLASE SEGURA

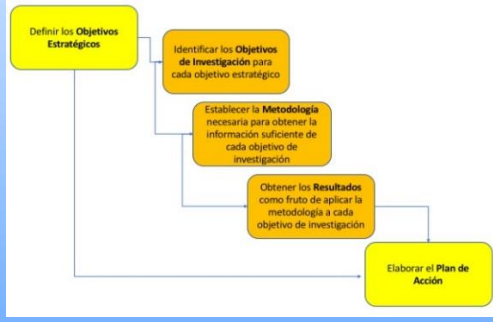
Autor: Miguel Rafael Fernández de León
Directores: José María Núñez Ortuño y Francisco Manuel Troncoso Pastoriza

Introducción

Buscar una solución para mitigar los ataques de perturbación del GPS en los cazaminas de la clase Segura, así como encontrar técnicas que, empleando la tecnología actual, permitan a estos buques mantener su posición y continuar con su misión incluso cuando dichas perturbaciones hayan sido efectivas.

Metodología

Metodología basada en el análisis y síntesis de una amplia variedad de documentación de fuentes confiables y autorizadas, como páginas web especializadas, trabajos académicos, *papers* de investigación, revistas científicas y publicaciones militares. El objetivo es lograr una comprensión profunda y exhaustiva del tema, fundamentada en la investigación y el análisis de fuentes relevantes.



Resultados

Diferentes técnicas para mitigar la perturbación GPS:
- Redes neuronales aplicadas al GPS
- Antenas antijamming
- Detección y filtrado de señales
- Criptografía

Antena Antijamming

Diferentes técnicas para mantener la posición:
- Triangulación 5G
- Navegación inercial
- Navegación mediante sistema eLoran

Conclusiones

No existe una técnica 100% segura para mitigar los efectos de una perturbación GPS en esta plataforma, pero la combinación de varias técnicas actuales, sí que pueden asegurar prácticamente una seguridad total.

En caso de producirse una perturbación de los GPS, no existe una técnica que permita continuar con las operaciones de medidas contra minas, conforme a los procedimientos actuales, pero si son válidas para salir de la zona de operaciones de forma segura.

Agradecimientos

A mis tutores y a la 1ª Escuadrilla de Cazaminas, segunda casa para mí.
A mi mujer Blanca, que después de unos duros años y mucho tiempo fuera de casa durante el mando del "Tarifa", todavía sigue animándome y apoyándome en todo lo que realizo.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

La tecnología 5G, amenazas para la seguridad y oportunidades para los sistemas de información

Autor: Fernández Fernández, Francisco Jesús (jesusfdez609@outlook.com)
Directores: Fernández Gavilanes, Milagros y Fondo Ferreiro, Pablo
(mfgavilanes@cud.uvigo.es / externo.pfondo@cud.uvigo.es)

Resumen – El estudio desarrolla las amenazas para la seguridad que supone el uso de la tecnología 5G, tanto para usuarios particulares como de las organizaciones, para después proponer medidas que las mitiguen. También se describen las oportunidades de uso que supone el empleo de esta tecnología.

El organismo de estandarización 3GPP (3rd Generation Partnership Project) desarrolla los estándares de comunicación móvil incluyendo la tecnología 5G, detallando el acceso al espectro radio, la estructura de la red de comunicaciones y las capacidades de los servicios, a fin de definir un sistema completo para estas comunicaciones. El estándar 5G no solo es desarrollado por este organismo, sino que también se ve modificado periódicamente, puesto que es un estándar en constante evolución. Otro organismo, el ETSI (European Telecommunications Standards Institute), publica los estándares de 5G aplicables que deben cumplirse cuando se despliegan estas redes en ámbito europeo.

Adicionalmente, las amenazas para la seguridad derivadas de su uso pueden ser explotadas con fines delincuenciales, estableciendo una desventaja tecnológica con los usuarios desconocedores de las vulnerabilidades. Este desajuste debe ser enmendado por los diferentes actores, pues podría llegar un momento en el que las capacidades de la tecnología sean tan superiores que, si la gestión de la seguridad sigue basada en sistemas tradicionales, demostraría ser ineficiente e insegura.

Pero el empleo de 5G supone una mejora en las capacidades de uso de las comunicaciones de las organizaciones, lo que implica aprovechar una serie de oportunidades para proporcionar nuevas funcionalidades a los sistemas de información dedicados a la seguridad y defensa, así como los utilizados por el resto de la sociedad.

Por todo ello, los datos masivos de comunicación, ya sea entre dispositivos industriales M2M (*machine to machine*), IoT (*internet of things*) o las comunicaciones entre dispositivos móviles de uso generalizado (*smartphones, tablets,* portátiles, etc.), van a cambiar el escenario de los grandes volúmenes de datos que se pueden explotar para diferentes propósitos, además de mejorar las comunicaciones.

Palabras clave – 5G, Seguridad, IoT, Amenazas, Oportunidades.

1. Introducción

La tecnología 5G representa un avance significativo en las comunicaciones móviles, pero su cambio hacia infraestructuras virtualizadas y su previsible impacto en actividades críticas hacen que la gestión de la seguridad sea crucial. Un estudio sobre las implicaciones de seguridad en 5G y sus aplicaciones en sistemas de información se vuelve esencial, dada la rápida expansión de esta tecnología en comparación con generaciones anteriores de redes móviles. La importancia radica en garantizar la correcta gestión de la seguridad de la información para evitar riesgos que podrían afectar los desarrollos que utilicen 5G.

El despliegue de esta tecnología presenta diversos desafíos y riesgos de seguridad que deben abordarse de manera integral. La capacidad mejorada de conectividad y la densidad de dispositivos aumentan la superficie de ataque, especialmente con la incorporación masiva de dispositivos IoT. La relevancia crítica de 5G en infraestructuras esenciales como redes eléctricas y sistemas de transporte implica que cualquier ataque o vulnerabilidad podría tener consecuencias graves. Además, las nuevas tecnologías introducidas, como la NFV (virtualización de funciones de red) y la segmentación de red, brindan beneficios, pero también plantean desafíos de seguridad que deben abordarse.

La dependencia de *software* y las interfaces abiertas aumentan el riesgo de vulnerabilidades y ataques. La protección de la privacidad de los datos se vuelve crucial, dada la cantidad y sensibilidad de la información transmitida. El cumplimiento de regulaciones y normativas, como el Real Decreto-Ley 7/2022 en España, es esencial para mitigar riesgos. Finalmente, los riesgos de seguridad de 5G no solo afectan la esfera tecnológica, sino que también tienen implicaciones a nivel nacional, requiriendo un enfoque estratégico y coordinado para abordarlos desde una perspectiva de seguridad nacional.

Por todas estas razones, es fundamental que la industria, los organismos reguladores, los Gobiernos y los investigadores de seguridad continúen colaborando para identificar, evaluar y mitigar los riesgos de seguridad asociados con las redes 5G.

La especificación del estándar está desarrollada por el consorcio 3GPP (3rd Generation Partnership Project) y utiliza un método estructurado denominado «Release» para desarrollar y lanzar actualizaciones y mejoras en la tecnología 5G. Cada Release representa un conjunto coherente de especificaciones técnicas y estándares que definen las capacidades, características y mejoras de la tecnología móvil. En el momento del desarrollo de este trabajo, la última versión cerrada del estándar es la Release 18 y se está trabajando en fijar la Release 19 para 2024.

La Agencia de la Unión Europea para la Ciberseguridad-ENISA publica el informe *Enisa Threat Landscape for 5G Networks*, dentro de la hoja de

ruta de gestión del riesgo en 5G, tras analizar las amenazas. En 2020 se publica la *5G toolbox*, orientada a mitigar los riesgos derivados de estas amenazas.

1.1 Hipótesis

La hipótesis enuncia que el estado actual de la seguridad en los desarrollos de redes actuales es insuficiente para implantar soluciones 5G de forma sólida y robusta. Es necesario contar con el probable desarrollo de paquetes de amenazas que puedan atacar a estas nuevas soluciones, así como paquetes de medidas que las puedan mitigar. Además, existe una oportunidad de mejora en los sistemas de información para la defensa y la seguridad.

1.2 Objetivos

Proporcionar una comprensión detallada de las redes de comunicación, centrándose en las redes 5G, delineando su operación, beneficios y aplicaciones. Además, se debe realizar un estudio exhaustivo sobre las amenazas de seguridad vinculadas a la tecnología 5G, proponiendo medidas efectivas de mitigación. Simultáneamente, se busca identificar oportunidades para enriquecer los sistemas de información dedicados a la seguridad y defensa mediante la integración de nuevas funcionalidades.

1.3 Relación entre hipótesis y objetivos

Los objetivos específicos, derivados de la contextualización de la tecnología 5G y sus futuros desarrollos, constituyen la base esencial para comprender el ecosistema completo, identificar oportunidades y amenazas y, finalmente, confirmar la hipótesis planteada. La relación intrínseca entre los objetivos y la hipótesis se destaca al estudiar amenazas específicas del 5G, demostrando la insuficiencia de las medidas de seguridad móvil previas y la necesidad de nuevas estrategias de mitigación. Asimismo, partiendo de los sistemas de información actuales de defensa y seguridad, se busca respaldar la idea de posibles oportunidades de mejora en dichos sistemas.

1.4 Importancia de la investigación

Un estudio como el presente trabajo es esencial para anticipar y mitigar riesgos de seguridad en la tecnología 5G, que está rápidamente convirtiéndose en el estándar para la comunicación móvil, impactando principalmente en los sectores de seguridad y defensa. La investigación sobre la seguridad en redes 5G es crucial debido a la interconexión más amplia y compleja de dispositivos, aumentando la superficie de ataque y exigiendo garantías de integridad, confidencialidad y disponibilidad de datos. La implementación de tecnologías emergentes, como IoT y la inteligencia artificial, intensifica la importancia de la seguridad, especialmente para dispositivos conectados, como vehículos autónomos y dispositivos

médicos. Desde una perspectiva económica, la confianza en las redes 5G es crucial para fomentar la inversión y el desarrollo, ya que las brechas de seguridad podrían afectar negativamente a la adopción de la tecnología, desacelerando el progreso y teniendo un impacto devastador en la economía global.

2. Desarrollo

El trabajo comienza con el estudio de las diferentes tecnologías, resumidas en la figura 1, donde se observa la evolución en la capacidad del ancho de banda de descarga de datos.

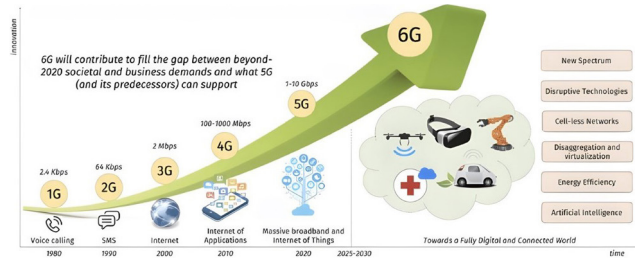


Figura 1. Evolución de las tecnologías de comunicación móviles

Como se observa, las distintas generaciones han experimentado una evolución significativa a lo largo del tiempo, desde sus primeras formas hasta las tecnologías avanzadas actuales. Este desarrollo ha sido impulsado por la demanda creciente de mayor velocidad, capacidad y eficiencia en la transmisión de datos.

El estándar 5G tiene como objetivo principal mejorar la calidad del servicio, especialmente en situaciones donde la latencia es crítica, lo que permite nuevos flujos de datos. Se establece una nueva arquitectura en la que las instancias cercanas a los clientes funcionan como una red local mediante la tecnología Edge Computing. Estas instancias utilizan el núcleo de red del operador, para facilitar comunicaciones a larga distancia.

En las redes 5G, el modelo de confianza se fundamenta en dos elementos esenciales: el SUPI (Subscription Permanent Identifier) y el SUCI (Subscription Concealed Identifier). El SUPI, un identificador único permanentemente asociado a la suscripción del usuario, contiene información crucial para la autenticación y configuraciones de seguridad, actuando como identificador principal durante las comunicaciones con la red. En contraste, el SUCI, un identificador temporal, salvaguarda la privacidad del usuario al ocultar el SUPI real, especialmente en la etapa inicial de conexión. Este enfoque protege la privacidad al limitar la exposición de información sensible en transacciones específicas, reduciendo así el riesgo de seguimiento no autorizado.

El proceso de confianza implica la interacción entre la USIM (Universal Subscriber Identity Module), donde se almacenan los parámetros necesarios para configurar el SUPI y el SUCI, y el núcleo de la red en el UDM (Unified Data Management), con autenticación de credenciales o ARPF (Authentication Credential Repository and Processing Function).

Como resultado de los parámetros de confianza, el proyecto SMARTER del 3GPP, iniciado en 2015, se centró en definir aplicaciones clave para la tecnología 5G, generando más de setenta casos de uso categorizados en tres grupos. Estos grupos incluyen eMBB (Enhanced Mobile Broadband) para aplicaciones basadas en datos con altas velocidades de datos y amplia cobertura, URLLC (Ultra-Reliable and Low Latency Communications) para casos de uso críticos que requieren baja latencia y alta confiabilidad, como cirugía a distancia y vehículos autónomos, y mMTC/MIoC (Massive Machine Type/Internet of Things Communications) para soportar un gran número de dispositivos en un área pequeña, típicamente asociados con IoT. Los casos de uso se caracterizan por los atributos de rendimiento necesarios para cada categoría.

Posteriormente, ENISA, en su *Threat Landscape for 5G Networks Report*, listó una serie de vulnerabilidades encontradas a partir de los puntos descritos anteriormente con detalles de cada una de las vulnerabilidades y los sistemas que afecta. También se intentó describir cómo estas vulnerabilidades se pueden explotar en ciberamenazas y cómo se pueden mitigar estas amenazas a través de controles de seguridad.

El informe de ENISA destaca las consideraciones de seguridad para diversos conjuntos de activos en redes 5G. Se señala que en la RAN (Radio Access Network) es esencial asegurar la latencia para aplicaciones críticas, aunque persiste la vulnerabilidad a ataques de denegación de servicio basados en perturbación de señales (*jamming*), y presenta una exposición significativa a ataques físicos. En el núcleo de red, los componentes *hardware* y *software*, junto con los procesos, son fuentes inherentes de vulnerabilidad, subrayando la importancia de la integración y la cadena de suministro como fuentes de riesgo. Para NFV (Network Function Virtualization), se destaca que la virtualización puede brindar una falsa sensación de seguridad, ya que el equipo donde se ejecuta el *software* de virtualización, dicho *software* y el hipervisor pueden comprometerse si se descubren vulnerabilidades.

En SDN (Software-Defined Networking), se resalta que, además de los riesgos asociados con la virtualización, la alta exposición de estos sistemas debe manejarse cuidadosamente, especialmente cuando están ubicados en instancias de terceros. Finalmente, en NSI (Network Slicing Instance), se subraya la seguridad proporcionada por la segmentación, pero se advierte sobre la importancia de prestar atención a las interfaces de gestión, las tecnologías de cifrado y la gestión de claves.

3. Resultados y discusión

Se ha concluido que las aplicaciones finales más importantes que ya se están desplegando sobre redes 5G y que se agrupan dentro de los casos de uso definidos por 3GPP son las mostradas en la figura 2.

Figura 2. Workplan de aplicaciones basadas en 5G según el 3GPP

La tecnología 5G promete transformar diversos sectores con sus aplicaciones innovadoras. En el ámbito de los vehículos autónomos, la comunicación casi instantánea se vuelve esencial para reacciones en tiempo real a su entorno. En ciudades inteligentes, la infraestructura y la gestión del tráfico se beneficiarán de la comunicación bidireccional entre vehículos y la infraestructura, mejorando la seguridad en el transporte. En la automatización industrial, 5G posibilitará una automatización completamente inalámbrica, permitiendo fábricas más eficientes y el control de máquinas en tiempo real.

Para la realidad aumentada y virtual, 5G mejorará la inmersión y participación, siendo aplicable en sectores industriales para tareas como reparación y mantenimiento. En el ámbito de los drones, 5G ampliará los límites en alcance e interactividad, impactando en áreas como búsqueda y rescate, seguridad fronteriza y servicios de entrega mediante drones. La integración de inteligencia artificial se acelerará gracias a 5G, siendo esencial para servicios como seguridad inteligente y predicciones por máquinas tras ejecutar autoaprendizaje.

La conexión masiva de dispositivos IoT permitirá la recopilación y análisis de datos a gran escala. Además, 5G será crucial para servicios que requieren comunicación confiable y rápida, como los servicios de emergencia. Para el entretenimiento y la formación, 5G ofrecerá experiencias de juego más inmersivas y aplicaciones de realidad virtual innovadoras. En aplicaciones industriales diversas, como salud, comercio, agricultura, manufactura y logística, 5G desempeñará un papel transformador, permitiendo desde dispositivos portátiles de alerta médica hasta la automatización de fábricas y la gestión en tiempo real de inventarios y procesos industriales.

Los resultados fundamentales derivados del análisis son diversos y destacan aspectos clave en la implementación del 5G. En primer lugar, se resalta el impacto transformador del 5G, considerándolo como una

evolución crítica en las redes de comunicación, con el potencial de alterar significativamente la sociedad y la economía. Sin embargo, se subraya la necesidad de equilibrar las oportunidades que ofrece con nuevos desafíos de seguridad, señalando la importancia de abordar estos riesgos de manera proactiva y con estrategias bien definidas, como requisito fundamental para aprovechar plenamente los beneficios del 5G y mitigarlos.

Por ello, se resalta el papel del 5G como catalizador de la innovación y la transformación digital en diversos sectores, especialmente en áreas críticas como la defensa y la seguridad. Para una implementación exitosa, destaca la necesidad de estrategias de seguridad sólidas, la adopción de mejores prácticas y un enfoque en la capacitación y concienciación sobre los desafíos y oportunidades inherentes al 5G.

4. Conclusiones

Las conclusiones destacadas del análisis sobre el 5G enfatizan su impacto transformador en las redes de comunicación, presentando capacidades innovadoras que pueden remodelar la sociedad y la economía. Sin embargo, se subraya la necesidad de abordar los desafíos asociados con estas oportunidades. La importancia del equilibrio entre las oportunidades y la seguridad se pone de manifiesto al considerar que la implementación exitosa del 5G requerirá estrategias proactivas y bien definidas. Se enfatiza la colaboración continua entre la industria, la academia y los reguladores, así como la adopción de estándares de seguridad globales.

El 5G se identifica como un catalizador para la innovación y la transformación digital, especialmente en sectores críticos como defensa y seguridad. Como recomendaciones estratégicas, se aconseja la implementación de sistemas basados en 5G mediante estrategias de seguridad sólidas, adopción de mejores prácticas y un enfoque en la capacitación y concienciación sobre los desafíos y oportunidades asociados con esta tecnología.

Finalmente, se detalla una serie de recomendaciones propuestas por el autor, clasificadas en varias categorías. Para garantizar la *seguridad en la implementación de redes 5G*, se enfatiza la adopción de estándares y buenas prácticas de seguridad, siguiendo directrices de organizaciones como 3GPP, ENISA, ETSI y la legislación nacional. La evaluación y gestión de riesgos se considera crucial, abordando vulnerabilidades en *hardware*, *software*, interfaces y la infraestructura de red mediante evaluaciones regulares.

La actualización constante de sistemas y dispositivos con las últimas medidas de seguridad es esencial, dada la dinámica de los vectores de amenazas. Se insta a desarrollar una estrategia de resiliencia de red, implementando redundancia y sistemas de detección y respuesta a intrusiones. La capacitación y la concienciación del personal se identifican como defensas clave contra ciberataques. Integrar la seguridad desde el diseño,

monitorizar y analizar el tráfico de red en tiempo real, así como colaborar en redes de intercambio de información, son recomendaciones adicionales para fortalecer la seguridad.

La planificación de la continuidad del negocio y la recuperación ante desastres se propone como medida esencial para minimizar interrupciones en caso de incidentes de seguridad o fallos de red. Siguiendo estas recomendaciones, las administraciones e instituciones pueden fortalecer su seguridad y aprovechar plenamente las capacidades avanzadas que ofrece la tecnología 5G en los sistemas de información.

Para una *exitosa y eficiente implantación de sistemas de información*, se enfatiza la necesidad de realizar una evaluación exhaustiva de las necesidades y requisitos específicos del sistema de información, considerando factores clave como volumen de datos, velocidad requerida y latencia. El diseño cuidadoso de la infraestructura basada en 5G es crucial, seleccionando *hardware* y *software* apropiados, planificando la cobertura y considerando la integración con redes existentes. Se sugiere la realización de pruebas piloto y un despliegue gradual para identificar posibles problemas y facilitar una transición escalonada.

La capacitación del personal, tanto en tecnologías 5G como en nuevas aplicaciones, es esencial, incluyendo a los usuarios finales. La integración sin problemas con sistemas existentes y la gestión robusta de seguridad y privacidad de datos son aspectos críticos. Se recomienda establecer un sistema de monitorización y soporte continuo para resolver rápidamente problemas y garantizar la alta disponibilidad. Mantener una evaluación y actualización continua del rendimiento de la red y las aplicaciones es clave para identificar áreas de mejora y adaptarse a nuevas tecnologías y estándares, asegurando la relevancia y eficacia del sistema a lo largo del tiempo.

Para maximizar las oportunidades que ofrece el 5G en *sistemas de información con aplicaciones de defensa y seguridad*, se hace hincapié en el desarrollo de sistemas de comunicación seguros y encriptados que capitalicen la alta velocidad y baja latencia del 5G, especialmente para operaciones tácticas y estratégicas en defensa, seguridad ciudadana y gestiones de crisis. La ciberseguridad se identifica como un elemento crucial, dada la apertura a nuevos posibles ataques cibernéticos dirigidos especialmente a estas estructuras por parte de actores interesados en fines de desestabilización o amenazas híbridas. La colaboración entre el sector público y privado se subraya para desarrollar soluciones innovadoras aprovechando el 5G. Asegurarse de que las implementaciones cumplan con estándares internacionales es esencial para garantizar la compatibilidad y seguridad.

Se acentúa también la importancia de la capacitación y concienciación del personal integrante de los colectivos de defensa y seguridad sobre los riesgos y beneficios del 5G. La integración del 5G con tecnologías emergentes

como inteligencia artificial, drones y vehículos autónomos se propone para mejorar la vigilancia, reconocimiento y capacidad de respuesta en situaciones de conflicto, gestión de crisis o de mantenimiento de la seguridad. Utilizar la capacidad del 5G para programas de entrenamiento avanzado, simulaciones realistas, y mejoras en la logística y gestión de recursos militares y civiles se considera vital. También se resalta el potencial del 5G para mejorar los servicios de emergencia, facilitando comunicaciones más rápidas y efectivas en gestión de crisis, así como su aplicación en sistemas de transporte inteligente para mejorar la seguridad vial y movilidad urbana.

Para finalizar, la hipótesis de este trabajo, que enfatiza la insuficiencia de la seguridad en las soluciones de redes actuales para la implantación robusta de tecnologías 5G, ha sido comprobada a través de un análisis del estado de tecnologías actuales y planteadas en redes que utilizarán este estándar. Se han identificado y analizado las lagunas existentes en los sistemas de seguridad actuales, evidenciando la necesidad de implantar nuevas estrategias y enfoques para enfrentar los desafíos únicos que presenta el 5G. Este resultado resalta la importancia de una evolución continua dada la evolución de las amenazas, y los desarrollos para mitigarlas, especialmente en el contexto de la seguridad y defensa nacional.

Referencias

Jefatura del Estado. (2022). Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación. *BOE-A-2022-4973*, pp. 41546-41564. [En línea]. Disponible en: https://www.boe.es/eli/es/rdl/2022/03/29/7

3GPP. (s.f.). 3GPP-The Mobile Broadband Standard. [Consulta: 8 de noviembre 2023].

3GPP. (s.f.). The 3GPP's System of Parallel Releases. *Releases*. [Consulta: 8 de noviembre 2023]. Disponible en: https://www.3gpp.org/specifications-technologies/releases

ENISA. (2020). ENISA Threat Landscape for 5G Networks Report. *Enisa Europa*. [Consulta: 12 de noviembre 2023]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Remmert, H. (2020). 5G Applications and Use Cases. *DIGI Connect with Confidence*. [Consulta: 12 de noviembre 2023]. Disponible en: https://www.digi.com/blog/post/5g-applications-and-use-cases.

Vaigandla, K., Bolla, S. y Karne, R. (2021). A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications. *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, pp. 3067-3076. doi: 10.30534/ijatcse/2021/211052021

ENISA. (2020). ENISA Threat Landscape for 5G Networks Report. [Consulta: 10 de noviembre 2023]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

La tecnología 5G, amenazas para la seguridad y oportunidades para los sistemas de información.

Universidad de Vigo

Autor: Fernández Fernández, Francisco Jesús.

Director/es: Fernández Gavilanes, Milagros y Fondo Ferreiro, Pablo.

Introducción

La tecnología 5G representa un avance significativo en las comunicaciones móviles, pero su cambio hacia infraestructuras virtualizadas y su previsible impacto en actividades críticas hacen que la gestión de la seguridad sea crucial. Un estudio sobre las implicaciones de seguridad en 5G y sus aplicaciones en sistemas de información se vuelve esencial, dada la rápida expansión de esta tecnología en comparación con generaciones anteriores de redes móviles. La importancia radica en garantizar la correcta gestión de la seguridad de la información para evitar riesgos que podrían afectar a los sistemas de información que utilicen desarrollos basados en comunicaciones 5G.

Desarrollo del estudio

Los nuevas desarrollos basados en 5G han sido impulsados por la demanda creciente de mayor velocidad, capacidad y eficiencia en la transmisión de datos. El estándar 5G tiene como objetivo principalmente el mejorar la calidad del servicio, especialmente en situaciones donde la latencia es crítica, y se requieran flujos de datos con mayor ancho de banda.

En la nueva arquitectura 5G, los recursos demandados se sitúan cercanos a los usuarios, funcionando como una red local mediante la tecnología Edge Computing, utilizando el núcleo de red del operador, para facilitar comunicaciones a larga distancia. El modelo de confianza se fundamenta en el SUPI (Subscription Permanent Identifier) y el SUCI (Subscription Concealed Identifier), pero en el núcleo de red se hereda la vulnerabilidad inherente en componentes hardware, software y procesos, subrayando la importancia de la integración de componentes y la cadena de suministro como fuentes de riesgo.

Resultados

Es de máxima importancia abordar las amenazas que surgen debido a posibles brechas entre los requisitos de seguridad publicados en los estándares de 5G y su implementación en los desarrollos finales.

Conclusiones

Para garantizar la seguridad en la implementación de redes 5G, se enfatiza la adopción de estándares y buenas prácticas de seguridad, siguiendo directrices de organizaciones como 3GPP y ENISA.

La evaluación y gestión de riesgos se considera crucial, abordando vulnerabilidades en hardware, software, interfaces y la infraestructura de red mediante evaluaciones regulares. Para una exitosa y eficiente implantación de sistemas de información, se enfatiza la necesidad de realizar una evaluación exhaustiva de las necesidades y requisitos específicos del sistema, seleccionando hardware y software apropiados, planificando la cobertura y considerando la integración con redes existentes. En sistemas de información con aplicaciones de Defensa y Seguridad, se enfatiza el desarrollo de sistemas de comunicación seguros y encriptados que capitalicen la alta velocidad y baja latencia del 5G, especialmente para operaciones tácticas y estratégicas. La ciberseguridad se identifica como un elemento crucial, dada la apertura a nuevos posibles ataques cibernéticos.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Fronteras inteligentes y su implantación en España

Autor: Fernández Pedroche, Rafael (rfp@interior.es)
Director: Álvarez Sabucedo, Luis Modesto (externo.llsabucedo@cud.uvigo.es)

Resumen – En el presente trabajo se pretende abordar la definición y modelado de una posible implementación de los sistemas de control fronterizo, que de alguna manera introduzca elementos que permitan mejorar los mecanismos ya en funcionamiento o incluso los que están por llegar.

Para abordarlo, en primer lugar, se realiza una revisión de la normativa europea y nacional sobre la implantación de las denominadas fronteras inteligentes en el marco de los reglamentos Entry Exit System (EES) y European Travel Information and Authorisation System (ETIAS). Posteriormente, se realiza un análisis de los procesos y sistemas actuales, incluidos aquellos que están siendo desplegados durante la redacción de este trabajo, para identificar aquellas características más relevantes y cumplir con los objetivos marcados por la Comisión Europea y los organismos encargados del control fronterizo y la seguridad dentro del espacio Schengen.

A continuación se realiza un análisis de las mejoras potenciales de estos requisitos en los sistemas actuales y de los que están por llegar en el control fronterizo español, profundizando en los detalles de estos sistemas, sus reglamentos y las especificaciones de los elementos que se registran en este sistema (documentos, huellas dactilares y captura facial). Posteriormente se realiza una propuesta de mejora mediante la introducción de equipamiento de automatización, nuevos sistemas de identificación de mayor precisión y capacidad e inclusión de una funcionalidad asociada a la red de *blockchain* EBSI para mejorar la transparencia de los procesos de control fronterizo.

Como resultado, se propone un sistema que incluye e integra elementos que abordan y que implementan las mejoras potenciales identificadas. Se proporciona una solución tecnológica global, incluyendo las tecnologías y dispositivos a utilizar por este sistema final, arquitectura y diagramas que reflejan el funcionamiento tecnológico y operativo de esta propuesta académica.

Palabras clave – Frontera, Schengen, España, Seguridad, EES, SES.

1. Introducción

Los ciudadanos nacionales de terceros países (TCN: Third Country Nationals) son ciudadanos con derecho a ingresar al espacio Schengen para una estancia de hasta noventa días dentro de cualquier periodo de ciento ochenta días, en su caso con un visado de turismo.

Se requiere dar respuesta a una serie de retos que surgen en la actualidad con el creciente número de cruces fronterizos dentro y fuera del espacio Schengen (alrededor de trescientos millones de cruces fronterizos TCN estimados para 2025) de los viajeros nacionales de terceros países. La ausencia de fronteras interiores en el espacio Schengen requiere una buena gestión de las fronteras exteriores, donde cada país tiene que controlar su frontera exterior en nombre de los demás Estados Schengen. En consecuencia, ningún Estado miembro puede hacer frente por sí solo a la inmigración irregular.

En el presente trabajo se pretende abordar la definición y modelado de una posible implementación de los sistemas de control fronterizo, que de alguna manera introduzca elementos que permitan mejorar los mecanismos ya en funcionamiento o, incluso, los que están por llegar. Para ello se ha realizado un análisis de lo ya existente y una propuesta para implementar las mejoras potenciales identificadas.

2. Desarrollo

Este TFM aborda el estudio de la situación actual en España y a nivel europeo; una revisión de la normativa nacional y europea en el ámbito normativo y técnico; el análisis de la implementación en España del futuro sistema de entradas y salidas en su versión de sistemas y equipos de control manual; el análisis e identificación de las mejoras potenciales que harían del sistema una solución más acorde a los nuevos tiempos y necesidades previstas.

Mejoras potenciales identificadas:

— Tiempo requerido para realizar el control fronterizo: esta mejora se basa en el tiempo que se requiere por parte de las autoridades fronterizas para realizar el paso de frontera de un viajero. Se verá a continuación que este tiempo está vinculado al tipo de viajero (TCN o no TCN) y tipo de control al que tiene que ser sometido, siendo también muy relevante el modo de funcionamiento y el equipamiento utilizado para realizar dicho control.

  Desde la entrada en vigor del *brexit* los ciudadanos de Reino Unido dejan de ser miembros de la Unión Europea y como tal pasan a ser considerados TCN.

  En los siguientes gráficos se pueden observar, con datos relativos al año 2019, los puestos fronterizos aéreos y marítimos más afectados

por volumen de entradas de ciudadanos británicos, así como aquellos que con menor volumen tienen alta tasa de estacionalidad.

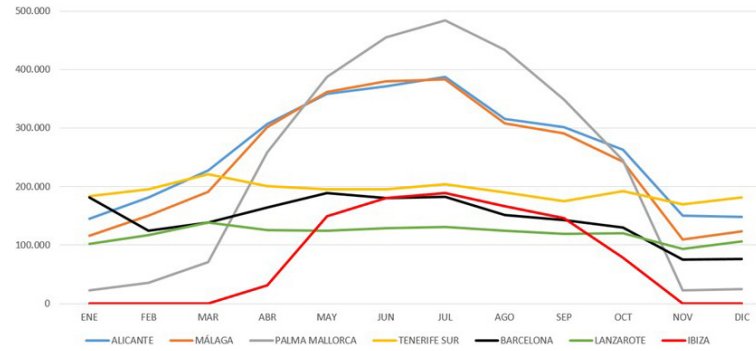


Figura 1. Estacionalidad de los principales aeropuertos por volumen. Fuente: Fronteras. PN

— Aumentar la precisión en cuanto a la identificación de las personas presentadas en frontera: la identificación fiable de las personas es una cuestión de suma complejidad. En primer lugar, la identificación y documentación de una determinada persona es responsabilidad de su país de origen. Esto acarrea numerosas implicaciones, las capacidades y recursos de cada país para asegurar la correcta identificación y documentación de sus nacionales son muy diversas, siendo en algunos casos muy deficientes o realizadas con pocas garantías de fiabilidad en la identificación de las mismas. En segundo lugar, los sistemas de identificación son múltiples y en el momento de realizar la identificación de una persona existen multitud de escenarios posibles que hay que contemplar.

  El uso de pasaportes electrónicos ha introducido la capacidad de almacenar datos biométricos, que están firmados digitalmente por el país emisor. Esta característica abre la posibilidad de evitar un registro biométrico adicional, permitiendo que los pasajeros con pasaportes electrónicos utilicen de inmediato sistemas fronterizos automatizados.

  El proceso de la adquisición de los datos biométricos de las personas acarrea numerosos desafíos. En primer lugar, los sistemas de captura o lectura de las huellas dactilares presentan diferentes problemáticas. A pesar de ser una tecnología biométrica ampliamente utilizada y confiable, los sistemas de captura de huellas dactilares con contacto tienen ciertas debilidades que pueden afectar a su precisión y fiabilidad en el contexto del control fronterizo.

  Los sistemas de identificación o reconocimiento nunca son 100 % precisos. Además de muchos otros factores, el más importante es el de la calidad de los datos biométricos introducidos al sistema. La calidad de los dispositivos y sensores, el usuario de los sistemas

y las condiciones ambientales en general juegan un importante papel.

El Instituto Nacional de Normas y Tecnología prueba regularmente la precisión de los sistemas biométricos faciales y de huellas dactilares. En el siguiente grafico se puede ver los resultados de las pruebas de identificación facial de 2006.

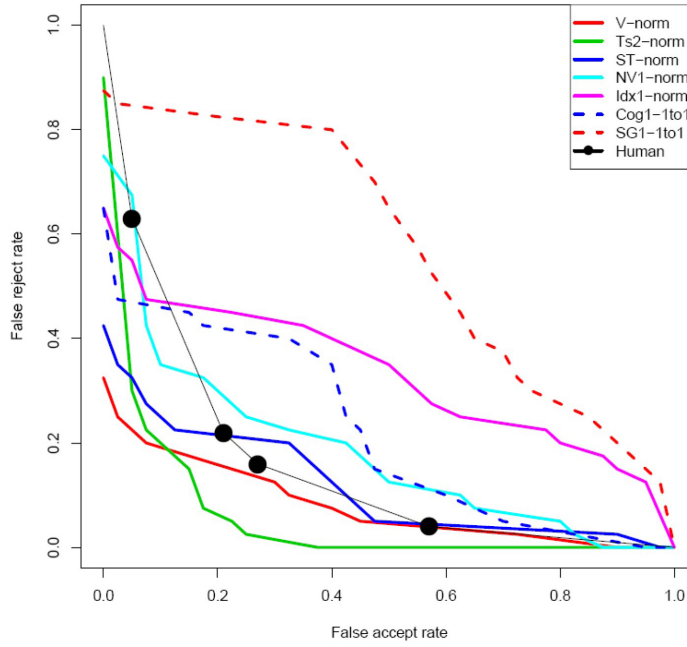


Figure 5: The ROC graph of several facial recognition algorithms (FRVT 2006 ran by NIST [FRVT06]).

Figura 2. Gráfico de varios algoritmos de reconocimiento facial. Fuente: NIST FRVT06

- Reforzar la seguridad interior y colaborar en la lucha contra el terrorismo: ya se han establecido los mecanismos necesarios para garantizar el acceso a esta información por las autoridades nacionales, nacionales e internacionales. Estos mecanismos incluyen los puntos de accesos centrales que incluyen las siguientes herramientas:
  - Herramienta de búsqueda que cumple con los requisitos marcados en el artículo 32.2 del Reglamento (UE) 2017/2226 y el artículo 52 del Reglamento 2018/1240.
  - Herramienta de estadísticas de uso y de información de resultados logrados (positivos y negativos), compatible para EES y ETIAS.
  - Una herramienta de identificación mediante huellas y mediante imágenes faciales.
- Reforzar la transparencia de los mecanismos de control fronterizo: se plantea la necesidad de trasladar al ciudadano toda la información

posible para su correcto entendimiento de los flujos y mecanismos implementados cuando es usuario o es sometido a estos procesos de control fronterizo.

Después de abordar y plantear mejoras potenciales se plantea una propuesta de requisitos para hacerlas posibles, detallando el modo de abordarlas y justificando el resultado perseguido. Se concluye con un diagrama de la arquitectura del sistema propuesto y una descripción mediante diagramas de flujos, explicando el modelo de funcionamiento de la solución proporcionada.

3. Resultados y discusión

Para la realización del esquema de arquitectura del sistema propuesto se ha partido del esquema nacional actualmente desplegado y definido en el expediente 21MO40 de la Plataforma de Contratación del Estado. Se han introducido los sistemas y elementos que mejoran la solución final.

Se plantea un sistema final con los siguientes elementos a desplegar:

SISTEMAS AUTOMATIZADOS DE CONTROL FRONTERIZO QUIOSCOS / PUERTAS ABC:

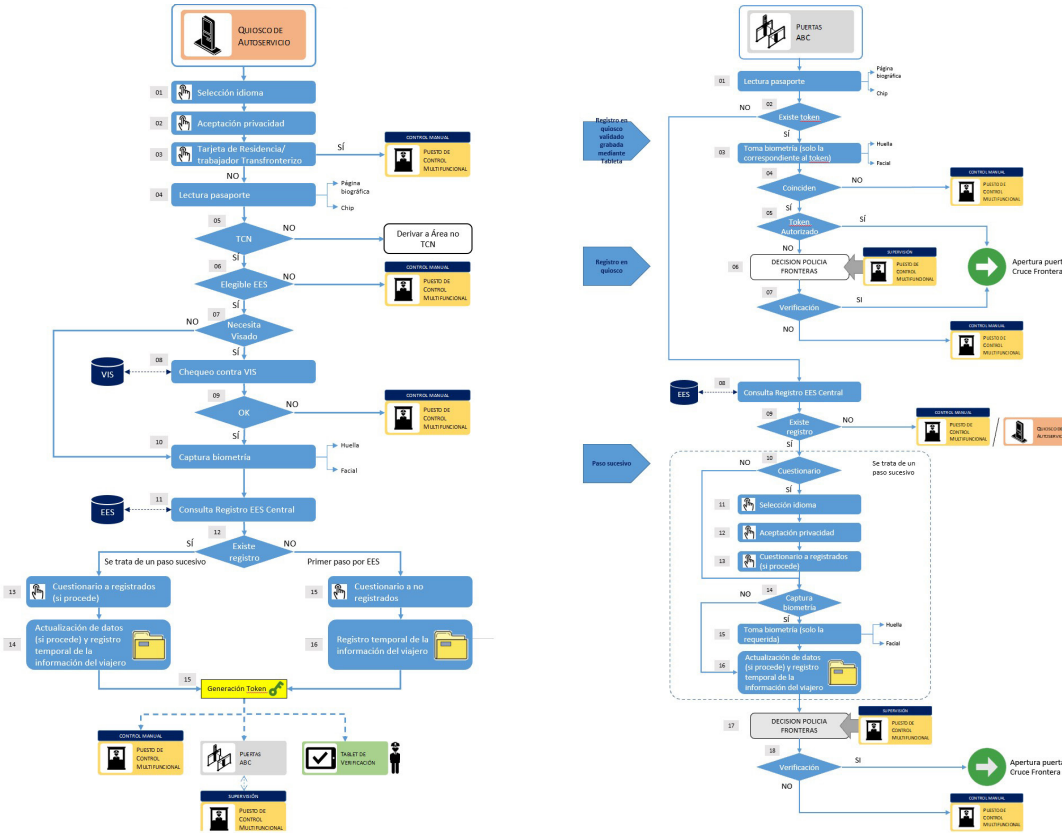


Figura 3. Operativa de alto nivel del quiosco de autoservicio (a) / ABC o e-Gate (b)

Equipamiento automatizado que permite el prerregistro de datos de los viajeros ubicado antes del Puesto de Control Manual (PCM) o de las puertas automatizadas. Esto permitirá al viajero introducir o capturar por sí mismo todos los datos necesarios (pasaporte y datos biométricos) y verificar su identidad. La verificación tras la preinscripción deberá ser realizada por la policía de fronteras en el PCM.

El registro ha de realizarse por todos los viajeros que realizan la entrada en territorio Schengen por primera vez, cuando hayan transcurrido tres años del anterior registro o cuando se den ciertas circunstancias. También es preciso realizar el registro para aquellos TCN que estuvieran en territorio Schengen cuando entre en vigor la norma y pretendan salir del mismo.

Equipamiento que integra elementos de identificación y una puerta automática (e-Gate) que permite el paso automatizado de fronteras. Una vez que el viajero ha realizado el registro, podrá llevar a cabo un paso automatizado por las puertas inteligentes; este paso estará supervisado y autorizado por la autoridad de fronteras a través de las tabletas de verificación.

TABLETAS PARA TAREAS DE REGISTRO / DE VERIFICACIÓN:

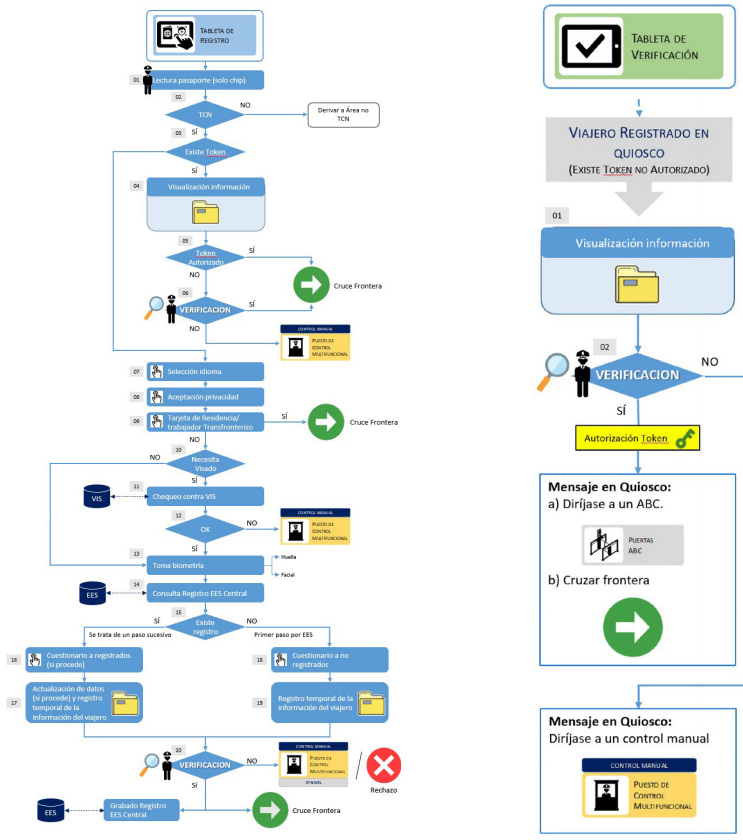


Figura 4. Operativa de alto nivel de la tableta de registro (a) / de verificación (b)

Abordarán necesidades específicas de captura y registro de datos en situaciones puntuales o en puntos fronterizos no utilizados con frecuencia. Donde no sea posible utilizar elementos fijos para los controles fronterizos y sea necesario disponer de dispositivos de movilidad, como, por ejemplo, dentro de medios de transporte como trenes o autobuses o para situaciones difíciles como la salida de vehículos con pasajeros de barcos.

Abordarán necesidades específicas de captura y verificación de datos en situaciones donde sea necesario dotar de movilidad al agente de fronteras que esté verificando el correcto funcionamiento de los elementos de automatización.

4. Conclusiones

Según se ha planteado y explicado en los puntos previos se resume en la tabla 1 el grado de cumplimiento de estos requisitos en lo que a las diferentes implementaciones del sistema nacional español se refiere.

Con la solución propuesta se mejoran en gran medida los puntos potencialmente mejorables que se habían detectado de los sistemas previos. En particular, la capacidad de absorber los flujos de viajeros que en los momentos de máxima afluencia se pueden producir y que simplemente con los puestos de control manual resultaba insuficiente (R1).

Por otro lado, mediante la introducción de nuevos elementos de captura biométrica (lectores de iris y lectores sin contacto de huellas dactilares) y la inclusión de nuevos datos contenidos en el chip del pasaporte se consigue mejorar la fiabilidad de la identificación de las personas (R2).

En relación al reforzamiento de la seguridad y colaboración policial (R3), se introduce un elemento que mejora la gestión de los diferentes usuarios potenciales del sistema PAC, el sistema de ventana única del Ministerio del Interior.

Y, por último, en relación con fomentar la transparencia para que el acceso a la información pública y las normas de buen gobierno sean los ejes fundamentales de toda acción política se ha incluido en el punto 6.4 una solución para dar mayor transparencia a todo el proceso mediante la utilización de la red de *blockchain* europea (EBSI).

En conclusión, se muestra la tabla 1 comparativa de como la solución propuesta implementa y hace posible las mejoras potenciales descritas.

	Requisito 1	Requisito 2	Requisito 3	Requisito 4
Modelo actual	NO CUMPLE	NO CUMPLE	NO CUMPLE	NO CUMPLE
Modelo EES en fase de despliegue	CUMPLE PARCIALMENTE	CUMPLE	CUMPLE	NO CUMPLE
Modelo propuesto	CUMPLE	CUMPLE	CUMPLE	CUMPLE

Tabla 1. Tabla comparativa requisitos

Referencias

Reglamento (UE) 2017/2226 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de denegación de entrada relativos a nacionales de terceros países que crucen las fronteras exteriores de los Estados miembros, se determinan las condiciones de acceso al SES con fines policiales y se modifican el Convenio de aplicación del Acuerdo de Schengen y los Reglamentos (CE) n.º 767/2008 y (UE) n.º 1077/2011. [Consulta: 7 de enero 2024]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2017-82468

Reglamento (UE) 2021/1152 del Parlamento Europeo y del Consejo de 7 de julio de 2021 por el que se modifican los Reglamentos (CE) nº 767/2008, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861 y (UE) 2019/817 en lo que respecta al establecimiento de las condiciones de acceso a otros sistemas de información de la UE a efectos del Sistema Europeo de Información y Autorización de Viajes. [Consulta: 7 de enero 2024]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80962

Frontex. European Border and Coast Guard Agency. (2021). *Technical Guide for Border Checks on Entry/Exit System (EES) related equipment*. [Consulta: 7 de enero 2024]. Disponible en: https://euagenda.eu/upload/publications/technical-guide-for-border-checks-on-ees-related-equipment.pdf

Frontex. (2007). BIOPASS Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports. Disponible en: https://www.frontex.europa.eu/assets/Publications/Research/Biopass_Study.pdf Frontex. (2010). BIOPASS II Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate. [Consulta: 7 de enero 2024]. Disponible en: https://www.frontex.europa.eu/assets/Publications/Research/Biopass_Study_II.pdf Decisión de Ejecución (UE) 2019/329 de la Comisión, de 25 de febrero de 2019, por la que se establecen las especificaciones para la calidad, resolución y uso de impresiones dactilares e imágenes faciales, para la verificación e identificación biométrica, en el Sistema de Entradas y Salidas (SES). [Consulta: 7 de enero 2024]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80311

Fronteras inteligentes y su implantación en España

Autor: Rafael Fernández Pedroche
Director/es: Luis Álvarez Sabucedo

Introducción y objetivo

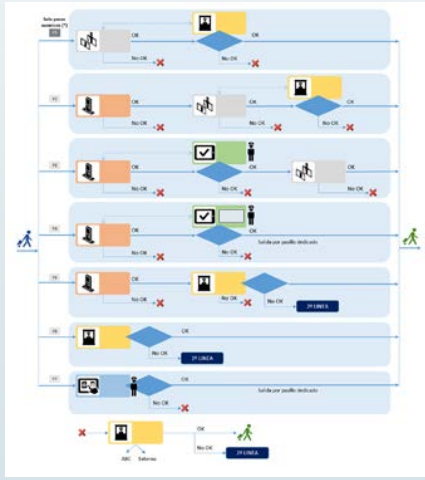
Los ciudadanos Nacionales de Terceros Países (*TCN: Third Country Nationals*) son ciudadanos con derecho a ingresar al Espacio Schengen como turistas.
La ausencia de fronteras interiores en el espacio Schengen requiere una buena gestión de las fronteras exteriores donde cada país tiene que controlar su frontera exterior en nombre de los demás Estados Schengen. En consecuencia, ningún Estado miembro puede hacer frente por sí solo a la inmigración irregular
El objetivo es realizar la definición y modelado de los sistemas de control fronterizo que desarrolle las mejoras potenciales identificadas en los actuales sistemas nacionales y europeos.

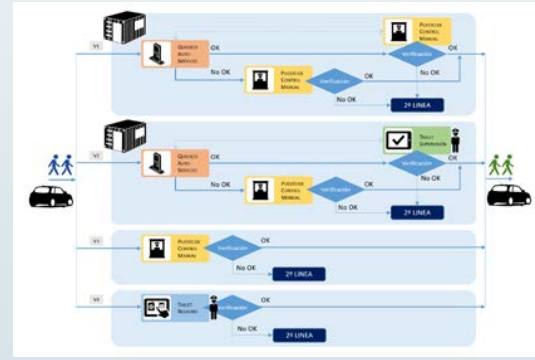
Metodología

Para llevar a cabo el objetivo principal, se ha procedido a identificar una serie de tareas que han permitido abordar el trabajo de una manera planificada y controlada.
Tarea 1: Revisión de la situación en España y del conjunto de la Unión europea, y concretamente en el conjunto del entorno Schengen.
Tarea 2: Revisión del marco legal y de la arquitectura del sistema Entry Exit System.
Tarea 3: Estudio del modelo nacional a corto plazo y que actualmente está en fase de despliegue. Y, en general análisis de las debilidades y fortalezas de los sistemas de control fronterizo español..

Resultados

Propuesta del sistema que desarrolla las mejoras potenciales identificadas. Después de llevar a cabo las tareas identificadas se plantea un modo de funcionamiento representado en los siguientes gráficos:





Conclusiones

Con la solución propuesta se consiguen las mejoras potenciales perseguidas y que se habían identificado en los sistemas previos.

Agradecimientos

A mi amada compañera de viaje Azucena por su paciencia y apoyo, especialmente en estos primeros días, semanas y meses de vida de nuestro maravilloso bebé Rodrigo.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

El ecosistema de ciberseguridad nacional y su adaptación a la normativa y estrategias de la UE

Autor: Gobierno López, Leandro (lgl@interior.es)
Directores: Atorrasagasti Morato, Aitor Sabino, Fernández García, Isidro, y Rodríguez Rodríguez, Francisco Javier (aatomor@mde.es / fjavierroriguez@cud.uvigo.es / externo.isferga@cud.uvigo.es)

Resumen – *Este TFM expone de forma somera el estado de situa*ción global entorno a la ciberseguridad y los elementos esenciales de la misma.

En él se hace una exposición resumida analítica e interrelacionada de las principales normas, estrategias y estándares en el ámbito internacional, europeo y nacional, que de una forma más o menos directa regulan aspectos de la ciberseguridad.

Todo ello contemplando las diferentes facetas de la ciberseguridad, como la creciente relevancia adquirida en la colaboración público-privada, el engarce de la cibercriminalidad dentro de la ciberseguridad, los nuevos retos y amenazas, así como la especial importancia que adquiere la prevención, protección, recuperación y respuesta de las redes y sistemas de información de las entidades de interés estratégico nacionales, los denominados operadores de servicios esenciales.

Incidiendo en ese último punto, se van a destacar las materias de mayor preeminencia y las novedades establecidas por la reciente Directiva NIS 2, que es la norma nuclear de la ciberseguridad para los Estados miembros de la Unión Europea.

Palabras clave – Ciberseguridad,Estrategias,Normas,Certificaciones, Servicios esenciales, NIS 2.

1. Introducción

1.1 Motivación

En cualquier actividad profesional mínimamente relacionada con las tecnologías de la información y las comunicaciones (en adelante, TIC), y más especialmente en el ámbito de la seguridad pública y la seguridad nacional, la necesidad de aplicar estrategias, normas y certificaciones relacionadas con la ciberseguridad resulta fundamental.

Pero esta necesidad se encuentra con el escollo de llegar a conocer no solo qué normas son aplicables, sino cuántas son, hacia dónde se dirigen las tendencias de los legisladores, las diferencias entre normas técnicas y certificaciones, hasta qué punto son de obligado cumplimiento los planes estratégicos o como se interrelacionan entre sí.

1.2 Objetivos

Este TFM pretende dar respuesta a todas las cuestiones arriba planteadas, para ello se han analizado multitud de normas, estrategias y certificaciones para seleccionar y plasmar todas aquellas que se consideran fundamentales en lo que hemos venido a denominar el ecosistema de la ciberseguridad.

De una forma sistemática, el lector va a disponer de todo ese «corpus» tan disperso. Pero no se trata de una mera recopilación, puesto que cuenta con un análisis específico de todos los aspectos que versan sobre la ciberseguridad en cada una de esas normas, estrategias y certificaciones. Asimismo, se explican las relaciones entre los diferentes preceptos estudiados y los organismos con roles destacados en el ámbito de la ciberseguridad.

Por otro lado, se han obtenido unas conclusiones que permiten dar respuesta a uno de los grandes retos en la regulación de la ciberseguridad: cómo adaptar la labor legislativa tradicional, con sus garantías y tiempos considerablemente dilatados, a la necesidad de responder al mundo digital, que evoluciona con gran celeridad.

1.3 La revolución de las tecnologías de la información y la comunicación

Las TIC están suponiendo un avance vertiginoso en múltiples campos para la humanidad y este avance se está llevando a cabo no como un mero desarrollo de una ciencia, sino como una verdadera revolución. Asimismo, dos son los elementos que provocan que esta revolución pueda tener la misma, sino más, relevancia que las revoluciones industriales y sociales acontecidas en los siglos pasados:

- Se está desarrollando de manera global en todos los países del mundo, no solo regionalmente.
- El ritmo de los cambios que las TIC ocasionan es sustancialmente más rápido.

Las características de esta revolución conllevan que la regulación de todos sus aspectos sea de una gran dificultad. Este cúmulo de circunstancias condicionan de tal modo, que la regulación no pueda acometerse desde un punto de vista tradicional. Es necesario afrontar esta desde diferentes jurisdicciones supranacionales y nacionales, así como por distintos órdenes jurisdiccionales y contando en una parte muy relevante con herramientas que parten de la iniciativa privada, como son las certificaciones, ya que sus plazos de implementación son bastante más cortos que la legislación tradicional.

1.4 Concepto de ciberseguridad y aspectos a considerar

Tras haber puesto sucintamente de relieve la importancia de las TIC pasamos a exponer una de sus dimensiones, cuyo desarrollo será el elemento nuclear de este TFM, la ciberseguridad. No obstante, como el resto de las materias de este TFM, se aborda desde un punto de vista normativo y regulatorio.

Definición de ciberseguridad aportada por el Reglamento (UE) 2019/881: «Todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas».

Más allá de esta definición y otras que se aportan en el TFM, hay que tener en consideración otros aspectos esenciales de la ciberseguridad que afectan sobremanera a la hora de entender esta dentro del contexto de las TIC y sobre todo a la hora de tratar de regularla.

En lo que respecta a la implementación de medidas de ciberseguridad, ha sido habitualmente considerado como poco menos que un obstáculo para la consecución de los objetivos de las organizaciones, ya sea por incrementar el coste y el tiempo de desarrollo de los proyectos, como porque las medidas de seguridad ralenticen y supongan mayor complejidad en la operación y mantenimiento de los sistemas. No obstante, las organizaciones se han dado cuenta de que invertir en la seguridad de sus redes y sistemas, aunque «caro», ciertamente resulta más rentable que afrontar «las consecuencias de un ciberataque u otro tipo de incidente.

Además, tratar de garantizar la seguridad de la información de las organizaciones ya no responde únicamente a sus intereses, sino que también ha de comprender a la cantidad ingente de información que estas poseen de sus usuarios, y es aquí es donde vuelve a cobrar sentido la supervisión de esas organizaciones por parte de autoridades nacionales e internacionales.

La coordinación y cooperación, nacional e internacional, entre las entidades implicadas es otra de las piedras clave en las múltiples normas e iniciativas de ciberseguridad. Estas suelen tener como principal finalidad

el intercambio de información y, en menor medida, la compartición de capacidades, para tratar de combatir los dos factores más críticos en los ciberincidentes, la velocidad y la deslocalización. También esta coordinación persigue la optimización de los canales ya establecidos, tratando de evitar la duplicidad de acciones redundantes innecesariamente.

Finalmente, otra de las cuestiones que siempre se suele tener en cuenta en estas normas e instrumentos de ciberseguridad es que, ante la transversalidad de las TIC, donde un único sistema puede implicar a diferentes países, bienes jurídicos y ámbitos sociales y organizativos muy diversos, la norma o instrumento no se circunscriba únicamente así misma ni pretenda ser omnicomprensiva (algo a todas luces demasiado ambicioso e ineficaz), sino que forzosamente se refiera a las normas e instrumentos sectoriales que tratan esas otras materias afectadas.

2. Desarrollo

Este TFM se articula en estos cinco capítulos.

— Introducción: muestra la necesidad de llevar a cabo este caso de estudio y da a conocer los elementos básicos que definen y componen la ciberseguridad, así como un somero estudio de situación y estadísticas.

— Normas sobre ciberseguridad: se compilan, explican e interrelacionan todos los preceptos legales, con mayor o menor relevancia, para la ciberseguridad en España.

Para una más cómoda comprensión y ordenación se catalogan en función del ámbito territorial de los organismos que los disponen (ámbito internacional, Unión Europea y normas nacionales).

— Estrategias sobre ciberseguridad: para lograr una visión global comprensiva de este ecosistema se explican las estrategias sobre ciberseguridad más relevantes, internacionales y nacionales.

Estas estrategias muestran de una forma muy amplia y clara el estado de situación de la ciberseguridad, tras lo cual establecen acciones para responder a los retos detectados. Resultando que en muchas ocasiones son el verdadero motivo de la actividad legislativa, ya que los organismos que las elaboran (la UE, el Gobierno de España, etc.) plasman como líneas de acción la promulgación de normas, que vienen a responder solo a una parte de los retos detectados por esas estrategias.

— Certificaciones de ciberseguridad: el ecosistema de ciberseguridad se fundamenta en sus aspectos más básicos y técnicos en cuanto a las medidas concretas de seguridad aplicables para dotar a las entidades de herramientas para proteger las dimensiones de la ciberseguridad, siendo objeto de estudio en este TFM el Esquema Nacional de Seguridad y la serie ISO/IEC-27000.

Conclusiones: tras haber puesto de relieve todo lo anterior, se logra obtener unas conclusiones respecto a la regulación del ecosistema mostrado.

2.1 La Directiva NIS 2 y las normas sectoriales, estrategias y certificaciones relacionadas

La gran profusión de preceptos analizados hace inviable que se puedan exponer en este documento con la coherencia debida sin que se extienda demasiado. No obstante, resulta inexcusable explicar la norma fundamental en la Unión Europea y, por tanto, de España, para la protección de las redes y sistemas informáticos, la Directiva NIS 2.

Esta directiva viene a ampliar y modificar la Directiva 2016/1148 (Directiva NIS), innovadora en su momento, pero ya ciertamente superada en varios aspectos. Seguidamente se destacan algunas de las facetas más relevantes reguladas por la Directiva NIS 2:

— Entidades esenciales e importantes: esta directiva cataloga a las entidades públicas y privadas que cumpliendo unos requisitos se encuentran incardinadas en los sectores estratégicos referidos en la tabla 1 y que han de cumplir con diversas obligaciones, como la implementación de medidas para la gestión de riesgos de ciberseguridad o las notificaciones de ciberincidentes sufridos.

Sectores de alta criticidad. Anexo I NIS 2	Otros sectores críticos. Anexo II NIS 2
Energía	Servicios postales y de mensajería
Transporte	Gestión de residuos
Banca	Fabricación, producción y distribución de sustancias y mezclas químicas
Infraestructuras de los mercados financieros	Producción, transformación y distribución de alimentos
Sector sanitario	Fabricación
Agua potable	Proveedores de servicios digitales
Aguas residuales	Investigación
Infraestructura digital	
Gestión de servicios de TIC (de empresa a empresa)	
Administración	
Espacio	

Tabla 1. Sectores estratégicos de la Directiva NIS 2

— Estrategias nacionales de ciberseguridad: se refuerzan los objetivos y líneas de acción, que ya establecía la Directiva NIS original y que han de cumplir los Estados miembros.

— Autoridades competentes: entre otras funciones, son las encargadas de llevar a cabo la supervisión y ejecución relativas a entidades esenciales e importantes, que contemplan la facultad de sancionar en caso de incumplimiento. Asimismo, se establecen mecanismos de

intercambio de información sobre ciberseguridad entre esas autoridades.

- Marcos nacionales de gestión de crisis de ciberseguridad: determina que los Estados miembros establezcan planes nacionales de respuesta a incidentes y crisis de ciberseguridad a gran escala. Para el caso de que estas crisis trasciendan el ámbito nacional se crea la Red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe).
- Equipos de respuesta a incidentes de seguridad informática (CSIRT): se regulan las competencias y funciones de los CSIRT nacionales de referencia, así como se crea de una Red de CSIRT, formada por los CSIRT representantes por cada Estado miembro.
- Base de datos y divulgación de las vulnerabilidades: para disminuir la amenaza de las vulnerabilidades se formalizan procedimientos para la divulgación coordinada de vulnerabilidades que ha de ser otro de los objetivos de las estrategias nacionales de ciberseguridad y ha de realizarse por los CSIRT.
- Grupo de Cooperación NIS: está formado por representantes de los Estados miembros, la Comisión y la ENISA y por la Red de CSIRT. Tiene entre sus cometidos reforzar la cooperación entre los Estados miembros, homogeneizar criterios, poner en común problemáticas para su resolución, proponer iniciativas, etc.
- Utilización de esquemas europeos de certificación de la ciberseguridad: la Directiva NIS 2 y el Reglamento de Ciberseguridad prevén que se pueda exigir a las entidades esenciales e importantes que estén certificadas en virtud de un esquema europeo de certificación de la ciberseguridad que pueda determinarse. Esto da una idea clara de la voluntad del legislador europeo de promover no solo el uso de certificaciones, sino que sean comunes a todo el entorno de la UE.

Además, hay que destacar que la Directiva NIS 2 está estrechamente relacionada a lo largo de todo su articulado con otras normas de la UE de gran preeminencia para la ciberseguridad, que también son objeto de estudio en este TFM, y para las que ejerce en la mayoría de las ocasiones de norma supletoria por su carácter transversal y estas, a su vez, tienen el carácter de sectoriales. Algunas de estas son: la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información; el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos); Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las TIC (Reglamento sobre la Ciberseguridad); Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (Reglamento DORA); borrador del Reglamento (UE), por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de

inteligencia artificial), o borrador del Reglamento (UE), por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar amenazas e incidentes de ciberseguridad, prepararse para ellos y responder a ellos (Ley de cibersolidaridad).

Igualmente importante es la relación entre la Directiva NIS 2 y la Estrategia de Ciberseguridad de la UE para la Década Digital (vigente entre 2020 y 2030). Como se explica en el TFM, la visión más flexible y amplia de un plan estratégico permite abordar múltiples aspectos y responder a los retos detectados con diversas líneas de actuación. En este caso, la Directiva NIS 2 responde de forma concreta a varios de los objetivos, como es la cooperación en el ámbito de la Unión e internacional.

También es reseñable que nuestra Estrategia Nacional de Ciberseguridad de 2019 tiene su origen y fundamento en el mandato emanado en la Directiva NIS, conforme a su trasposición al ordenamiento nacional.

Precisamente, la trasposición nacional de esa Directiva NIS se llevó a efecto con el Real Decreto Ley 12/2018 de seguridad de las redes y sistemas de información y el Real Decreto 43/2021 que lo desarrolló, mientras que la trasposición de la Directiva NIS 2 se está acometiendo en estos momentos.

Por su parte, como ya se ha visto, las certificaciones también son contempladas en la Directiva NIS 2, y en el caso de la trasposición española que se hizo de su antecedente, ya se dejaba constancia del Esquema Nacional de Seguridad.

De este modo, la Directiva NIS 2 resulta paradigmática, pues no solo es la piedra de clave legal de la UE respecto al resto de normas comunitarias que tratan sobre la ciberseguridad, sino que también hace engarce entre los planes estratégicos y los estándares de certificación, europeos y nacionales.

3. Conclusiones

Además de proporcionar un estudio de las normas, estrategias y certificaciones fundamentales para la ciberseguridad, este TFM permite llegar a una serie de conclusiones.

La innegable complejidad de la ciberseguridad tiene su correspondencia en una multitud de normas, estrategias y estándares. Pero resulta indiscutible que las normas son la piedra angular de ese ecosistema. No solo porque son de obligado cumplimiento, sino porque, respecto a las estrategias, son las que concretan y regulan algunos de los objetivos, algunas veces demasiado ambiciosos, de los planes estratégicos. Y sin dejar de destacar que, en ocasiones, son las propias normas las que determinan la obligación de elaborar esas estrategias, como ocurre con la Directiva NIS 2 y las estrategias nacionales de ciberseguridad.

A su vez, en cuanto a la relación entre las normas y los estándares de certificación, estos desarrollan aquellos elementos eminentemente técnicos en los que las normas no suelen entrar a detallar para no resultar en exceso complejas o dilatar en demasía los plazos para su elaboración.

Sin embargo, como resulta patente, el mero hecho de legislar, aunque sea de forma prolija, no consigue responder satisfactoriamente a las problemáticas consustanciales a la ciberseguridad, como son el origen internacional de las ciberamenazas o la ya mentada vertiginosa evolución de las TIC.

Todo ello ha provocado una regulación de las TIC y, por ende, de la ciberseguridad, que ha tenido que adaptarse a estos condicionamientos para resultar eficaz.

La transversalidad y afectación de las TIC a prácticamente todos los aspectos de la sociedad conlleva que un enfoque tradicional no sea el adecuado.

De este modo, cada vez más se llevan a cabo planes estratégicos con un objeto de estudio muy amplio, que tras su elaboración permite acometer, con la flexibilidad que les caracteriza, diferentes soluciones a los retos identificados. Siendo en varias de las ocasiones, como este TFM deja constancia, una de las soluciones un llamamiento al legislador para que regule una faceta concreta de esos retos.

En cuanto a la dimensión internacional de la ciberseguridad, que viene dada, por mencionar solo algunos factores, por las relaciones entre las redes y sistemas de las organizaciones, los proveedores de servicios radicados en el extranjero (un ejemplo paradigmático son los servicios que se prestan en la nube) o los ataques de los ciberdelincuentes que aprovechan las lagunas del auxilio penal internacional para cometer sus delitos desde otros países, es crucial contar con una armonización internacional.

Y en esta promoción de normas comunes se ha avanzado mucho, sin duda dentro de la Unión Europea, pero también a nivel global con convenios como el de Budapest, que en un periodo razonablemente corto de tiempo ya ha sido ampliado con dos protocolos adicionales y cuyo notable éxito ha propiciado el proyecto de la convención de las Naciones Unidas contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos que se está negociando en estos momentos.

Asimismo, en el plano más técnico, es donde los estándares internaciones de certificación han puesto de relieve su utilidad, pues plantean un marco común donde las organizaciones internacionales que se someten al proceso de certificación en un país conforme a un estándar pueden hacer valer esa certificación en otro. Lo que, sin llegar a suponer una seguridad jurídica propiamente dicha, facilita la confianza entre los actores, a la vez

que evita trabas al desarrollo e implantación de esas organizaciones, ya sean públicas o privadas.

En relación con la dimensión temporal de la regulación de la ciberseguridad, dos herramientas se han mostrado particularmente útiles a la hora de superar la obsolescencia.

Por un lado, la Unión Europea recurre cada vez más a los actos delegados de la Comisión, lo que agiliza sobremanera la actualización de reglamentos y directivas, que de seguir el cauce convencional de modificación por el Parlamento y el Consejo resultarían desfasados antes de poder llevarse a cabo esa necesaria actualización.

Por otra parte, concluimos resaltando nuevamente la utilidad de los estándares de certificación, a los que las normas pueden recurrir para regular aspectos no solo técnicos, sino que pueden adaptarse con mucha más agilidad y rapidez a una realidad cambiante que el proceso necesario para modificar una ley o incluso un reglamento.

Por este motivo, se aboga desde aquí, a la luz de la materia estudiada, en emplear en mayor medida estos estándares de certificación y culminar ese proceso de armonización internacional y europeo que está siendo ya promovido entre otras normas, por la Directiva NIS 2.

El ecosistema de ciberseguridad nacional y su adaptación normativa y estrategias de la UE

Universidad de Vigo

Autor: Leandro Gobierno López

Directores: Isidro Fernández García, Aitor Sabino Atorrasagasti Morato y Francisco Javier Rodríguez Rodríguez.

Introducción

Exposición resumida analítica e interrelacionada de las principales normas, estrategias y estándares en el ámbito internacional, europeo y nacional, que de una forma más o menos directa regulan aspectos de la ciberseguridad.

Metodología

Se contemplan las diferentes facetas de la ciberseguridad, como la reciente relevancia adquirida en la colaboración público-privada, el engarce de la cibercriminalidad dentro de la ciberseguridad, los nuevos retos y amenazas, así como la especial importancia que adquiere la prevención, protección, recuperación y respuesta de las redes y sistemas de información de las entidades de interés estratégico nacionales, los denominados operadores de servicios esenciales.

Resultados

Resulta indiscutible que son las normas la piedra angular de ese ecosistema. No solo porque son de obligado cumplimiento, sino porque, respecto a las estrategias, son las que concretan y regulan algunos de los objetivos, algunas veces demasiado ambiciosos, de los planes estratégicos. Y sin dejar de destacar que en ocasiones son las propias normas las que determinan la obligación de elaborar esas estrategias, como ocurre con la Directiva NIS 2 y las estrategias nacionales de ciberseguridad.

Conclusiones

En relación a la dimensión temporal de la regulación de la ciberseguridad dos mecanismos se han mostrado particularmente útiles a la hora de superar las dificultades de legislar adecuándose a la revolución digital.

La UE cada vez recurre más a los actos delegados de la Comisión, lo que agiliza sobremanera la actualización de reglamentos y directivas, que de seguir el cauce convencional de modificación por el Parlamento y el Consejo resultarían desfasados antes de poder llevarse a cabo esa necesaria actualización.

Por otra parte, resaltando la utilidad de los estándares de certificación a las que las normas pueden recurrir para regular aspectos no solo técnicos, sino que pueden adaptarse con mucha más agilidad y rapidez a esa realidad cambiante.

Anonimización, ocultación y eliminación de huella digital

Autor: Gómez Burgaz, Ignacio (igburgaz@yahoo.es)
Directores: González Coma, José y Vales Alonso, Javier (jose.gcoma@cud.uvigo.es / externo.jvales@cud.uvigo.es)

Resumen – La necesidad y el uso de Internet en el mundo actual nos sugiere analizar diversos métodos y acciones que tanto un usuario individual como una organización pueden llevar a cabo para navegar, obtener y gestionar información de manera anónima en el entorno digital. Este objetivo se plantea con el propósito de asegurar una comunicación y navegación anónima y segura, eludiendo la detección, seguimiento y monitorización por terceros.

Desde la privacidad de cualquier usuario en el espacio virtual hasta la configuración de un entorno seguro en el contexto de una organización se explora la forma de implementar medidas de seguridad para salvaguardar la privacidad y realizar actividades como la recopilación de información. Adicionalmente, se abordan las normativas jurídicas y consecuencias legales asociadas a la ley de protección de datos, la privacidad y el derecho al olvido.

Se proponen estrategias aplicables para el uso y la navegación no solo en ordenadores personales, sino también en dispositivos móviles e, incluso, dentro de la red de trabajo de una organización.

A lo largo del desarrollo del trabajo, se realizará un análisis detallado de las técnicas de anonimización y ocultación existentes, evaluando sus características y aplicaciones específicas. Este análisis se extenderá al estudio de las características de los diferentes navegadores y buscadores, explorando sus funcionalidades y las posibles huellas digitales generadas por los usuarios.

Finalmente, se abordará en detalle la huella digital generada por la actividad de navegación, incluyendo el registro en diversas plataformas. Se examinará el funcionamiento de herramientas de seguimiento como *cookies* y *supercookies*, y se propondrán diversos métodos para evitar la monitorización por parte de herramientas y servicios de análisis que puedan estar integrados o incrustados en dispositivos y plataformas.

Palabras clave – Anonimicidad, Ocultación, Huella digital, Seguridad informática, Privacidad digital

1. Introducción

El trabajo aborda la evolución histórica de Internet desde ARPANET hasta la popularización de la World Wide Web, destacando su impacto transformador a nivel individual y social, pero también los desafíos para la privacidad. Se destaca la recopilación de datos en línea y la importancia de la anonimización, ocultación y eliminación de huella digital para preservar la privacidad y seguridad en Internet.

Los objetivos de investigación se centran en desarrollar técnicas efectivas de anonimización y ocultación, evaluar riesgos y vulnerabilidades, identificar debilidades en técnicas existentes, discutir el cumplimiento normativo (como GDPR) y destacar herramientas y buenas prácticas. También se resalta la importancia de la educación en ciberseguridad y se proponen casos de uso específicos, como en atención médica y finanzas.

La justificación del tema se basa en la creciente importancia de preservar la privacidad en la era digital. El trabajo se compromete a revisar exhaustivamente las técnicas de anonimización, ocultación y eliminación de huella digital, explorando su aplicación en diversos contextos y abordando desafíos, limitaciones y soluciones. Se destaca la relevancia normativa y legal en diferentes países.

A lo largo del trabajo se busca proporcionar una comprensión profunda de estas técnicas, contextualizándolas en el marco legal y promoviendo la convivencia armoniosa entre la tecnología y la protección de los derechos individuales en el mundo digital en constante evolución.

2. Desarrollo

2.1 Fundamentos teóricos

La protección de datos se erige como un tema fundamental en la sociedad actual, dada la expansión sin precedentes de la era digital. Este derecho, respaldado por legislaciones como la Constitución española y la Carta de los Derechos Fundamentales de la Unión Europea, concede a las personas control sobre sus datos y busca prevenir el uso indebido de la información. Además, la protección de datos contribuye a fortalecer la seguridad de la información, siendo esencial para contrarrestar el ciberdelito. A nivel legal, normativas como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea establecen el marco para la protección de este derecho.

La privacidad digital siempre ha sido una preocupación, pero en la era digital, las grandes bases de datos y la facilidad de recopilación de información en Internet intensifican las inquietudes. La privacidad digital abarca el control sobre datos personales y no personales, evitando su uso ilícito y resguardando la dignidad y derechos de los individuos. La recopilación

automática de datos en línea ha elevado las preocupaciones sobre la privacidad.

La huella digital, también conocida como huella electrónica, comprende la información generada al utilizar Internet. Incluye desde los sitios web visitados hasta correos electrónicos y datos compartidos en línea. Este rastro digital puede ser empleado para rastrear actividades en línea de una persona. La huella digital se compone de datos públicos, publicados por otros y generados por el propio individuo. La información puede ser recopilada, compartida e, incluso, filtrada por *hackers*, lo que destaca la importancia de comprender y gestionar la huella digital.

Existen dos categorías de huellas digitales: activas y pasivas. La huella digital activa se forma a través de la compartición intencionada de datos en línea, como publicaciones en redes sociales. Por otro lado, la huella digital pasiva se genera a partir de datos recopilados sin el consentimiento informado del usuario. Ambas son valiosas para diversas aplicaciones, desde la permanencia relativa de la información hasta la reputación digital, verificación de huellas digitales para empleo y educación, malinterpretación de contenido y la prevención de cibercrimen.

La privacidad digital es esencial por varias razones. Permite mantener el control sobre la información personal, previene el robo de identidad, el fraude y otros abusos en línea. Además, es crucial para preservar la autonomía y libertad en el entorno digital, evitando el uso no autorizado de datos con fines publicitarios o políticos. La privacidad digital contribuye a la seguridad, tanto en el ámbito digital como físico, gestionando adecuadamente la información personal según las leyes establecidas. La falta de atención a la configuración de privacidad y la lectura de políticas puede resultar en el uso indebido de datos que afecta la vida diaria de las personas.

El ámbito de la privacidad digital está respaldado por varios marcos legales y regulaciones en diferentes países y regiones. En España, la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) establece obligaciones claras, mientras que la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) regula el uso de tecnologías de la información. A nivel europeo, el RGPD unifica las normas para el tratamiento de datos personales. Fuera de la UE, normativas como la Ley de Privacidad del Consumidor de California (CCPA) y la Ley de Protección de Datos Personales en Brasil (LGPD) destacan la atención global hacia la privacidad digital.

En la esfera internacional, la ONU ha aprobado diversas resoluciones que subrayan la importancia de proteger la privacidad en la era digital, asegurando que cualquier intervención en este derecho cumpla con los principios de legalidad, necesidad y proporcionalidad. Estas resoluciones resaltan que los derechos fundamentales, incluida la privacidad, deben ser

protegidos en el ámbito digital, considerando el impacto de nuevas tecnologías como la inteligencia artificial.

La protección de datos y la privacidad digital se erigen como cuestiones cruciales en el entorno digital contemporáneo. La comprensión de conceptos como la huella digital, su tipología, importancia y la legislación que la respalda, es esencial para preservar los derechos individuales y la seguridad en un mundo cada vez más conectado.

2.2 Anonimización de datos

Respecto a la anonimización de datos, se vuelve a destacar su importancia en la protección de la privacidad de las personas y el cumplimiento de normativas. Los objetivos de la anonimización incluyen minimizar el riesgo de identificación, garantizar la irreversibilidad del proceso y auditar el uso de datos anonimizados. Se presentan diversas técnicas teóricas, como la aleatorización, generalización y seudonimización, y se detallan ejemplos y enfoques específicos, como la privacidad diferencial.

En cuanto a la aleatorización, se describe su aplicación para equilibrar grupos en estudios y la adición de ruido como una medida para dificultar la identificación de individuos. La permutación y aleatorización estratificada también se estudian.

La privacidad diferencial se presenta como un conjunto de técnicas para recopilar y compartir datos con certeza matemática de no perjudicar ni identificar a los individuos. Se explican conceptos como Privacidad Diferencial Epsilon, Local y Global.

En el enfoque de generalización, se enfatiza la importancia de reducir la precisión de datos de manera intencionada para preservar la privacidad. Se describen modelos como K-Anonimato, L-Diversidad y T-Proximidad, cada uno diseñado para mitigar riesgos específicos de reidentificación.

La reducción de la precisión de datos mediante técnicas como redondeo se menciona como una estrategia simple, pero con la advertencia de posible pérdida de información relevante.

Referente a la seudonimización como práctica esencial para proteger la privacidad de los datos sensibles, se busca reemplazar la información PII (Personal Identifying Information), PHI (Protected Health Information) y PCI (Payment Card Industry) a través de diversas técnicas. La PII incluye datos identificativos personales, la PHI abarca información médica, y la PCI se refiere a datos de transacciones con tarjetas de pago.

En contraste con la anonimización tradicional, la seudonimización es reversible, permitiendo almacenar información adicional para una posible reidentificación autorizada. El trabajo explica técnicas clave, como el Contador, Generador de Números Aleatorios (GNA), Función Criptográfica

de Hash, Código de Autenticación de Mensajes (CAM), Cifrado y Perturbación de Datos, destacando sus ventajas y desafíos específicos.

Las políticas de seudonimización, como la determinista, con aleatorización de documentos y completamente aleatorizada, se presentan como elementos fundamentales en la implementación práctica de estas políticas. Además, se comentan técnicas avanzadas como árboles de Merkle, cadenas de Hash, filtros de Bloom y seudónimos de transacciones vinculables.

Destacan como desafíos significativos en el proceso de anonimización los avances tecnológicos, el riesgo de reidentificación, la pérdida de utilidad y los cambios en el contexto. También se discuten limitaciones, como la complejidad de datos y la escalabilidad en la aplicación de la seudonimización. Se enfatiza la necesidad de elegir técnicas adecuadas, considerando tanto la protección como la utilidad requerida, junto con las consideraciones éticas y legales inherentes a esta práctica vital.

2.3 Ocultación de la huella digital

La importancia de ocultar la huella digital en el entorno digital actual, se realiza para minimizar los riesgos de la fuga de información, la violación de privacidad y la corrupción de datos. Ante la vigilancia electrónica masiva y recolección ilícita de datos, muchos usuarios recurren a herramientas de comunicación anónimas. Los investigadores han desarrollado sistemas de anonimato que construyen capas de red sobre Internet, permitiendo la comunicación sin revelar la identidad, la IP o la ubicación.

En este capítulo se exploran métodos de ocultación, como el uso de redes de comunicación anónimas (ACN), esenciales para proteger la privacidad de periodistas, activistas y ciudadanos en regímenes opresivos. Estas redes protegen la identidad del remitente y destinatario, así como el contenido del mensaje.

Las redes anónimas se pueden clasificar según el nivel de latencia y el nivel de anonimato. Se acentúa la importancia de medir el anonimato, con el desarrollo de métricas y metodologías. Se desarrollan redes anónimas como Mix Network y DC-Nets, que permiten la comunicación anónima mediante técnicas criptográficas.

Se presenta la evolución de las redes de comunicación anónima, desde Mix Network hasta cMix y PrivaTegrity, redes diseñadas para ser más eficientes. Se explora el Proyecto TOR, dividido en sus tres generaciones, y su red basada en el enrutamiento por cebolla, que proporciona anonimato y privacidad en línea.

Además, se explica el concepto de redes *peer-to-peer* (P2P) y su aplicación en la comunicación anónima, destacando su arquitectura descentralizada, robusta y escalable. Se menciona la inspiración de Tim Berners-Lee para la World Wide Web basada en P2P.

El texto aborda las redes P2P desde diferentes perspectivas, destacando aspectos relacionados con la seguridad, clasificación, estructura y ejemplos específicos de estas redes.

Se explica que las redes P2P no tienen servidores especiales para autenticar usuarios, y cada ordenador gestiona su propia seguridad. Se expone la necesidad de crear cuentas de usuario independientes y la responsabilidad de los usuarios para realizar copias de seguridad. Se comenta las desventajas de la seguridad débil y la falta de almacenamiento centralizado en las redes P2P.

Una de las clasificaciones de las redes P2P las divide en estructuradas y no estructuradas. Las no estructuradas son comunes y se utilizan para diversas aplicaciones, pero pueden ser más lentas y vulnerables a ataques. La búsqueda de información en estas redes genera un tráfico significativo y puede no garantizar resultados exitosos.

Las redes P2P estructuradas, como las basadas en Distributed Hash Table (DHT), organizan nodos de manera específica para permitir búsquedas eficientes. Sin embargo, pueden ser menos robustas en redes con alta rotación de nodos.

Otra clasificación de redes P2P es que las clasifica en centralizadas, descentralizadas, distribuidas e híbridas, respecto a la localización de nodos y recursos. Se destacan ejemplos como Napster y BitTorrent para la indexación centralizada, Gnutella para la distribuida, y Skype para la híbrida.

Se introduce la red I2P como una red P2P descentralizada enfocada en la anonimicidad. Se destaca su uso de cifrado de extremo a extremo, túneles unidireccionales y resistencia a la censura. Se menciona su funcionamiento mediante enrutadores y túneles virtuales.

Otras redes P2P, como Freenet, ZeroNet, GNUnet, IPFS, Matrix, Mesh Networks, OpenBazaar, RetroShare, Diaspora, WhisperSystems/Signal, Tox, Syndie, Osiris, OneSwarm, Tribler, GlobaLeaks y SecureDrop, son presentadas como ejemplos de redes específicas que buscan descentralizar la web, ofrecer mayor privacidad y resistencia a la censura.

La importancia de minimizar la huella digital en Internet nos ayuda a proteger la privacidad y prevenir posibles amenazas. La huella digital se compone de dos partes: activa y pasiva. Se proporciona un catálogo de buenas prácticas para disminuir la exposición en línea, que incluye configuraciones de sistemas operativos, actualizaciones automáticas y el uso de redes privadas virtuales (VPNs).

En cuanto a la navegación, se sugiere el uso de protocolo HTTPS, evitar el uso de equipos compartidos y optar por motores de búsqueda privados. También se destaca la importancia de configurar la privacidad y seguridad en las cuentas en línea, desactivar JavaScript, cifrar archivos y bloquear *cookies* y rastreadores.

En relación con las contraseñas, se recomienda el uso de contraseñas complejas, administradores de contraseñas y la autenticación de dos factores. Se advierte sobre los riesgos de almacenar contraseñas en los gestores de contraseñas de los navegadores.

En el ámbito del correo electrónico, se sugiere el uso de servicios cifrados, la eliminación de cuentas inactivas, la creación de cuentas de correo *spam* y el uso de alias. También se aborda la importancia de cancelar suscripciones y ser cauteloso al registrarse con cuentas de Google, Facebook o Twitter.

En redes sociales, se destaca la necesidad de revisar y ajustar configuraciones de privacidad regularmente, limitar la información personal compartida y ser consciente de los riesgos asociados con las interacciones en línea.

Se menciona la importancia de la educación digital, la conciencia sobre *phishing*, el control de descargas e instalaciones de programas, y el monitoreo constante del uso de dispositivos móviles. En general, se enfatiza la importancia de adoptar prácticas seguras en línea para proteger la privacidad y la seguridad personal.

Respecto a los métodos de ocultación utilizada por los *hackers*, se comenta la importancia de ocultarse tanto en el mundo físico y como en el digital. Los *hackers* emplean diversas técnicas para eludir la detección, ya sea de la policía o profesionales de seguridad. Estas incluyen cifrado, esteganografía, ofuscación, VPNs, *proxies*, suplantación de direcciones MAC, uso de máquinas virtuales, evasión de motores de búsqueda y *botnets*.

Se resalta que, aunque los *hackers* buscan constantemente métodos más sofisticados, suelen aprovecharse de sistemas vulnerables que carecen de medidas de seguridad básicas. Una vez dentro de un sistema, los *hackers* pueden permanecer ocultos durante meses, imitando el comportamiento de usuarios legítimos y utilizando tácticas como el fraude por correo electrónico empresarial.

La presencia de actores maliciosos dentro de organizaciones es otra de las amenazas más comunes, normalmente materializado por empleados descontentos o sobornados, que facilitan el acceso no autorizado y la fuga de información sensible. Se menciona la importancia de los sistemas operativos orientados a la seguridad, destacando Linux como un ejemplo, debido a la necesidad de conocimientos informáticos avanzados para su utilización, la oportunidad de inspeccionar su código al ser abierto y a la diversidad de distribuciones existentes.

En la sección sobre navegadores web, se mencionan diversos navegadores centrados en la privacidad y la seguridad, como Opera, TOR, Firefox, Brave, entre otros. También se aborda la seguridad y privacidad en el

DNS, destacando la elección de servidores DNS alternativos, como Google Public DNS y Cloudflare DNS.

El trabajo introduce los protocolos DNS over TLS, DNS over HTTPS y DNS over QUIC, que buscan mejorar la seguridad y privacidad en las comunicaciones DNS mediante el cifrado de las consultas. Además, se aborda el concepto de Server Name Indication (SNI) y se presenta el Encrypted Client Hello (ECH) como una mejora significativa para preservar la privacidad en el protocolo TLS, cifrando todo el proceso de comunicación y enlace.

Se subraya la constante evolución de las técnicas de ocultación de los *hackers* y la importancia de medidas de seguridad tanto en sistemas operativos como en navegadores web y comunicaciones DNS para mitigar riesgos y prevenir ataques cibernéticos.

Referente a la importancia de la navegación anónima en Internet por razones de privacidad, seguridad y libertad, se pone en conocimiento la formación de alianzas de inteligencia, como «5 Eyes», «9 Eyes» y «14 Eyes», que han generado preocupaciones sobre la vigilancia y el intercambio de información a nivel internacional.

Se propone la implementación de un sistema seguro para protegerse de las amenazas digitales generadas por alianzas de diferentes actores, y se menciona la importancia de elegir cuidadosamente un proveedor de VPN que no esté asociado con estas alianzas. Además, se aborda la relevancia de considerar la jurisdicción del proveedor de servicios, la ubicación de sus servidores y sus políticas de no almacenamiento de registros.

Se describen varios protocolos VPN y se sugiere utilizar aquellos más seguros, como OpenVPN o IKEv2/IPsec. También se destaca la importancia del uso de sistemas operativos seguros y privados, como TAILS, y se mencionan medidas adicionales, como el cifrado completo del disco duro o la eliminación de metadatos, para mejorar la seguridad.

Se aborda el uso de PGP para el intercambio seguro de archivos y la esteganografía como técnica para ocultar información dentro de otros datos. Se introduce la combinación del navegador TOR con una VPN para proteger la privacidad en línea.

Se exploran diferentes enfoques para utilizar TOR, ya sea a través de VPN o VPN a través de TOR, destacando sus ventajas y desafíos. Se mencionan los nodos puente y los nodos puente ofuscados, como medidas para eludir la censura y mejorar la privacidad en la red TOR.

Finalmente, se aborda el uso de *proxies* para ocultar la identidad, clasificándolos en transparentes, anónimos y élite. Se destaca la importancia de elegir el nivel de anonimato según las necesidades del usuario y se enfatiza en la confiabilidad del proveedor de *proxies*, así como en la combinación con cifrado para mejorar la seguridad y privacidad de la conexión.

2.4 Eliminación de la huella digital

La huella digital en Internet se genera a través de diversas formas de recopilación de información mientras un usuario navega por la red. Entre las fuentes destacadas se encuentran las *cookies*, la dirección IP del dispositivo, la información proporcionada voluntariamente por el usuario y otros datos recopilados automáticamente durante la navegación. Estos datos son utilizados para seguir la actividad en línea del usuario y ofrecer contenido o anuncios personalizados.

Las *cookies*, que son archivos pequeños almacenados en el dispositivo del usuario, desempeñan un papel clave en la generación de la huella digital. Pueden ser propias o de terceros, persistentes o de sesión, técnicas, de personalización, de análisis y publicitarias. Las *cookies* también crean a partir del consentimiento del usuario, por la entidad que las gestiona, el tiempo de actividad y la finalidad, abarcando aspectos técnicos, de personalización, análisis y publicidad.

Además, se habla de la existencia de «supercookies», como TrustPid, que plantean preocupaciones sobre privacidad al asignar una IP fija a cada usuario y siendo más difíciles de desactivar. Las «cookies zombie» son un tipo de *supercookies* que persisten en múltiples ubicaciones del almacenamiento local, dificultando su eliminación. Las *cookies* Flash y «evercookies» son otros tipos de *cookies* persistentes y difíciles de eliminar, que se utilizan para rastrear la actividad en línea, incluso después de borrar las *cookies* convencionales.

En cuanto a la información proporcionada por una dirección IP, esta incluye la ubicación geográfica general, el proveedor de servicios de Internet (ISP), el tipo de conexión y detalles sobre el dominio asociado con dicha dirección IP. Estos datos pueden revelar información relevante sobre el usuario y su conexión a Internet.

Dentro de los conceptos de huella digital y la privacidad en línea, se destacan los diferentes tipos de información que pueden ser recopilados, así como los métodos para identificar y gestionar esta información. El trabajo comienza explicando cómo la información sobre el tipo de dispositivo y el *software* utilizado puede ser utilizada para rastrear la actividad en línea de un usuario. Se mencionan técnicas para conseguir información como el escaneo de puertos y la identificación de direcciones IP.

Posteriormente, se destaca cómo la información personal puede ser obtenida a través de la interacción voluntaria del usuario con diversos sitios web, especialmente en redes sociales, donde se recopila una gran cantidad de datos, desde perfiles públicos hasta los «me gusta» y las reseñas. También se explica la recopilación automática de datos mientras se navega por Internet, incluyendo la detección de la huella digital.

Se describen métodos para identificar y evaluar la huella digital generada por una persona, mediante búsquedas en motores de búsqueda como el uso de herramientas especializadas. Se aborda el concepto de «egosurfing» como una práctica para gestionar la propia huella digital. También se sugieren métodos para eliminar o reducir la visibilidad de la huella digital, incluyendo acciones como cortar la difusión de datos en Internet, solicitar la eliminación de información de datos en redes sociales o llevar a cabo una limpieza digital profunda.

Además, se introduce el movimiento «DeGoogle», que aboga por reducir la dependencia de los servicios de Google para proteger la privacidad. Se resalta la importancia de adoptar un enfoque consciente al realizar actividades en línea y se mencionan herramientas y servicios que respetan la privacidad.

El «derecho al olvido» se presenta como un concepto relacionado con la privacidad, permitiendo a las personas solicitar la eliminación de información personal obsoleta o inexacta en Internet. Se destacan desafíos y riesgos asociados con la eliminación de la huella digital, como la persistencia de datos, dificultades en la eliminación total y posibles impactos en la reputación *online*.

3. Conclusiones

El trabajo desarrolla la importancia de la privacidad y seguridad en entornos digitales, reconociendo que lograr el anonimato total es impracticable. Destaca la importancia de seleccionar soluciones adaptadas a las necesidades y objetivos específicos, enfatizando el sentido común y la precaución. Se identifican diversas soluciones en constante evolución, con contribuciones de expertos en varias disciplinas.

Se proporciona una compilación exhaustiva de soluciones y orientaciones para mejorar la concienciación y prácticas de los usuarios en la configuración y navegación por Internet. Se busca no solo ofrecer soluciones específicas, sino también cultivar una mentalidad informada y proactiva. Al seguir las recomendaciones, los usuarios pueden identificar amenazas potenciales y utilizar Internet de manera segura, promoviendo la participación consciente en la protección de su seguridad digital.

Se reconocen limitaciones, como la restricción de tiempo para explorar en profundidad ciertos aspectos y la falta de recursos para demostraciones prácticas. A pesar de ello, se destaca la perspectiva informada respaldada por la mejor información disponible. El trabajo concluye señalando áreas para futuras investigaciones, centrándose en las tecnologías emergentes como la inteligencia artificial, el *blockchain*, el internet de las cosas, la computación cuántica, la realidad aumentada y otras. Se subraya que la seguridad y privacidad seguirán siendo desafíos en constante evolución en estos entornos tecnológicos en desarrollo.

Navegación astronómica sin situación de estima

Autor: Germán Francisco Lázaro Pérez
Director: José González Coma

Introducción

Dependencia excesiva de tecnologías de posicionamiento (GPS)

Alternativa: navegación astronómica

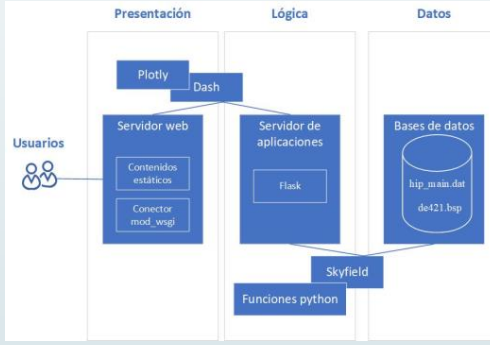
Desarrollo de aplicación web que permite navegación astronómica con y sin situación de estima

Utiliza tecnologías modernas como Plotly (Scattergeo), Dash y Skyfield

Resultados

Metodología

Arquitectura en capas



Interfaz interactivo

Conclusiones

Importancia de la navegación astronómica

Precisión adecuada de los diferentes métodos de navegación astronómica

Gran usabilidad: solución gráfica avanzada e interactiva

Adecuada para entornos de enseñanza y aprendizaje

Amplios márgenes de mejora y posibilidad de integración con otras herramientas

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Navegación astronómica sin situación de estima

Autor: Lázaro Pérez, Germán Francisco (glazper@inta.es)
Director: González Coma, José (jose.gcoma@cud.uvigo.es)

Resumen – Este TFM aborda la problemática actual de la dependencia de los buques de sistemas de posicionamiento, como el GPS, que pueden ser susceptibles a fallos o no estar disponibles. Se propone una alternativa basada en técnicas tradicionales de localización, específicamente el posicionamiento mediante la observación de astros, utilizando las alturas de cuerpos celestes como fuente de información.

El TFM se centra en el estudio de los principios que respaldan esta técnica de posicionamiento celeste y su implementación práctica en un lenguaje de programación. El objetivo principal es desarrollar una aplicación web que permita a sus usuarios implementar dos métodos diferentes de navegación astronómica, uno que emplea la situación de estima y otro que prescinde de esta información, y comparar el rendimiento de ambos métodos. De esta manera, se busca determinar la importancia de la situación de estima en la resolución del problema.

La culminación de este proyecto se traduce en el desarrollo de una aplicación web implementada en Python. La aplicación web ofrece una interfaz intuitiva y accesible, proporcionando a los usuarios una experiencia fluida y eficiente. El desarrollo de la aplicación web se ha llevado a cabo utilizando Dash, una biblioteca de Python que permite la creación de aplicaciones web interactivas y visualizaciones de datos de manera eficiente. Dash destaca por su capacidad para combinar la potencia de librerías como Plotly para gráficos interactivos y Skyfield para cálculos astronómicos precisos.

El resultado es una herramienta que demuestra la aplicación efectiva de las técnicas estudiadas, ofreciendo una solución concreta a los desafíos planteados en la dependencia de sistemas externos para el posicionamiento de buques.

Palabras clave – Posicionamiento, Navegación astronómica, Situación de estima, Aplicación web, Python.

1. Introducción

1.1 Motivación

Desde los primeros días en que los marinos se aventuraron en los océanos, el desafío principal ha sido determinar su ubicación precisa. Los astros, siendo la única referencia para los navegantes en alta mar, les permitieron culminar con éxito sus travesías, dando origen a lo largo del tiempo a los procedimientos conocidos como navegación astronómica. Este enfoque de navegación es esencial para los marinos, ya que les proporciona la capacidad de zarpar desde un puerto siguiendo una ruta planificada en alta mar y llegar a su destino final sin depender de sistemas de posicionamiento por satélite. En lugar de ello, confían únicamente en la carta náutica, la observación de los astros y un sólido conocimiento de la navegación.

El GPS, aunque revolucionario, está sujeto a posibles fallos o interrupciones, ya sea debido a condiciones atmosféricas adversas, interferencias maliciosas o simplemente a la falta de señal en ubicaciones remotas.

Por tanto, resulta necesaria la búsqueda de soluciones autónomas y confiables para la determinación de la posición de las embarcaciones, frente a la dependencia exclusiva de sistemas modernos de posicionamiento. En este sentido, es necesario destacar la importancia de una técnica tradicional como es la navegación astronómica, que permite a los marinos determinar su ubicación utilizando observaciones de cuerpos celestes.

Pero el uso de técnicas tradicionales de navegación no debe implicar la renuncia a la utilización de tecnologías modernas. Más al contrario, es necesario encontrar una combinación idónea de navegación astronómica y nuevas tecnologías que permitan un enfoque holístico y robusto. Esta sinergia puede aumentar la seguridad y eficiencia en la navegación, ofreciendo alternativas en situaciones de fallo tecnológico y mejorando la comprensión y práctica de métodos tradicionales en un contexto moderno.

1.2 Objetivos

El objetivo fundamental de este TFM se centra en desarrollar una herramienta práctica y educativa que contribuya al entendimiento de la navegación astronómica. En concreto, trata del diseño, desarrollo e implementación de una aplicación web interactiva y de fácil uso que permita la comparación sistemática entre dos variantes de la navegación astronómica: sin situación de estima y con situación de estima previa, demostrando si este factor afecta o no, y hasta qué punto en caso afirmativo, en la precisión y eficacia en la determinación de la posición.

Una aplicación web que compara la navegación astronómica con y sin situación de estima resulta valiosa, porque permite entender las diferencias y ventajas de cada método en diversas situaciones marítimas, facilitando la toma de decisiones informadas sobre qué método utilizar

en diferentes circunstancias. Además, puede ser un recurso educativo excelente, ayudando a los alumnos y usuarios en general a desarrollar habilidades en ambos métodos de navegación.

Pero esta herramienta busca no solo facilitar la comprensión y aplicación de la navegación astronómica, sino que también pretende incorporar nuevos elementos en el futuro que mejoren esta experiencia de aprendizaje. Para conseguir este objetivo, resulta prioritario trabajar en un diseño que permita realizar de forma sencilla futuras integraciones con otras herramientas para una progresiva ampliación de sus funcionalidades.

2. Desarrollo

Resulta necesario entender los fundamentos de la navegación astronómica, pues son esenciales para desarrollar y entender el funcionamiento de una aplicación web que permite la comparación entre la navegación astronómica sin situación de estima y con situación de estima. A continuación, se describen brevemente los principales conceptos fundamentales.

2.1 Fundamentos de navegación astronómica

La navegación marítima se conceptualiza como la disciplina que engloba el conocimiento y la habilidad para dirigir una embarcación de manera segura desde un punto de partida hasta un destino determinado. Existen varios tipos de navegación según las técnicas empleadas para obtener la posición. Y en concreto, la navegación astronómica trata del uso de cuerpos celestes, como estrellas y planetas, para determinar la posición y orientación de un buque en alta mar.

La esfera celeste es un modelo imaginario utilizado en astronomía, que proporciona un marco de referencia unificado para describir la posición aparente de estrellas, planetas y otros objetos celestes. Este modelo considera que todas las estrellas están ubicadas en la superficie de una esfera de radio arbitrario[1] que rodea la Tierra, y donde la Tierra además se ubica en su centro. El meridiano celeste de un astro es la línea imaginaria que conecta los dos polos celestes y pasa por dicho astro.

Dado un observador concreto, el eje de referencia asociado a dicho observador es la denominada vertical, que se define como la prolongación del radio terrestre que se extiende desde el observador en la Tierra hacia arriba, pasando por el cénit (punto del cielo situado directamente sobre el observador). El meridiano celeste del observador se define entonces como la línea imaginaria que conecta los polos celestes y el cénit del observador. De forma similar, se define como «horizonte astronómico» (del observador) a la línea de la esfera celeste que resulta de su propia intersección

[1] En la práctica de la navegación astronómica, la distancia a las estrellas es irrelevante.

con el plano perpendicular a la vertical que pasa por el centro de la esfera celeste, llamado horizonte.

Las coordenadas celestes son sistemas de coordenadas que se utilizan para especificar la posición de objetos celestes en la esfera celeste. Los dos sistemas más comunes en navegación astronómica son el de coordenadas horarias y el de coordenadas horizontales.

Las coordenadas horarias son un sistema de referencia análogo a las coordenadas geográficas en la Tierra (latitud y longitud), pero a diferencia de estas, las coordenadas horarias se basan en la posición aparente de los astros en la esfera celeste. Como las coordenadas geográficas, son totalmente independientes de la posición del observador. El equivalente a la latitud geográfica es la declinación de un astro, C_a, y se define como el ángulo medido en un meridiano celeste que indica cuán al norte o al sur de la línea ecuatorial se encuentra un objeto celeste. Los objetos al norte tienen declinaciones positivas, mientras que los objetos al sur tienen declinaciones negativas. El equivalente a la longitud geográfica es el horario en Greenwich del astro, h_{G*}, y se define como el ángulo medido en el ecuador celeste que va desde el meridiano celeste de Greenwich, en sentido horario, hasta el meridiano celeste del astro, tomando un valor entre 0° y 360°.

A diferencia de las coordenadas horarias, las coordenadas horizontales describen las posiciones de cuerpos celestes en el cielo en relación con un observador. El azimut de un astro se refiere a la dirección en la que se encuentra dicho astro desde la perspectiva de un observador, y se define como el ángulo medido en el horizonte astronómico entre el punto cardinal norte y la vertical del astro, en sentido horario, tomando un valor entre 0° y 360°. La altura de un astro se define como la medida angular vertical desde el horizonte astronómico hasta el astro. Se mide en grados, con 0° en el horizonte y 90° (máximo) en el cénit. La distancia cenital, C_a, se define como la distancia angular desde el astro hasta el cénit del observador. Es decir, es el ángulo complementario de la altura: $C_a \equiv 90° - a$.

Un círculo máximo es el círculo más grande que se puede trazar en la superficie de una esfera y su centro coincide con el centro de la esfera. Ejemplos de círculos máximos en la esfera terrestre son los meridianos y el ecuador, pero no los paralelos. Un triángulo esférico es una porción de la superficie de una esfera delimitada por tres círculos máximos que se cortan entre sí. Para resolver analíticamente un triángulo esférico con lados de longitud a, b, y c y ángulos opuestos A, B, y C, respectivamente, es suficiente con aplicar un único teorema de la trigonometría esférica, el denominado teorema de los cosenos:

$$\cos a = \cos b \cos c + \sin b \sin c \cos A \qquad 3.1 \quad 4.1\ (1)$$

Todos los cálculos necesarios para situarse mediante navegación astronómica buscan obtener las coordenadas geográficas (latitud l y longitud L) de un navegante que, en un determinado momento, observa a un astro

(o astros) con unas determinadas coordenadas horizontales (azimut y altura), y dispone de las coordenadas horarias de los mismos (horario en Greenwich y declinación). En cada instante, y para cada astro observado, existe una relación única entre estos tres pares de coordenadas. Y esta relación se puede plasmar de forma gráfica sobre la esfera celeste, en forma de un triángulo esférico.

2.2 Navegación astronómica sin situación de estima: círculos de alturas iguales

Un círculo de alturas iguales es el círculo de posiciones desde donde el observador ve a un determinado astro con la misma altura (pero distinto azimut). Si se traza una circunferencia con centro en la proyección vertical del astro sobre la superficie terrestre, denominada polo de iluminación, y radio su distancia cenital, el observador debe encontrarse en cualquier punto de dicha circunferencia.

Por tanto, si se obtienen simultáneamente las alturas de dos o más astros, los puntos de corte de los respectivos círculos de alturas nos indicarán la posición real de la embarcación. Para calcular las coordenadas de estos puntos de corte, basta con aplicar reiteradamente el teorema de los cosenos (1) para averiguar los valores faltantes en los triángulos esféricos formados.

2.3 Navegación astronómica con situación de estima: rectas de altura

A diferencia del caso anterior, antes de realizar las observaciones astronómicas se debe tener una situación de estima, basada en el rumbo y velocidad de la embarcación desde la última posición conocida. Y puesto que se dispone de una situación de estima inicial razonable, se puede aceptar que los círculos de alturas iguales obtenidos estarán cerca de la situación de estima. Dado que el círculo de alturas es usualmente muy grande (para una altura medida de 45°, su radio sería de 2700 millas), se puede aproximar dicha parte a una línea recta, tangente al círculo de alturas, denominada recta de altura.

Sabemos que el azimut no es más que la línea recta que une la situación de estima. Y, por tanto, que también une la situación real de la embarcación, dada la enorme distancia al polo de iluminación, comparada con la distancia entre la situación real y estimada. Entonces, si obtenemos las alturas del astro desde la posición real y la estimada, tenemos que esa diferencia de alturas es en realidad la distancia a la que está el punto más próximo del círculo de alturas, a medir desde la situación de estima y en la dirección del azimut. Desde este punto obtenido se traza una recta perpendicular al azimut (la tangente al círculo de alturas), que es el «trozo» del círculo de alturas, aproximado a una recta (recta de altura), correspondiente a la zona próxima a la situación de estima. Y el corte de al menos dos rectas de altura nos da la posición real de la embarcación.

2.4 Desarrollo de la aplicación web

En el marco de este proyecto se ha desarrollado una aplicación web diseñada para facilitar la introducción, visualización y análisis de datos relacionados con la navegación astronómica, incluyendo la implementación de gráficos interactivos y herramientas para interpretar observaciones astronómicas y calcular posiciones basadas en datos astronómicos precisos. En concreto, para el desarrollo de esta aplicación se ha utilizado el lenguaje de programación Python y dos herramientas principales: Dash y Plotly. Dash es un marco de trabajo de Python para construir aplicaciones web analíticas y Plotly es una librería de gráficos que permite crear visualizaciones interactivas. La combinación de Dash y Plotly ha resultado fructífera, ya que ha permitido una interacción en tiempo real con los datos y una representación gráfica clara y detallada.

Plotly permite visualizar datos geográficos sobre un mapa interactivo de la Tierra, utilizando las coordenadas geográficas (latitud y longitud) de los puntos a representar. Además, los gráficos generados por Plotly son interactivos. Esto significa que los usuarios pueden hacer *zoom*, arrastrar el mapa, y pasar el cursor sobre los puntos para obtener más información mediante *tooltips*. Utilizando estas capacidades, la aplicación puede mostrar gráficos comparativos que ilustran las diferencias en la situación astronómica con y sin estimaciones.

También se ha integrado la librería Skyfield en la aplicación. Skyfield es una librería utilizada en astronomía computacional que, basándose en bases de datos astronómicas proporcionadas por la NASA y por la ESA, es capaz de calcular posiciones de planetas, estrellas y otros cuerpos celestes en cualquier instante y con gran precisión. Esta determinación exacta de las posiciones de los astros ha permitido, en primer lugar, prescindir del uso de otro tipo de fuentes como el Almanaque Náutico y, en segundo lugar, ha sido la base para la posterior implementación de los cálculos necesarios para determinar la posición geográfica de una embarcación utilizando las técnicas de navegación astronómica explicadas anteriormente.

La aplicación web se ha estructurado en un modelo de tres capas, presentación, lógica y datos (figura 1):

1) Capa de presentación o *frontend*: se han utilizado las herramientas Dash y Plotly para crear una interfaz de usuario interactiva y visualmente atractiva, permitiendo a los usuarios ingresar datos, interactuar con la aplicación y visualizar los resultados de los cálculos de navegación astronómica de manera clara y comprensible.
2) Capa de lógica de negocio o *backend*: esta capa actúa como un intermediario entre la capa de presentación y la capa de acceso a datos. Aquí se encuentra el motor de cálculo astronómico impulsado por Skyfield y funciones Python desarrolladas *ad hoc*. Esta capa es responsable de realizar todos los cálculos astronómicos y las

simulaciones de navegación astronómica, procesando las entradas del usuario y generando los datos posicionales necesarios.

3) Capa de acceso a datos: es la capa más baja, que interactúa directamente con las bases de datos astronómicos. Está integrada en la librería Skyfield.

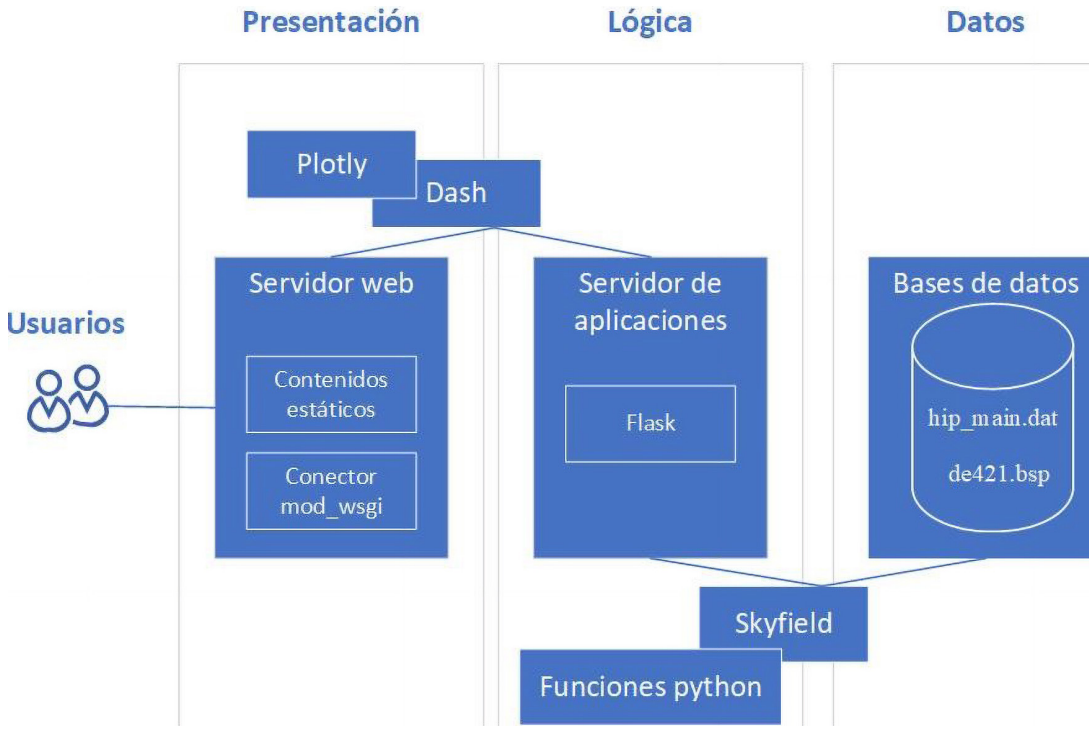


Figura 1. Arquitectura lógica de la aplicación

2.5 Infraestructura y despliegue

Una vez finalizado el desarrollo de la aplicación web, se ha procedido a hacer accesible la misma por Internet. Para ello, se ha desplegado la aplicación en un servidor en la nube con Ubuntu Server 20.04 LTS y el servidor web Apache, que se ha configurado para que sea capaz de comunicarse con la aplicación.

Ha sido necesario asignar un nombre de dominio a la dirección IP pública del servidor donde se aloja la aplicación. A tal efecto, se ha adquirido el dominio «navegacionastronomica.es» y se han generado y configurado certificados TLS para garantizar una conexión segura y encriptada.

En la tabla 1 se describen los componentes más importantes del sistema.

5.1 Componentes del sistema	
6.1 Nombre	**7.1 Descripción/Versión**
8.1 Servidor	9.1 Ubuntu Server 20.04 LTS
10.1 Servidor web	11.1 Apache 2.4
12.1 Dominio	13.1 navegacionastronomica.es
14.1 Contenidos estáticos	15.1 Imágenes
16.1 Conector	17.1 mod_wsgi
18.1 Servidor de aplicaciones	19.1 Flask 3.0
20.1 Aplicativo	21.1 Aplicación web desarrollada en Python 3.8 con el framework Dash 2.14.
22.1 Principales librerías	23.1 Dash, Plotly, Skyfield
24.1 Bases de datos	25.1 «Hipparcos Data» y «Ephemeris DE421»

Tabla 1. Componentes principales del sistema

3. Resultados y discusión

Con base en unos datos de entrada de ejemplo, a modo de caso práctico, se calculan las posiciones reales de una embarcación en alta mar utilizando los dos tipos de navegación astronómica (con y sin estima previa) y se realiza un estudio pormenorizado de los resultados obtenidos, ofreciendo datos que demuestren qué tipo de navegación es más precisa, y en qué casos esto es así.

Para que la aplicación pueda realizar los cálculos, el usuario debe introducir los siguientes datos relativos a las observaciones realizadas sobre

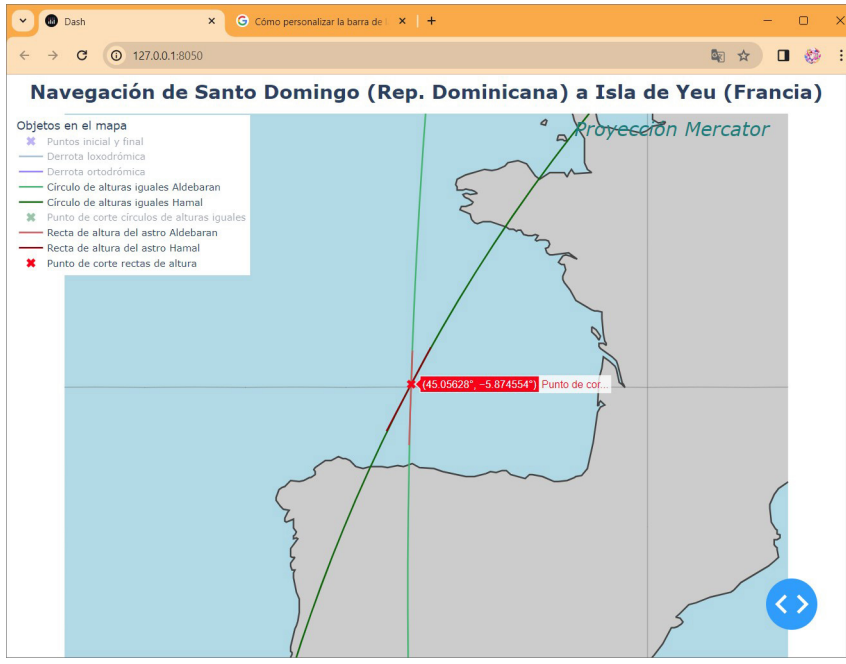


Figura 2. Proyección Mercator de Plotly Scattergeo

los astros: astros observados, fecha-hora UT de la observación de cada astro, alturas observadas, y latitud y longitud de la situación de estima. A continuación, la aplicación presentará los círculos de alturas y las rectas de altura calculadas, junto con los puntos de corte entre ellas, incluidas su latitud y longitud, tal y como se puede ver en la figura 2.

Se calcula la situación real de la embarcación mediante el método sin estima previa (círculos de alturas iguales). Para comprobar la precisión del cálculo mediante rectas de altura y poder compararlo con el método anterior, se introducen diferentes situaciones de estima, cada vez más alejadas de la posición real de la embarcación, en un intervalo entre 0 y 500 millas.

Comparando los resultados (figura 3), vemos que la tendencia es clara: cuanto más error tiene la situación de estima, mayor error tiene la situación calculada mediante el método de rectas de altura. Sin embargo, no deja de sorprender la capacidad que tiene este método de manejar aceptablemente estimaciones muy alejadas de la posición real. Así, vemos que situaciones con un error de 100 millas sobre la situación real pueden servir todavía razonablemente bien como situaciones de estima, y dar resultados muy aceptables con un error final de menos de dos millas.

Figura 3. Influencia de la situación de estima en la precisión del método de rectas de altura

4. Conclusiones

Una vez finalizado el proyecto, se puede afirmar que se han alcanzado sobradamente los objetivos propuestos, obteniendo una aplicación web interactiva que permite la aplicación sencilla de dos técnicas poderosas de navegación, como son la navegación astronómica sin situación de estima, basada en el corte de círculos de alturas iguales, y la navegación astronómica con situación de estima, basada en el corte de sendas rectas de altura.

A mayor abundamiento, el trabajo demuestra la efectividad de la navegación astronómica sin depender o dependiendo de posiciones estimadas, reafirmando la importancia y la relevancia de los métodos tradicionales de navegación marítima y evidenciando la viabilidad y eficacia de este tipo de navegación en el contexto actual. El desarrollo, implementación y despliegue exitosos de la aplicación web demuestra cómo las técnicas de navegación celeste pueden complementar e incluso sustituir a los sistemas modernos de posicionamiento (p. ej. GPS) en determinadas circunstancias.

Además, la aplicación tiene el potencial de ser utilizada en programas educativos para enseñar navegación astronómica, ofreciendo una plataforma interactiva y práctica para los alumnos.

Referencias

Mederos L. (2020). Navegación astronómica. Boadilla del Monte, Madrid: Ediciones Tutor, S.A.. ISBN: 978-84-16676-90-3.

Rhodes Mill. Skyfield, Elegant Astronomy for Python. Disponible en: https://rhodesmill.org/skyfield/

Plotly. Dash Python User Guide. Disponible en: https://dash.plotly.com/

Navegación astronómica sin situación de estima

Autor: Germán Francisco Lázaro Pérez
Director: José González Coma

Introducción

Dependencia excesiva de tecnologías de posicionamiento (GPS)

Alternativa: navegación astronómica

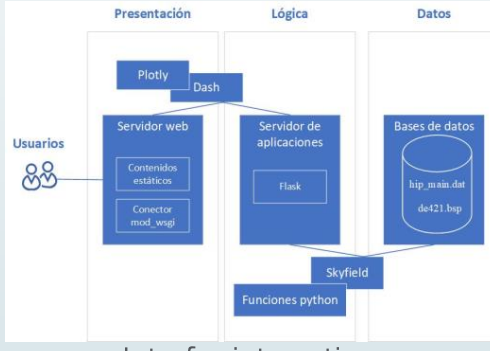
Desarrollo de aplicación web que permite navegación astronómica con y sin situación de estima

Utiliza tecnologías modernas como Plotly (Scattergeo), Dash y Skyfield

Resultados

Metodología

Arquitectura en capas



Interfaz interactivo

Conclusiones

Importancia de la navegación astronómica

Precisión adecuada de los diferentes métodos de navegación astronómica

Gran usabilidad: solución gráfica avanzada e interactiva

Adecuada para entornos de enseñanza y aprendizaje

Amplios márgenes de mejora y posibilidad de integración con otras herramientas

Análisis y evaluación de sistemas basados en IA para la detección de *fake news* en español / inglés. Una revisión sistemática de literatura

Autor: Martínez Sánchez, José Manuel (jmartinezs@oc.mde.es)
Directores: Fernández Gavilanes, Milagros y Álvarez Sabucedo, Luis M. (mfgavilanes@cud.uvigo.es / externo.lsabucedo@cud.uvigo.es)

Resumen – Dado el alcance de Internet y las redes sociales, su inmediatez y su facilidad de interacción, la mayoría de los ciudadanos ha elegido estos medios como su principal fuente de información. La falta de control sobre la veracidad de estas noticias está provocando altos niveles de desinformación en la población, lo que representa una seria amenaza para la sociedad. Su alto volumen y la velocidad a la que se producen y propagan hacen necesaria la utilización de medios automáticos que sirvan de ayuda a las agencias informativas y al público en general. En este contexto, numerosos estudios abordan el problema desde diferentes perspectivas, lo que puede provocar que un investigador que intente avanzar en este campo se sienta desorientado.

El objetivo perseguido es realizar una revisión sistemática de la literatura publicada hasta la fecha, orientada a noticias en español o inglés y que se basen en la utilización de la inteligencia artificial para conseguirlo. Para ello se ha utilizado la metodología PRISMA, que proporciona un marco para identificar, seleccionar y evaluar estudios relevantes en este campo. La selección se realizó a partir de artículos de revistas científicas y actas de conferencias técnicas, publicados en cinco bibliotecas digitales: ACM Digital Library, IEEE Xplore, Science Direct, Scopus y Web of Science.

Como resultado, se obtuvo la identificación de las características más frecuentes, las técnicas más utilizadas y los niveles de acierto de cada una. Al final, se proporcionan unas conclusiones y posibles áreas de desarrollo que puedan servir como orientación a investigaciones futuras en este campo.

Palabras clave – *Fake news*, Detección, Inteligencia artificial, *Machine learning*, NLP.

1. Introducción

Desde la antigüedad, existen *fake news*, noticias falsas creadas con el objetivo de sembrar desinformación en la sociedad y obtener un beneficio con ello, pero nunca han supuesto una amenaza tan grave como en la actualidad. La razón se encuentra en su facilidad de creación y su rapidez de difusión mediante Internet y las redes sociales. Esto hace que las agencias de información y los medios de comunicación, que hasta ahora ejercían la tarea de verificación de la información, se vean incapaces de acreditar o desmentir el ingente volumen de noticias que se genera. Para agravar más el problema, cada día más personas utilizan las redes sociales como principal fuente de información para saber qué sucede en el mundo. Esto se debe a su rapidez, economía y posibilidad de expresar su opinión en comparación con las fuentes periodísticas clásicas.

Existen varias opciones para abordar el problema. La más sencilla es la concienciación de los usuarios de las redes sociales para que no transmitan aquello de lo que no están seguros que sea cierto. Sin embargo, esta opción es difícil de llevar a cabo, porque las *fake news* están específicamente diseñadas para ser reenviadas, pues provocan sentimientos intensos en los lectores de indignación, sorpresa, afinidad o repulsa. Además, en caso de duda, no es sencillo comprobar su certeza, pues muchas veces están redactadas de forma ambigua y poco clara. Otra opción son las agencias de verificación, que realizan una labor de divulgación de todas las noticias falsas que llegan a su alcance, pero aquí el problema es que no tienen capacidad para comprobarlas al ritmo que se generan y no pueden impedir su propagación.

Por todo lo anterior, se ve la necesidad de la creación de soluciones tecnológicas que permitan detectar las *fake news* de forma automática, eficiente y fiable. Con los últimos avances en inteligencia artificial (IA), concretamente en el procesamiento del lenguaje natural (NLP) y el *machine learning* (ML), el aumento de la capacidad de cálculo y la capacidad de manejar grandes volúmenes de datos, estas soluciones empiezan a dar buenos resultados en los estudios prácticos que se están realizando.

No obstante, el alto interés de la comunidad científica sobre este asunto provoca que haya gran cantidad de literatura técnica y que un investigador que quiera desarrollar un estudio en este sector se sienta abrumado por ella.

1.1 Objetivos

Este trabajo tiene como objetivo facilitar una visión de cómo se está aplicando la IA, concretamente el NLP y el ML, en la detección de *fake news* en español o inglés. Para ello se plantean las siguientes preguntas de investigación a resolver:

1) PI 1. ¿Cuáles son las áreas de la IA con aplicación en la detección de *fake news*?
2) PI 2. ¿Qué técnicas se están usando en la detección de *fake news* y con qué resultados?
3) PI 3. ¿Qué retos y limitaciones se están encontrando en la detección de *fake news*?

2. Desarrollo

Para resolver las cuestiones planteadas en los objetivos de este trabajo, se ha realizado una revisión sistemática de la literatura científica publicada. En su desarrollo se han seguido las directrices de la metodología PRISMA y se ha utilizado como herramienta de apoyo la aplicación Parsifal.

2.1 Criterios de elegibilidad

En la planificación del modelo, se fijaron los criterios de inclusión y exclusión que permitirían detectar aquellos artículos que se consideraran válidos para la revisión y descartar los que no. Entre los primeros, se recogió que debían tratar sobre el tema abordado, utilizar técnicas de IA y ser estudios primarios con una perspectiva técnica realizados en los últimos cinco años. Por otro lado, los criterios de exclusión eliminaron los que estuvieran orientados o idiomas concretos que no fueran inglés o español, trataran sobre temas o eventos concretos, estuvieran basados en imágenes o vídeos, fueran trabajos teóricos o revisiones, o no aportaran datos concretos de su ejecución, entre otros.

2.2 Estrategia de búsqueda

Para la búsqueda de documentos, se seleccionaron cinco de las bases de datos y librerías digitales más utilizadas en la comunidad científica: ACM Digital Library, IEEE Xplore, Science Direct, Scopus y Web of Science. Siendo la última búsqueda efectuada el 30 de noviembre de 2023.

A continuación, se confeccionó la siguiente cadena de búsqueda que cubría, de forma general, los requisitos del enunciado. Esta consulta sería utilizada en todas las bases de datos, con pequeños ajustes requeridos por cada plataforma.

«*fake news*» AND (detection OR identification OR classification)

AND («artificial intelligence» OR «AI» OR «machine learning» OR «ML» OR «deep learning» OR «DL»)

AND («natural language processing» OR «NLP»)

AND (technique* OR model* OR method* OR algorithm*)

AND (approach* OR study) AND (accuracy OR performance) AND (dataset* OR feature*)

2.3 Proceso de selección

Estos artículos precisaban de una selección basada en los criterios de elegibilidad definidos. Se realizaría un primer cribado automático con base en el título del documento. Para ello, se amplió la cadena de búsqueda utilizada anteriormente. La cadena restringía que el título debía hacer referencia a las *fake news* y a su detección, o sus sinónimos. Además, se evitaba la inclusión de revisiones, encuestas o temas concretos como covid, procesos electorales o finanzas. Por último, se excluyeron aquellos artículos que, directamente en el título, se definían como relativos a un determinado idioma o país no hispano.

De estas bases de datos, se exportarían los metadatos de los artículos en formato BibTeX, para ser importado en la herramienta Parsifal. Desde allí, se procedería a la eliminación automática de los duplicados y a la lectura de los resúmenes para seguir descartando los no procedentes. Por último, mediante una lectura ligera de la introducción, se seleccionarían los documentos que pasaban a la siguiente fase y serían objeto de una evaluación más profunda.

2.4 Proceso de extracción de datos

Basándose en las preguntas de investigación a resolver, se definió un conjunto de datos que resultaran relevantes, como, por ejemplo, modelos de ML y NLP empleados, características de las noticias estudiadas, conjuntos de datos utilizados y resultados obtenidos en los estudios.

El procedimiento consistía en exportar desde Parsifal los metadatos a una tabla Excel, añadiendo columnas para recoger los datos adicionales definidos en la planificación para su extracción. A continuación, se introduciría cada texto en formato pdf en una herramienta denominada ChatPDF, basada en GPT, y se le realizarían las preguntas de una batería previamente preparada. Este proceso serviría como toma de contacto con el documento y orientación para una mejor compresión.

Por último, se realizaría la lectura detallada del documento con una triple función: verificar los criterios de selección, evaluar su calidad y extraerlos para incluirlos en el documento Excel.

Finalmente, para evaluar la calidad de los estudios incluidos, se definieron varias preguntas con sus posibles respuestas y baremos en la plataforma Parsifal, así como una puntuación mínima a superar por cada artículo para tener una calidad mínima para entrar en la investigación.

3. Resultados

3.1 Selección de estudios

Usando las herramientas y métodos presentados en la fase anterior, se procedió a la ejecución del proyecto según indica la metodología PRISMA.

Efectuada la consulta sobre las fuentes, con los criterios de búsqueda descritos en la planificación, fueron identificados 692 estudios. A continuación, se inició la fase de cribado en la que redujo el número a 286, basándonos principalmente en consultas automáticas sobre el título. Por último, tras filtrar los últimos cinco años, se alcanzó la cantidad de 275 estudios.

Estos artículos se cargaron en Parsifal y se detectaron los duplicados, quedando 209 textos pendientes de clasificar. Tras la lectura de los resúmenes, se seleccionaron 162 publicaciones, y finalmente, después de una lectura ligera de la introducción, se eligieron 68 estudios que pasaron a la última etapa.

En la fase de idoneidad, finalmente, 33 estudios fueron seleccionados y 35 fueron descartados. Las principales causas para ello fueron no ser estudios primarios, sino comparativas o encuestas, utilizar noticias en otros idiomas o tener componentes multimodales en sus modelos.

En cuanto a la evaluación de la calidad, aunque algunos artículos no cumplieron algunos de los requisitos en su totalidad, todos superaron la puntuación mínima requerida para ser incluidos.

3.2 Presentación y síntesis de resultados

En esta etapa se presentaron los estudios seleccionados mediante de tablas que detallaban las características estudiadas, las técnicas utilizadas, los resultados obtenidos y un breve resumen del modelo. Para facilitar la síntesis de la información, se utilizaron gráficos aclaratorios.

En primer lugar, se estudiaron las características utilizadas en los distintos enfoques, divididas en dos bloques, según se basaran en la propia noticia (contenido) o en elementos que la rodeasen (contexto). Dentro del contenido, se dividieron a su vez en enfoques basados en el conocimiento de los datos y los basados en el estilo: léxico, sintáctico y discurso. En cuanto al contexto, los principales componentes fueron: fuentes, usuarios y propagación.

Así, como se muestra en la figura 1a, se observó que veinticuatro de los estudios se basaban en el contenido, ocho en ambos conceptos y solamente

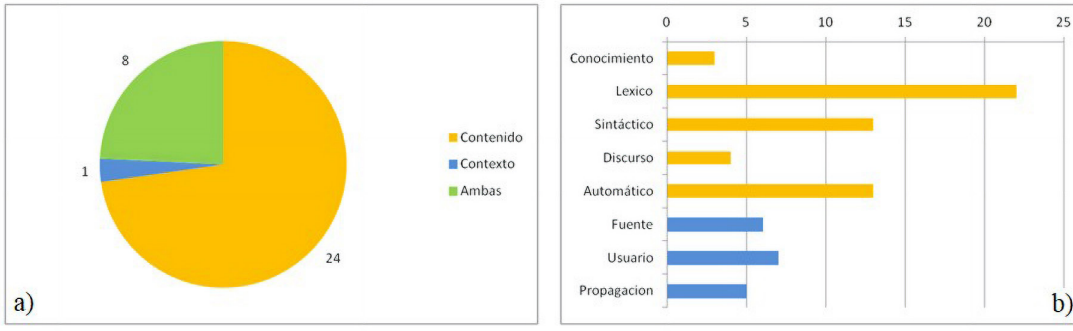


Figura 1. Enfoques utilizados en la detección de *fake news*. Fuente: elaboración propia

uno lo hacía exclusivamente en el contexto. Más en detalle, como refleja la figura 1b, se observó que, dentro del contenido, lo más frecuente eran las características basadas en el estilo, concretamente en el léxico. Aunque hubo un número relevante de artículos que, aun basándose en el contenido, las características extraídas no tenían un significado específico para ellos, pues se habían extraído de forma automática mediante *embeddings*.

En segundo lugar, se presentaron resultados sobre los métodos de extracción de características con NLP, como se puede observar en la figura 2a. Dado que la mayoría de los trabajos realizaban tareas previas de preprocesamiento y adecuación del texto, se decidió no incluirlas con el fin de clarificar la gráfica. Se puede observar que las técnicas más utilizadas fueron las basadas en la frecuencia de aparición de los términos en los documentos, como BoW, n-grams, TF y TF-IDF, esta última especialmente. Si bien es cierto que muchos estudios servían como fase previa de otras tareas más complejas. Adicionalmente, también podemos ver otro grupo formado por *embeddings* de Word2Vec, GloVe y BERT, que son utilizados como entrada del texto en bastantes estudios.

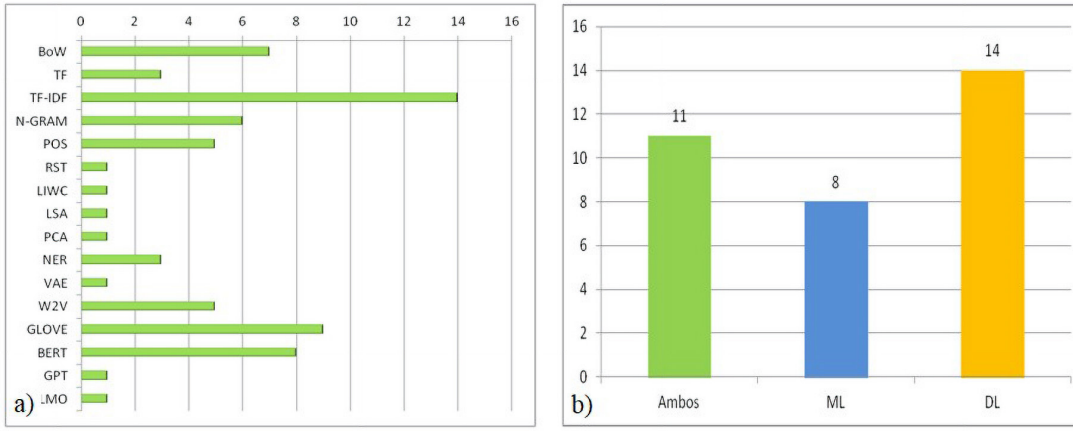


Figura 2a. Técnicas de NLP utilizadas. 2b. Tipos de ML y DL utilizados. Fuente: elaboración propia

Continuando con la presentación de resultados, pasamos a estudiar las técnicas de aprendizaje utilizadas: ML y su subconjunto Deep Learning (DL). A la vista de los gráficos, parece que hay una mayor tendencia a utilizar DL en la detección de *fake news*, aunque hay una cantidad relevante de modelos mixtos, como podemos visualizar en la figura 2b.

Si nos adentramos en las técnicas de ML utilizadas en los trabajos presentados, en la figura 3a vemos que la más utilizada es Support Vector Machine (SVM), clasificador sencillo de implementar que da muy buenos resultados. La regresión logística (LR) es también muy utilizada, al igual que el *random forest* (RF), si bien es cierto que estas técnicas se utilizan

muchas veces como proceso final de clasificación de un ensamble de otros modelos, en ocasiones incluso de DL.

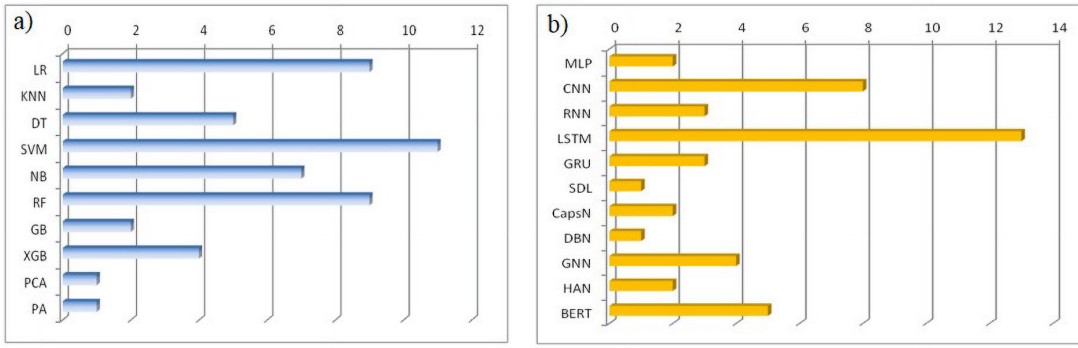


Figura 3a. Técnicas de ML empleadas. b) Técnicas de DL empleadas

En lo relacionado con las técnicas de DL, podemos apreciar en la figura 3b que la más utilizada, con diferencia, es la red neuronal Long Short Term Memory (LSTM), en la mayoría de los casos acompañada de mecanismos de atención. Pero si unimos todas las redes neuronales recurrentes (RNN) y sus variaciones, es decir RNN, LSTM, GRU y HAN, la hegemonía de estos tipos es abrumadora. Esto no es muy sorprendente, pues son las más utilizadas en el NLP desde hace algunos años. En cuanto a los *transformers*, empiezan a hacer su aparición con modelos basados en BERT, pero parece que en estos estudios aún no se está produciendo una avalancha a la misma velocidad que en otros campos, como chats, navegadores o traductores.

Por último, en cuanto a los resultados obtenidos por los estudios, se observan valores bastante altos, por encima de 0,90 en algunos trabajos, concretamente hay seis por encima de 0,99. En muchos casos, esto se puede deber a que se hayan utilizado, como datos de prueba para validar los modelos, particiones aleatorias del mismo conjunto de datos de entrenamiento. El problema es que esos datos tienen un mismo origen, y por lo tanto son bastante parecidos, lo que hace que se pueda producir cierto sobreajuste en el entrenamiento del modelo y, por lo tanto, su comportamiento cuando se le presenten datos nuevos empeore bastante. Otra circunstancia que también pueden desvirtuar los resultados es el tamaño de los *datasets*, así como su originalidad y realismo.

4. Discusión

4.1 PI 1. ¿Cuáles son las áreas de la IA con aplicación en la detección de *fake news*?

En esta investigación se han contrastado numerosos artículos sobre la detección automática de *fake news*, y en todos ellos se han identificado

dos componentes principales de IA que han participado en el proceso: NLP y ML.

En cuanto al NLP, se ha detectado que en la mayoría de los trabajos se efectúa un procesamiento del conjunto de datos con el objetivo de obtener una representación vectorial de su contenido, y de su contexto en su caso, con un número de dimensiones reducido pero muy representativo de la información que necesitamos para identificar las *fake news*.

Así, en cuanto al contenido, encontramos distintas perspectivas: desde léxicas, como, por ejemplo, palabras con sentimientos polarizados, que utilizan términos ambiguos o con doble significado; hasta sintácticas, donde priman los tipos de palabras que se usan. También relacionadas con el contenido, tenemos algunas que tratan de ver discordancias entre distintas partes de la noticia, principalmente entre titulares y texto principal. Por último, tenemos un número considerable que no especifican de qué tipo son las características utilizadas, porque son extraídas de los datos mediante DL.

En cuanto al contexto, parece que hay tres focos de interés: por un lado, lo relacionado con las fuentes, como su credibilidad o su postura; por otro lado, los usuarios, su perfil, su reacción ante los contenidos o su relación con las fuentes; y por último, la propagación, donde se contempla su rapidez, alcance, profundidad, etc. Algunos modelos realizan combinaciones de los tres.

Finalmente, tenemos algunos artículos que tratan de crear modelos con grafos de conocimiento, basándose en el contenido de las noticias, que sirvan para realizar verificación de hechos.

4.2 PI 2. ¿Qué técnicas se están usando en la detección de *fake news* y con qué resultados?

Respecto a los modelos más utilizados, son los de DL y los mejores resultados también son los de esta rama del ML. Dentro de las redes neuronales utilizadas, si bien las más utilizadas son las RNN, en su modalidad de LSTM, los resultados son, en general, igual de buenos en las redes neuronales profundas.

En cuanto a los resultados, parecen bastante prometedores, pero da la sensación de que los niveles de acierto están ligeramente altos para lo que parece razonable. Esto parece indicar que los datos quizá estén sobreexplotados y los modelos estén un poco sobre ajustados.

4.3 PI 3. ¿Qué retos y limitaciones se están encontrando en la detección de *fake news*?

En resumen, podríamos decir que la principal limitación es la falta de datos adecuados y actualizados, provocada por la rapidez con la que se generan y modifican las noticias falsas, y el principal reto a afrontar es la

creación de modelos híbridos que tengan más en cuenta el contexto como elemento verificador.

5. Conclusiones

La conclusión principal a la que se ha llegado es que, si tenemos suficientes noticias clasificadas, seremos capaces de construir un modelo capaz de predecir, con gran exactitud, si una nueva noticia pertenece a una clase u otra. Sin embargo, debido a la constante evolución de los contenidos falsos, probablemente, esto no permitirá, por sí solo, determinar con mucha certeza si es falsa o no.

En relación con futuros avances, un elemento que podría tener bastante repercusión sería la creación de un conjunto de datos de gran tamaño, disponible, multilingüe, actualizado y fiable. Esto permitiría hacer comparaciones entre distintos estudios y avanzar en la dirección correcta.

Otra posible vía de estudio sería investigar la posibilidad de utilizar modelos preentrenados de lenguaje en varios idiomas en el modelo, de forma que permitieran utilizar algoritmos de detección sobre plataformas multilingües.

Por último, dada la velocidad de propagación de las *fake news* en las plataformas en línea y redes sociales, podría ser interesante que estas contaran con mejores elementos de trazabilidad que permitieran detectar patrones de noticias falsas más fácilmente. Adicionalmente, dado que las noticias pueden saltar de una aplicación a otra, sería interesante que hubiera una mayor colaboración entre las distintas plataformas para implementar estrategias comunes de control y mitigación.

Como conclusión final, una reflexión. Si al final se consiguiese y se implantase un sistema de catalogación automática de noticias falsas para reducir el nivel de desinformación de la sociedad, ¿quién decidiría lo que es verdad?, ¿una máquina basándose en los datos?, ¿qué datos y quién se los daría?

Referencias

UCM. (2020). Las *fake news* siempre han existido, peros hoy en día se han visto catapultadas por las redes sociales. *Oficina de transferencia de resultados de investigación*. Disponible en: https://www.ucm.es/otri/noticias-las-fake-news-siempre-han-existido-pero-hoy-en-dia-se-han-visto-catapultadas-por-las-redes-sociales

Fundación Telefónica. (2023). Fake News. La fábrica de mentiras. *Espacio*. Disponible en: https://espacio.fundaciontelefonica.com/evento/fake-news-la-fabrica-de-mentiras/

Page, M. J. *et al.* (2023). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* 2021;372:n71. Disponible en: https://www.bmj.com/content/bmj/372/bmj.n71.full.pdf

Rodríguez-Sedano, F. J. (2019). Uso de herramienta on-line Parsifal para la elaboración de una revisión sistemática de la literatura (SLR). *Zenodo*. Disponible en: https://zenodo.org/records/2603914

Zhou, X. y Zafarani, R. (2018). Fake News: A Survey of Research, Detection Methods, and Opportunities. Association for Computing Machinery. Disponible en: https://arxiv.org/pdf/1812.00315v1.pdf

Johnson, J., Ramakrishna Murty. M. y Navakanth I. (2023). A detailed review on word embedding techniques with emphasis on word-2vec. *Springer Nature*. Disponible en: https://doi.org/10.1007/s11042-023-17007-z.

Géron, A. (2019). *Hands-on Machine Learning with Scikit-Learn, Keras & TensorFlow*. O'Reilly. Segunda edición.

Madhavan, S. y Jones, M.T. (2024). Deep learning architectures. *IBM Developer*. Disponible en: https://developer.ibm.com/articles/cc-machine-learning-deep-learning-architectures/

Abedalla, A. (2020). A Closer Look at Fake News Detection: A Deep Learning Perspective. En: *Proceedings of the 3rd International Conference on Advances in Artificial Intelligence*. Istanbul, Turkey.

Análisis y evaluación de sistemas basados en IA para la detección de Fake News en español / inglés. Una revisión sistemática de literatura.

Universidade Vigo

Autor: José Manuel Martínez Sánchez
Directores: Milagros Fernández Gavilanes, Luis M. Álvarez Sabucedo

Introducción

Fake news → desinformación → beneficio
Internet → fácil y rápidas → amenaza
Agencias información → incapaces verificar
Personas → confían → redes sociales
Combatirlas → automática → IA (ML y NLP)
Muchos enfoques → revisión → orientación

Objetivos

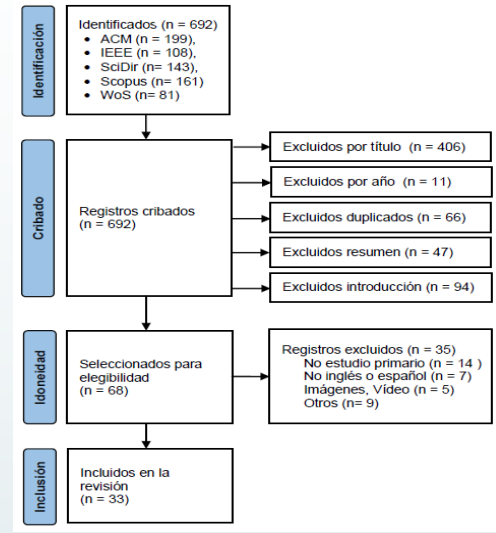
Facilitar visión de usos de IA en detección de fake news en español/ inglés: técnicas y resultados.

- ❖PI1.¿Cuáles son las áreas de la IA con aplicación en la detección de fake news?
- ❖PI2.¿Qué técnicas se están usando en la detección de fake news y con qué resultados?
- ❖PI3.¿Qué retos y limitaciones se están encontrando en la detección de fake news?

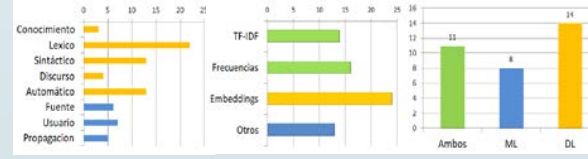
Metodología

Revisión sistemática de literatura:
Metodología PRISMA, con Parsifal y ChatPDF.
Criterios de elegibilidad:
Estudios primarios científicos sobre el tema.
Búsqueda de información:
Bibliotecas digitales: ACM Digital Library, IEEE Xplore, Science Direct, Scopus y WoS.
Selección:
Parsifal, duplicados y aplicación criterios.
Extracción de datos:
Excel, ChatPDF batería preguntas y lectura:
Evaluación de Calidad: Preguntas y baremo.

Resultados



- ❖R. PI1. Todos estudios: NLP (extracción características) y ML. Enfoques contenido y contexto. Dominio de léxico y sintaxis. También automáticos extracción mediante DL.
- ❖R. PI2. Técnicas NLP: TF-IDF y otras frecuencias *Embeddings*. ML: Predominio de DL. Más usadas redes neuronales recurrentes y redes profundas. Casos combinación ML y DL. Buenos resultados: *Accuracy* y F1 > 0,90. Posible *overfitting*.
- ❖R. PI3. Reto: Modelos híbridos tengan en cuenta contexto. Limitación: Falta de datos actualizados por rapidez fake news.



Conclusiones

Con suficientes noticias etiquetadas podremos crear modelos que clasifiquen con exactitud, pero debido a rápida evolución, probablemente no podamos detectarlas con mucha certeza.
Si se implantase un modelo de detección de fake news, ¿Quién diría lo que es verdad? ¿Quién facilitará los datos a las máquinas?

Retos

- ✓Creación de un conjunto de datos de gran tamaño, disponible, multilingüe, actualizado y fiable que permitiera hacer estudios y compararlos entre sí.
- ✓Utilizar modelos preentrenados en varios idiomas para crear plataformas de detección multilingües.
- ✓Mejorar la trazabilidad de las redes sociales y la colaboración para definir estrategias comunes.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

El análisis de *malware* en redes corporativas aisladas

Autor: Otero Díaz, Iván (i.otero@mde.es)
Director: Álvarez Sabucedo, Luis (externo.lsabucedo@cud.uvigo.es)

Resumen – El trabajo propone un enfoque integral para fortalecer la ciberdefensa en las Fuerzas Armadas, centrado en la implementación de una Plataforma de Análisis Controlado de Amenazas, sustentado en un análisis multimotor que dé servicio a las redes de trabajo acreditadas y aisladas.

El sistema propuesto integra la capacitación del personal, un eficiente mecanismo de reporte de alertas semiautomático y un sistema de cuarentena y análisis para mejorar la detección temprana de amenazas. La participación de los usuarios de la red como sensores humanos distribuidos en la gestión proactiva de artefactos sospechosos constituirá una capa adicional de seguridad de las redes de trabajo acreditadas.

La evaluación de la reputación de archivos basada en las interacciones de nuestro personal se convierte en un criterio clave, aprovechando la cantidad de reenvíos y las detecciones de los diferentes motores de *antimalware* comerciales. Además, el sistema recopila y presenta reportes de análisis de múltiples fuentes, proporcionando una visión colectiva de las amenazas en el ámbito de usuario y también específicos para los administradores de seguridad. Adicionalmente, archiva de forma segura los archivos sospechosos anteriores y es capaz de informar cuando existen cambios en la evaluación de la amenaza debidos a la actualización de las firmas de detección.

Este enfoque integral pretende constituirse en una estrategia efectiva para mejorar la defensa digital de las redes operacionales militares aprovechando la proactividad de los usuarios y los avances tecnológicos para enfrentar amenazas en constante evolución. Todo ello, sin comprometer su acreditación ni el aislamiento que tan efectivo ha demostrado ser para defender infraestructuras digitales,.

Palabras clave – Ciberdefensa, Análisis multimotor, Concienciación, Redes aisladas, *Malware*.

1. Introducción

La creciente digitalización de la sociedad ha llevado a una interconexión generalizada, desde dispositivos cotidianos hasta entornos corporativos. Este fenómeno también ha exacerbado las amenazas cibernéticas, con el *malware* siendo una de las principales preocupaciones. Los costos asociados con los ataques de *malware* son significativos, con pérdidas económicas y daño a la reputación corporativa.

El ámbito militar, en particular, enfrenta desafíos únicos, donde la resiliencia de las Fuerzas Armadas ante ataques cibernéticos es crítica para la defensa nacional. Se destaca la importancia de la concienciación y capacitación del personal militar para detectar amenazas en sus redes corporativas, pero aún se carece de un mecanismo de alerta global eficiente.

El trabajo propone una solución integral, la «Plataforma de Análisis Controlado de Amenazas», que se basa en el capital humano para la detección temprana de amenazas cibernéticas. Se aborda la colaboración, diversidad de enfoques y tecnologías avanzadas como fundamentales para enfrentar las amenazas digitales. El sistema propuesto incluye un análisis multimotor, reporte de alertas, cuarentena y análisis automático de archivos sospechosos, así como un sistema de evaluación de reputación y reportes de análisis comprensibles.

La metodología empleada es la de casos de uso, desglosando el proceso en componentes manejables y facilitando la comprensión de las interconexiones y dependencias del sistema. Se aborda la problemática de las redes corporativas aisladas y acreditadas, con un análisis profundo de las medidas de protección actuales.

2. Marco actual

Desde los primeros días de la era digital, ha habido programadores y entusiastas que, impulsados por la curiosidad, intereses económicos o el deseo de notoriedad, exploran las capacidades avanzadas y alternativas de la tecnología. La crónica del *malware* comienza con el gusano Morris en 1988, programado por Robert Tappan Morris. Aunque inicialmente inocente, el gusano se propagó incontrolablemente, marcando un hito al demostrar que los programas informáticos podían convertirse en armas silenciosas.

La década de los noventa estuvo marcada por la proliferación de virus y troyanos, como «Melissa,» «CIH» («Chernobyl») y «ILOVEYOU,» causando estragos en sistemas y redes a nivel mundial. Con el nuevo milenio, surgieron amenazas como los gusanos «Blaster» y «Sasser,» aprovechando vulnerabilidades en Windows, junto con *malware* de naturaleza económica y el auge del *ransomware*, destacando casos como «WannaCry»

y «NotPetya.» Mientras estas amenazas conocidas proliferaban, las Amenazas Persistentes Avanzadas (APT) operaban en las sombras, desarrollándose con motivaciones políticas o para obtener información con fines militares. Ejemplos, que hoy en día conocemos, incluyen «Stuxnet» y «Duqu», diseñados para desestabilizar programas estatales de naciones con intereses contrarios.

Si bien el futuro presenta desafíos adicionales con la proliferación de la inteligencia artificial, el internet de las cosas (IoT) y la computación cuántica, también ofrece oportunidades para mejorar las defensas cibernéticas, ya que la historia del *malware* ha demostrado que el ingenio humano despunta tanto en la creación como en la destrucción de sistemas informáticos y los documentos que contienen.

En el ámbito de la seguridad cibernética corporativa, los Centros de Operaciones de Seguridad (COS) juegan un papel crucial. Los servicios *antimalware* de un COS se centran en el análisis de *malware* y el análisis forense, desempeñando un papel vital en la identificación y prevención de ataques en redes corporativas extensas.

El análisis de *malware*, a cargo de expertos altamente especializados, implica descomponer ejecutables para comprender sus objetivos y métodos. Dada la escasez de estos profesionales, se destaca la necesidad de implementar sistemas de triaje para optimizar su tiempo. El análisis forense digital, por otro lado, se centra en recopilar y analizar evidencia digital en caso de incidentes de seguridad, contribuyendo a la atribución de ataques y proporcionando inteligencia valiosa.

En estas redes, masivas, la concienciación de los usuarios se revela como un eslabón crucial, ya que, a menudo, son el objetivo más fácil de atacar y por ello se propone un enfoque de «sabiduría colectiva», promoviendo la responsabilidad compartida y recompensando a aquellos que contribuyen a la detección de amenazas. La formación continua y estrategias como la gamificación pueden mejorar la eficacia de estos usuarios, a la vez que fomentan la colaboración y el compromiso con la organización.

La resiliencia de la red, especialmente en contextos militares, se vuelve crítica para mantener operativas las funciones de mando y control, incluso en medio de ciberataques. Se destaca la importancia de liderazgo efectivo y programas de concienciación específicos para líderes cercanos junto con la gestión de la inteligencia corporativa, ya que plantea desafíos en el intercambio de información sobre amenazas digitales entre corporaciones. Se sugiere un enfoque de «Zero Trust» para gestionar los riesgos asociados con el intercambio de inteligencia.

La fusión de datos y la generación de inteligencia son esenciales en redes corporativas extensas. A lo largo del trabajo se propone un repositorio

común tipo «Data Lake», para garantizar la consistencia y accesibilidad de datos, mejorando la colaboración entre Centros de Operaciones de Seguridad, ya que la lucha contra el *malware* y las amenazas cibernéticas requiere de un enfoque holístico que involucre tanto la tecnología como la inteligencia humana, destacando la importancia de la colaboración, la concienciación y la innovación constante.

3. Estado del arte

Garantizar la seguridad de la información es de una importancia crítica en entornos corporativos. En el documento se trata específicamente de los problemas inherentes a las redes aisladas y acreditadas que son comúnmente utilizadas por ministerios y grandes organizaciones públicas. Estas redes se caracterizan por estar completamente desconectadas, tanto física como lógicamente, de otras redes, especialmente de Internet. La transferencia de datos en estos entornos se realiza a través de medios aislados y altamente controlados.

La relevancia de la seguridad de la información es especialmente relevante cuando los datos son considerados activos extremadamente valiosos. Las redes aisladas se presentan como fundamentales para la estrategia de seguridad de grandes empresas, ya que ayudan a reducir significativamente el riesgo de ataques externos y son esenciales para mantener la confidencialidad de la información sensible. Pero no solo se debe abordar el peligro de las amenazas externas, sino también de las internas.

Se sugieren, por tanto, políticas como la segregación lógica y el control de acceso para hacer frente a amenazas provenientes de dentro de la organización. Además, se destaca la importancia del análisis de riesgos en todo el ciclo de vida de la seguridad, y se resalta la necesidad de contar con personal altamente especializado en seguridad y administración de sistemas.

En cuanto a las herramientas de seguridad, se hace un estudio somero de las familias más habituales, desde antivirus y *antimalware* hasta sistemas de detección de intrusiones. Cabe señalar la evolución de la industria antivirus hacia soluciones basadas en la nube y que, a pesar de las ventajas de estas tecnologías, muy útiles para los usuarios domésticos, no satisfacen las necesidades ministeriales ni son capaces de cumplir con los desafíos específicos asociados con su implementación en redes acreditadas. Por ejemplo, la exigencia actual de contar en estas redes con Sistemas de Información y Gestión de Eventos de Seguridad (SIEM) o con soluciones de Detección y Respuesta Extendida (XDR) en la operación segura de un sistema, ponen de manifiesto la dificultad potencial de implementar soluciones puramente comerciales, ya que, prácticamente todas, están basadas en la nube.

En la tabla 1 se puede ver un cuadro resumen comparativo de las diferentes herramientas de seguridad para ayudar en la toma de decisiones.

Redes acreditadas y aisladas	Detección proactiva	Incorpora IA	Usabilidad	Impacto rendimiento	Escalabilidad	Aislado	Colaboración Multifabricante	Interfaz e Informes	Actualizaciones Automáticas en Aislado	Costo total de Propiedad
Antivirus local			x	x	x					x
HIDS			x	x	x					x
NIDS			x	x	x					x
SIEM/XDR	x	x					x			x
ADA	x	x			x	x	x	x		x
Plataforma de Análisis Controlado de Amenazas	x		x		x	x	x	x	x	x

Tabla 1. Comparativa de familias de herramientas frente a los criterios de evaluación seleccionados

Por ello se aborda la generación de una plataforma para el análisis controlado de amenazas, brindando una visión más completa de cómo abordar los desafíos de seguridad en estos entornos específicos.

4. Modelo propuesto

El sistema propuesto se basa en una infraestructura de máquinas virtuales con diferentes motores antivirus comerciales y un motor basado en reglas YARA para análisis forense interno. Se destaca la importancia de adherirse a estándares de seguridad y privacidad en entornos aislados acreditados.

4.1 Casos de uso

Para su mejor comprensión se define la Plataforma de Análisis Controlado de Amenazas a través de casos de uso y un esquema UML del mismo. Esta plataforma permitiría a usuarios autorizados en la red a proteger analizar archivos sospechosos sin conexión a internet, utilizando un sistema multimotor y contemplando todo el proceso, desde la identificación del archivo sospechoso hasta la presentación de resultados al usuario.

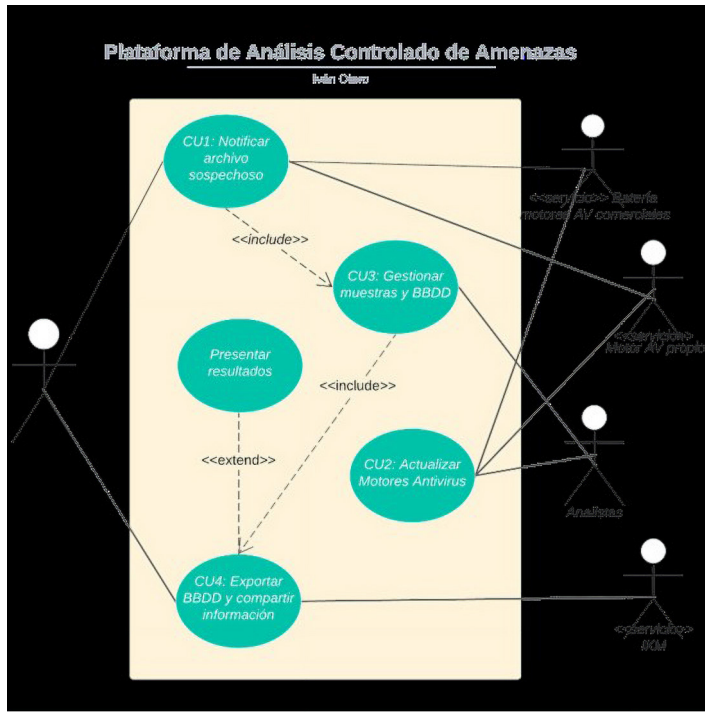


Figura 1. Diagrama de Casos de Uso

Casos de Uso:

CU1. Notificar archivo sospechoso:

- Descripción: usuarios envían archivos sospechosos para su análisis y reciben resultados a través de una interfaz web en intranet.
- Actores: usuario de la Red, Plataforma de Análisis Controlado de Amenazas.
- Flujo del proceso: desde la identificación del archivo sospechoso hasta la presentación de resultados y acciones del usuario.

CU2. Actualizar Motores Antivirus:

- Descripción: proceso automático para mantener actualizados los motores antivirus, garantizando la seguridad de la red.
- Actores: Sistema Automático de Actualización, proveedor de antivirus.
- Flujo del proceso: actualización, pausa, clonación, transferencia a la red interna.

CU3. Gestionar muestras y bases de datos:

- Descripción: gestión de bases de datos internas para evitar reanálisis innecesarios y alertar sobre posibles amenazas.
- Actores: bases de datos, analistas de *malware* y forenses, usuarios Iniciales.

— Flujo del proceso: prevención de reanálisis, registro de usuarios y muestras, alertas y análisis manual.

CU4. Exportar bases de datos y compartir información:

— Descripción: exportación de bases de datos de *malware* detectadas para alimentar sistemas en otras redes, incluyendo un motor antivirus propio.

— Actores: bases de datos, motor antivirus propio.

— Flujo del proceso: generación del motor antivirus propio, exportación de bases de datos.

4.2 Modelo de implementación

Por último, se proponen algunas posibles tecnologías actuales que podrían conformar los elementos básicos del sistema, sin pretender que estas propuestas sean definitivas o exclusivas y pudiendo adaptarse a otras necesidades u otras tecnologías preexistentes en los sistemas a proteger. La plataforma, por tanto, es adaptable, y está diseñada para redes aisladas, siguiendo estándares de seguridad y privacidad

— **Virtualización:** vSphere, EXSi, vCenter.

— **Sistemas operativos:** Windows Server, Windows 10.

— **Seguridad:** Diodos certificados.

— **Base de datos:** MongoDB.

— **Presentación de datos:** Power BI Server.

— **Motor antivirus propio:** Yara.

5. Conclusiones

En el documento se aborda la complejidad de la ciberseguridad, centrándose en las amenazas APT (Amenazas Persistentes Avanzadas) y la necesidad de adaptarse a la evolución tecnológica. Se destaca que las tecnologías emergentes, como la inteligencia artificial, el internet de las cosas y la computación cuántica, presentan desafíos adicionales para la ciberdefensa, a la vez que se enfatiza que la protección contra amenazas requiere un enfoque proactivo, combinando la innovación tecnológica con principios de seguridad sólidos. La importancia del factor humano, abogando por la concienciación, formación continua y la creación de una cultura de trabajo basada en la seguridad es esencial para afrontar las amenazas presentes y, con toda probabilidad, las futuras.

Se introduce, a nivel conceptual, un sistema de ciberdefensa que utiliza un enfoque multimotor, combinando soluciones antivirus de diferentes fabricantes y aprovechando la inteligencia colectiva del personal para alimentarlo de muestras que son sospechosas a los ojos de personal concienciado. La creación de un motor antivirus propio basado en firmas YARA

de producción propia se destaca como una ventaja adicional a la batería de productos comerciales.

Se concluye que el sistema propuesto no solo cumple con los estándares de seguridad y confidencialidad de las redes de trabajo acreditadas, sino que transforma el capital humano en una fortaleza. Se sugieren líneas de investigación futuras, como la evaluación militar de mitigaciones comerciales y la creación de un servicio de análisis de amenazas compartido entre varios departamentos ministeriales.

Esta propuesta se ha enfocado en remarcar la importancia de la ciberseguridad, destacando la necesidad de adaptarse a las amenazas emergentes y la colaboración a dos niveles, el humano y el corporativo, como clave para fortalecer las defensas digitales.

El Análisis de Malware en Redes Corporativas Aisladas

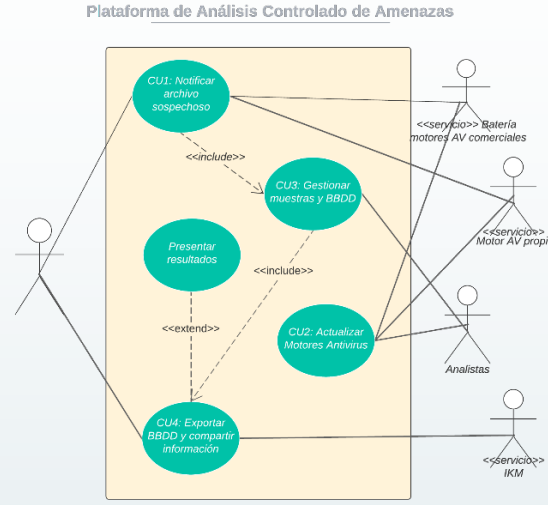
Autor: Iván Otero Díaz
Director: Luis Álvarez Sabucedo

La creciente digitalización de la sociedad ha llevado a una interconexión generalizada, desde dispositivos cotidianos hasta entornos corporativos que ha derivado en el crecimiento desmedido de las amenazas cibernéticas. De entre estas, el malware es una de las principales preocupaciones.

Los costos asociados con los ataques de malware son significativos tanto a nivel económico como reputacional. En el ámbito militar, en particular, debemos añadir que su capacidad de resiliencia ante ataques cibernéticos es crítica para la defensa nacional. Por ello, las redes dedicadas al planeamiento operativo siempre han estado protegidas y su principal modo de defensa ha sido el aislamiento.

Problemática actual

Es en este tipo de redes, protegidas con procedimientos escrupulosos de acceso, bastionadas con políticas estrictas de software y con hardware específicamente acreditado dónde implantar nuevas medidas de seguridad se hace extremadamente difícil pero necesario frente al auge del número de amenazas.
Si bien podrían identificarse más retos a superar a la hora de defender estas redes operativas y asegurar la continuidad de sus funciones, el trabajo se ha centrado en tres.
Los usuarios: Desde hace décadas se les culpa de ser el eslabón más débil de los sistemas y el que más superficie de ataque presenta. Para ellos se generan campañas de concienciación y cursos específicos con el objetivo de mitigar su vulnerabilidad intrínseca.
Los analistas de seguridad: Personal altamente especializado y escaso cuya formación es costosísima en tiempo y que se ve, en muchos casos, arrollada por la cantidad de incidentes.
Las compañías de software de seguridad: La mayoría de sus clientes son particulares o PYMES que no necesitan tanta protección. Sus modelos de negocio están evolucionando hacia servicios en nube que no se adaptan a las necesidades de redes que trabajen con información clasificada.



Solución

El trabajo propone una solución integral que mitigue el impacto de los tres retos señalados con la creación de una "Plataforma de Análisis Controlado de Amenazas" que incluye un análisis multi-motor, reporte de alertas, cuarentena y análisis automático de archivos sospechosos, así como un sistema de evaluación de reputación y reportes de análisis comprensibles.
Este sistema, que funciona como un servicio añadido en la red aislada que protege, se basa en el capital humano y las inversiones en su concienciación para la detección temprana de amenazas. Convirtiendo así, a los usuarios, en una nueva capa de protección proactiva.
Proporciona un sistema de triaje y automatiza muchas de las tareas que lleva a cabo el grupo de analistas. Además, presta múltiples funcionalidades dirigidas a la visualización de datos que ayuden a la toma de decisión informada y a la colaboración con otros equipos de respuesta a incidente.
El sistema multi-motor de análisis automático gracias a sus actualizaciones diarias automáticas basa su potencia en el conocimiento de múltiples fabricantes de soluciones comerciales, pero sin hacer uso de sus tecnologías de nube.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Empleo de la infraestructura hiperconvergente en la creación del nodo FMN de CGMAD

Autor: Piñero Vilela, Óscar (opinvil@fn.mde.es)
Directores: Ares Tarrío, Miguel Ángel y Troncoso Pastoriza, Francisco Manuel (externo.miguelares@cud.uvigo.es / ftroncoso@cud.uvigo.es)

Resumen – Este TFM analiza la implementación de una infraestructura hiperconvergente (HCI) en el nodo FMN (Federated Mission Networking) del Cuartel General Marítimo de Alta Disponibilidad de la Armada española (CGMAD). El objetivo principal es evaluar las ventajas y desafíos de adoptar soluciones HCI frente a modelos tradicionales y convergentes en el ámbito del Ministerio de Defensa.

La metodología empleada incluye una revisión exhaustiva de la literatura sobre HCI, un análisis comparativo de las principales soluciones del mercado y un estudio detallado del proceso de implementación en el CGMAD. Se utiliza la metodología PMBOK para la gestión del proyecto, estructurando la implementación en fases de iniciación, planificación, ejecución, monitoreo y cierre.

Los resultados muestran que la solución HCI de HPE SimpliVity fue seleccionada por su compatibilidad con la infraestructura existente, la experiencia previa del personal y la optimización de recursos. La implementación se completó en sesenta días laborables, abordando desafíos como incompatibilidades de *hardware* y problemas de rendimiento.

Se concluye que la adopción de HCI en el CGMAD ha mejorado la eficiencia operativa, la escalabilidad y la gestión de recursos de TI. Sin embargo, se identificaron retos como los altos costes iniciales y la necesidad de formación especializada. El trabajo proporciona recomendaciones para futuras investigaciones, incluyendo la integración de inteligencia artificial y la optimización para cargas de trabajo específicas en entornos HCI.

Palabras clave – Hiperconvergencia, Gestión de proyectos PMBOK, HPE SimpliVity, FMN (Federated Mission Networking), HCI (Infraestructura Hiperconvergente).

1. Introducción

1.1 Contexto y motivación

La infraestructura de Tecnologías de la Información (TI) ha experimentado una evolución significativa en las últimas décadas, pasando de modelos tradicionales basados en sistemas de almacenamiento y servidores independientes a soluciones más integradas y eficientes, como la HCI. La adopción de HCI ha demostrado ser una alternativa viable y ventajosa en comparación con los modelos tradicionales y convergentes, especialmente en términos de eficiencia, escalabilidad y reducción de costes.

En el contexto empresarial actual, las organizaciones enfrentan desafíos cada vez mayores para mantenerse competitivas y responder a las demandas cambiantes del mercado. La gestión eficiente de los recursos de TI se ha convertido en un factor crítico para el éxito de las empresas, ya que la infraestructura de TI es fundamental para soportar y habilitar las operaciones del negocio. En este sentido, la adopción de soluciones HCI puede proporcionar a las organizaciones una ventaja competitiva al permitirles optimizar sus recursos de TI y mejorar la eficiencia en el desarrollo y la gestión de proyectos.

La motivación para abordar este tema radica en la creciente importancia de la HCI en el ámbito empresarial y la necesidad de comprender y evaluar sus ventajas y desventajas en comparación con los modelos tradicionales y convergentes. Además, el análisis de proyectos realizados siguiendo estos diferentes modelos de infraestructura permitirá una evaluación más completa y fundamentada de la conveniencia de adoptar soluciones HCI en diferentes contextos empresariales.

1.2 Objetivo

El objetivo principal de este TFM es analizar y comparar las ventajas y desventajas de adoptar soluciones de HCI frente a modelos tradicionales y convergentes en el ámbito del Ministerio de Defensa y más concretamente en el CGMAD. Para ello, se llevará a cabo una valoración desde el punto de vista de la dirección del proyecto, considerando aspectos clave, como los costes (humanos, equipamiento, licencias, etc.), riesgos y eficiencia en el desarrollo de proyectos de TI.

Este análisis permitirá a los profesionales y responsables de la toma de decisiones en el ámbito de las tecnologías de la información comprender mejor las implicaciones de adoptar soluciones HCI en sus organizaciones y evaluar si esta opción es adecuada para sus necesidades y objetivos específicos. Además, se espera que los resultados de este TFM contribuyan al conocimiento académico y práctico en el campo de la dirección de proyectos de TI y la gestión de infraestructuras de TI.

2. Desarrollo

Tras realizar un amplio análisis sobre el estado del arte de la HCI, en el trabajo se proporciona una visión integral y actualizada de lo que es la HCI. La infraestructura de TI ha evolucionado significativamente (figura 1), pasando de modelos tradicionales a convergentes y finalmente a hiper-convergentes. La HCI combina computación, almacenamiento y redes en una única solución definida por *software*, ofreciendo una mayor eficiencia, flexibilidad y escalabilidad en comparación con los modelos anteriores.

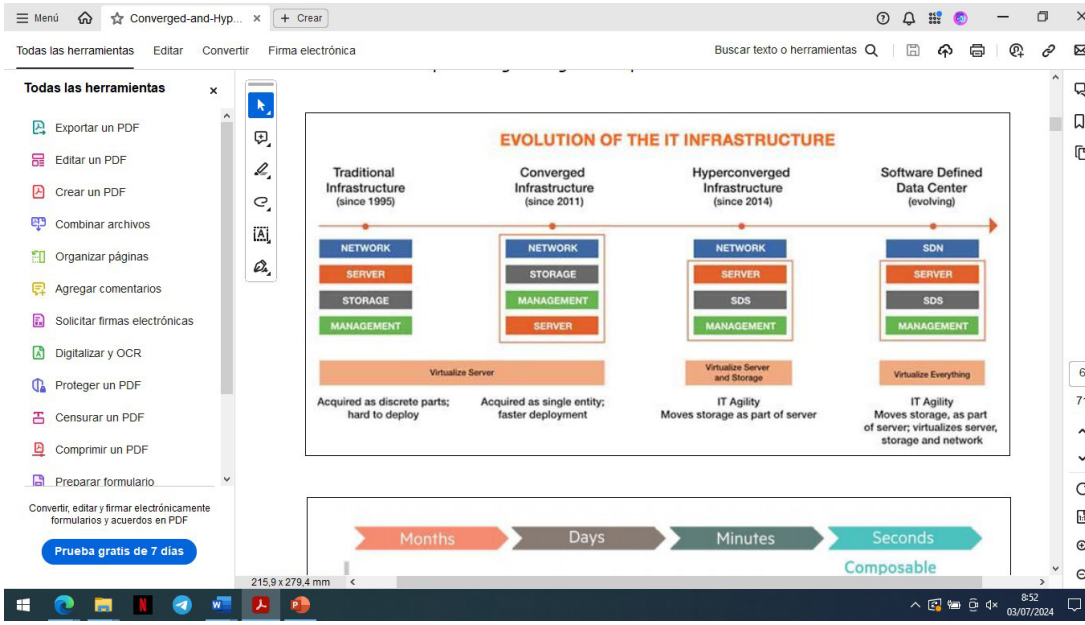


Figura 1. Evolución de la infraestructura de TI

La adopción de HCI proporciona múltiples beneficios, incluyendo una gestión simplificada, reducción de costes operativos y de capital, y una mejora en la eficiencia operativa. La integración de todos los recursos en una única plataforma permite una administración centralizada, reduciendo la complejidad y el riesgo de errores humanos.

A pesar de sus ventajas, la HCI también presenta desafíos como los altos costes iniciales de implementación y el riesgo de dependencia de un único proveedor (Vendor Locking). Es crucial evaluar cuidadosamente estos aspectos antes de adoptar una solución HCI para asegurar que se alinea con las necesidades y objetivos de la organización.

El mercado de HCI, analizado en el informe *The Forrester Wave™: Hyperconverged Infrastructure, Q4 2023* (figura 2) (Forrester, 2023), está dominado por varias empresas líderes, incluyendo Nutanix, VMware, HPE, Cisco y Dell EMC. Cada una ofrece soluciones con características distintivas que responden a diferentes necesidades y escenarios de uso, destacándose por su capacidad de innovación y ejecución en el mercado.

Vendor	Product evaluated
Cisco	Cisco HyperFlex Systems
Hewlett Packard Enterprise	HPE SimpliVity
Huawei	Huawei FusionCube 1000, FusionCube 500
IBM	IBM Storage Fusion HCI
IEIT SYSTEMS	IEIT SYSTEMS InCloud Rail
Microsoft	Microsoft Azure Stack HCI
Nutanix	Nutanix Cloud Platform
Sangfor Technologies	Sangfor HCI — Hyper Converged Infrastructure
Scale Computing	Scale Computing SC//Platform (SC//HyperCore, SC//Fleet Manager)
SmartX	SmartX HCI
VMware	VMware vSAN

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figura 2. Proveedores evaluados e información sobre productos

Existen diversas opciones de despliegue de HCI, que incluyen productos de *software* HCI, productos de *hardware* HCI y productos HCI integrados (*hardware* y *software*). La elección de la opción adecuada depende de factores como la infraestructura existente, la experiencia del equipo de TI, los requisitos de escalabilidad y los costes operativos a largo plazo.

3. Resultados y discusión

El proyecto se enmarca en la creación de un nodo laboratorio FMN para el CGMAD y el objetivo principal es implementar una HCI que permita albergar servicios CORE y COI, cumpliendo con los requisitos establecidos por el comité FMN. Esta implementación es crucial para la participación de España en ejercicios de Verificación, Validación y Confirmación (V2CN) dentro del marco FMN, asegurando la interoperabilidad con otros nodos y sistemas de la red FMN.

Tras un análisis comparativo de diferentes soluciones HCI (Nutanix Prism, HPE SimpliVity y Dell EMC VxRail), se optó por la solución HPE SimpliVity. Esta elección se basó en varios factores clave, incluyendo la compatibilidad con la infraestructura existente, la experiencia previa del personal técnico con la tecnología HPE SimpliVity y la coherencia con otros nodos HCI ya implementados en el ámbito del Ministerio de Defensa.

El proyecto se estructuró en seis fases principales, empleando la metodología PMBOK (figura 3), con una duración total estimada de sesenta días laborables: Iniciación y Planificación; Diseño y Adquisición; Implementación; Pruebas y Optimización; Formación y Documentación, y

Cierre. Se estableció un equipo multidisciplinario que incluía un jefe de proyecto, arquitectos de sistemas, ingenieros especializados en virtualización y redes, y especialistas en seguridad informática y gestión del cambio. La planificación detallada incluyó la identificación de riesgos potenciales y estrategias de mitigación.

Figura 3. Ciclo de vida del proyecto según PMBOK

La implementación siguió un enfoque metódico que abarcó la preparación del entorno físico, la configuración inicial del *hardware*, la implementación del *software* HCI, la configuración de redes y seguridad, y la migración de datos y aplicaciones.

Se realizaron pruebas exhaustivas para garantizar el correcto funcionamiento y cumplimiento de los estándares de seguridad y rendimiento. Estas incluyeron pruebas de funcionalidad, rendimiento, seguridad, integración, y validación de *backup* y recuperación. Se utilizaron herramientas específicas como VMware vSphere Performance Monitoring Tools y HCIbench para evaluar el rendimiento del sistema. Además, se llevaron a cabo auditorías de seguridad y pruebas de compatibilidad FMN para asegurar el cumplimiento de los requisitos establecidos.

Por motivos de confidencialidad del proyecto, no se incluye en este documento la composición de la infraestructura, ofertas recibidas de fabricantes y proveedores, análisis de riesgos, detalle de las tareas del proyecto o los problemas identificados y las soluciones adoptadas. Toda esa información se encuentra recogida en la memoria del TFM.

4. Conclusiones

La implementación del nodo hiperconvergente HCI de CGMAD ha sido un proyecto ambicioso y complejo que ha requerido una planificación meticulosa y una ejecución precisa. A lo largo de este trabajo se han abordado diversos aspectos técnicos, económicos y operativos para garantizar el éxito de la implementación. La solución HPE SimpliVity ha demostrado ser altamente efectiva en este aspecto, al permitir una gestión centralizada y simplificada de la infraestructura. La capacidad de agregar nodos

adicionales de manera sencilla y sin interrupciones ha permitido adaptar la infraestructura a las necesidades cambiantes de la organización.

La consolidación de recursos en una única plataforma ha reducido la necesidad de *hardware* y *software* separados, disminuyendo los costes operativos. Además, la gestión simplificada ha permitido una asignación más eficiente de los recursos humanos, reduciendo el tiempo y esfuerzo necesarios para administrar y mantener la infraestructura. Las sesiones de formación especializadas han asegurado que el equipo técnico esté bien preparado para gestionar y mantener la nueva infraestructura. La documentación detallada y los procedimientos operativos desarrollados han proporcionado una base sólida para la gestión diaria y la resolución de problemas.

La importancia de una planificación detallada y una gestión de riesgos efectiva ha sido destacada, así como la necesidad de una comunicación constante y efectiva con todas las partes interesadas. La experiencia adquirida durante este proceso será muy valiosa para futuras implementaciones y actualizaciones del sistema. La adopción de HCI ha proporcionado una base sólida para futuras expansiones y actualizaciones, asegurando que la infraestructura de TI pueda seguir soportando las operaciones críticas.

La adopción de una HCI conlleva implicaciones significativas en cualquier organización. En términos de eficiencia operativa, HCI simplifica la gestión al integrar computación, almacenamiento y redes en una única solución, reduciendo la complejidad y el riesgo de errores. Ofrece mayor escalabilidad y flexibilidad, permitiendo ajustar recursos según las necesidades.

Aunque la implementación inicial puede ser costosa, a largo plazo puede reducir gastos operativos y de capital. HCI facilita la integración con soluciones de nube híbrida, mejorando la flexibilidad y resiliencia.

La gestión centralizada simplifica la administración de TI, permitiendo una respuesta más ágil a las demandas del negocio. HCI mejora el rendimiento y la disponibilidad del sistema, crucial para operaciones continuas.

En cuanto a seguridad, centraliza la implementación de políticas, pero puede generar dependencia de un proveedor. El impacto en el personal de TI implica una posible reducción de necesidades especializadas, pero requiere actualización de habilidades para optimizar la nueva infraestructura.

Los próximos desafíos o líneas de investigación en el campo de la HCI pueden ser:

a) Integración de IA y ML en HCI.
b) Optimización del rendimiento para cargas de trabajo específicas.
c) Interoperabilidad y estándares abiertos.
d) Integración de HCI con la nube.

Referencias

NUTANIX. (2023, 8 agosto). What is Hyperconverged Infrastructure (HCI). Disponible en: https://www.nutanix.com/hyperconverged-infrastructure

CompuSoluciones. (2022, 4 abril). Hiperconvergencia, ¿qué es y qué beneficios tiene? Disponible en: https://www.compusoluciones.com/blog/convergencia-e-hiperconvergencia/

Kowalke, R. (2019). Enterprise Architecture Technical Brief: Converged and Hyper-Converged Infrastructure. *Virginia Information Technologies Agency (VITA).* Virginia.

VIP Enterprise WordPress. (2023). The Forrester Wave™: Hyperconverged Infrastructure, Q4 2023.

NATO (2021). FMN, FMN Spiral 4 Specification. *Supplement to the Final FMN Spiral 4 Specification.*

Project Management Institute. (2017). Guía del PMBOK. *PMI.*

El Análisis de Malware en Redes Corporativas Aisladas

Autor: Iván Otero Díaz
Director: Luis Álvarez Sabucedo

La creciente digitalización de la sociedad ha llevado a una interconexión generalizada, desde dispositivos cotidianos hasta entornos corporativos que ha derivado en el crecimiento desmedido de las amenazas cibernéticas. De entre estas, el malware es una de las principales preocupaciones.

Los costos asociados con los ataques de malware son significativos tanto a nivel económico como reputacional. En el ámbito militar, en particular, debemos añadir que su capacidad de resiliencia ante ataques cibernéticos es crítica para la defensa nacional. Por ello, las redes dedicadas al planeamiento operativo siempre han estado protegidas y su principal modo de defensa ha sido el aislamiento.

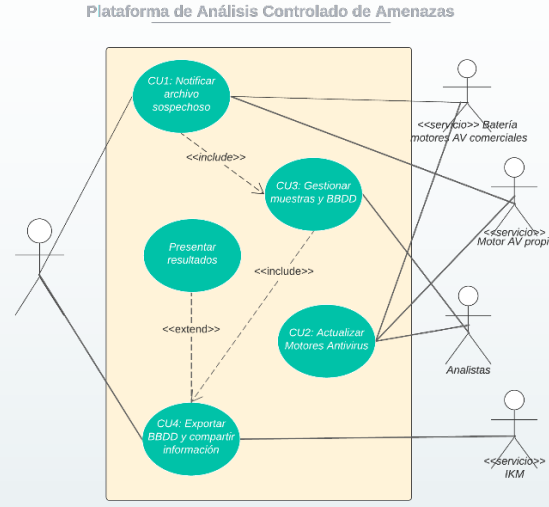
Problemática actual

Es en este tipo de redes, protegidas con procedimientos escrupulosos de acceso, bastionadas con políticas estrictas de software y con hardware específicamente acreditado dónde implantar nuevas medidas de seguridad se hace extremadamente difícil pero necesario frente al auge del número de amenazas.
Si bien podrían identificarse más retos a superar a la hora de defender estas redes operativas y asegurar la continuidad de sus funciones, el trabajo se ha centrado en tres.

Los usuarios: Desde hace décadas se les culpa de ser el eslabón más débil de los sistemas y el que más superficie de ataque presenta. Para ellos se generan campañas de concienciación y cursos específicos con el objetivo de mitigar su vulnerabilidad intrínseca.

Los analistas de seguridad: Personal altamente especializado y escaso cuya formación es costosísima en tiempo y que se ve, en muchos casos, arrollada por la cantidad de incidentes.

Las compañías de software de seguridad: La mayoría de sus clientes son particulares o PYMES que no necesitan tanta protección. Sus modelos de negocio están evolucionando hacia servicios en nube que no se adaptan a las necesidades de redes que trabajen con información clasificada.



Solución

El trabajo propone una solución integral que mitigue el impacto de los tres retos señalados con la creación de una "Plataforma de Análisis Controlado de Amenazas" que incluye un análisis multi-motor, reporte de alertas, cuarentena y análisis automático de archivos sospechosos, así como un sistema de evaluación de reputación y reportes de análisis comprensibles.
Este sistema, que funciona como un servicio añadido en la red aislada que protege, se basa en el capital humano y las inversiones en su concienciación para la detección temprana de amenazas. Convirtiendo así, a los usuarios, en una nueva capa de protección proactiva.
Proporciona un sistema de triaje y automatiza muchas de las tareas que lleva a cabo el grupo de analistas. Además, presta múltiples funcionalidades dirigidas a la visualización de datos que ayuden a la toma de decisión informada y a la colaboración con otros equipos de respuesta a incidente.
El sistema multi-motor de análisis automático gracias a sus actualizaciones diarias automáticas basa su potencia en el conocimiento de múltiples fabricantes de soluciones comerciales, pero sin hacer uso de sus tecnologías de nube.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Gemelo digital de entorno operativo marítimo: propuesta de arquitectura de integración de datos y operación

Autor: Ramírez Morán, Sergio (srammor@ea.mde.es)
Directores: Fernández Gavilanes, Milagros y Pérez Collazo, Carlos
(mfgavilanes@cud.uvigo.es / carlos.perez.collazo@cud.uvigo.es)

Resumen – El mundo experimenta la cuarta revolución industrial, marcada por tecnologías disruptivas como la inteligencia artificial, *big data*, el internet de las cosas, etc., habilitadoras del denominado gemelo digital, el cual, basándose en la disponibilidad de datos masivos sobre un determinado proceso o sistema, crea un modelo virtual del mismo capaz de proporcionar valiosa información del funcionamiento actual y futuro. En este contexto, instituciones meteorológicas y marítimas han reconocido el valor de datos y modelos predictivos abiertos para mejorar, entre otras, la planificación y operación marítima. Esta información, junto con la que las propias plataformas marítimas son capaces de generar, debidamente integradas mediante técnicas de inteligencia artificial y *big data*, constituyen una base prometedora para el desarrollo de un gemelo digital de un entorno marítimo operativo que permita a las plataformas disponer de una mayor consciencia situacional en su entrono de operaciones, lo que se traducirá en una mayor seguridad, efectividad y eficiencia en el cumplimiento de su misión. Sin embargo, las limitaciones de capacidad informática y comunicaciones en plataformas navales plantean desafíos. Para abordarlos, se plantea el diseño conceptual de una arquitectura de integración de datos que permita el desarrollo de ese gemelo digital y esté basada en tres niveles: un sistema central terrestre que crea y mantiene el gemelo digital, usando todas las fuentes disponibles; una plataforma naval que ejecuta un modelo local actualizado con datos propios, y plataformas desplegables que proporcionan información adicional. Asociadas a esta arquitectura se definen las estrategias de operación que permiten su funcionamiento.

Palabras clave – Gemelo digital oceánico, Entorno operativo marítimo, Operaciones marítimas, GIS.

1. Introducción

La cuarta revolución industrial, marcada por tecnologías disruptivas como inteligencia artificial (*IA*), *big data*, robótica e internet de las cosas (*IoT*), ha transformado las organizaciones a todos los niveles. En este contexto, instituciones oceanográficas y meteorológicas comparten abiertamente datos relevantes, aprovechables para diversas aplicaciones, incluida la planificación de misiones marítimas. Las plataformas navales, con sensores avanzados, generan datos en tiempo real, ofreciendo la oportunidad de mejorar la conciencia del entorno y las decisiones operativas. Para integrar todos estos datos y desarrollar modelos predictivos, se propone un sistema basado en *big data* e IA, creando un «gemelo digital» de condiciones marítimas y climatológicas. Sin embargo, la potencia necesaria para este modelo hace impracticable su instalación en plataformas navales, requiriendo la integración en centros de procesamiento de datos terrestres. Además, la limitación de ancho de banda en comunicaciones satelitales o de largo alcance complica la realimentación continua de datos al gemelo digital en entornos alejados de la costa. Resolver estas problemáticas implica analizarlas detenidamente, diseñar una arquitectura de integración de información y establecer una estrategia de operación para mejorar la eficacia, eficiencia y seguridad de las misiones marítimas.

1.1 Objetivos

Este TFM tiene como principal objetivo el diseño de una arquitectura conceptual de integración de datos que habilite el desarrollo, explotación y actualización de un gemelo digital de un entorno operativo marítimo. La arquitectura propuesta aborda las limitaciones en cuanto a capacidad informática instalable en plataformas navales y las limitaciones en las comunicaciones operativas que dificultan la realimentación de los datos al gemelo digital. Para ello, se propone una arquitectura por niveles. En un primer nivel existe un sistema central terrestre, con gran potencia de cómputo y comunicaciones, que crea y mantiene el gemelo digital usando todas las fuentes de datos disponibles. En el segundo nivel, la plataforma naval, que desplegará en escenarios operativos con comunicaciones limitadas, ejecutará un modelo local del gemelo digital actualizado con datos propios y datos proporcionados por el sistema central bajo petición. En el último nivel se situarían las plataformas desplegables desde el segundo nivel, que proporcionarán información adicional. Para optimizar la integración de la información y la operatividad de las plataformas en estos contextos operativos con limitaciones, se plantean una serie de estrategias de operación y se analizan los pros y contras de la solución propuesta. El modelo conceptual resultante podrá servir de marco de referencia para una futura implementación real.

1.2 Metodología

Para alcanzar los objetivos, se presenta, en primer lugar, un estudio del estado del arte de lo que es un gemelo digital y, en concreto, un gemelo

digital oceánico y los proyectos existentes relacionados. Se describen las fuentes de datos disponibles, tanto externas como propias, así como los formatos de datos y las posibilidades para el almacenamiento, gestión, intercambio y explotación de los mismos. Con base en todo lo anterior, se propone una arquitectura conceptual que se adapta al escenario mencionado, así como las estrategias de operación asociadas que permitan un aprovechamiento óptimo de la información disponible y que se traduzca en la mejora operativa de las misiones. Se recalca el carácter conceptual del trabajo, enfocado más en las ideas, posibilidades tecnológicas y estrategias, y no tanto en las implementaciones o consideraciones de carácter más puramente técnico.

2. Estado del arte

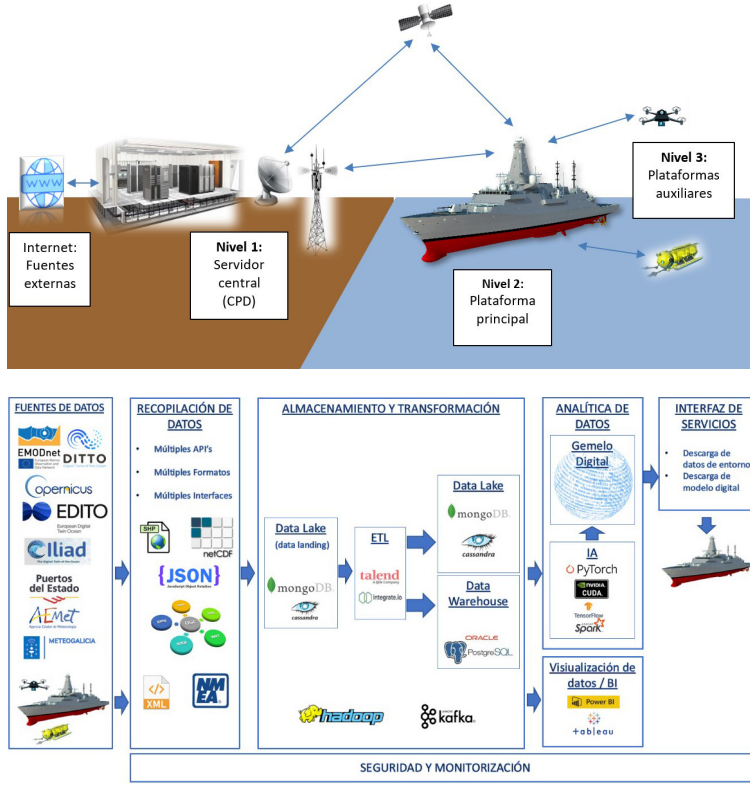
Adil Rasheed *et al.* definen el gemelo digital como «una representación virtual de un activo físico habilitada a través de datos y simuladores para predicción, optimización, seguimiento, control y mejora en la toma de decisiones en tiempo real». Gracias a los avances en sistemas informáticos, especialmente en inteligencia artificial y *big data,* los gemelos digitales son y serán una realidad. Existen diferentes tipos de gemelos digitales, entre ellos, el gemelo digital de tipo predictivo *data-driven,* que a partir de datos masivos elaborará los modelos usando técnicas de *big data* e IA. Este concepto ha sido abordado por instituciones internacionales relacionadas con la investigación de los océanos, dando lugar a los gemelos digitales oceánicos de EDITO, Ocean Twin o DECADE-DITTO. Estos proyectos se nutren de datos de organizaciones internacionales como EMODnet o Copernicus, y nacionales como AEMET, Puertos del Estado o MeteoGalicia. Estos proporcionan multitud de datos y predicciones de diversa naturaleza, como salinidad, viento, temperatura, oleaje, precipitaciones, etc., y en formatos que, aunque son estándares (formatos OGC, NetCDF, Shapefile, JSON, XML, etc.) son muy diversos. Por su parte, las plataformas navales también pueden generar sus propios datos del entorno cercano a partir de sus sensores y sistemas (sensores meteorológicos, sistemas inerciales, cámaras, sonar, radar, etc.). La explotación de todos estos datos requerirá arquitecturas *big data* con importantes requisitos de almacenamiento y procesado, que solo pueden implementarse en potentes CPD terrestres. En estas infraestructuras se llevará a cabo el ciclo típico de recolección, extracción, transformación, carga, análisis y explotación de los datos, que resultará en la generación de los modelos que luego serán utilizados en las plataformas para la navegación, alimentándolos con datos locales y actualizaciones provenientes del sistema terrestre. Pero esto último implica la entrada en juego de la variable de las comunicaciones, que en el entorno marítimo no es nada trivial y requiere el empleo de comunicaciones satelitales o de alta frecuencia (HF) cuyo ancho de banda es limitado, lo que va en contra del funcionamiento de un gemelo digital, que requiere realimentación continua del sistema real. Estas limitaciones en las comunicaciones,

unidas a la heterogeneidad de los datos, obligan también a buscar alternativas de representación del entorno que sean flexibles y compactas como los modelos de cuadrículas jerárquicas como GeoHash, S2, teselas de Bing, o el modelo H3 de Uber, que será el finalmente elegido.

3. Desarrollo

3.1 Arquitectura del sistema

En esta sección se presenta la arquitectura del sistema de gemelo digital propuesta. Como ya se mencionó, es una arquitectura por niveles, donde el primer nivel corresponde al sistema central terrestre, con gran potencia de cómputo y comunicaciones, que crea y mantiene el gemelo digital usando todas las fuentes de datos disponibles. El segundo nivel corresponde a la plataforma naval, que desplegará en escenarios operativos con comunicaciones limitadas (vía satélite y quizá HF) y ejecutará un modelo local del gemelo digital actualizado con datos propios y datos proporcionados por el nivel 1 bajo petición. En el nivel 3 se situarían las plataformas desplegables desde la plataforma naval, que proporcionarán información adicional a esta última. En la figura 1a se muestra la arquitectura mencionada y los diagramas de bloques de los niveles 1 y 2 en las figuras 1b y 1c respectivamente.



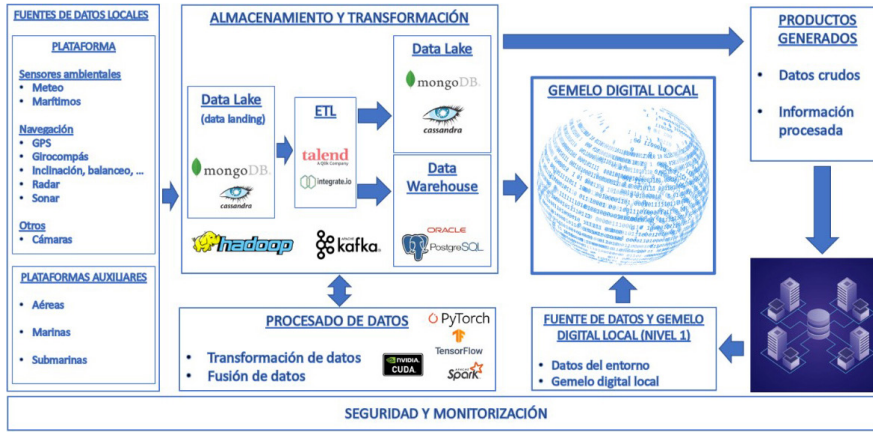


Figura 1a. Arquitectura global conceptual del sistema. 1b. Diagrama de bloques del nivel 1. 1c. Diagrama de bloques del nivel 2

Como se puede ver en la figura 1b, correspondiente al nivel 1, el sistema central integra los datos de todas las fuentes, en sus diferentes formatos y utilizando las diferentes API e interfaces que correspondan (Internet, satélite, radio HF...). Los guardará en el Data Lake, donde los preprocesará para su explotación por los diferentes algoritmos que den lugar a los modelos que componen el gemelo digital. Algunos de estos modelos estarán disponibles vía servicio para las plataformas que los soliciten; estos podrán ser tanto modelos entrenados para su ejecución local, como los datos de las condiciones marítimas en el entorno y periodo que se indique en la solicitud.

En la figura 1c, correspondiente al nivel 2, vemos que la plataforma recolecta los datos de los sensores propios y de las plataformas auxiliares (nivel 3) en un Data Lake donde prepara los datos para alimentar el gemelo digital local. Este también integra los datos actualizados que solicita al nivel 1 cuando lo necesite y tenga conectividad. A su vez, también enviará informes resumidos del entorno local al sistema central para que integre esos datos y proporcione actualizaciones a otras plataformas. Estas comunicaciones se harán normalmente a través de enlaces de ancho de banda pequeño (satélites y HF), por lo que el volumen de datos deberá limitarse. En el diagrama se puede ver que la plataforma también enviará datos en crudo al sistema central para que este mejore los modelos, pero esto solo se hará cuando la conexión permita descargas masivas de datos, por ejemplo, en puerto.

3.2 Operación del sistema

El objetivo de esta sección es detallar los diferentes contextos en los que puede operar el sistema y cuál será la forma de funcionar para aprovechar todas las posibilidades del modelo propuesto y lidiar con las diferentes limitaciones existentes. Los escenarios que se plantean son los siguientes:

Escenario 1: sin restricciones de conectividad entre nivel 1 y nivel 2 (p.ej. en puerto)

— Caso de uso 1.1. Solicitud del nivel 2 al nivel 1 de modelos y datos de entorno:

a) Solicitud del modelo de predicción de la plataforma al sistema central para un uso en una zona determinada y un periodo determinado (figura 2a).

b) Solicitud de descarga de datos de un entorno operativo («datos de misión para un área y durante un periodo de tiempo indicados para su uso operativo (figura 2b).

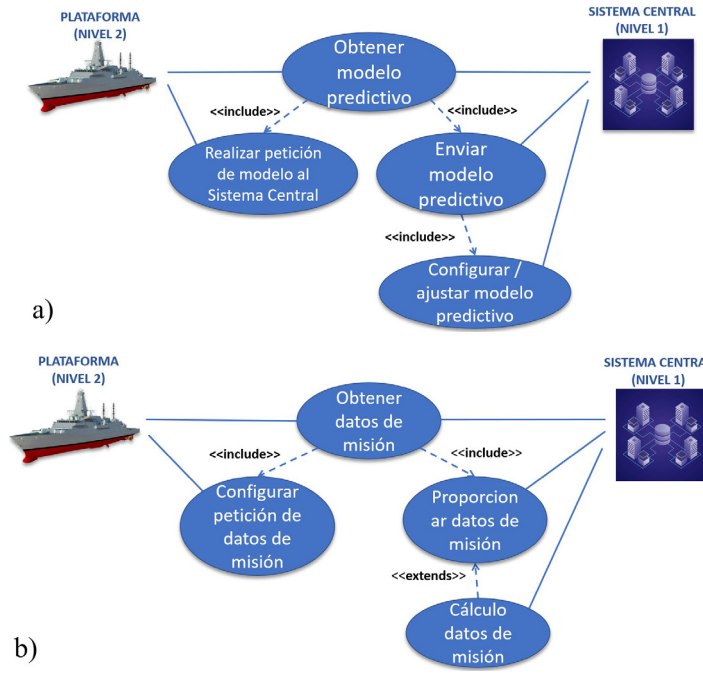


Figura 2a. Solicitud del modelo predictivo. 2b. Solicitud de los datos de misión

— Caso de uso 1.2. Descarga de datos crudos desde el nivel 2 al nivel 1. La plataforma descarga los datos en crudo registrados durante la operación al sistema central para su almacenamiento en el Data Lake y posterior explotación (figura 3).

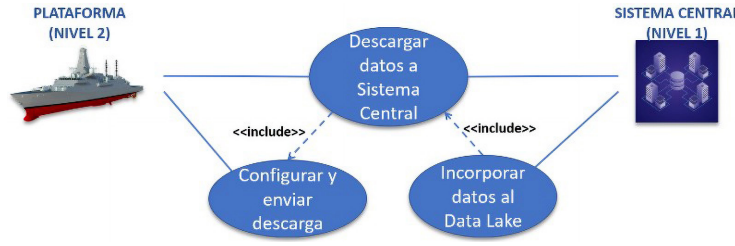


Figura 3. Descarga de datos crudos de la plataforma al sistema central

Escenario 2: conectividad restringida entre nivel 1 y nivel 2.

- Caso de uso 2.1. Solicitud del nivel 2 al nivel 1 de datos de entorno, igual que el caso 1.1.b), pero en este caso con conectividad reducida (HF o satélite), por lo que puede ser necesario reducir resolución (figura 2b).
- Caso de uso 2.2. Descarga de información resumida desde el nivel 2 al nivel 1, para que este mejore las predicciones en el corto plazo y actualice al resto de plataformas (figura 4).

Figura 4. Envío de informes periódicos de la plataforma al sistema central

Escenario 3: Sin conectividad en la plataforma de Nivel 2 con el Nivel 1

- Caso de uso 3.1. La plataforma operará en modo *stand-alone,* usando modelo pre-entrenado y datos propios. El nivel 1 no está accesible, por lo que la plataforma usará su modelo local alimentado por datos de sus propios sensores y de las plataformas auxiliares (figura 2e).

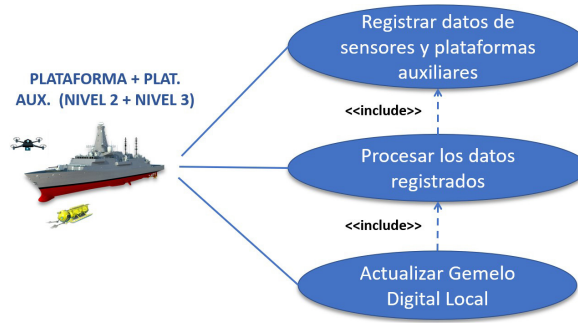


Figura 5. Funcionamiento de la plataforma en modo stand-alone

4. Resultados y discusión

En esta sección se reseñan los principales aspectos positivos o ventajas de la solución propuesta, así como las cuestiones que afectan negativamente o suponen limitaciones a su desarrollo.

Como aspectos positivos de esta solución destaca fundamentalmente la posibilidad de disponer de un modelo del entorno en las plataformas

desplegadas (gemelo digital local) que proporciona estimaciones de las condiciones de navegación, aun sin tener conectividad con el sistema central, siempre y cuando se haya descargado previamente de este último. El modelo, junto con las estimaciones para un entorno concreto, se podrá actualizar cuando se disponga de conectividad, incluso aunque sea limitada y, a su vez, podrá realimentar al gemelo digital central con información real actualizada para la mejora de las predicciones y su actualización a otras plataformas desplegadas. Además, se podrá controlar el volumen de datos a intercambiar para adaptarlo al escenario y, cuando haya conectividad de banda ancha, descargar todos los datos en crudo capturados en las plataformas al sistema central para la mejora de los modelos o el desarrollo de otros nuevos.

Como principales limitaciones o dificultades se debe señalar, en primer lugar, la dependencia del sistema central para la obtención de modelos y datos de los entornos de operación actualizados. En este caso, dependiendo del tiempo de indisponibilidad del sistema central, esto podría influir negativamente en la operatividad de las plataformas. Por otro lado, el sistema requiere que las plataformas lleven instaladas una instrumentación potente y fiable, así como una alta capacidad informática, tanto de procesado como de almacenamiento, para aprovechar al máximo la información generada en estas y que permite alimentar el gemelo digital local y el central. Otro aspecto negativo a destacar es la enorme complejidad asociada a los modelos predictivos. Las diferentes fuentes de información externas y locales, de naturalezas diferentes, con múltiples tipos y formatos de datos, distintas frecuencias de actualización, procedentes de múltiples áreas geográficas, con diferentes resoluciones, etc., suponen un desafío muy complejo para el desarrollo de los modelos predictivos basados en IA. Su entrenamiento requerirá un trabajo enorme, con muchos ciclos de prueba y error, y unos requisitos computacionales también enormes.

Como se puede ver, es una solución tan ambiciosa y prometedora como compleja y exigente. Por ello, una futura implementación basada en esta solución conceptual debería abordarse mediante una aproximación de tipo incremental, analizando y priorizando los diferentes requisitos y funcionalidades, su complejidad y viabilidad, siempre con la vista puesta en la mejora de la operatividad de las plataformas que despliegan en las misiones.

5. Conclusiones

Se ha abordado, desde un punto de vista conceptual o funcional, la problemática asociada a la implementación de un gemelo digital marítimo en un entorno operativo donde desplegarían plataformas navales para llevar a cabo sus misiones y en el que existen limitaciones de comunicaciones que dificultan mantener actualizado el gemelo digital. Dicha problemática implica una complejidad muy elevada, tanto en el aspecto tecnológico, como por las condiciones propiamente operativas. Por ello, va a requerir

considerar una gran multitud de aspectos, algunos de los cuales pueden ser críticos para el éxito de la solución, y otros muchos obligarán a tomar decisiones que lleven a soluciones de compromiso. No obstante, las tecnologías e infraestructuras, tanto de sistemas de información como de comunicaciones, están avanzando rápidamente y es posible que algunas limitaciones existentes actualmente dejen de serlo en los próximos años.

Por otro lado, queda patente que los datos masivos son la base de la tecnología del gemelo digital. Afortunadamente, en la actualidad se está trabajando de forma importante en varios proyectos de ámbito internacional sobre gemelos digitales oceánicos que pondrán a disposición de quien los necesite datos, predicciones y modelos cada vez más completos y precisos. Sin embargo, aún falta para llegar a este punto y se anticipa que será en los próximos años cuando se produzca un salto cuantitativo y cualitativo.

Teniendo en cuenta lo anterior, se ha planteado una solución conceptual basada en una arquitectura de diferentes niveles, acompañada de estrategias de operación que permiten aprovechar al máximo los datos disponibles en los diferentes escenarios operativos con las limitaciones indicadas. Una implementación basada en esta solución no solo mejoraría la consciencia situacional a las plataformas en esos escenarios, sino que además permitiría evolucionar el gemelo digital para mejorar sus predicciones a medida que se vayan incorporando más datos generados por las plataformas en el transcurso de sus misiones. En este sentido, se considera que se han cumplido los objetivos de este trabajo y que la solución propuesta puede usarse como marco de referencia para una futura implementación.

Como líneas de trabajo a seguir a partir de aquí, se plantean diferentes posibilidades, como enfocarse en el análisis del modelo, considerando los aspectos más cuantitativos de la integración, analizando las necesidades y limitaciones de volumen de datos a transmitir, la información más relevante, la resolución de los modelos y el ancho de banda de comunicaciones disponibles. También se podrían abordar cuestiones más relacionadas con los modelos predictivos en este contexto, como el grado de mejora de las predicciones del gemelo digital en el nivel 1, producido por la integración de los informes resumidos enviados por las plataformas; o el funcionamiento del modelo entrenado en el nivel 1 y ejecutado en la plataforma, inicializado con datos del nivel 1, y luego actualizado únicamente con los datos locales; o abordar la cuestión de representación del entorno en 3D como extensión del modelo de celdas H3 de Uber. También se podrían estudiar diferentes soluciones o ecosistemas *big data* para el modelo propuesto, o la integración de los datos de múltiples plataformas cercanas sin pasar por el sistema central. En definitiva, existen multitud de líneas de trabajo para desarrollar una solución real operativa que permita a las plataformas llevar a cabo sus misiones de forma más segura, eficaz y eficiente.

Referencias

Ministerio de Industria, Energía y Turismo. (s.f). La Transformación Digital de la Industria Española. Informe Preliminar. *Industria Conectada 4.0*. Disponible en: https://www.industriaconectada40.gob.es/SiteCollectionDocuments/informe-industria-conectada40.pdf

Rasheed, A., San, O. y Kvamsdal, T. (2019, 3 de octubre). Digital Twin: Values, Challenges and Enablers. *arXiv*. Cornell University. doi: 10.48550/arXiv.1910.01719.

EDITO-Infra. (s.f.). European Digital Twin Ocean - Powered by EDITO. [Consulta: 22 de diciembre 2023]. Disponible en: https://edito-infra.eu/

Iliad. (s.f.). Digital Twins of the Ocean - The Iliad Project. [Consulta: 22 de diciembre 2023]. Disponible en: https://ocean-twin.eu/

OcenaExpert. (2023). Ocean Decade Action Factsheet: Digital Twins of the Ocean (DITTO). [Consulta: 22 de diciembre 2023]. Disponible en: https://oceanexpert.org/document/29741

European Commision. (s.f.). European Marine Observation and Data Network (EMODnet). [Consulta: 22 de diciembre 2023]. Disponible en: https://emodnet.ec.europa.eu/en

Programme of the European Union. (s.f.). C. D. S. Ecosystem. Explore data | Copernicus Data Space Ecosystem. [Consulta: 22 de diciembre 2023]. Disponible en: https://dataspace.copernicus.eu/explore-data

Vicepresidencia Tercera del Gobierno de España. (s.f.). AEMET OpenData. [Consulta: 22 de diciembre 2023]. Disponible en: https://opendata.aemet.es/centrodedescargas/productosAEMET?

Puertos del Estado. (s.f.). Prediccion de oleaje, nivel del mar; Boyas y mareografos. [Consulta: 22 de diciembre 2023]. Disponible en: https://www.puertos.es/es-es/oceanografia/Paginas/portus.aspx

MeteoGalicia. (2012). Introducción al uso de los servicios Thredds. [Consulta: 22 de diciembre 2023]. Disponible en: https://www.meteogalicia.gal/datosred/infoweb/numerico/thredds/Manual_uso_Thredds.pdf

Open Geospatial Consortium. (s.f.). Open Geospatial Consortium - Home Page. [Consulta: 22 de diciembre 2023]. Disponible en: https://www.ogc.org/

MongoDB (2023). The Big Data Guide. [Consulta: 22 de diciembre 2023]. Disponible en: https://www.mongodb.com/basics/big-data-explained

Spectus (s.f.). Hierarchical Grid Systems - Tiling Tools - Spectus - A Cuebiq Group LLC Company. [Consulta: 22 de diciembre 2023]. Disponible en: https://spectus.ai/web-apps/tiling-tools/

Gemelo Digital de Entorno Operativo Marítimo: Propuesta de arquitectura de integración de datos y operación

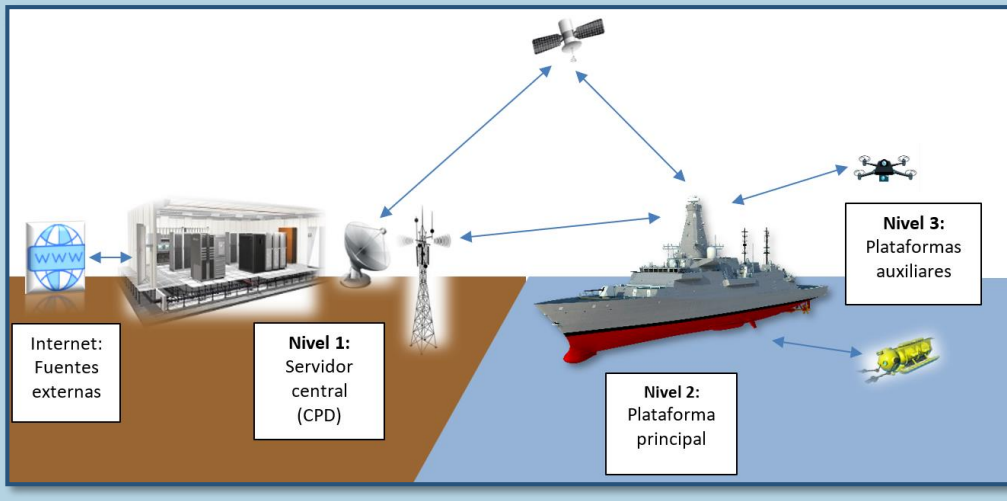
Autor: Sergio Ramírez Morán

Universidad de Vigo

Directores: Milagros Fernández Gavilanes, Carlos Pérez Collazo

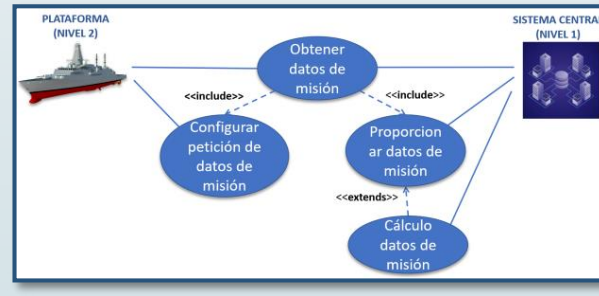
Propósito

Diseño de una **arquitectura conceptual de integración de datos** y unas **estrategias de operación** que habiliten el funcionamiento del **gemelo digital de un entorno operativo marítimo** que permitirá mejorar la seguridad, eficacia y eficiencia de las misiones.



Metodología

- Estudio del **estado del arte:** gemelos digitales oceánicos, fuentes de datos externas y propias de las plataformas, procesos y herramientas *Big Data*, comunicaciones navales y sistemas de representación *GIS* de celdas jerárquicas.
- Diseño de la **arquitectura conceptual en tres niveles** y las **estrategias de operación** que permiten su funcionamiento en los diferentes escenarios.



Resultados y discusión

- La solución permitirá la **mejora de la consciencia situacional de las plataformas en los entornos operativos**, al tiempo que proporcionará nuevos datos al gemelo digital para la mejora continua de los modelos.
- Los requisitos del sistema **implicarán potentes infraestructuras tecnológicas *Big Data***, así como el desarrollo de **complejos modelos predictivos basados en inteligencia artificial**.
- La solución propuesta podrá servir como **marco de referencia para una implementación real**.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Diseño de un Centro de Procesamiento de Datos Modular para Edge Computing

Autor: Rojo Mínguez, Pablo (pablo.rojo@alumnos.uvigo.es)
Directores: Suárez Lorenzo, Fernando y Rodríguez Martínez, Francisco J.
(externo.fernandosuarez@cud.uvigo.es / externo.franjrm@cud.uvigo.es)

Resumen – El Centro de Procesamiento de Datos (en adelante CPD) es aquella instalación diseñada para albergar equipos informáticos y de telecomunicaciones, permitiendo el procesamiento, almacenamiento y gestión de uno de los activos más valiosos de cualquier organización, la información. La mayoría de las organizaciones son conscientes del valor que posee la información para el negocio y por eso es imperativa la necesidad de una instalación que garantice la disponibilidad y la seguridad.

La necesidad de las organizaciones de almacenar, procesar y salvaguardar la información es innegable. Desde la toma de decisiones hasta la protección de datos y la continuidad del negocio, la información es un recurso esencial en la era digital. Las organizaciones que no priorizan la gestión de la información corren el riesgo de quedar rezagadas y enfrentar serias consecuencias. Por lo tanto, invertir en tecnología y prácticas sólidas de gestión de datos se ha convertido en un imperativo en el mundo empresarial actual.

Hoy en día, el enfoque principal es el de la eficiencia energética y el aprovechamiento espacial, ya que una instalación eficiente reduce el consumo energético y las emisiones de dióxido de carbono al medioambiente, así como el subsiguiente ahorro de costes.

En el contexto actual, la información se ha vuelto más móvil que nunca. Los avances tecnológicos han permitido a las organizaciones acceder a datos desde cualquier lugar, lo que ha aumentado la flexibilidad y la productividad. Sin embargo, esta movilidad también plantea desafíos en términos de seguridad y privacidad. Es esencial contar con políticas y tecnologías que protejan la información en tránsito.

La pérdida de datos críticos debido a un fallo técnico o un desastre natural puede ser devastadora. Por lo tanto, las organizaciones implementan estrategias de respaldo y recuperación de datos para garantizar la disponibilidad continua de la información.

Palabras clave – Centro de Procesamiento de Datos, Contenedor, Edge Computing, Soberanía del dato.

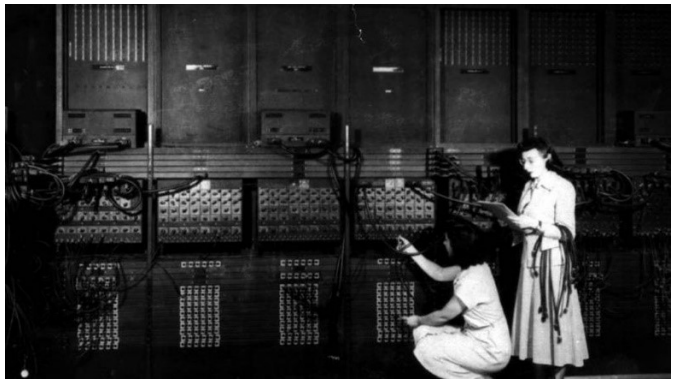
1. Introducción

Los CPD han evolucionado significativamente desde sus inicios. Algunos de los hitos más destacados son:

— Orígenes: los *mainframe* eran el CPD

En las décadas entre 1940 y 1960, se construían en torno a los equipos *mainframe* y eran utilizados por grandes corporaciones y entidades gubernamentales para tareas como la gestión de nóminas, el mantenimiento de registros y el procesamiento de transacciones.

Superordenadores como ENIAC (1946) supondrían el primer centro de datos, esta supercomputadora usaba la tecnología de válvulas de vacío, ocupaba un espacio de más de 150 m^2 y era muy compleja de operar y mantener. Unos años después, en 1954, llegó TRADIC dando un salto en la computación por la introducción de los transistores.



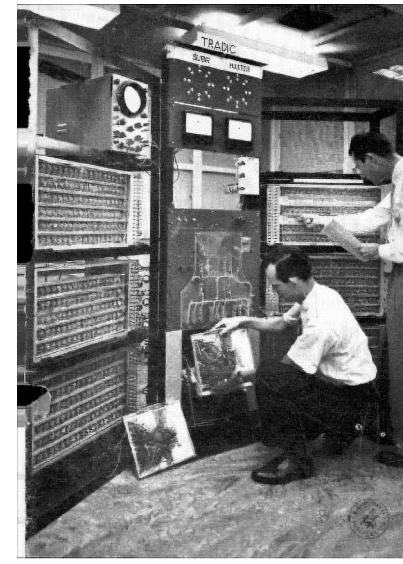


Figura 1. ENIAC y TRADIC. Fuente: Wikimedia Commons

— La computación paralela y la computación distribuida

El avance de la microelectrónica en las décadas de los setenta y ochenta propició la miniaturización y mayor accesibilidad a las computadoras, dando paso a la creación de CPD de tamaño medio, aptos para organizaciones más pequeñas. En contraste con sus predecesores, estos CPD requerían menos personal para su operación y mantenimiento.

La computación paralela y distribuida tiene muchas ventajas sobre la computación secuencial, que es el uso de una sola unidad de procesamiento para resolver un problema. Las ventajas de la computación paralela y distribuida incluyen:

- Incremento de la velocidad de ejecución.
- Mejora del rendimiento.
- Mayor capacidad de cálculo.
- Reducción de los costes.

— Explosión de los noventa: clústers y *grid computing*

En la década de los noventa surgen los primeros grupos de computadoras, conocidos como *clústeres*. Un clúster consiste en la interconexión de varias computadoras a través de una red de alta velocidad, de manera que operen como una unidad única. Esto tiene como propósito mejorar el rendimiento, la eficiencia y la disponibilidad, a la vez que resulta más asequible que utilizar computadoras individuales.

Figura 2. Clúster de tipo Beowulf. Fuente: https://www.climatemodeling.org/

Esto posibilitó la creación de CPD de tamaño medio, ideales para organizaciones pequeñas.

Comparados con los CPD iniciales, estos requerían menos personal para operar y mantener. El equipo en estos CPD estaba compuesto principalmente por técnicos y operadores.

El siguiente paso en la evolución fue el *grid computing* (o computación en malla), que hacía uso de las comunicaciones sobre Internet para trabajar en un determinado problema. Utilizaba todos los recursos de varios ordenadores para funcionar como un supercomputador.

La explosión de la demanda de servicios informáticos a raíz del desarrollo de Internet y la World Wide Web en las décadas de 1990 y 2000 dio pie a la necesidad de los CPD de gran tamaño. Estos centros se erigen en zonas apartadas con electricidad económica y amplio espacio.

Asimismo, se hizo necesario contar con estrictas medidas de seguridad para salvaguardar datos y *hardware*. Los CPD de gran tamaño se convirtieron en el soporte vital de organizaciones, instituciones gubernamentales y personas, gestionando transacciones financieras, redes de telecomunicaciones y almacenando información de clientes.

1.1 El presente y futuro de los CPD

Los CPD seguirán siendo una pieza fundamental en la economía moderna a medida que la tecnología evolucione. Actualmente, gracias al surgimiento de normativas (que se expondrán más adelante) es posible cumplir con unas necesidades de alimentación, climatización, rendimiento y fiabilidad muy altas en instalaciones complejas.

Se espera que se descentralicen y distribuyan aún más, almacenando y procesando datos de diversas fuentes, como teléfonos inteligentes, tabletas y dispositivos «vestibles».

El futuro de los CPD está lleno de oportunidades. Los operadores que sean capaces de adaptarse a las nuevas tendencias y desafíos tendrán un papel importante en el desarrollo de la economía digital.

Figura 3. Dos ejemplos de centros de datos de Microsoft. Fuente: Microsoft News

2. Desarrollo

Podemos concretar que los principales objetivos que se persiguen con el diseño y la implantación de los modernos CPD se orientan hacia la eficiencia y la disponibilidad.

2.1 Eficiencia

Las dos magnitudes más extendidas para medir la eficiencia energética del CPD son las siguientes:

- Power Usage Effectiveness (PUE).
- Data Center Infrastructure Efficiency (DCIE).

Al igual que en otros sectores, debido en parte al encarecimiento de la energía y también a la cada vez mayor conciencia ecológica, reportar la huella de carbono está siendo cada vez más habitual. En los CPD se consume mucha electricidad y se genera mucha energía térmica que se desperdicia. El uso de CPD supone un consumo del 1 % de la energía a nivel mundial y las TIC suponen ya el 2 % de las emisiones globales de gases de efecto invernadero a la atmósfera. La distribución de consumo energético en un CPD la podemos ver en la siguiente imagen:

Figura 4. Consumos en un CPD

En lo que respecta a la refrigeración, es importante señalar que cualquier dispositivo eléctrico genera calor como subproducto de su funcionamiento, y es fundamental disiparlo para evitar que la temperatura interna alcance niveles no deseables.

La cantidad de energía transmitida a través de las líneas de datos por los equipos TIC es mínima. En consecuencia, la totalidad de la energía suministrada por la red eléctrica, en forma de corriente alterna, se transforma principalmente en calor. En este sentido, la energía térmica en vatios (W) que generan los equipos equivale a su consumo energético en vatios.

En cuanto a las unidades de climatización, es importante mencionar que estas generan una cantidad significativa de calor, que es dirigido hacia el exterior del entorno del CPD. Aunque este calor no impacta directamente en la carga térmica interna del centro de datos, sí tiene efectos negativos en la eficiencia del sistema de climatización. Por lo tanto, este factor es tenido en cuenta al determinar las dimensiones adecuadas para el sistema de aire acondicionado.

2.2 Disponibilidad

La mayoría de las causas de las paradas de servicio del CPD se producen por fallos en las infraestructuras de alimentación y refrigeración. Sin embargo, otro gran porcentaje se corresponde a los errores humanos, por lo que es imprescindible promover los buenos hábitos en el CPD.

La disponibilidad se mide como el porcentaje de tiempo que el CPD se encuentra proporcionando servicio. Encontramos varias normativas internacionalmente aceptadas de cara a la medición de esta característica:

- Uptime Institute Tiers (I-IV).
- EN 50600 Availability classes (1-4).
- TIA 942-C Ratings (1-4).
- 10 Syska Hennessy Criticality Levels.
- ANSI/BICSI Classes (F0-F4).

Como norma mundialmente aceptada, la ANSI/TIA 942-C, aprobada inicialmente en 2005 por ANSI/TIA (American National Standards Institute-Telecomunications Industry Association), clasifica a este tipo de centros en varios grupos, llamados TIER, indicando así su nivel de fiabilidad en función del nivel de disponibilidad y se obtienen ventajas fundamentales, como son:

- Nomenclatura estándar.
- Funcionamiento a prueba de fallos.
- Aumento de la protección frente a agentes externos.
- Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.

Estos niveles los podemos ver en la tabla2.

TIER	% DISPONIBILIDAD	% PARADA	TIEMPO ANUAL DE PARADA
TIER I	99,67 %	0,33 %	28,82 horas
TIER II	99,74 %	0,25 %	22,68 horas
TIER III	99, 982 %	0,02 %	1,57 horas
TIER IV	100,00 %	0,01 %	52,56 minutos

Fuente: TIA-942

Tabla 2. Niveles o TIER de disponibilidad

2.3 Edge Computing y soberanía del dato

El *Edge Computing* o computación frontera es un concepto vertiente de la computación distribuida, que consiste en el almacenamiento, tratamiento y análisis de los datos lo más cerca posible de donde estos se generan.

Lleva las aplicaciones empresariales más cerca de los datos, como los dispositivos IoT o los servidores locales. Esto tiene varias ventajas, como la reducción de la latencia, la posibilidad de realizar análisis en tiempo real, una mejor seguridad de los datos y una mayor eficiencia de costes.

La *soberanía del dato* se refiere al control y la autoridad que un país o entidad tiene sobre la información generada y almacenada dentro de sus fronteras.

En un mundo digital interconectado, la gestión efectiva de los datos es crucial para proteger la privacidad y la seguridad. Este concepto implica establecer regulaciones y políticas que aseguren que los datos sensibles estén resguardados de manera adecuada, evitando su explotación sin consentimiento.

La soberanía del dato también aborda preocupaciones sobre la dependencia de servicios extranjeros para el almacenamiento y procesamiento de información. Es un equilibrio delicado entre aprovechar los beneficios

de la globalización digital y salvaguardar los intereses nacionales en términos de seguridad y privacidad.

2.4 Puntos clave del diseño

Con estos conceptos sobre la mesa, el diseño de un CPD Modular busca proporcionar estas características, pero con un diseño que permite evitar la obra civil tradicional, para la que es necesario disponer de un gran espacio y un proyecto que, para algunas organizaciones, se antoja demasiado complejo, costoso en tiempo y dinero y, en definitiva, inviable.

Un CPD Modular basa su diseño en el desarrollo de un contenedor, que le proporciona las características de resistencia, aislamiento, climatización y eficiencia energética que se necesitan en este tipo de proyectos.

De la misma manera que se pueden utilizar contenedores prediseñados con medidas que se ajustan a normativa estándar, también se puede construir en medidas personalizadas para adaptarse a espacios concretos.

Una vez que se obtienen las necesidades a cubrir, el desarrollo de esta infraestructura se realiza con componentes que se pueden encontrar en los CPD tradicionales, aunque adaptados al tamaño del contenedor, estos son:

- Suelo técnico.
- Sistemas de climatización.
- Sistemas de alimentación eléctrica.
- Sistemas de alimentación ininterrumpida.
- Sistemas contra incendios.

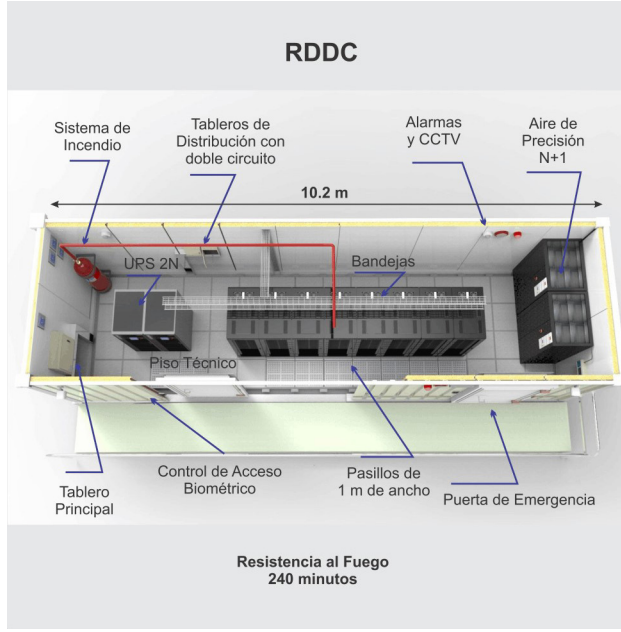


Figura 5. Muestra de un CPDM completo. Fuente: Area Data Paraguay S.A.

3. Conclusiones

Los Centros de Procesamiento de Datos han experimentado una notable evolución en las últimas décadas, adaptándose a las cambiantes necesidades de la tecnología y las empresas. Esta evolución ha pasado por diversas etapas, desde un enfoque más centralizado hasta la actualidad, donde la consolidación y virtualización de sistemas son la norma.

En sus inicios, los CPD eran estructuras centralizadas que albergaban servidores y equipos de procesamiento de datos en un solo lugar físico. Sin embargo, esta configuración se volvió limitada a medida que la demanda de capacidad y disponibilidad aumentaba. Como resultado, se produjo una transición hacia un enfoque más distribuido, con múltiples centros de datos repartidos geográficamente.

Hoy en día, la tendencia predominante en la gestión de CPD es la consolidación y virtualización de sistemas. Esto implica la creación de infraestructuras altamente eficientes y escalables, donde la virtualización de servidores y almacenamiento desempeña un papel crucial. Estas tecnologías permiten a las empresas maximizar la utilización de recursos y reducir costes operativos significativamente.

Además de la virtualización, un aspecto crítico en la gestión de CPD es la infraestructura de soporte. Esto incluye sistemas de refrigeración avanzados para mantener temperaturas óptimas, sistemas de alimentación ininterrumpida (SAI) para garantizar la continuidad de la energía eléctrica, sistemas de detección y extinción de incendios para la seguridad y sistemas de seguridad y monitorización avanzados.

Un CPD bien diseñado es fundamental para cualquier organización en la era digital. No solo garantiza la disponibilidad, continuidad y estabilidad del entorno de TI, sino que también mejora la eficiencia operativa y optimiza el retorno de la inversión.

Esto se logra adoptando las mejores prácticas en diseño y gestión de CPD. Estas prácticas permiten a las organizaciones enfrentar los desafíos tecnológicos actuales y futuros de manera más efectiva. Al mantenerse al día con las tendencias tecnológicas emergentes, un CPD puede adaptarse y evolucionar, asegurando que la organización esté preparada para el futuro.

Además, un CPD bien gestionado puede proporcionar a las organizaciones una ventaja competitiva en un mundo cada vez más digitalizado. Al garantizar que los sistemas y servicios críticos estén siempre disponibles y funcionen a su máximo rendimiento, las organizaciones pueden ofrecer un mejor servicio a sus clientes, mejorar su productividad y, en última instancia, impulsar el crecimiento del negocio.

Por lo tanto, invertir en el diseño y gestión de un CPD es una decisión estratégica que puede tener un impacto significativo en el éxito a largo plazo de una organización.

Referencias

Wikipedia. (s.f.). Centro de Procesamiento de Datos. [Consulta: 17 de agosto 2023]. Disponible en: https://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

Wikipedia. (s.f.). ENIAC. [Consulta: 29 de agosto 2023]. Disponible en: https://es.wikipedia.org/wiki/ENIAC

Wikipedia. (s.f.). TRADIC [Consulta: 22 de agosto 2023]. Disponible en: https://en.wikipedia.org/wiki/TRADIC

Bravo, J. M. (s.f.). Multicomputadores tipo cluster. *Uhu*. [Consulta: 22 de agosto 2023]. Disponible en: http://www.uhu.es/josem.bravo/AD/Tema3.pdf

Hoffman, F. M. y Hargrove, W. W. (s.f.). High Performance Computing: An Introduction to Parallel Programming With Beowulf. *climatemodeling*. [Consulta: 22 de agosto 2023]. Disponible en: https://www.climatemodeling.org/~forrest/osdj-2000-11/

Roach, J. (2020). Microsoft descubre que los centros de datos submarinos son confiables, prácticos y utilizan energía sustentable. *Microsoft News Center*. [Consulta: 22 de agosto 2023]. Disponible en: https://news.microsoft.com/es-xl/features/microsoft-descubre-que-los-centros-de-datos-submarinos-son-confiables-practicos-y-utilizan-energia-sustentable/

Europa Pres. (2021). Las TIC emiten más gases de efecto invernadero que la aviación. [Consulta: 22 de agosto 2023]. Disponible en: https://www.europapress.es/ciencia/cambio-climatico/noticia-tic-emiten-mas-gases-efecto-invernadero-aviacion-20210910173106.html

TIA. (s.f.). ANSI/TIA-942 Standard. [Consulta: 21 de agosto 2023]. Disponible en: https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

Diseño de un Centro de Procesamiento de Datos Modular para Edge Computing

Autor: Pablo Rojo Mínguez
Director/es: Fernando Suárez Lorenzo, Francisco J. Rodríguez Martínez
Universidad de Vigo

Introducción

¿Es posible que un Centro de Procesamiento de Datos Modular pueda ser una alternativa real al despliegue tradicional o a una solución en la nube?

A través de este TFM se propondrá la respuesta a esta pregunta, teniendo en cuenta las actuales tendencias y las necesidades que se pueden cubrir con este tipo de instalaciones

Metodología

Tras la **toma de requisitos**, en la que se dimensiona la arquitectura hardware necesaria, viene la fase de producción de la infraestructura, que se puede formar en una ubicación del proveedor y transportarse por medios de locomoción que cumplan con los estándar o bien fabricar la estructura en la propia ubicación del cliente.
La **flexibilidad** de este tipo de despliegues es evidente, evitando obra civil tradicional (aunque es necesario el acondicionamiento de espacios) y pudiendo proporcionar el servicio en tiempos mucho menores.
Dispone de **elementos** que facilitan la posterior operación de componentes:

- Suelo técnico
- Racks estándar
- Panelados
- Sistemas de refrigeración
- Sistemas contraincendios

La **ubicación de los componentes hardware** se realiza como si de una infraestructura tradicional se tratara, ya que son los mismos elementos, cumpliendo con la misma normativa para aprovechar el estandarizado.

Resultados

Un Centro de Procesamiento de Datos bien diseñado es fundamental para cualquier organización en la era digital. No solo garantiza la disponibilidad, continuidad y estabilidad del entorno de Tecnologías de la Información (TI), sino que también mejora la eficiencia operativa y optimiza el retorno de la inversión.
Esto se logra adoptando las mejores prácticas en diseño y gestión de CPD. Estas prácticas permiten a las organizaciones enfrentar los desafíos tecnológicos actuales y futuros de manera más efectiva. Al mantenerse al día con las tendencias tecnológicas emergentes, un CPD puede adaptarse y evolucionar, asegurando que la organización esté preparada para el futuro.

Conclusiones

- Es una buena alternativa a los CPD tradicionales evitando Obra Civil
- Proporciona altos niveles de eficiencia de climatización y modularidad
- Flexibilidad de crecimiento, en la misma instalación o añadiendo módulos sin necesidad de añadir "edificios"
- Posibilidad de transporte ante un cambio de ubicación
- Frente a la nube: Seguridad, disponibilidad y soberanía del dato

Agradecimientos

A mi mujer Vicen, por animarme a cursar este Máster y apoyarme en los momentos que más cuestan.
A mi tutor Fernando, por responder siempre a mis dudas y ayudarme a enfocar cuando las ideas se dispersaban.
A mis compañeros de este Máster, de todos he aprendido algo que me llevo para el futuro.

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Estudio del estado del arte de la computación perimetral y el internet de las cosas aplicados a sistemas y tecnologías de la información para la defensa

Autor: Álvarez Sánchez, David (dalvsa4@mde.es)
Director: Nocelo López, Rubén (rubennocelo@cud.uvigo.es)

Resumen – Este TFM se centra en la integración del internet de las cosas (Internet of Things, IoT) con la computación perimetral (Edge Computing), un tema de creciente importancia en la era digital. La estructura del trabajo incluye una introducción y objetivos, un análisis del estado del arte, un estudio de la integración de IoT con Edge Computing, casos de aplicación y, finalmente, conclusiones y líneas futuras.

En la introducción se establece el contexto y la motivación del estudio, resaltando la relevancia y el impacto del IoT y la computación perimetral en el mundo tecnológico actual. Se definen los objetivos del trabajo y se presenta la estructura general del mismo.

El análisis del estado del arte se divide en dos secciones principales: una dedicada al IoT, incluyendo su historia, los tipos de sensores utilizados y los principales desafíos que enfrenta; y otra enfocada en la computación perimetral, comparándola con el paradigma tradicional de computación en la nube y discutiendo aspectos como la ubicación del procesamiento de datos, la latencia, y una comparativa de casos de uso.

La integración de IoT con Edge Computing se analiza desde perspectivas legales y arquitectónicas. Se examinan las regulaciones actuales y normas internacionales, y se detallan las arquitecturas de tres, cuatro y cinco capas, enfatizando los elementos clave en la arquitectura IoT-Edge. También se discuten protocolos de comunicación y tecnologías esenciales.

Los casos de aplicación presentados incluyen el sector de la salud, las ciudades inteligentes (transporte, red eléctrica, agricultura y acuicultura) y el uso militar, destacando el IoT en el campo de batalla y el uso de drones en redes Edge. El trabajo concluye con un resumen de los hallazgos y perspectivas de futuras investigaciones, señalando posibles direcciones para el estudio de la integración de IoT con la computación perimetral.

Palabras clave – Internet de las cosas, Computación perimetral, Latencia, Seguridad multimedia, Vehículos aéreos no tripulados.

1. Introducción

1.1 Contexto y motivación

En la era actual, caracterizada por un crecimiento exponencial en la generación de datos y la necesidad de procesamiento en tiempo real, el internet de las cosas (Internet of Things, IoT) y la computación perimetral (Edge Computing) emergen como pilares fundamentales en la transformación digital de múltiples sectores. Este TFM se centra en explorar la convergencia de estas dos tecnologías, proporcionando una comprensión profunda de su estado actual, desafíos y potencial de aplicación en diferentes contextos, especialmente en el de la defensa.

El IoT ha emergido como un paradigma disruptivo, transformando objetos cotidianos en entes inteligentes capaces de comunicarse entre sí, recoger y transmitir datos y tomar decisiones. Esta red de dispositivos interconectados promete una eficiencia sin precedentes y una nueva forma de interactuar con el mundo físico. Sin embargo, su potencial depende en gran medida de la capacidad para procesar y analizar los datos generados de manera eficiente, lo cual plantea desafíos en términos de ancho de banda, latencia y seguridad.

Es aquí donde la computación perimetral se convierte en un complemento fundamental. Al trasladar el procesado de datos y servicios desde el núcleo de la red a la periferia de esta, es decir, cerca de donde se generan los datos, conseguimos, por un lado, aliviar la carga sobre las infraestructuras de red centralizadas y, por otro, reducir la latencia y mejorar la eficiencia del ancho de banda. Estas características son de vital importancia en aplicaciones de defensa, donde decisiones rápidas y seguras pueden suponer la vida o la muerte.

En nuestro sector de aplicación, el IoT ofrece una gran variedad de posibilidades, desde una logística mejorada hasta la vigilancia avanzada o sistemas de armas autónomos. La integración de dispositivos IoT en sistemas de defensa está revolucionando la manera en la que se llevan a cabo las operaciones militares, aumentando la percepción del entorno táctico, mejorando la toma de decisiones y potenciando la eficacia operativa.

Estos avances también traen consigo desafíos significativos. La seguridad de los datos, la gestión del espectro electromagnético y la integración de sistemas heterogéneos son solo algunos de los obstáculos que deben superarse para aprovechar plenamente el potencial de esta tecnología.

Este trabajo propone examinar cómo la integración del IoT y el Edge Computing puede revolucionar las operaciones de defensa. A través de un análisis del estado del arte, estudios de caso y exploración de arquitecturas tecnológicas, se busca no solo comprender el panorama actual de estas tecnologías sino también identificar tendencias emergentes, desafíos pendientes y oportunidades para futuras investigaciones y aplicaciones prácticas.

La motivación principal de este trabajo radica en la necesidad de entender a fondo cómo la convergencia del IoT y la computación perimetral puede ser aprovechada para fortalecer y modernizar las capacidades en el ámbito de la defensa, un sector donde la innovación tecnológica juega un papel crucial en la seguridad nacional.

1.2 Objetivos

El presente TFM tiene como fin estudiar la sinergia entre el IoT y el Edge Computing, con un enfoque particular en su aplicación en el sector de la defensa. Los objetivos se detallan a continuación:

- Analizar el estado actual del IoT y la computación perimetral: profundizar en avances recientes, tendencias y desafíos principales. Explorar el impacto de estas tecnologías en diversos sectores y realizar comparativas, como entre Edge Computing y Cloud Computing, destacando sus ventajas e inconvenientes.
- Estudiar la integración del IoT y la computación perimetral: comprender los conceptos fundamentales a través de un desarrollo teórico seguido de un análisis de la integración de ambas tecnologías.
- Estudio de casos prácticos: investigar casos específicos de aplicación del IoT y la computación perimetral en distintos sectores como el de la salud y las ciudades inteligentes, con especial mención al ámbito militar.
- Identificación de desafíos: reconocer áreas en las que estas tecnologías pueden ser mejoradas, especialmente en lo que respecta a la seguridad y la gestión eficiente de datos.
- Desarrollo de recomendaciones y líneas futuras: el objetivo de este punto será, con base en el estudio previo, ofrecer recomendaciones para futuras implementaciones y desarrollos tecnológicos en el IoT y la computación perimetral en la defensa.

2. Estado del arte

Este capítulo se centra en el estado actual del internet de las cosas y la computación perimetral, abordando sus avances, tendencias y desafíos.

2.1 Estado del arte del internet de las cosas

- Historia: aunque el término internet de las cosas es ampliamente utilizado, no existe una definición única y exclusiva. En se define el concepto como una red abierta y completa de objetos inteligentes que tienen la capacidad de autoorganizarse, compartir información, datos y recursos, y reaccionar y actuar frente a situaciones y cambios en el entorno. Este concepto de IoT ha evolucionado desde ideas simples a sistemas complejos que tienen repercusión en diversos aspectos de la vida cotidiana y la industria. El término fue acuñado por Kevin Ashton en 1999 y, desde entonces, la tecnología ha avanzado sig-

nificativamente, con ejemplos tempranos como la primera máquina expendedora conectada a Internet en 1982. El crecimiento de IoT ha sido exponencial, con proyecciones que indican un aumento significativo en el número de dispositivos conectados hacia 2030.

- Sensores: los sensores son componentes clave en IoT, encargados de recopilar información del entorno y convertirla en señales digitales. Existe una amplia gama de tipos de sensores utilizados en diversas aplicaciones, desde sensores de temperatura hasta sensores de nivel y de velocidad.
- Desafíos principales: el IoT enfrenta desafíos significativos, como la seguridad y privacidad de los datos, la interoperabilidad y estándares, legislación y regulación, escalabilidad, gestión y análisis de datos masivos, y consumo energético y sostenibilidad.

2.2 Estado del arte de la computación perimetral

- Introducción: Edge Computing es un cambio paradigmático en el procesamiento y análisis de datos, realizándolos cerca del lugar de generación en lugar de en centros de datos centralizados. Esta tecnología es esencial para IoT, mejorando la eficiencia del ancho de banda, reduciendo la latencia y mejorando la seguridad y privacidad de los datos.
- Comparativa con la computación en la nube: Edge Computing ofrece beneficios sobre Cloud Computing, como la reducción de latencia y respuesta más rápida. Mientras que la computación en la nube centraliza recursos, Edge Computing los distribuye, llevando el procesamiento de datos más cerca de donde se generan. Aunque Edge Computing ofrece ventajas en términos de latencia y procesamiento local, la escalabilidad puede ser un desafío. Los costes de mantenimiento y la eficiencia energética también son consideraciones importantes. Además, este paradigma plantea desafíos únicos en términos de seguridad y privacidad, ya que distribuye el procesamiento y almacenamiento de datos a través de múltiples dispositivos, lo que requiere un enfoque de seguridad robusto y distribuido.
- Casos de Uso: Edge Computing es particularmente adecuado para aplicaciones sensibles al tiempo, como la automatización industrial, vehículos autónomos, gestión de ciudades inteligentes y monitorización en tiempo real en el sector de la salud. En la defensa, donde la rapidez de respuesta y la seguridad de los datos son críticas, permite el procesamiento de datos en tiempo real, mejorando la eficacia operativa.

3. Integración del IoT con Edge Computing

La integración IoT-Edge Computing está redefiniendo la arquitectura de los sistemas de Tecnologías de la Información (TI) y ampliando su aplicación en diversos sectores. Esta convergencia permite que grandes cantidades

de datos, generados por dispositivos y sensores interconectados, se procesen más cerca de su origen. Este enfoque reduce la latencia y mejora las respuestas en tiempo real, siendo esto crucial en áreas donde la rapidez es esencial, como en algunos casos del sector sanitario o el propio ámbito militar.

El marco legal y regulatorio juega un papel significativo en la implementación de estas tecnologías. Normativas como el GDPR en Europa y leyes similares en Estados Unidos y China buscan equilibrar la innovación tecnológica con la protección de datos personales y la seguridad cibernética. Estas regulaciones imponen límites y obligaciones en la recolección y uso de datos personales, enfatizando la importancia de la seguridad desde el diseño inicial de los productos IoT.

Las arquitecturas IoT-Edge varían desde estructuras simples de tres capas hasta complejas de cinco capas. Estas definen cómo se conectan los dispositivos, se manejan los datos y se procesa la información, influyendo en el rendimiento y funcionalidad de los sistemas. Las capas van desde la percepción (sensores y dispositivos) hasta la aplicación y el negocio, abarcando funciones que van desde la recopilación de datos hasta el análisis y la toma de decisiones empresariales.

Las tecnologías de comunicación y los protocolos, como LPWAN, Zigbee, Wi-Fi, Bluetooth Low Energy, RFID y NFC, son esenciales para una comunicación coherente y confiable en el ecosistema IoT. Los protocolos como MQTT, CoAP, AMQP y HTTP, por su parte, facilitan la comunicación y el procesamiento de datos, destacándose por su eficiencia, seguridad y adaptabilidad a diferentes entornos y aplicaciones.

Este capítulo sienta las bases teóricas para una comprensión profunda de la integración del internet de las cosas con la computación perimetral, ofreciendo una visión detallada de las diversas arquitecturas y tecnologías que están configurando el futuro de los sistemas interconectados.

4. Casos de aplicación

Este capítulo se centra en cómo IoT y Edge Computing están siendo implementados en tres áreas vitales: salud, ciudades inteligentes y el sector militar. Iniciaremos con el sector salud, donde estas tecnologías están haciendo avanzar la atención al paciente y optimizando la gestión de datos médicos. Destacaremos casos específicos que ilustran la influencia positiva de IoT y Edge Computing en la mejora de la eficiencia y la efectividad del cuidado de la salud.

4.1 Ámbito de la salud

Los sistemas sanitarios conectados (Healthcare Internet of Things, H-IoT) generan una cantidad masiva de datos a través de diversos nodos sensoriales, desde dispositivos portátiles de monitoreo de pacientes

hasta sensores integrados en equipos médicos avanzados. La gestión eficiente de estos datos es fundamental para el funcionamiento óptimo de los sistemas de salud. Aquí es donde el Edge Computing descentraliza los recursos computacionales y extiende los servidores de la nube mediante nodos de borde. Esta descentralización permite un procesamiento más cercano a la fuente de datos, mejorando la velocidad y la eficiencia en el manejo de la información de salud.

La integración de la computación en el borde en los sistemas H-IoT no solo mejora el rendimiento de la red al reducir la utilización del ancho de banda y la congestión, sino que también optimiza los requerimientos energéticos, logra integridad de datos y mejora la seguridad de la red y la calidad del servicio. Estas mejoras son fundamentales en aplicaciones de salud donde la rapidez y la precisión en el procesamiento de datos son esenciales para decisiones clínicas críticas y para mejorar los resultados de salud de los pacientes.

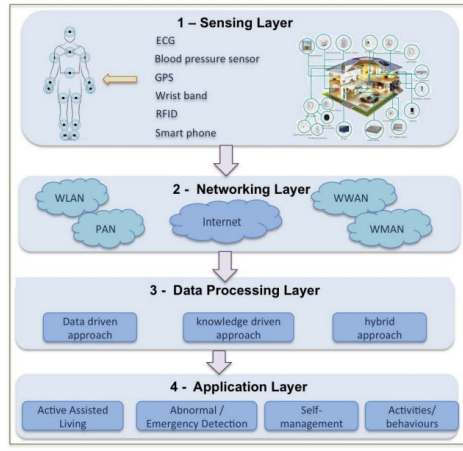


Figura 1. Modelo de trabajo en H-IoT

4.2 Ciudades inteligentes

En el contexto de las ciudades inteligentes, estas tecnologías están jugando un papel transformador en la manera en que se gestionan y se desarrollan las infraestructuras urbanas. En el ámbito del transporte, estos avances tecnológicos han llevado a la creación de sistemas de tráfico y estacionamiento más eficientes, facilitando así la movilidad urbana y reduciendo la congestión. Estos sistemas, alimentados por datos recopilados de sensores y dispositivos conectados, ayudan en la toma de decisiones para la planificación del transporte público y la infraestructura vial.

Además, la integración del IoT en la red eléctrica da lugar a lo que se conoce como la red eléctrica inteligente (Smart Grid). Esta tecnología

permite una gestión más eficaz y segura de la distribución de energía, adaptándose a las necesidades cambiantes de las ciudades. Paralelamente, en el sector de la agricultura y acuicultura urbanas, el uso de sensores IoT está transformando las prácticas agrícolas, permitiendo un manejo más eficiente y sostenible de los recursos. Estas innovaciones no solo mejoran la eficiencia de los servicios urbanos, sino que también contribuyen a mejorar la calidad de vida de los ciudadanos y fomentan un desarrollo urbano más sostenible.

4.3 Ámbito militar

El concepto del internet de las cosas se ha expandido más allá de sus aplicaciones civiles, adentrándose en el terreno del combate y la estrategia militar. En este contexto, el IoT se transforma en lo que conocemos como «Internet of Battlefield Things» (IoBT), un entramado de dispositivos interconectados que proporcionan datos críticos en tiempo real.

Adentrándonos en las aplicaciones específicas del IoT en el sector militar, uno de los usos más destacados es la recolección de conciencia del campo de batalla, donde drones y cámaras conectadas tienen un rol fundamental a la hora de mapear terrenos y posiciones enemigas, transmitiendo datos vitales al centro de mando.

Figura 2. IoBT

Los drones tienen la capacidad de revolucionar la estrategia militar en el campo de batalla. Equipados como servidores de borde aéreos o relés, ofrecen movilidad, flexibilidad y eficiencia de costes, convirtiéndolos en soluciones óptimas para el entorno de la defensa. Los UAV (Unmanned Aerial Vehicles) permiten a los dispositivos IoT descargar sus tareas computacionales, ya sea procesándolas localmente o enviándolas a servidores de borde o nube cercanos. Esta capacidad de procesamiento distribuido es fundamental para operaciones que requieren una toma de decisiones rápida y precisa, como el seguimiento de objetivos en tiempo real o la evaluación de situaciones complejas.

La implementación de UAV en sistemas de Edge Computing mejora significativamente la colaboración y sincronización entre unidades terrestres y aéreas. Actuando como nodos intermedios, no solo recopilan, sino que también procesan y distribuyen inteligencia de manera eficiente y segura. Esta tecnología es crucial en operaciones que abarcan amplias áreas geográficas o en entornos de difícil acceso, donde las comunicaciones tradicionales podrían estar comprometidas. Así, los drones habilitados para Edge Computing mantienen una ventaja táctica para las Fuerzas Armadas, maximizando la recopilación de datos y minimizando la latencia, lo que les permite operar con una conciencia situacional superior y, por tanto, en ventaja estratégica.

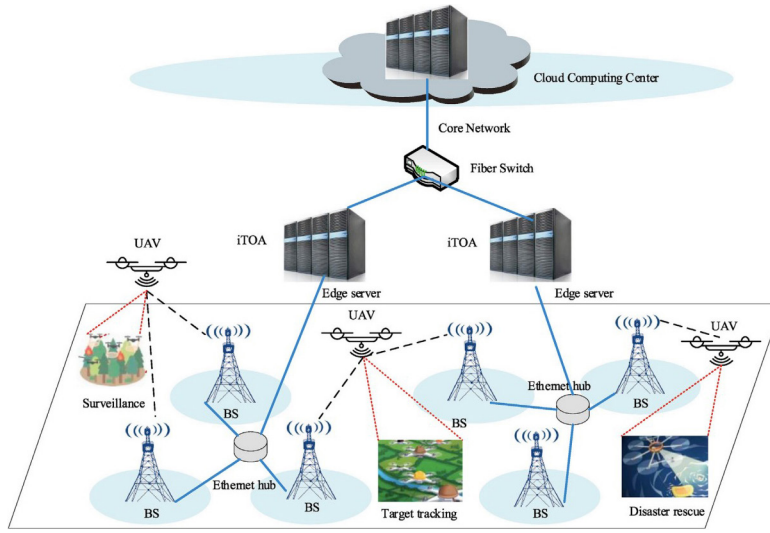


Figura 3. Estructura de una red de Edge Computing basada en drones

En la red ilustrada en la figura 3, los UAV operan como nodos de borde móviles y relés que procesan y transmiten datos, y simultáneamente como usuarios finales que llevan a cabo operaciones específicas como la vigilancia y el rescate. Esta configuración demuestra la capacidad de los UAV para integrarse en una red de Edge Computing, desempeñando múltiples funciones críticas dentro de la misma infraestructura y mejorando así la eficiencia y efectividad de las operaciones militares.

5. Conclusiones

En este TFM se ha realizado un análisis profundo a través de las complejidades y el potencial del internet de las cosas y la computación perimetral, destacando especialmente su relevancia en el sector de la defensa. A lo largo de este estudio, hemos visto la evolución del IoT desde sus orígenes hasta su estado actual, donde se manifiesta como un paradigma disruptivo, transformando la interacción entre el mundo digital y el físico. Sin

embargo, este avance no está exento de desafíos, como la seguridad de los datos, la privacidad, la escalabilidad y la interoperabilidad, que son cruciales para su desarrollo sostenible y seguro.

En el corazón de este análisis, la integración del IoT con la computación perimetral ha surgido como una solución estratégica para superar limitaciones inherentes a cada tecnología por separado. Esta sinergia es particularmente potente en contextos donde la rapidez y la eficiencia en el procesamiento de datos son críticos. Hemos observado cómo las regulaciones actuales y los estándares internacionales forman el esqueleto legal y ético que sustenta esta integración, garantizando que su implementación sea segura y responsable. Además, el estudio de las arquitecturas de múltiples capas en estos sistemas ha revelado cómo se pueden estructurar de manera eficiente para optimizar el rendimiento y la seguridad, especialmente en aplicaciones sensibles como las militares.

La exploración de casos prácticos en sectores como la salud, las ciudades inteligentes y, más intensamente, en la defensa, muestra solo una pequeña parte del amplio espectro de aplicaciones del internet de las cosas y la computación en el borde. En el ámbito militar, en particular, la fusión de estas tecnologías está marcando el comienzo de una era revolucionaria. La mejora en la percepción del entorno táctico y el fortalecimiento de las capacidades operativas son solo algunos de los beneficios de esta integración. La capacidad de tomar decisiones fiables y rápidas en el campo de batalla, apoyadas por datos procesados en tiempo real y cerca de donde se generan, subraya el valor incalculable de esta sinergia tecnológica.

En conclusión, este trabajo ha revelado que, aunque el IoT y la computación perimetral presentan desafíos individuales, su combinación abre un nuevo abanico de posibilidades, ofreciendo soluciones innovadoras a problemas complejos en varios sectores. La integración de estas tecnologías no solo aborda eficazmente sus limitaciones individuales, sino que también potencia sus fortalezas, lo que es especialmente crucial en el sector de la defensa, donde la eficiencia, la seguridad y la rapidez son de vital importancia. Este estudio no solo proporciona una comprensión profunda de estas tecnologías en el presente, sino que también sienta las bases para su evolución y aplicación futura, abriendo caminos para investigaciones adicionales y desarrollos tecnológicos avanzados.

Referencias

Madakam, S, Ramaswamy, R. Tripathi S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, 3(05), 164.

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal*, 22(7), 97-114.

Carnegie Mellon University. (s.f). The «Only» Coke Machine on the Internet. Disponible en: cs.cmu.edu/~coke/history_long.txt

Intersoft Consulting. (s.f.). General Data Protection Regulation (GPDR). Disponible en: gdpr-info.eu/

Wan, J., Gu, X., Chen, L. y Wang, J. (2017, October). Internet of things for ambient assisted living: challenges and future opportunities. En: *2017 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, pp. 354-357). IEEE.

Kott, A., Swami, A. y West, B. J. (2016). The internet of battle things. *Computer,* 49(12), 70-75.

Xia, X., Fattah, S. M. M. y Babar, M. A. (2023). A survey on UAV-enabled edge computing: Resource management perspective. *ACM Computing Surveys*, 56(3), 1-36.

Wu, W., Zhou, F., Wang, B., Wu, Q., Dong, C. y Hu, R. Q. (2022). Unmanned aerial vehicle swarm-enabled edge computing: Potentials, promising technologies, and challenges. *IEEE Wireless Communications*, 29(4), 78-85.

Chen, J., Chen, S., Luo, S., Wang, Q., Cao, B. y Li, X. (2020). An intelligent task offloading algorithm (iTOA) for UAV edge computing network. *Digital Communications and Networks*, 6(4), 433-443.

Estudio del estado del arte de la computación perimetral y el Internet de las Cosas aplicados a sistemas y tecnologías de la información para la Defensa

Autor: David Álvarez Sánchez
Director: Rubén Nocelo López
Universidade Vigo

Introducción

En la era actual, surge la necesidad de recoger, transmitir y procesar una gran cantidad de datos en tiempo real. Para ello se hace uso de:

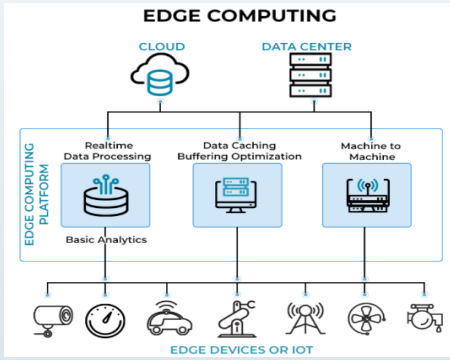
IoT: La interconexión digital de objetos cotidianos con Internet, permitiendo la recopilación y el intercambio de datos.

Edge Computing: El procesamiento de datos cerca de la fuente de datos, reduciendo la latencia y mejorando la rapidez de respuesta.

El objetivo del trabajo es explorar la sinergia entre IoT y Edge Computing para impulsar la innovación en aplicaciones militares.

Internet de las Cosas

Computación perimetral



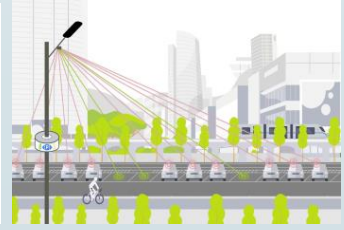
Conclusiones

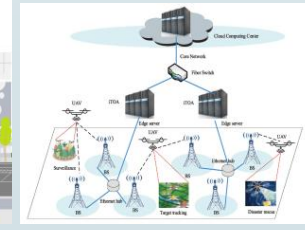
Eficiencia mejorada: La integración de IoT y Edge Computing demuestra un aumento significativo en la eficiencia operacional y la reducción de latencia en comunicaciones críticas.

Toma de decisiones estratégica: El análisis en tiempo real de datos a través de IoT y Edge Computing agiliza la toma de decisiones críticas en operaciones de defensa.

Conciencia situacional reforzada: La combinación de IoT con la computación perimetral proporciona una comprensión más profunda y un monitoreo más eficiente del campo de batalla.

Aplicaciones





Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

El arte de la ciberresiliencia

Autor: Artiles Burgos, M. Soraya (martbur@mde.es)
Directores: Vales Alonso, Javier y Rodelgo Lacruz, Miguel (externo.jvales@cud.uvigo.es / mrodelgo@cud.uvigo.es)

Resumen – La capacidad para anticipar, resistir, recuperarse y adaptarse a ciberataques a las infraestructuras TIC de defensa es crucial para el normal desarrollo de las misiones de defensa nacional, las cuales se desarrollan en un escenario mayoritario de tecnologías de la información y la comunicación. Este trabajo pretende estudiar las estrategias y acciones que se tienen que llevar a cabo para reducir la superficie de exposición en las infraestructuras TIC de defensa y que son aplicables al contexto de sistemas de información complejos en grandes organizaciones.

El objetivo de este trabajo es la definición de un conjunto de acciones de automatización de tareas de ciberresiliencia, gracias al desarrollo de una plataforma de gestión continua de la superficie de exposición a amenazas. Además, se plantea el desarrollo de un modelo de aprendizaje automático para reconocer el estado de riesgo de la superficie. Este algoritmo aprenderá de la inseguridad observada a diario y contribuirá a priorizar las acciones de mitigación. Asimismo, se proponen acciones para fortalecer la seguridad de los activos y garantizar el cumplimiento normativo en ciberseguridad.

Junto con estas acciones de automatización, que deben ejecutarse dentro una plataforma con acceso restringido en la infraestructura TIC de defensa, se implementan asimismo acciones manuales de seguimiento, coordinación y comunicación por parte de diversos roles de la organización para la reducción de la superficie de exposición. En síntesis, el objetivo final de este trabajo es el análisis y diseño de desarrollos innovadores que aborden la construcción de un entorno ciberresiliente para la reducción de la superficie de exposición. Esto se logrará mediante la implementación del conjunto de acciones de ciberresiliencia y su despliegue en una infraestructura TIC heterogénea y compleja, de forma que se pongan en juego todas las capacidades de automatización y coordinación de los actores que defienden y fortifican la columna vertebral digital de la defensa.

Palabras clave – Ciberresiliencia, Resiliencia, Ciberseguridad, Superficie, Vulnerabilidad

1. Introducción

1.1 Marco conceptual

Las acciones destinadas a la protección de las redes y sistemas de información se desarrollan en el ciberespacio y requieren claramente la reducción de la superficie de exposición. Estas acciones tienen que ver menos con actuaciones intrincadas y laberínticas, y más con algunos principios básicos como los definidos por el general, estratega militar y filósofo de la antigua China, Sun Tzu. Estos principios se aplican exclusivamente a la propia defensa de una infraestructura TIC:

1. **Principio de la unidad** (Unir para vencer)**:** Sun Tzu fomentaba la colaboración entre diferentes equipos con distintas responsabilidades. En el ámbito de la ciberseguridad, la colaboración entre las diferentes unidades de una organización, como el equipo de seguridad, personal de tecnologías de la información y otros departamentos, permite obtener una visión unificada de los puntos débiles de la infraestructura. Esta colaboración mejora la visión conjunta y contribuye a la reducción de la superficie de exposición ante posibles amenazas.
   - El supremo arte de la guerra es someter al enemigo sin luchar. La oportunidad de derrotar al enemigo está en tus manos; no en la oportunidad que el enemigo te brinda.
2. **Principio del conocimiento** (Conocimiento del enemigo y del entorno): Sun Tzu enfatizaba la importancia de conocer a tu enemigo y el terreno en el que te enfrentas. En ciberresiliencia, esto se traduce en la necesidad de conocer todos los elementos de la infraestructura, comprender las ciberamenazas, los posibles actores maliciosos y las vulnerabilidades en la infraestructura TIC.
   - Conoce al adversario y sobre todo conócete a ti mismo y serás invencible.
   - La información es poder.
3. **Principio de adaptación** (Conocer las debilidades propias). Sun Tzu abogaba por la inteligencia para la adaptación en la estrategia. En ciberresiliencia, esto significa que las organizaciones deben ser capaces de ajustar sus estrategias y defensas con base en las vulnerabilidades encontradas y conforme a cómo evolucionan las ciberamenazas.
   - Sé flexible y reflexiona antes de realizar un movimiento.
   - No debes depender de las condiciones favorables, ni de las condiciones desfavorables, sino que debes estar preparado para adaptarte a las condiciones.
   - La invencibilidad está en uno mismo, la vulnerabilidad en el adversario.

4. **Principio de la economía** (Priorizar los esfuerzos): Sun Tzu aconsejaba utilizar los recursos de manera eficiente. En ciberresiliencia, esto significa asignar recursos de seguridad de manera eficaz, centrándose en áreas críticas de la infraestructura.

Si se envían refuerzos a todas partes, se es débil en todas partes.

Grandes resultados pueden ser conseguidos con pequeños esfuerzos.

5. **Principio de terreno** (Disponer los mensajeros sobre el terreno): Sun Tzu argumenta que tener espías o agentes secretos bien ubicados en el campo de batalla es esencial para obtener información valiosa sobre el enemigo, sus movimientos, su moral y sus planes. Esto permite a un comandante tomar decisiones informadas. En ciberseguridad, esto se traduce en el despliegue de agentes por toda la infraestructura y a todos los niveles para poder obtener información de debilidades, amenazas a través de la simulación, configuraciones y potenciales caminos de ataque. La comunicación efectiva es clave para la ciberresiliencia.
   - La disposición de las tropas es clave para lograr la victoria, ya que una disposición adecuada puede maximizar las fortalezas y minimizar las debilidades de los soldados.
   - Solo cuando conoces cada detalle de la condición del terreno puedes maniobrar y luchar.
   - Los que no saben tener mapas, hacer reconocimientos o utilizar guías locales, son incapaces de obtener ventaja del terreno.

6. **Principio de la planificación** (Planificar y reflexionar): Sun Tzu enfatizaba la importancia de la planificación cuidadosa y la estrategia. En ciberresiliencia, esto se traduce en la necesidad de acumular la mayor cantidad de datos sobre el terreno de forma que se puedan planificar planes de respuesta a incidentes y estrategias de recuperación en caso de un ataque.
   - Reflexionar antes de hacer un movimiento.
   - Resolver dificultados antes de que surjan.
   - Las tácticas sin estrategia son el ruido antes de la derrota.

7. **Principio del engaño** (Fingir debilidad): Sun Tzu hablaba sobre la importancia de confundir al enemigo. En ciberseguridad, esto implica la utilización de tácticas de señuelo y detección temprana para identificar posibles amenazas.
   - Conocer al enemigo y utilizar al enemigo para derrotar al enemigo.
   - Para conocer a tu enemigo debes convertirte en tu enemigo.
   - Engaña al enemigo moviendo algo que él está obligado a observar.

8. **Principio de sorpresa** (Evaluación constante): Sun Tzu hacía hincapié en la importancia de la valoración estratégica de las tropas, el

enemigo y el terreno como parte fundamental de la ejecución de una campaña militar. En ciberresiliencia la realización de evaluaciones regulares de riesgos y vulnerabilidades en la infraestructura TIC consigue mantener un ciclo de mejora continua en la ciberdefensa de esta infraestructura.

— La manera de evitar lo que es seguro es estar en guardia, lo que es probable es estar preparado, pero lo que es completamente inesperado es ser completamente desconcertante.

9. **Principio de la defensa** (Defender en profundidad): Sun Tzu recomendaba la construcción de defensas en profundidad para protegerse contra los ataques enemigos. En ciberseguridad, esto se traduce en el bastionado de los activos de la infraestructura. Por otra parte, se incluye el cumplimiento con normativa específica de seguridad para llegar a una defensa casi total.

— La defensa es para tiempos de escasez, el ataque para tiempos de abundancia.

Si bien no se pueden aplicar los principios de Sun Tzu directamente a la ciberresiliencia, su enfoque en la estrategia, la adaptación y el conocimiento del enemigo puede proporcionar una base sólida para abordar los desafíos de ciberseguridad a los que se enfrenta una infraestructura TIC hoy en día.

1.2 Objetivos

La definición de los objetivos de este trabajo requiere del análisis de su cumplimiento con la situación actual de la infraestructura, y el contraste de los resultados y rendimiento en un futuro planificado. Para ello se deberá llevar a cabo la recolección de datos actuales y se establecerán metas futuras que permitirán ajustar los valores obtenidos para ir cumpliendo los objetivos establecidos. El resultado del cumplimiento de los KPI[1] se comprobará en las conclusiones de este trabajo.

En este contexto, se detallan los objetivos esenciales del presente trabajo, que buscan avanzar más allá de la clásica gestión de vulnerabilidades, que se centra en la identificación de activos, vulnerabilidades y parches, hacia la gestión de la exposición. La figura 1 complementa esta información al mostrar los indicadores clave de rendimiento actuales asociados a cada objetivo y los niveles que deben alcanzarse para asegurar un nivel adecuado de ciberresiliencia en la infraestructura TIC de defensa.

— Objetivo 1. Definición de acciones de comunicación y coordinación para la reducción de la superficie de exposición en infraestructuras TIC.

[1] KPI, por sus siglas en inglés (Key Performance Indicators).

El trabajo propone la definición de acciones de comunicación transparente y coordinación efectiva con todas las partes interesadas para la reducción de la superficie de exposición de las infraestructuras TIC de defensa, teniendo en cuenta que esta reducción implica la disminución de los puntos de acceso y las vulnerabilidades que podrían ser aprovechadas por los potenciales atacantes.

— Objetivo 2. Desarrollo de un entorno ciberresiliente que permite reducir la superficie de exposición en infraestructuras TIC.

  Por otra parte, el trabajo proporciona el desarrollo de una plataforma basada en un enfoque distribuido que recolecta información del ecosistema de agentes desplegados en los activos de la organización. Toda la información obtenida será analizada, cohesionada y centralizada para permitir una toma de decisiones rápida y eficaz.

— Objetivo 3. Cumplimiento con la normativa en ciberseguridad.

  Finalmente, el trabajo proporciona un análisis del cumplimiento con la normativa de ciberseguridad existente en la propia infraestructura de la organización. Esta normativa puede referirse a: guías de configuración segura (por ejemplo CCN-STIC[2]), legislación nacional en materia de seguridad, como son, el Esquema Nacional de Seguridad), y reglamentos europeos en materia de ciberseguridad y ciberresiliencia (por ejemplo, Directiva 2016/1148 y Reglamento 2019/881).

Figura 1. Objetivos para la reducción de la superficie de exposición. Fuente: elaboración propia

[2] Índice de guías CCN-STIC. Disponible en:https://www.ccn-cert.cni.es/guias/indice-de-guias.html

2. Acciones de ciberresiliencia

Los objetivos definidos anteriormente (figura 1) se llevarán a cabo a través del desarrollo de una serie de acciones de ciberresiliencia que permitan una reducción efectiva de la superficie de exposición (o superficie de ataque) para prevenir la explotación de vulnerabilidades, así como una clara mejora de las capacidades de ciberresiliencia de la organización.

Asimismo, estas están basadas en los principios estratégicos de Sun Tzu. La figura 2 resume la trazabilidad entre las estrategias clásicas de resiliencia, los objetivos definidos en este trabajo y las acciones para llevar a cabo la reducción de la superficie de exposición:

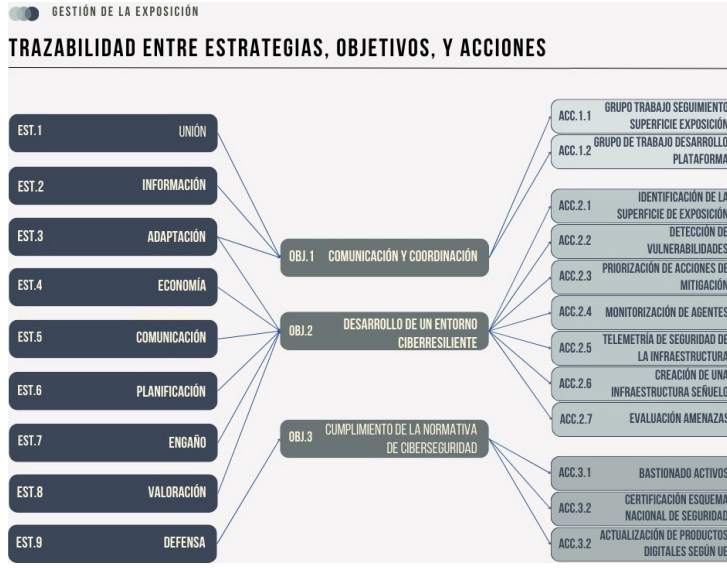


Figura 2. Trazabilidad estrategias, objetivos y acciones de ciberresiliencia para la reducción de la superficie de exposición. Fuente: elaboración propia

3. Metodología e implementación

Para llevar a cabo las acciones de ciberresiliencia, es necesario seguir una metodología de desarrollo de la plataforma con un enfoque integral estructurado y organizado. Esto implica diseñar, construir e implementar una solución para la Gestión Continua de la Exposición a Amenazas (CTEM[3]) que tenga la capacidad de evolucionar y añadir nuevas funcionalidades, basándose en los criterios definidos por los usuarios y posteriormente verificados por ellos mismos.

En este contexto, se han considerado ciertos principios que favorecen la implementación mediante una aproximación ágil y segura, al mismo tiempo que cumplen con los fundamentos establecidos para un enfoque

[3] CTEM, por sus siglas en inglés (Continuous Threat Exposure Management).

CTEM según las recomendaciones de Gartner. Este proceso comienza con una cuidadosa selección de herramientas, evaluándolas a través de pruebas de concepto. Posteriormente, se recopila la información de las herramientas seleccionadas mediante interfaces de programación de aplicaciones (API). Destaca especialmente el ciclo de vida del desarrollo, enfocándose de manera crucial en la participación activa de los usuarios de la plataforma. Además, se han implementado controles de seguridad específicos del Esquema Nacional de Seguridad con un cumplimiento de nivel ALTO. Este enfoque integral asegura la solidez y la continua adaptabilidad de la plataforma a lo largo de su evolución. La figura 3 presenta una de las funcionalidades de la plataforma CTEM, en particular aquella que proporciona detalles sobre el estado de la superficie de exposición.

Por otra parte, se ha diseñado un algoritmo de aprendizaje automático

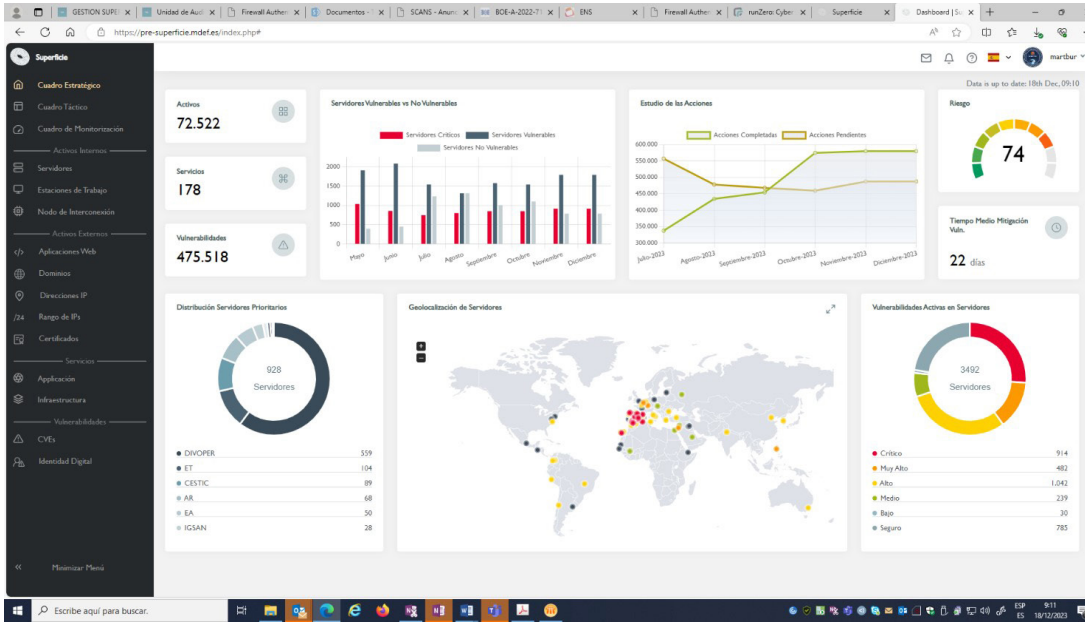


Figura 3. Plataforma SUPERFICIE-Panel estratégico. Fuente: elaboración propia

para el reconocimiento del estado de riesgo de la superficie, que permita al CISO[4] poder llevar a cabo una adecuada y precisa toma de decisiones basada en un dato simple y entendible: el estado de riesgo de la superficie de la infraestructura TIC. El modelo de inteligencia artificial escogido es el de aprendizaje supervisado mediante un modelo de regresión lineal múltiple[5]. Este enfoque de aprendizaje automático permite identificar el estado

[4] CISO, por sus siglas en inglés (Chief Information Officer).

[5] La regresión lineal múltiple es una técnica estadística que se utiliza para modelar la relación entre una variable dependiente (o de respuesta) y dos o más variables independientes (o predictoras). A diferencia de la regresión lineal simple, que involucra solo dos variables (una variable predictora y una variable de respuesta), la regresión lineal

de vulnerabilidad potencial de la superficie de exposición en función de las características seleccionadas (i.e. media de vulnerabilidades identificadas por activo en función del número de servidores conectados). Tras su implementación, se ha concluido que el coeficiente de determinación obtenido no es óptimo (i.e. 80 %) para el objetivo esencial de cuantificar la superficie anómala (figura 4). Se concluye, por tanto, que debería emplearse un modelo diferente, dado que los datos sugieren una relación no lineal entre sus variables.

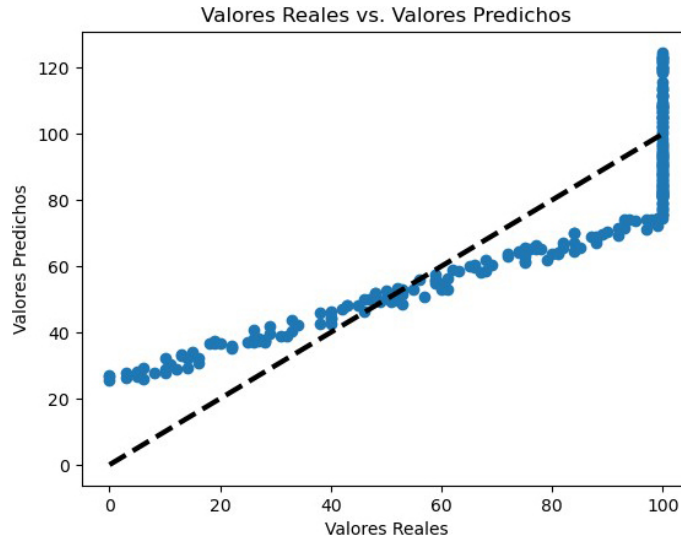


Figura 4. Algoritmo de regresión lineal múltiple. Valores reales versus reales predichos. Fuente: elaboración propia

Finalmente, es importante señalar que los usuarios de la propia plataforma «crecen con ella» y permiten su evolución hacia las funcionalidades que posibiliten una reducción máxima de la superficie de exposición.

4. Conclusiones

Gracias a la definición de indicadores de rendimiento que se pueden verificar en la operación diaria de la propia plataforma CTEM, se posibilita el seguimiento de los valores de partida y la medición periódica del progreso de la plataforma hacia los objetivos establecidos (figura 5). Este trabajo ha expuesto con precisión la medición de los valores iniciales y su consecución, alcanzando un grado de realización cercano al 100 % de los criterios previamente establecidos.

múltiple permite analizar cómo múltiples variables independientes están relacionadas con la variable de respuesta.

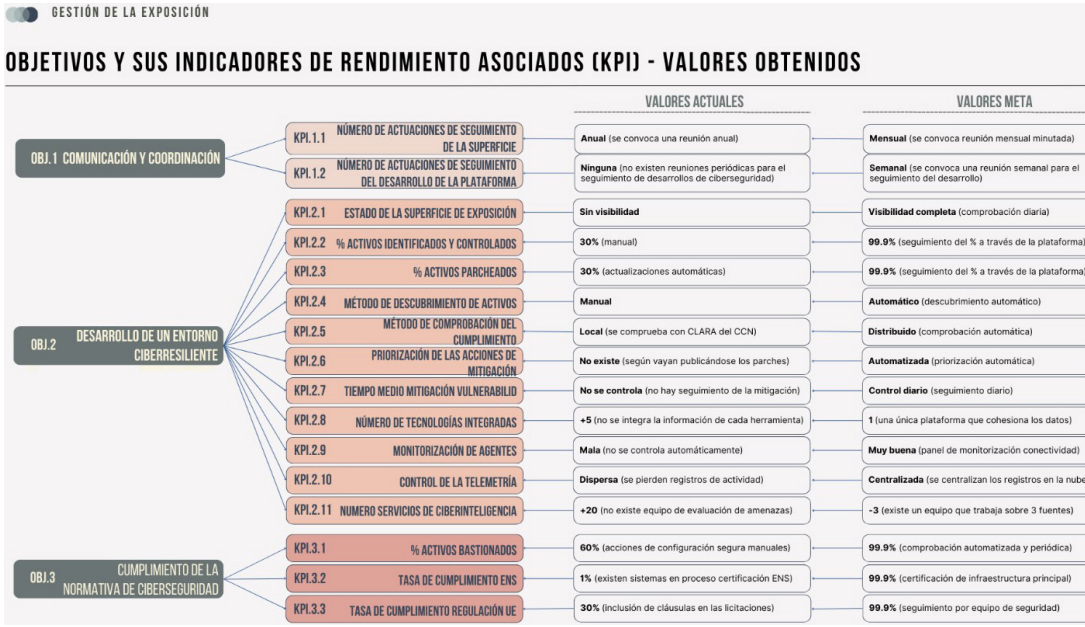


Figura 5. Objetivos y sus indicadores clave de rendimiento. Fuente: elaboración propia

En resumen, para alcanzar un nivel avanzado de madurez conforme al programa CTEM y lograr una optimización máxima, es fundamental seguir una serie de pasos clave. Esto implica medir sistemáticamente el nivel de riesgo de la organización, identificar proactivamente riesgos a través del aprendizaje y la predicción de amenazas futuras, priorizar acciones de mitigación basadas en evaluaciones previas de amenazas, integrar las capacidades del Equipo de Evaluación de Amenazas con las del Equipo de Seguridad Defensiva e incorporar nuevos desarrollos con enfoque en la seguridad, que incluyan algoritmos de inteligencia artificial para cuantificar la superficie anómala. Al implementar estas etapas de manera óptima, se logrará una infraestructura resiliente y mejor preparada para resistir los desafíos del entorno.

Referencias

Millán Martínez, J. M. (2022). Operaciones en el ciberespacio: ¿esas desconocidas? *Revista Ejército*, n.º 972.

Bhardwaj, A. y Goundar, S. (2018, abril). Reducing the threat surface to minimise the impact of cyber-attacks. *ScienceDirect*. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S1353485818300345

Tzu, S. (siglo V a. C.). *El arte de la guerra*.

Ministerio de Asuntos Económicos y Transformación. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*, n.º BOE-A-2022-7191.

Unión Europea. (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. *Diario Oficial de la Unión Europea*, n.º L 194/1.

Unión Europea. (2019). Reglamento (Ue) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). *Diario Oficial de la Unión Europe*a, n.º L 151/15, 2019.

D'Hoine, J., Shoard, P. y Schneider, M. (2023, 11 octubre). Implement Continuous Threat Exposure Management (CTEM) Program. *Gartner*. Disponible en: https://www.gartner.com/doc/reprints?id=1-2APCAC3H&ct=220729&st=sb

El arte de la ciberresiliencia

Autor: M Soraya Artiles Burgos
Director/es: Javier Vales Alonso y Miguel Rodelgo Lacruz

Universidad de Vigo

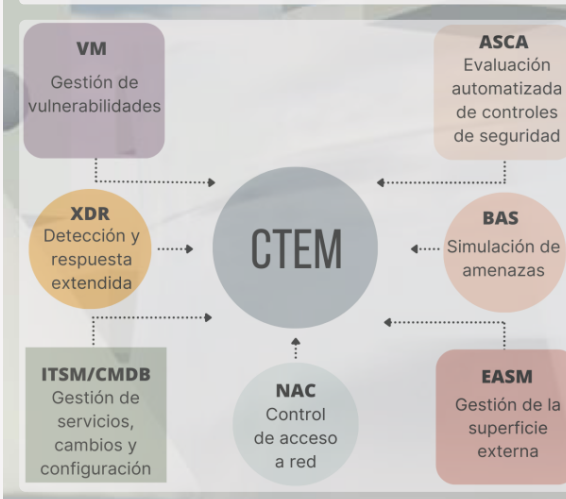
Acciones de ciberresiliencia

- **ACC 1.1** Reducción superficie exposición
- **ACC.1.2** Desarrollo plataforma
- **ACC .2.1** Identificación superficie
- **ACC 2.2** Detección vulnerabilidades
- **ACC 2.3** Priorización mitigación
- **ACC 2.4** Monitorización agentes
- **ACC 2.5** Telemetría seguridad
- **ACC 2.6** Superficie señuelo
- **ACC 2.7** Evaluación amenazas
- **ACC 3.1** Bastionado
- **ACC 3.2** Certificación ENS
- **ACC 3.3** Regulación EU

Reducción de la superficie de exposición

Las acciones de ciberresiliencia, inspiradas en los principios de Sun Tzu definidos en su obra "El arte de la guerra", constituyen una base esencial para reducir la superficie de exposición de una infraestructura TIC. Dichas acciones permiten identificar con exactitud todos los activos a proteger y priorizar tanto las estrategias de mitigación de vulnerabilidades como el bastionado de dichos activos Además, se concentra toda la información en una plataforma única de mando y control (CTEM), lo que optimiza la toma de decisiones basada en datos recabados diariamente.

Por otro lado, resulta fundamental el desarrollo de un modelo de aprendizaje automático para evaluar el nivel de riesgo de la superficie. Este algoritmo, que se nutre del estado de inseguridad diaria, jugará un papel fundamental en la priorización de las acciones de mitigación y bastionado.



Plataforma CTEM

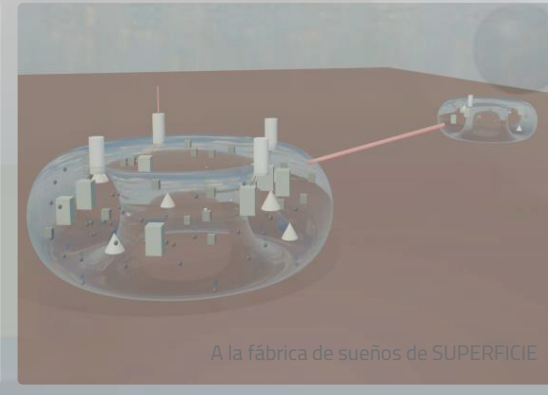
La plataforma para la Gestión Continua de la Exposición a Amenazas (CTEM) recopila toda la información de las herramientas de ciberseguridad de la infraestructura TIC.

Esta información es cuidadosamente cohesionada para reconocer el estado de riesgo de la superficie de exposición.

Superficie de exposición

Conjunto de activos, sistemas de información, datos y conexiones que son visibles y accesibles desde el entorno digital.

Puede existir una superficie señuelo para evaluar la infraestructura desde el exterior.



Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Seguridad en redes 5G Militares Desplegables

Autor: Cartujo Olmo, Pablo (pcarolm@fn.mde.es)
Director: Gil Castiñeira, Felipe (externo.felipegil@cud.uvigo.es)

Resumen – En este TFM se realiza un análisis exhaustivo sobre la implementación y los desafíos de seguridad de las redes 5G en contextos militares. En una primera parte se describen las capacidades avanzadas de las redes 5G, incluyendo su alta velocidad y flexibilidad, que son cruciales para las operaciones militares modernas. Se enfoca en cómo estas redes mejoran la comunicación en escenarios tanto navales como terrestres, pero también destaca la importancia de abordar sus vulnerabilidades ante ciberataques. A continuación se profundiza en la infraestructura de las redes 5G, detallando su funcionamiento y las soluciones específicas desarrolladas para la Armada por Telefónica.

Se analizan en detalle las vulnerabilidades de estas redes, constatando un avance en cuanto a las medidas de seguridad ante ciberataques comparadas con las redes 4G. Esto se debe a su mayor complejidad y al uso de nuevas tecnologías que aún están en proceso de maduración en términos de seguridad o a impresiones en la implementación de los estándares.

Ante estas evidencias se propone una serie de medidas para mitigar estos riesgos, entre las que se incluyen el desarrollo de protocolos de seguridad más robustos, la implementación de sistemas de detección y respuesta a intrusiones y la constante actualización y revisión de las prácticas de seguridad. Además, sugiere la investigación y adopción de nuevas soluciones técnicas que puedan reforzar la ciberdefensa en el contexto de las redes 5G militares.

Finalmente, el documento concluye con una reflexión sobre la importancia crítica de asegurar las redes 5G en el ámbito militar. Subraya que, aunque las redes 5G ofrecen numerosas ventajas en términos de rendimiento y capacidad, la seguridad debe ser una prioridad para garantizar el desarrollo de la nube de combate.

Palabras clave – 5G, LTE, Ciberataque, Ciberespacio, Ciberdefensa, Sistema.

1. Introducción

Las redes 5G en sus múltiples configuraciones son una tecnología compleja con múltiples posibilidades de funcionamiento que se deben conocer para entender las soluciones que se pueden utilizar en el mundo militar. Es de vital importancia entender la evolución que ha supuesto el sistema 5G frente a los sistemas tradicionales en cuanto al modelo de creación de redes y los múltiples sistemas radio que es capaz de manejar.

La evolución de las redes de telecomunicaciones móviles ha sido significativa en las últimas décadas, comenzando con la 1G, que introdujo las comunicaciones móviles analógicas, y avanzando a la 2G, que trajo consigo la digitalización y los servicios de mensajes. La 3G mejoró la capacidad y velocidad, enfocándose en la transmisión de datos y soporte para Internet, mientras que la 4G se centró en la alta velocidad y la computación en la nube. La 5G, siendo una evolución natural, hereda y mejora tecnologías de generaciones anteriores, ofreciendo mayor velocidad y capacidad, y plantea nuevos desafíos y consideraciones en cuanto a seguridad.

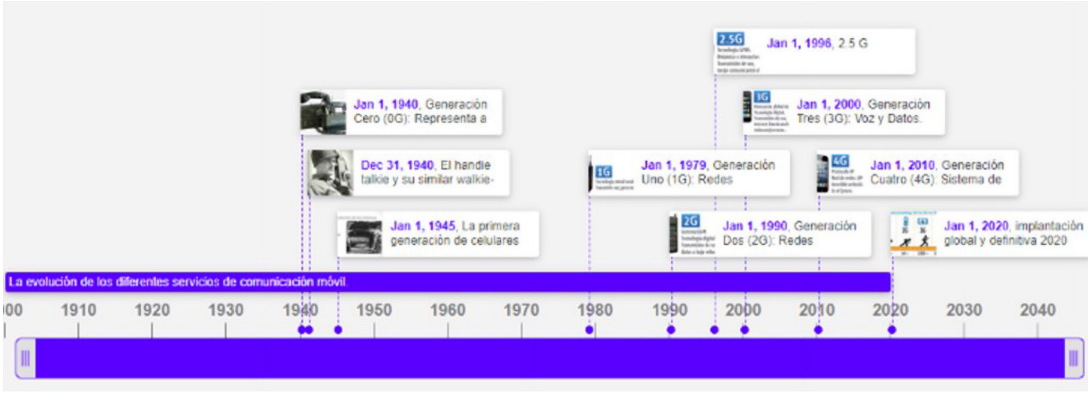


Figura 1. Evolución de las redes móviles

Las redes 5G aprovechan tecnologías ya existentes como la Multiple-Input Multiple-Output (MIMO), basándose en el principio de que, utilizando múltiples antenas, se pueden enviar y recibir múltiples flujos de datos simultáneamente, lo que aumenta significativamente la capacidad y la calidad de la conexión. También aplican tecnologías nuevas como el *slicing,* mediante el cual se introduce la virtualización de redes y la computación lógica para facilitar aplicaciones emergentes que pueden tener diversos requisitos de servicio. Por medio del *slicing* se divide una red física en múltiples redes lógicas virtualizadas únicas sobre una infraestructura común de múltiples dominios. A través de este concepto, se pueden asegurar tanto QoS como recursos de red.

Con estas mejoras técnicas, la 5G presenta como principales beneficios frente a tecnologías anteriores una ostensible mejora en la tasa de

transferencia de datos, en la latencia, en la eficiencia energética, en el volumen de tráfico soportado y en la densidad de conexiones.

A la hora de desplegar las redes 5G existen dos modelos: el modelo Stand Alone (SA) y el modelo Non Stand Alone (NSA). El 5G SA es el modelo de implementación, donde el 5G proporciona una red 5G de extremo a extremo; en esta arquitectura, tenemos una red independiente como 5G New Radio. SA presenta una arquitectura 5G pura y esta implementación se basará en el uso de 5G para el plano de control y el plano de usuario. La opcion Non Stand Alone, por el contrario, responde a una red 5G respaldada por la infraestructura 4G y las radios 5G acopladas a la LTE EPC. Es decir, las redes NSA ofrecen conectividad tanto a través de 4G AN (E-UTRA) como de 5G (NR). Esta doble característica también se denomina EN-DC, o doble conectividad E-UTRAN-NR.

Un problema al que deben de hacer frente las 5G es la gestión del espectro, las frecuencias son un bien escaso y muy demandado dentro de las comunicaciones tanto civiles como militares y su uso debe de ser regulado por la administración. Existen numerosas iniciativas para la gestión del espectro, entre las que se encuentra Authorized Shared Access (ASA); creado como una herramienta para evaluar las bandas asignadas al servicio móvil, Mobil Service, (MS) mediante las regulaciones de radio, pero identificado y utilizado para diferentes propósitos derivados de decisiones nacionales de las administraciones (u organizaciones regionales). Al final, como ha sido el caso con las 5G, se ha tenido que compartir el espectro en este sentido, uno de los ejemplos internacionales de mayor importancia es el conocido como Servicio de Radio de Banda Ancha para Ciudadanos (CBRS) americano. En el CBRS, los niveles de acceso se dividen en tres niveles: el primer nivel de acceso a acceso para titulares está compuesto por los radares navales en aguas litorales y el servicio comercial de satélites fijos, Fixed Satellite Service (FSS); el segundo nivel consiste en

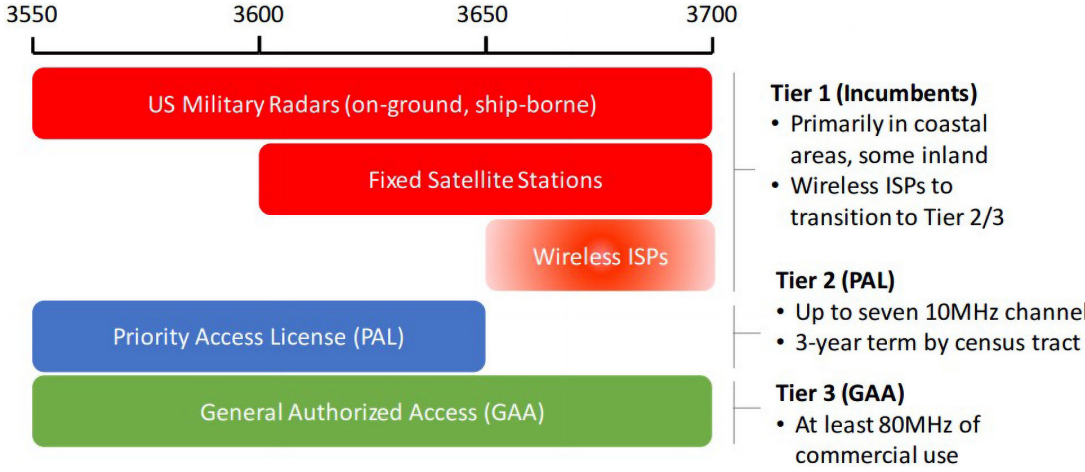


Figura 2. CBRS Tier 1-3

Licencias de Acceso Prioritario (PALs), y el tercer nivel comprende a los usuarios oportunistas conocidos como Usuarios Autorizados Generales (GAA). La asignación de canales a diferentes niveles y las configuraciones relacionadas son realizadas por el SAS.

2. Desarrollo

2.1 Despliegue 5G en la Armada

En el pasado, la Armada experimentó con la tecnología 4G-LTE, implementada en los BAM «Furor» y «Audaz», únicamente para los Trozos de Visita y Registro. Con la implementación de las redes 5G, las capacidades logradas anteriormente mejoran de forma exponencial en términos de fiabilidad, velocidad y alcance, haciéndose extensivo a todo espectro de las operaciones navales, en la forma del concepto «nube de combate». Este concepto, tanto a nivel nacional como internacional, cada vez está ganando más importancia. Esta «nube» será un sistema complejo, sobre el que se desarrollen e integren los servicios necesarios para alcanzar la superioridad en la información que permita reducir los tiempos del ciclo de decisión, disponiendo de la información correcta en el lugar adecuado y en el momento preciso, y proporcionando una capa de comunicaciones de calidad, lo que ya se conoce como «burbuja táctica».

Para ello se ha planteado tres escenarios:

- Proyecto Base Naval, escenario litoral. Despliegue de Nodo Fijo: La solución propuesta debe permitir el empleo de una combinación de frecuencias de radio que posibiliten la conectividad de los distintos elementos en un ambiente litoral como extensión o apoyo a unidades navales o intra base, maximizando la distancia operativa y mitigando posibles problemas de interferencias. Las bandas que se consideran más adecuadas para optimizar este proyecto son las de 700 MHz y 4.4 GHz, aunque podría evaluarse la posibilidad de emplear la banda de 26 Ghz, en principio desestimada por el bajo alcance que ofrece.
- Proyecto buques de la Armada: la instalación de equipos 5G en una plataforma naval y los equipos necesarios para explotar esta capacidad entre al menos dos buques de la Armada. Esta solución debe permitir su despliegue temporal en otras unidades, hasta que la implantación de la tecnología 5G sea alcanzada en todas las unidades navales.
- Por otro lado, la instalación de un nodo SA en un buque permite establecer comunicaciones buque-cosas y el establecimiento de una burbuja de comunicaciones alrededor del buque que posibilitará el empleo de vehículos no tripulados, el establecimiento de las comunicaciones con otras unidades que se encuentren dentro de la burbuja y sensorizar gran parte de los sistemas del buque. También permitiría la conexión a los nodos en ambiente litoral.

— Proyecto Unidades de Infantería de Marina. Como complemento a los dos proyectos anteriores se realizó un diseño de red con las antenas necesarias para establecer una burbuja de comunicaciones y con toda la preinstalación necesaria para integrar un 5G CN en un vehículo táctico de Infantería de Marina.

Simultáneamente se probaron las antenas y alcances en el «palo integrado» de las fragatas F-110 y en los buques de mando con resultados satisfactorios.

2.2 Seguridad en las redes 5G

Aunque generalmente la red 5G es considerada una evolución tecnológica, en tanto incrementa la capacidad y cobertura, puede ocurrir que en algunos aspectos no sea más segura que la red 4G. Esto es porque en virtud del desempeño de la red se han hecho concesiones de seguridad; Por su carácter inalámbrica puede sufrir ataques de emulación de la BS; o también debido al factor de su gran velocidad de transporte de datos y el soporte creciente de las aplicaciones, las cuales generan nuevas brechas de seguridad, tanto en el ámbito de los proveedores de servicios, como de los usuarios finales.

Por otra parte, existen ciertas mejoras en cuanto a la seguridad. Una parte importante no había sido considerada en las redes anteriores a 5G, mientras que en otros campos solo se mejoran las capacidades de seguridad.

Pese a estas mejoras frente a las anteriores versiones, lo cierto es que, entre otras causas, con una mayor velocidad de datos, la red 5G puede ser objeto de ataques, por ejemplo, de Denegación de Servicio Distribuido (DDoS) más fuertes y precisos.

Así, la seguridad debe de abordarse desde diferentes enfoques.

— La seguridad de las redes 5G no se puede abordar desde un único frente, sino que se plantean seis diferentes enfoques:
— Seguridad en el acceso a la red: características de seguridad que permiten a un terminal de usuario autenticarse y acceder a la red al proporcionar protección en las interfaces de radio.
— Seguridad en el dominio de la red: características de seguridad que permiten a los nodos de la red intercambiar señalización y datos de usuario de manera segura.
— Seguridad en el dominio del usuario: características de seguridad que permiten el acceso seguro de los usuarios a los dispositivos móviles.
— Seguridad en el dominio de la aplicación: características de seguridad que permiten el intercambio seguro de mensajes entre aplicaciones en los dominios de usuario y proveedor.

— Seguridad en el dominio de la Arquitectura Basada en Servicios (SBA): un nuevo conjunto de características de seguridad que permite a las funciones de red de la SBA comunicarse de manera segura dentro de los dominios de servicio y otros dominios de red. Visibilidad y configurabilidad de la seguridad: características de seguridad que permiten al usuario estar informado sobre qué características de seguridad están en funcionamiento.

2.3 Seguridad en las redes 5G de la Armada

Los sistemas 5G en la Armada presentan como hemos visto ciertas singularidades con respecto a los sistemas comercializados por los operadores o los ISP. Estas singularidades, a la vez, son también unas medidas de seguridad en sí mismas. Entre otras, podemos destacar que se trata de sistemas que cuentan con su propia RAN, su propio *core* y con una cantidad limitada y conocida de UE. Estos terminales usan su propia SIM, que como hemos visto llevan su propio sistema de cifrado.

Además, los elementos de la red están protegidos de forma física. Por ejemplo, la RAN de un operador cualquiera puede estar colocada en la azotea de un edificio de una comunidad de vecinos cualquiera. Sin embargo, la RAN militar se encontrará en una unidad militar o baja lo protección continua de esta.

También debemos de recordar que los UE no hacen *roaming*, no se conectan a otras redes, aunque se traten de redes comerciales seguras. De hecho, no se pueden conectar ni siquiera a la red del *partner* tecnológico. Asimismo. tampoco está contemplada la posibilidad de que se una a las redes 4G con las que cuenta la Armada.

Por todo lo anterior, las vulnerabilidades a estos sistemas están más restringidas que las de las redes 5G de las operadoras. Sin embargo, afrontan otras problemáticas, como la confidencialidad de la información que manejan, así como la disponibilidad de la misma y la robustez en las comunicaciones.

De cara a analizar las vulnerabilidades para este escenario en cuestión, vamos a admitir que el atacante no pude tener nunca acceso físico, a las SIM *card*, a la estación base, o al CN para obtener acceso a las claves de sesión a las claves criptográficas. Por el contrario, en nuestras premisas sí que establecemos que el atacante puede o está dispuesto a interceptar la señal radio, realizar ataques MiM, *spoofing* y que es capaz de transmitir en la misma frecuencia que nuestra BS y con igual o más potencia.

En este sentido se estudian las vulnerabilidades que se consideran más factibles, teniendo en cuenta el modelo de red que se ha adoptado, como son: la autenticación mediante MAC, o el aprovechamiento de los mensajes MIB, Master_Info_Block, y los mensajes SIB, System_Info_Block, o la Defensa contra *jamming* y *spoofing*. Se han desdeñado todas a aquellas otras que no se aplican, bien porque afectan a factores como el *roaming*

que son no aplicables o porque se consideran solventadas con la infraestructura aplicada. En este sentido se propondrán soluciones a estas carencias de seguridad.

Finalmente se anticipan soluciones consideradas prometedoras, entendiendo como tales las necesidades que se pueden plantear como evolución a la propuesta actual. Con las autolimitaciones impuestas, también se han generado barreras a ciertas capacidades de la tecnología que desde esta opinión deben de al menos ser contempladas de cara a futuros desarrollos o a mejoras en el ciclo de vida. También se pueden identificar soluciones a problemas que pueden ocurrir cuando se establezcan escenarios diferentes, como la inclusión de usuarios itinerantes en la red 5G militar, el uso de antenas sobre dron cautivo para ampliar alcances, el uso de *slices* en frecuencias alternativas o el aumento de la potencia de transmisión.

3. Conclusiones

Las redes 5G son la apuesta de futuro en las comunicaciones tácticas, especialmente en las navales. Si bien han surgido problemas, como la repartición del espectro –problema grave en ambientes como el marítimo en el que no existen *a priori* otras fuentes de radiación que las propias–, no parecen ser un verdadero problema. En otros escenarios, como los terrestres o los litorales, sí puede plantear dificultades, ya que la banda elegida puede entrar en conflicto con intereses civiles. De todas formas, estas dificultades pueden ser fácilmente soslayables mediante legislación o aumento de potencia.

Lo que sí parece indudable es la gran cantidad de casos de uso que se le pueden atribuir y la capacidad adicional que otorgará a las naciones capaces de explotar sus capacidades. Es de resaltar que otras potencias militares estén interesadas en nuestras soluciones y que seamos como nación y sector industrial pioneros en este campo. Desde el punto de vista del autor, esta primacía se ha conseguido por varios factores, entre los que destaca el concurso de un ISP importante nacional como es Telefónica, así como los esfuerzos que se realizaron con el desarrollo del 4G naval.

Los esfuerzos realizados para crear soluciones multiescenario, como son el terrestre, naval puro y litoral, han dado como fruto soluciones ya depuradas y experimentadas sobre el terreno, con esa capacidad desplegable que caracteriza a la Armada. El concepto de nube de combate o nube táctica parece estar maduro, mientras que se observa una clara evolución en cuanto a capacidades sobre los primeros intentos sobre redes 4G. La continuidad y la segura evolución parece garantizada con las pruebas realizadas con el «palo integrado» de la futura F110. El haber confirmado su viabilidad es de suma importancia, ya que la inclusión de nuevas antenas perjudicaría seriamente a un diseño tan notable como lo es la mueva serie de fragatas de alta capacidad.

Salvando la bondad del diseño y la capacidad de integración en futuras unidades, cobra especial relevancia el factor de la seguridad. Si la seguridad en las redes de comunicaciones es un factor sumamente importante, lo es aún más para las redes militares. Las redes 5G no son ajenas a ello y ha evolucionado notablemente en comparación con sus predecesoras. En gran medida, las 5G implementan nuevas formas de securización de las redes o mejoran las ya existentes. No obstante, muchas de estas medidas, si bien son contempladas por la asociación encargada de estandarizarlas, en gran cantidad de ocasiones dejan al libre albedrío del operador la implementación de parte de ellas. Por lo tanto, las redes 5G militares deben de hacerse cargo e implementar todas estas medidas o, en su defecto, sustituirlas por otras que al menos las igualen en capacidades.

A estos efectos, durante esta monografía se han explorado los mecanismos y las vulnerabilidades de seguridad. De todas las amenazas a las redes 5G conocidas, la solución implementada es la menos vulnerable. Se trata de una solución SA con todo el equipamiento de red propietario y aislado. Este esquema plantea una red SA con CN, RN y UE propietarios y aislada de otras redes. A su vez, tampoco permite la conexión a otras redes como 4G. Tras analizar las vulnerabilidades que pueden afectarle se puede considerar una red segura, más aun teniendo en cuenta que se trata de una red cifrada.

A partir de esta configuración, las posibilidades que puede aportar a un entorno táctico son muy elevadas, gracias a la velocidad, baja latencia y disponibilidad que otorga. Sobre el terreno, la solución puede aportar capacidades tácticas en entornos de comunicaciones degradadas, como es la «nube de combate». A medida que la efectividad de las redes 5G militares se continúe, aumentarán los casos de uso.

Si el proyecto dron cautivo se formaliza de manera correcta el escenario «litoral» pasará a ser aquel cualquiera en el que concurse un destacamento de Infantería de Marina y un buque de la Armada. Es decir, debido al alcance que van a proporcionar estos elementos, el elemento de instalación en tierra podrá ser cualquier elemento móvil y además será sumamente discreto.

Como líneas de acción a futuro, entendemos que las redes 5G militares deben de disponer de la capacidad de permitir el acceso a las redes militares de usuarios no pertenecientes a la infraestructura original. Es decir, permitir que un tercer Estado se conecte a nuestra red con sus propios terminales. Aprovechando la capacidad de crear *slices,* se pueden segregar estos terminales dándoles capacidad, por ejemplo, para disponer de comunicaciones telefónicas mediante el uso de la salida satélite de nuestro nodo. Esta característica tendría un componente «efectista» de cara a la opinión pública y representaría una gran publicidad como país generador de tecnología.

Por último, se considera que la no inclusión de tecnologías menos capaces como las 4G o LTE es un acierto, porque crearía puntos únicos de fallo en cuanto a vulnerabilidades.

Referencias

Brito, J. R. (2019). Evolucion de las rede móviles hasata hoy en día y el impacto de la red móvil de quinta generación. *Revista ReDTiS*, vol. 3, n.º 3, 17 diciembre.

Jordão, M. y Carvalho, N. B. (2018). Massive MIMO Antenna Transmitting Characterization. En: *IEEE MTT-S International Microwave Workshop Series on 5G Hardware and System Technologies (IMWS-5G)*. Dublin, Ireland.

Zamfirescu, C., Iugulescu, R., Crăciun, R., Vulpe. A., Li, F. Y. y Halunga, S. (2024). Network slice allocation for 5G V2X networks: A case study from framework to implementation and performance assessment. *ScienceDirect,* vol. 45, n.º 100691.

Parvez, I et al. (2018). A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. En: *IEEE Communications Surveys & Tutorials*, vol. 20, n.º 4, pp. 3098-3130.

Akshatha, N. M., Jha, P. y Karandikar, A. (2018). A Centralized SDN Architecture for the 5G Cellular Network. En: *IEEE 5G World Forum (5GWF).*

Sultan. (2022). 5G System Overview. 3GPP Rel 19. *3GPP.*

Buckwitz, K., Engelberg, J. y Rausch, G. (2014). Licensed Shared Access (LSA) — Regulatory background and view of Administrations. En: *9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM).* Oulu, Finland.

Mun, K. (2017). Ongo: New Shared Spectrum Enables Flexible Indoor and Outdoor Mobile Solutions and New Business Models, *Mobile Experts. Ongo White Paper*.

Thomas, R. y Scholler, F. (2021). Overview of NIAG Study SG-254. *Orange-Thales*.

Newman, L.N. (2019, diciembre). 5G Is More Secure Than 4G and 3G—Except When It's Not. *Wired.* [Consulta: 22 de noviembre 2023]. Disponible en: https://www.wired.com/story/5g-more-secure-4g-except-when-not/

Gonzalez, C. (2019). Desafíos de Seguridad en Redes 5G. *Revista Technology Inside by CPIC*, vol. 3, n.º 3, pp. 36-45.

Seguridad en Redes 5G Militares Desplegables

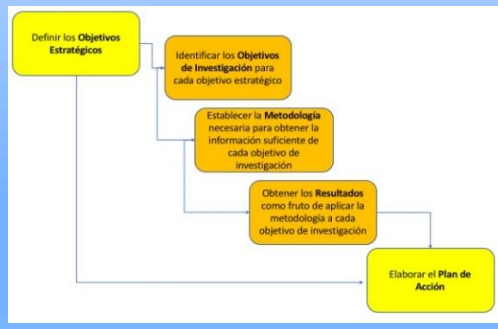
Autor: Pablo Cartujo Olmo
Director: Felipe Gil Castiñeira

Introducción

El objetivo de este trabajo es realizar un estudio sobre las redes 5G exponiendo el funcionamiento e infraestructura de las redes 5G, describir la aproximación al sistema desarrollada conjuntamente por la Armada y Telefónica y que actualmente se ha puesto al servicio de Defensa. Una vez familiarizados con la infraestructura se evaluarán sus vulnerabilidades tanto genéricas de la redes 5G diferenciando las generales, comunes a todas las redes 5G como las particulares institucionales de nuestra infraestructura sectorial

Metodología

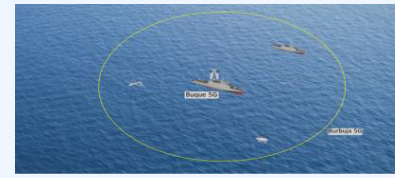
Metodología basada en el análisis y síntesis de una amplia variedad de documentación de fuentes contrastadas, como páginas web especializadas, trabajos académicos, conferencias científicas, investigaciones académicas, revistas científicas y publicaciones militares. El objetivo es lograr una comprensión profunda y exhaustiva del tema, fundamentada en la investigación y el análisis de fuentes relevantes.



Resultados

Las redes 5G en la configuración propuesta por la Armada presenta las siguientes ventajas:

- Solución multi escenario.
- Mayor seguridad que soluciones convencionales.
- Nube táctica.



Líneas de futuro y capacidad de mejora:

- Dron cautivo
- Accesos segregados a la red.

Conclusiones

En el desarrollo de la solución 5G adoptada por la

Armada ha primado la robustez y la seguridad con el objetivo de crear la denominada nube de combate. Esta solución será plenamente integrable en las futuras unidades navales y ofreciendo una superficie de exposición a ataques ciber que las soluciones comerciales

Agradecimientos

A mi tutor D. Felipe Gil y mi mujer Maria Jose, que por su comprensión y apoyo. Recuerdo especial a mi Tía Maria del Carmen Olmo.

Transición de Tetrapol a LTE

Autor: Cerrato Moreno, Sandra (cerrato.moreno@policia.es)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – Este trabajo tiene como objetivo presentar las iniciativas de la Oficina de Programa SIRDEE para atender las demandas de los usuarios finales en comunicaciones críticas. Se abordarán los desafíos y beneficios asociados con la migración de Tetrapol a LTE en el contexto de las redes de comunicación críticas.

La rápida evolución tecnológica está impulsando a las organizaciones a abandonar sistemas heredados en favor de soluciones más avanzadas que satisfagan las necesidades operativas de los usuarios finales. Actualmente, enfrentamos un gran reto: la transición desde Tetrapol, una tecnología sólida y establecida, aunque antigua, hacia una plataforma moderna como LTE.

Este proceso de migración implica explorar tanto los desafíos como las oportunidades que surgen en el ámbito de las redes de comunicación críticas. La transición no solo busca modernizar la infraestructura existente, sino que también abre nuevas posibilidades para las comunicaciones de emergencia a nivel nacional y europeo.

Palabras clave – Tetrapol, LTE, Comunicación crítica, Migración tecnológica, Redes inalámbricas, Seguridad.

1. Introducción y contexto

La evolución de las comunicaciones críticas en España, específicamente la transición del sistema SIRDEE (Sistema Integral de Radiocomunicaciones Digitales de Emergencia del Estado) basado en tecnología Tetrapol hacia una solución de banda ancha LTE, representa un desafío significativo y una oportunidad para mejorar las capacidades de comunicación de los servicios de emergencia y seguridad pública.

El sistema SIRDEE, implementado en el año 2000, ha proporcionado comunicaciones seguras y fiables para las Fuerzas y Cuerpos de Seguridad del Estado durante más de dos décadas. Sin embargo, la creciente demanda de servicios de datos de alta velocidad, vídeo en tiempo real y otras aplicaciones avanzadas han impulsado la necesidad de evolucionar hacia tecnologías más modernas como LTE.

2. Características y limitaciones de Tetrapol

Tetrapol, la tecnología actual de SIRDEE, ofrece:

— Alta fiabilidad y seguridad para comunicaciones de voz.
— Cobertura nacional del 95 % del territorio.
— Capacidad para soportar alrededor de 70 000 usuarios.
— Cifrado robusto de extremo a extremo.

Sin embargo, presenta limitaciones:

— Velocidades de datos bajas (2.4 Kbps).
— Capacidad limitada para servicios multimedia.
— Dificultad para interoperar con sistemas más modernos.

3. Ventajas de LTE para comunicaciones críticas

LTE ofrece numerosas mejoras:

— Mayores velocidades de datos (hasta 100 Mbps de descarga).
— Soporte para aplicaciones multimedia y vídeo en tiempo real.
— Mejor eficiencia espectral.
— Mayor flexibilidad y capacidad de evolución.
— Posibilidad de aprovechar infraestructuras comerciales existentes.

4. Desafíos de la transición

La migración de Tetrapol a LTE presenta varios retos:

— Garantizar la continuidad del servicio durante la transición.
— Asegurar la cobertura y disponibilidad equivalentes a Tetrapol.
— Mantener los niveles de seguridad y cifrado.

— Gestionar los costos de implementación y operación.
— Adaptar los procedimientos operativos y formar al personal.

5. Estrategia de Implementación

La Oficina de Programa SIRDEE ha optado por un enfoque gradual:
— Despliegue inicial de una red LTE privada en bandas de 45 MHz y 700 MHz.
— Pruebas piloto en regiones seleccionadas (por ejemplo, Alicante).
— Evaluación de soluciones híbridas que combinen red privada y comercial.
— Desarrollo de capacidades de interoperabilidad entre Tetrapol y LTE.

6. Aspectos técnicos clave

Varios elementos técnicos son cruciales para el éxito de la transición:
— Implementación de eMBMS (evolved Multimedia Broadcast Multicast Services) para optimizar el uso del espectro.
— Desarrollo de soluciones de interoperabilidad entre Tetrapol y LTE.
— Implementación de priorización y preferencia para usuarios de seguridad pública en redes comerciales.
— Asegurar la resistencia y redundancia de la nueva infraestructura.

7. Comparativa Internacional

El documento analiza experiencias de otros países en la transición a comunicaciones de banda ancha para seguridad pública:

Estados Unidos (FirstNet):
— Asociación público-privada con AT&T.
— Uso de banda de 700 MHz (20 MHz de espectro dedicado).
— Priorización y preferencia para usuarios de seguridad pública.

Reino Unido (ESN):
— Basado en red comercial 4G con priorización.
— Retrasos significativos en la implementación.

Francia:
— Modelo híbrido con core de red dedicado y RAN comercial.
— Uso de bandas de 700 MHz y 450 MHz.
— Legislación para garantizar priorización y roaming nacional.

Alemania:
— Mantenimiento de red TETRA para voz.

— Solución híbrida para datos con infraestructura comercial y dedicada.

8. Aspectos regulatorios y legislativos

La transición requiere cambios en el marco regulatorio:

— Asignación de espectro dedicado (bandas de 450 MHz y 700 MHz).
— Legislación para garantizar la priorización en redes comerciales.
— Regulaciones sobre interoperabilidad y seguridad.

9. Pruebas y evaluación

Se han realizado diversas pruebas para evaluar las soluciones propuestas:

— Pruebas de laboratorio y campo con múltiples proveedores.
— Evaluación de interoperabilidad entre diferentes capas (radio, core, servicios).
— Pruebas de cobertura y capacidad en entornos reales.

10. Planificación y cronograma

El proceso de transición se extiende a lo largo de varios años:

— 2022-2023: pruebas piloto y evaluación de soluciones.
— 2023-2024: inicio del despliegue en regiones seleccionadas.
— 2024-2030: expansión gradual de la cobertura LTE.
— Mantenimiento de la red Tetrapol durante el periodo de transición.

11. Consideraciones económicas

La transición implica inversiones significativas:

— Costos de infraestructura para la nueva red LTE.
— Actualización y mantenimiento de la red Tetrapol existente.
— Adquisición de nuevos terminales y equipamiento.
— Costos de formación y adaptación operativa.

Se están evaluando diferentes modelos de financiación, incluyendo asociaciones público-privadas y el uso compartido de infraestructuras.

12. Impacto operativo y formación

La transición a LTE tendrá un impacto significativo en las operaciones:

— Necesidad de adaptar procedimientos operativos.
— Formación extensiva para usuarios finales y personal técnico.
— Gestión del cambio organizacional.

13. Seguridad y resiliencia

Mantener altos niveles de seguridad es una prioridad:

- Implementación de cifrado de extremo a extremo en LTE.
- Asegurar la resistencia de la infraestructura ante desastres naturales y ataques.
- Desarrollo de capacidades de operación en modo directo (DMO) en LTE.

14. Interoperabilidad internacional

Se está trabajando en la interoperabilidad con sistemas de otros países:

- Colaboración en el marco de proyectos europeos.
- Consideración de estándares internacionales (3GPP, ETSI).
- Planificación para comunicaciones transfronterizas.

15. Conclusiones y perspectivas futuras

La transición de Tetrapol a LTE representa un paso crucial en la modernización de las comunicaciones críticas en España. Aunque el proceso es complejo y presenta numerosos desafíos, ofrece la oportunidad de mejorar significativamente las capacidades de comunicación de los servicios de emergencia y seguridad pública.

Puntos clave para el éxito de la transición:

- Enfoque gradual y flexible.
- Garantía de continuidad del servicio.
- Mantenimiento de altos niveles de seguridad y disponibilidad.
- Colaboración estrecha entre el sector público y privado.
- Adaptación continua a las necesidades operativas y avances tecnológicos.

El futuro de las comunicaciones críticas en España se perfila como un sistema híbrido que combina redes privadas y comerciales, ofreciendo servicios avanzados de voz, datos y vídeo, con la flexibilidad necesaria para adaptarse a las necesidades cambiantes de los servicios de emergencia y seguridad pública.

Referencias

3GPP. (2019). TR 21.915 V1.1.0. Release 15 Description. Disponible en: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3389

3GPP. (2015). 3GPP TSG CT Meeting #69: Release 13 analytical view version Sept..

Abichar, Z., Kamal, A., Chang, J. (2010). Planning of relay station locations in IEEE 802. *Research Gate*. Disponible en: https://www.researchgate.net/publication/224154380_Planning_of_relay_station_locations_in_IEEE_80216_WiMAX_networks

Aiache, H., Knopp, R., Koufos, K., Salovuori, H. y Simon, P. (2009). Increasing Public Safety Communications Interoperability: The CHORIST Broadband and Wideband Rapidly Deployable Systems. *Colab.* Disponible en: https://colab.ws/articles/10.1109%2FICCW.2009.5208003

Alonso, J., Ferrús, R. y Sallent, O. (2015). Alternativas de despliegue y asignación de espectro para las redes radio de emergencia de banda ancha. *Bit,* N.º 201, pp. 45-49.

ETSI. (2014) . Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems in the UHF frequency range. *ETSI TR 102 628*. Disponible en: https://www.etsi.org/deliver/etsi_tr/102600_102699/102628/01.02.01_60/tr_102628v010201p.pdf

ITU. (2017). Report ITU-R M.2377-1. Radiocommunication objectives and requirements for Public Protection and Disaster Relief. Disponible en: https://1f8a81b9b0707b63-19211.webchannel-proxy.scarabresearch.com/pub/R-REP-M.2377-1-2017

Rey Carrión, D. (2019). Evolución de la Red de Radiocomunicaciones digitales de emergencias de la Región de Murcia (Red RADIECARM). *Crat UPCT.* Universidad Politécnica de Cartegena. Disponible en: http://hdl.handle.net/10317/8741

TCCA. (2019). White Paper. Public Safety prioritisation on commercial networks. TCCA White Paper. Disponible en: https://tcca.info/documents/2019-June_TCCA_Public_Safety_Prioritisation.pdf/

— (s.f.). www.tetrapol.es.

Transición de Tetrapol a LTE

Autor: Sandra Cerrato Moreno
Director/es: Miguel Rodelgo Lacruz

Introducción

La transición del sistema SIRDEE de Tetrapol a LTE en España representa un desafío significativo y una oportunidad para mejorar las comunicaciones críticas. Busca satisfacer la creciente demanda de servicios avanzados como datos de alta velocidad y video en tiempo real. Esta transición se alinea con tendencias globales de modernización en redes de seguridad pública, enfrentando retos de continuidad, cobertura y costos, mientras ofrece oportunidades para mejorar la eficacia operativa.

Metodología

La metodología para la transición de Tetrapol a LTE en España sigue un enfoque gradual y sistemático:

1. Realización de pruebas piloto en regiones seleccionadas para evaluar el rendimiento de LTE.

2. Implementación de una red LTE privada en bandas de 450 MHz y 700 MHz, con despliegue progresivo.

3. Desarrollo de soluciones de interoperabilidad entre Tetrapol y LTE para garantizar la continuidad del servicio.

4. Evaluación de modelos híbridos que combinen infraestructura privada y comercial para optimizar costos y cobertura.

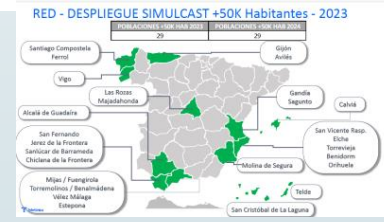
5. Mantenimiento de la red Tetrapol existente durante la transición, con migración gradual de usuarios y servicios a LTE.

Resultados

Los resultados del estudio muestran un progreso significativo en la preparación para la transición de SIRDEE de Tetrapol a LTE, identificando los principales motivadores y desafíos técnicos. Se ha iniciado el despliegue de LTE en la banda B28 en Alicante, con pruebas piloto y evaluaciones positivas de las capas de servicios, radio, core y terminales. El gran objetivo es proporcionar un terminal seguro con funcionalidades avanzadas, manteniendo la interoperabilidad con los sistemas existentes y garantizando la cobertura y calidad de servicio necesarias para las comunicaciones críticas.

Conclusiones

Se esta trabajando el la implementación del LTE en el Ministerio del interior con el objetivo de dotar de una tecnología más avanzada a las FFCCSS



Agradecimientos

Agradezco a la Escuela Naval Militar y la Armada Española por la oportunidad de realizar este Máster en sus instalaciones. Mi gratitud se extiende a todos los profesores por su dedicación y enseñanzas. Valoro enormemente el apoyo y la amistad de mis compañeros de máster. Finalmente, expreso mi sincero agradecimiento al Comisario José Antonio Cebrián de Barrio por su invaluable apoyo profesional y personal.

Sistema de distribución electrónica de claves en el ámbito de defensa

Autor: Fernández-Amigo Aguado, Pablo (pferagu@fn.mde.es)
Directores: Ares Tarrio, Miguel Angel y Álvarez Sabucedo, Luis Modesto
(externo.miguelares@cud.uvigo.es / externo.lsabucedo@cud.uvigo.es)

Resumen – En este trabajo se pretende identificar la aplicabilidad del desarrollo y posterior implantación de un Sistema de Distribución Electrónica de Claves (EKMS ESP) en el ámbito de defensa, con el propósito de distribuir claves de ámbito OTAN desde la Agencia Nacional de Distribución (en adelante NDA ESP) a las cuatro cuentas principales de los Ejércitos, Armada y Estado Mayor de la Defensa, aprovechando la actual Infraestructura Integral de Información para la Defensa (I3D) para establecer la red de transporte.

El sistema EKMS ESP debe poder distribuir claves electrónicas de una manera segura y rápida a las cuentas principales, con una gestión centralizada desde NDA ESP, que además sea escalable en función de la disponibilidad de nodos que puedan añadirse a las Subcuentas de los distintos ámbitos o incluso a los usuarios finales. Asimismo, dicho sistema debe poder ser acreditable por la Oficina Nacional de Seguridad (ONS). Para ello, los equipos cripto y electrónica de red que se empleen en la misma deben estar certificados o en disposición de estarlo.

Esta arquitectura de red permite resolver tres problemas actuales asociados a la estructura de la cadena cripto en el Ministerio de Defensa: el coste logístico de desplazarse con un dispositivo de carga de claves desde las cuentas principales hasta NDA ESP, la disponibilidad del material criptográfico lo antes posible para su distribución posterior a unidades (especialmente, a aquellas que van a ser desplegadas en zonas de operaciones o participan en ejercicios internacionales), y la seguridad en la protección de las mismas al no depender de uno o varios mensajeros.

Palabras clave – Claves criptográficas, Ámbito, Redes, Cifradores, Distribución.

1. Introducción

1.1 El cifrado de la información clasificada en el ámbito de defensa

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 y 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, es imprescindible contar con medios que aseguren la adecuada protección de la información clasificada que se emplea en las redes militares. Desde hace varias décadas se han empleado los cifradores como dispositivos fundamentales para cifrar las comunicaciones, tanto en el ámbito de la OTAN como en el nacional.

Hasta hace unos años, los cifradores empleaban claves físicas (cinta perforada) que los operadores debían cargar manualmente en el equipo para que este pudiera operar. Hoy día, todas las claves que produce y distribuye DACAN en el ámbito de la OTAN son de formato electrónico. Además, la doctrina OTAN (2) establece que la distribución de este material criptográfico se hará por medios electrónicos siempre que sea posible, para evitar posibles compromisos de seguridad.

1.2 Distribución de claves en el Ministerio de Defensa y la modernización cripto

En lo relativo a la distribución de claves de ámbito OTAN, el organismo responsable de distribuirlas a los países de la Alianza es la Agencia de Distribución y Contabilidad (en adelante DACAN). Cada país dispone de un organismo llamado Agencia Nacional de Distribución (NDA por sus iniciales en inglés, en caso de España, NDA ESP), que recibe las claves en formato electrónico por un sistema de gestión electrónica llamado NEKMS. Después, cada NDA es responsable de distribuir este material a sus cuentas criptográficas subordinadas. En el ámbito de defensa, estas cuentas son las pertenecientes al Ejército de Tierra, la Armada, el Ejército del Aire y el Estado Mayor de la Defensa (EMAD). Cada ámbito es responsable, una vez recibidas las claves criptográficas, de realizar la distribución a sus subcuentas criptográficas, y de estas a las unidades.

Un factor que se debe tener en cuenta es la profunda modernización criptográfica que se está llevando en el seno de la Alianza, y que en su documento incluye como elemento clave el desarrollo de sistemas de distribución electrónica de claves. Se pretende desarrollar una infraestructura de gestión electrónica de claves (NKMI) que permita a cada país desarrollar su propio sistema nacional y pueda incorporarse a esta infraestructura con las debidas condiciones de seguridad e interoperabilidad.

1.3 El sistema de distribución electrónica de claves del Ministerio de Defensa

Con los condicionantes vistos hasta ahora, el objetivo por lo tanto es desarrollar un sistema de distribución de claves que cumpla las siguientes características:

- El sistema debe poder ser acreditable por la Oficina Nacional de Seguridad (ONS). Para ello, los equipos cripto y electrónica de red que se empleen en la misma deben estar certificados o en disposición de estarlo.
- El sistema debe de emplear una red de transporte que sea común a los ámbitos que van a emplearlo: Ejército de Tierra, Armada, Ejército del Aire, EMAD y la Agencia Española de Distribución (NDA ESP).
- El sistema debe ser escalable, para que pueda ajustarse fácilmente a posibles cambios en la estructura de la organización.
- El sistema debe disponer de una configuración dinámica para necesidades temporales, como por ejemplo la distribución de claves criptográficas en un área de operaciones.
- El sistema debe permitir una gestión centralizada que permita una distribución desde NDA ESP a los usuarios de la red.

Además, el sistema debe de incorporar las siguientes funcionalidades:

- Almacenamiento seguro de claves.
- Importación y exportación de claves electrónicas en el sistema.
- Gestión y distribución electrónica de claves.
- Contabilidad y registro de claves y equipos criptográficos.

2. Desarrollo

2.1 Estado del arte

Como ya se ha comentado, la OTAN está en un proceso de modernización criptográfica profundo, puesto que hay una gran variedad de productos criptográficos cuya obsolescencia hace que estén descertificados o próximos a descertificar. En algunos casos, existen productos ya identificados como sustitutos de cifradores antiguos, pero en otros no, y solo los países criptoproductores (fundamentalmente EE. UU. y Reino Unido y, en menor medida, Alemania, Francia, Italia y España) tienen capacidad de desarrollar dispositivos que puedan cumplir los requisitos necesarios.

Una de las áreas que se quiere potenciar con el desarrollo de la NATO Key Management Infraestructure (NKMI) es, precisamente, la distribución electrónica de claves. El objetivo es desarrollar un estándar que permita una interoperabilidad entre los sistemas nacionales de distribución de claves y los dispositivos criptográficos para el usuario

final (ECU[1]). Teniendo en cuenta que algunos de los ECU pueden haber sido a proveedores extranjeros, la integración de estos con el sistema nacional de distribución de claves que tenga dicho país puede simplificarse con la adopción de una especificación de interoperabilidad de claves.

Conviene mencionar también el hecho de que los equipos criptográficos que actualmente se emplean en la distribución vía OTAT/OTAD[2] también se ven afectados por la descertificación del algoritmo criptográfico que emplean. Esté método de distribución de claves electrónicas, muy empleado en las marinas de la OTAN, aunque solo sirve para casos puntuales (no se pueden transmitir grandes volúmenes de datos) es una de las áreas que deben ser renovadas.

Por último, hay que mencionar que en el ámbito nacional también se están modernizando los cifradores bajo la supervisión del Centro Criptológico Nacional, debido a que aún se emplean modelos antiguos de la familia EPICOM en algunos casos, pero la telegestión de estos equipos no se ve afectada, y no es objeto de este trabajo.

2.2 Arquitectura objetivo

En el modelo planteado, se pretende implantar una red de nodos con funcionalidad EKMS[3] desarrollados por la empresa TECNOBIT, utilizando las capacidades de transporte de la red I3D[4] del Ministerio de Defensa. El desarrollo de este sistema en el ámbito de defensa está contemplado en el documento como uno de los servicios de Infraestructura tecnológica.

La jerarquía del sistema es a modo de árbol, donde el nodo principal de NDA ESP tiene como nodos dependientes de él a los nodos del Ejército de Tierra, Armada, Ejército del Aire y EMAD. Al ser un sistema distribuido los nodos no tienen porqué estar en la misma sala o zona geográfica, pueden estar localizados en distintos puntos del país siempre y cuando estén conectados a la misma red.

Al estar conectando dos sistemas (la red EKMS-ESP y la red I3D), deberemos cumplir con lo establecido en la Instrucción Técnica, e implementar un Sistema de Protección de Perímetro (SPP), que es una combinación de recursos *hardware* o *software* llamados Dispositivos de Protección de Perímetro, cuya finalidad es mediar entre el tráfico de salida y entrada. Para este caso se establece una Pasarela en una zoma desmilitarizada (DMZ) con un cifrador IP.

---

[1] End Cryptographic Unit.

[2] OTAD: Over the air distribution /OTAT: Over the air transmission.

[3] Electronic Key Management System: Sistema de gestion electronica de claves.

[4] Infraestructura Integral de Información para la Defensa.

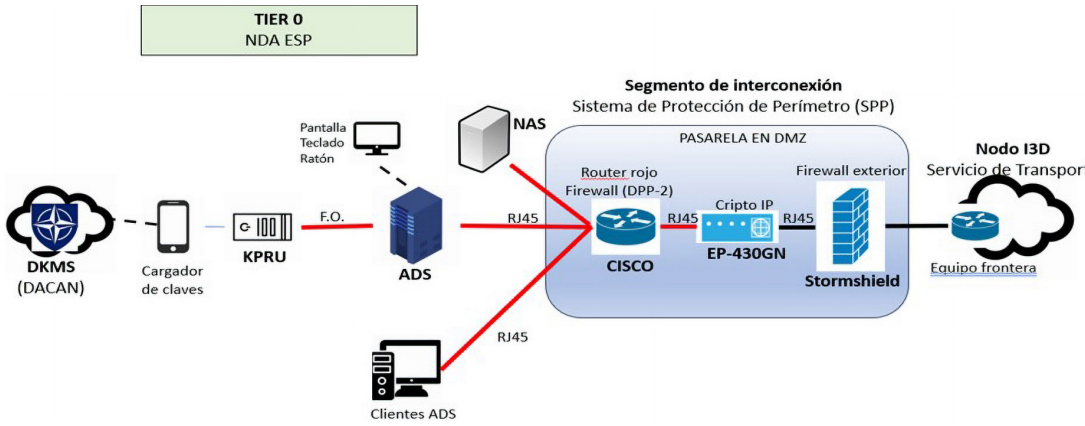


Figura 1. Ejemplo de interconexión entre nodo EKMS y red I3D

La información que se transporte por esta red irá cifrada con varias capas, una la que dan los propios nodos a las claves, más la de otorgan los cifradores IP que se colocarán en el segmento de interconexión. Esto significa que las claves viajan «en negro», y solo pueden ser utilizadas en destino una vez desencriptadas.

2.3 Gestión de los nodos EKMS-ESP

Para la gestión remota de los distintos equipos existirá un Nodo de Gestión de Servicios de Seguridad (NGSS), controlando y supervisando la actividad dentro de la red y asegurando la configuración del segmento de interconexión según los procedimientos que establece el CCN para la gestión de la información clasificada.

Existirán estaciones de gestión y control remoto de la seguridad que dispongan de acceso remoto a la LAN EKMS-ESP, así como a los cifradores IP y a los cortafuegos Stormshield. La responsabilidad del nodo NGSS sería de NDA ESP como autoridad del sistema, punto clave y cabeza en la jerarquía de la red.

La gestión remota de los cortafuegos se realizaría mediante la implementación de una Red Privada virtual (VPN), utilizando protocolo IPSEC, otorgando seguridad y la integridad en la gestión de los *firewalls*. En cuando a la gestión de los cifradores IP, debe de hacerse mediante un centro de gestión de cifradores IP semejante al que existe en la Cuenta de Cifra del EMAD o de la Armada. Por último, para la gestión remota de los router CISCO, se propone establecer un túnel GRE permitiendo las comunicaciones encaminamiento entre los router rojos de la EKMS-ESP.

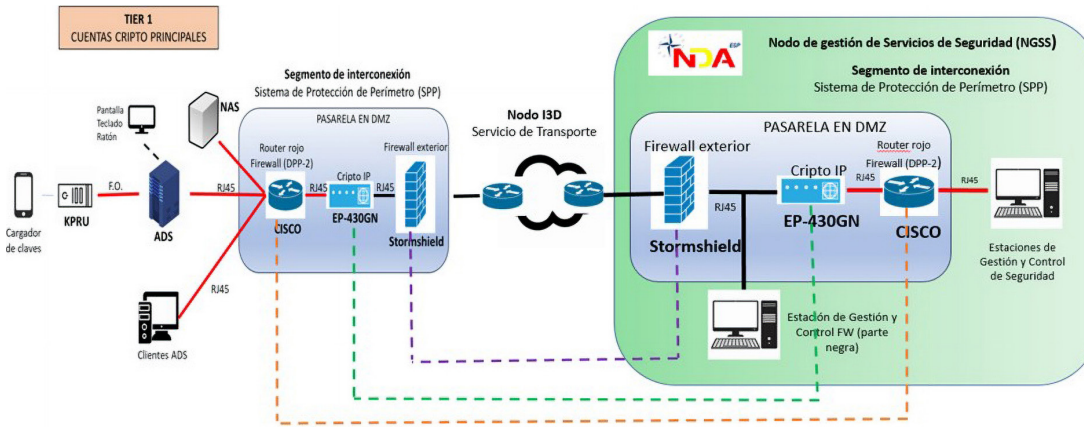


Figura 2. Conexión entre NGSS y nodos EKMS

3. Conclusiones

El establecimiento del sistema EKMS-ESP en este primer nivel puede ser la base para escalar la red progresivamente en los distintos ámbitos, marcando un hito en la gestión del material criptográfico del ámbito de defensa. La Armada es el ámbito mejor posicionado, puesto que cuenta con nodos EKMS para sus subcuentas de cifra y se plantea la adquisición de nodos de menor nivel para las unidades.

En el aspecto operativo, la red EKMS-ESP facilita una gestión eficiente y centralizada de las claves de cifrado. Esto no solo mejora la rapidez y eficacia en la distribución de claves, sino que también reduce la posibilidad de errores humanos, un factor crítico en la gestión de la seguridad de la información. El sistema permite no solo una distribución más ágil de las claves, sino una producción de la documentación asociada a las mismas (partes de transferencia, de destrucción, inventarios, etc.) más sencilla para los criptocustodios de cada unidad, logrando un mayor control y seguimiento de un material tan sensible.

La implantación de este sistema no solo es necesaria desde el punto de vista de la seguridad, si no por la futura descertificación de los equipos que se usan para hacer distribución OTAD/OTAT, que imposibilitará la distribución de las claves electrónicas por esta vía en el futuro en casos puntuales y de necesidad.

Estratégicamente, la implantación de este sistema colocaría al Ministerio de Defensa en la vanguardia en términos de capacidades de cifrado y seguridad de la información. Esto no solo refuerza la postura de defensa nacional, sino que puede contribuir a la imagen de España como un aliado de confianza y tecnológicamente avanzado dentro del seno de la OTAN.

Referencias

Centro Criptográfico Nacional. Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación.

Centro Criptográfico Nacional. CCN-STIC-302. Interconexión de sistemas de las Tecnologías de la Información y las Comunicaciones que manejan información clasificada.

I.M. Staff. (2020). Cryptographic Modernisation Timed Roadmap V7 (NATO SECRET).

Ministerio de Defensa. (2016). Instrucción 58/2016 Arquitectura Global CIS/TIC del Ministerio de Defensa. Secretaría de Estado de Defensa, 28 de octubre de 2016.

Sistema de Distribución Electrónica de claves en el ámbito de Defensa

Autor: Pablo Fernández-Amigo Aguado
Director: Miguel A. Ares Tarrio / Luis Álvarez Sabucedo

Universidad de Vigo

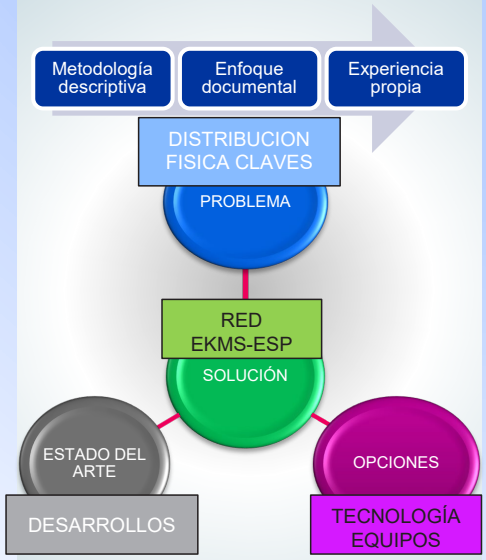
Introducción

NECESIDAD DE SOLUCIÓN PARA FACILITAR DISTRIBUCION DE CLAVES DIGITALES OTAN DESDE AGENCIA NACIONAL DE DISTRIBUCION (NDA ESP) A CUENTAS PRINCIPALES DE LOS EJERCITOS

Resultados

Distribución actual mediante mensajeros ineficiente, ralentiza la obtención de las Cuentas Principales y su posterior distribución a las unidades

Metodología



Conclusiones

LA RED EKMS-ESP APORTA:
-RAPIDEZ EN LA DISTRIBUCIÓN DE CLAVES OTAN.
-SEGURIDAD REFORZADA DEL MATERIAL CRIPTO.
-ESCALABILIDAD DE LA RED SEGÚN DISPONIBILIDAD DE NODOS EKMS.
-SIMPLICIDAD EN LA GESTIÓN DIARIA DE CLAVES EN LAS CUENTAS PRINCIPALES.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2024

El marco FMN como potenciador de la eficacia operativa de la OTAN y de las naciones

Autor: Gajete Molina, Óscar Javier (ogajmol@et.mde.es)
Director: Núñez Ortuño, José M.ª (jnunez@cud.uvigo.es)

Resumen – El nuevo concepto estratégico de la OTAN hace hincapié en la rápida evolución de las tecnologías y la necesidad de una mayor agilidad y flexibilidad para hacer frente a los nuevos retos. Tal y como señalaba recientemente el general Lavigne, jefe del Mando de Transformación de la Alianza (ACT), «el concepto 2030 de la OTAN requiere adoptar un enfoque centrado en los datos y avanzar en la federación de nuestras redes si queremos obtener el éxito en las operaciones multidominio (MDO)».

Precisamente, el núcleo de la transformación de la OTAN es la convergencia de las MDO y la transformación digital (DT), con el fin de obtener una toma de decisiones basada en datos con la mayor velocidad y precisión posible. Para ello, es fundamental mejorar la interoperabilidad, entendida por la Alianza como «la capacidad de actuar juntos de manera coherente, efectiva y eficiente para lograr los objetivos tácticos, operativos y estratégicos de los aliados».

El concepto FMN (Federated Mission Networking) se deriva de la experiencia de la AMN (Afghanistan Mission Network) y fue desarrollado por la OTAN para asegurar la interoperabilidad entre las naciones de la Alianza y otras organizaciones y naciones afiliadas. FMN engloba personas, procesos y tecnología y su misión es mejorar el mando y control (C2) y la toma de decisiones en las operaciones y ejercicios de sus afiliados, para conseguir una mayor eficacia y operatividad tanto en el presente como en el futuro.

La participación de nuestras Fuerzas Armadas en misiones internacionales requiere garantizar la máxima interoperabilidad con nuestros aliados, de ahí la importancia para España de disponer de esta capacidad para el establecimiento de redes de misión federadas. En este TFM se analiza cómo funciona FMN y su contribución a la mejora de la eficacia operativa de la OTAN y de las naciones, identificando los retos y los riesgos a los que se enfrentan sus miembros en los nuevos escenarios operativos.

Palabras clave – Federación, Misión, Interoperabilidad, Escenario, Afiliado.

1. Introducción

El concepto NATO Network Enabled Capability (NNEC) señala que uno de los principales retos de la Alianza es la capacidad de compartir información en red para su empleo en las operaciones, con el fin de obtener ventaja en el combate, mediante la superioridad en la información, en el conocimiento y en la decisión.

FMN es una capacidad que abarca multitud de aspectos tales como la doctrina, el planeamiento de recursos, la definición y obtención de medios, la instrucción y adiestramiento, la seguridad y la organización. Su objetivo es posibilitar la acción conjunta de los participantes en una red de misión federada desde el primer momento del despliegue y contribuir a optimizar la toma de decisiones en tiempo real.

En la actualidad, la OTAN y FMN afrontan los nuevos retos derivados de la transformación digital y de las operaciones multidominio. En el entorno estratégico futuro, la visión de FMN contempla la adaptación de todos los afiliados, transformando sus capacidades para seguir manteniendo la ventaja estratégica. Los recursos disponibles son limitados y son numerosas las misiones a las que hay que hacer frente, de ahí que además de la reutilización de estándares sea necesario fomentar unas economías de escala que favorezcan la interoperabilidad y el intercambio de información. De esta manera, FMN contribuye a la mejor preparación para las operaciones futuras, con un rápido despliegue de fuerzas que proporciona unas capacidades federadas y una eficaz toma de decisiones en cualquier entorno operativo.

2. Desarrollo

La principal característica de las Fuerzas Armadas para el entorno 2035 será la agilidad, tanto en el ámbito de la organización como del personal que la integra. Si nos centramos en las operaciones multidominio, uno de los requisitos clave para el éxito de la misión es la interoperabilidad. De todo lo anterior se puede afirmar que, independientemente del escenario donde desplieguen nuestras unidades, tanto en las áreas urbanas como en los grandes espacios con baja densidad de población, será necesario actuar de forma conjunta para disminuir el tiempo necesario en la toma de decisiones.

La diferencia entre las operaciones multidominio y las operaciones conjuntas, que ya eran conocidas en nuestra doctrina, viene sobre todo por la complejidad del entorno operativo. Para responder a las nuevas amenazas, la OTAN, los aliados y otros actores han de sincronizar todas sus capacidades (militares y no militares) para actuar como una sola fuerza en todos los dominios. Los principios de las operaciones multidominio son el posicionamiento y gradación de la fuerza, el empleo de formaciones resilientes y las capacidades convergentes que posibiliten la maniobra.

Por otro lado, la transformación digital en el entorno táctico contempla una deslocalización de la información en redes dinámicas y descentralizadas, con sistemas de telecomunicaciones modulares, escalables y que emplean arquitecturas abiertas. Esto supone, entre otras cosas, acortar los tiempos para desarrollar las nuevas capacidades que han de desplegarse en las misiones y resaltar la importancia de las tecnologías de uso dual.

La OTAN puso en marcha su plan de transformación digital, cuya estrategia fue aprobada el pasado mes de mayo de 2023, que establece entre sus objetivos estratégicos realizar operaciones multidominio, la interoperabilidad en todos los dominios (tierra, mar, aire, ciber y espacio), la mejora de la conciencia situacional y la optimización del proceso de toma de decisiones a todos los niveles.

El Concepto de Red de Misión Futura (FMN) fue desarrollado por orden del Comité Militar de la OTAN durante el año 2011 fruto de la colaboración entre el Mando Aliado de Transformación (ACT) y el Mando Aliado de Operaciones (ACO), a partir de las lecciones aprendidas de la AMN, del informe proporcionado por el Centro de Excelencia de Mando y Control (C2CoE) y otros documentos sobre el alcance y plan de acción de FMN. Su objetivo era establecer una capacidad de red de misión federada para el intercambio de información entre la OTAN, los aliados y otras entidades no pertenecientes a la OTAN que participaran en las operaciones.

Este concepto describe tres componentes: gobernanza, Marco FMN y Redes de Misión (Mission Network o MN). Se entiende por gobernanza la orientación de la iniciativa FMN a alto nivel para conseguir una gestión efectiva, tanto del Marco FMN como de las Redes de Misión (MN). El Marco FMN se puede definir como una estructura integral que proporciona procesos, planes, plantillas, arquitecturas y herramientas para analizar, planear, implementar, operar, evolucionar y mejorar las Redes de Misión (MN) de la OTAN y de las naciones en entornos federados.

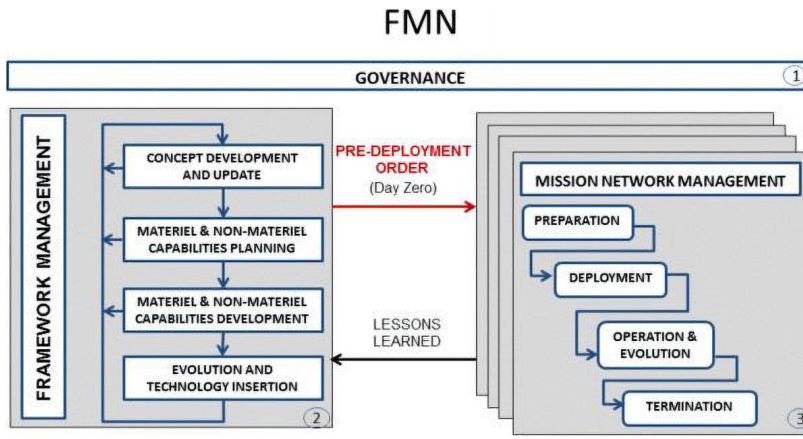


Figura 1. Componentes FMN

El Plan de Implementación de FMN (NFIP) es un documento que tiene como objetivo el establecimiento de una capacidad, entendida como un conjunto de herramientas (procesos, organización, tecnología y estándares) para generar redes de misión federadas, eficaces y eficientes, que permitan mejorar tanto el C2 como la toma de decisiones en misiones y ejercicios.

El documento que describe el Marco FMN es la Directiva de Gestión de FMN, que detalla la misión, estructura, responsabilidades y tareas de los órganos de gestión de FMN. Las dos actividades principales del Marco FMN son el Proceso Marco FMN (con sus productos y las relaciones de estos productos con los órganos de gestión) y el Apoyo del Proceso Marco FMN a la instanciación de misiones (permite reducir el tiempo necesario para conectar fuerzas durante una instancia). Entre los objetivos del Marco FMN está facilitar que los afiliados creen capacidades FMN que les permitan interconectar sus fuerzas en un determinado entorno o instancia. Para ello, cuenta con la estructura de gestión de FMN compuesta por el Grupo de Gestión (MG), la Secretaría FMN y sus correspondientes grupos de trabajo o *Working Groups* (WG).

El Marco FMN favorece la identificación de deficiencias en la MN al contemplar no solo la preparación, operación y finalización de la red, sino que incorpora las lecciones aprendidas que sirven para retroalimentar el ciclo. Se trata de mantener todo el contacto posible entre el Marco FMN, los afiliados y la instancia o MN específica que se desarrolla. Para la gestión del Marco FMN se emplean dos herramientas fundamentales, la Hoja de Ruta de Gestión y la *Hoja de Ruta de Especificaciones de la Espiral*. El *Roadmap* de gestión se compone de tres elementos, el ciclo de vida de la Espiral FMN, el plan a diez años para sincronizar y dirigir las actividades del Marco FMN y el cronograma de hitos con los eventos principales para determinar las tareas y los plazos que permitan cumplir con los objetivos de la visión FMN.

La *Hoja de Ruta de la Especificaciones de la Espiral FMN* (*FMN Spiral Specification Roadmap*) es un documento que establece el desarrollo de capacidades operativas a diez años para la implementación de las espirales. Recordemos que este desarrollo es incremental y que cada espiral establece los pasos donde en un periodo de tiempo (detallado en el cronograma) se alcanzan unos objetivos previamente definidos por los afiliados. De ahí la importancia para los participantes de adecuar el nivel de ambición (LoA) y la sincronización de todos los implicados a la hora de obtener unos resultados positivos en cada implementación.

Los objetivos que se establecen en cada espiral tienen un efecto directo en la mejora de capacidades (Capability Enhancements o CPE) del Modelo en «V» de FMN. Los CPE son importantes porque transforman los requisitos operativos en mejoras de carácter técnico y a nivel de procedimientos.

3. Resultados y discusión

Tras la propuesta de las especificaciones de la espiral, los afiliados disponen de información sobre los posibles riesgos de cara a la fase de desarrollo de capacidades y pueden decidir su LoA para dicha espiral. Una vez aprobada la versión final de las especificaciones de la espiral en desarrollo, los afiliados la utilizarán como referencia para sincronizar todos los procesos que permitan la evolución y disponibilidad de las capacidades FMN.

La Línea Base FMN está formada por los diferentes elementos de configuración» (Configuration Elements o CI) de las capacidades CIS y de comunicaciones que han sido aprobadas por los afiliados para el entorno FMN. Este producto permite disponer de una instantánea actualizada de las capacidades disponibles, para evaluar el grado de cumplimiento para el alistamiento FMN de los afiliados en función de las especificaciones de la espiral y del nivel de ambición declarado. La mejora incremental en la que se basan las espirales se puede apreciar en el aumento de capacidades FMN disponibles para los participantes en la instanciación de redes, incluyendo requisitos mínimos según el tipo de afiliado (A, B, C según se pretenda proporcionar una MNE, una MNX o simplemente ser un participante, capacidades para uso común de todos los integrantes de la MN o capacidades iniciales para empleo individual).

En el año 2021, el Management Group aprobó una actualización de las instrucciones de incorporación, afiliación y salida para la Mission Network (JMEI de MN). Contienen un «conjunto de publicaciones que brindan orientación sobre gobernanza y gestión, procedimientos, servicios, infraestructuras y atributos de datos necesarios para que las MN proporcionen a los participantes un entorno operativo donde puedan compartir información de forma segura y confiable».

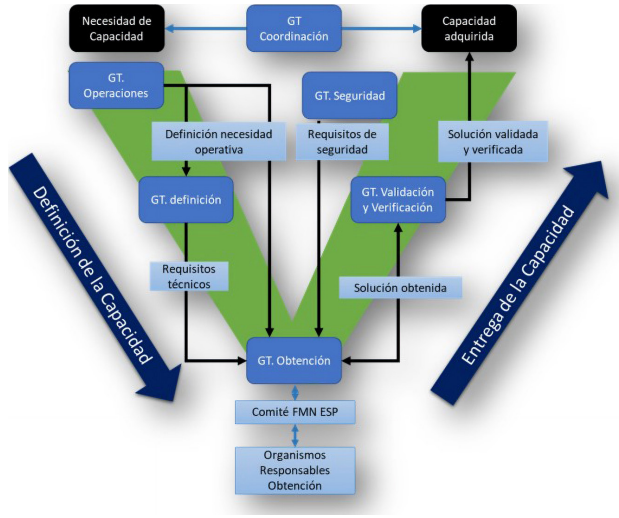


Figura 2. Modelo en V, FMN-ESP

El documento JMEI es fundamental porque permite a los participantes de las redes de misión disponer de una guía para la federación de sus redes nacionales. Dicha referencia sirve para el establecimiento, operación y mantenimiento de la MN, al proporcionar instrucciones técnicas y plantillas de configuración que describen la arquitectura y el nivel mínimo de interoperabilidad de los servicios de la red. Veremos en este trabajo el papel que desempeñan tanto el Secretariado FMN como los diferentes grupos de trabajo para la mejora continua de la instanciación de redes de misión. Entre las actividades desarrolladas por la estructura FMN destaca el proceso de gestión de cambios a la *Baseline,* en el cual la participación de los afiliados FMN ha ido en aumento. Se han estudiado también los servicios en los que está habiendo una mayor implicación, aportando igualmente datos sobre los tipos de servicio.

Hay que destacar la importancia de la iniciativa Interoperability Continuum de OTAN para fomentar la interoperabilidad, con los eventos TIDE Hackathon, TIDE Sprint y, sobre todo, el ejercicio CWIX (exploración, experimentación y evaluación de interoperabilidad de la Coalición), aprobado por el MC de OTAN y enfocado al ámbito técnico y operativo. Los ejercicios CWIX permiten a las naciones experimentar, probar y eliminar riesgos de sus sistemas desplegables antes de llevar a cabo sus misiones La principal sede donde se ejecuta el ejercicio CWIX es el Centro de Entrenamiento de la Fuerza Conjunta (Joint Force Training Centre o JFTC) de Bydgoszcz (Polonia).

En el caso particular de España y dentro de los objetivos del Plan de Acción FMN-ESP, el EMAD es responsable de evaluar la disponibilidad operativa de las unidades y el grado de alistamiento (FMN-Readiness) de los Ejércitos y de la Armada. Con este fin se realiza el ejercicio V2CN FMN (ejercicio de verificación, validación y confirmación nacional) con el que se comprueba el cumplimiento de los requisitos técnicos, operativos y la capacidad FMN de España.

Actualmente, los afiliados trabajan en las mejoras de la espiral 5, que se encuentra en fase de desarrollo, incorporando a sus objetivos individuales nuevas capacidades. El objetivo principal es alcanzar el hito 2 de interoperabilidad, estando previsto su fase de empleo operativo en misiones y ejercicios a partir de 2028. Contiene entre sus especificaciones mejoras para dar los primeros pasos en la implantación de la estrategia de seguridad centrada en el dato (Data Centric Security). Los grupos de trabajo FMN nacionales propondrán soluciones operativas para implementar la seguridad de la tecnología 5G o potenciar el empleo de las comunicaciones HF con nuevos servicios y protocolos.

4. Conclusiones

FMN supone para la OTAN un capacitador de primera magnitud para la consecución de sus objetivos y se encuentra alineada con el Concepto

Estratégico de 2022 y la Agenda 2030. La iniciativa FMN aborda la interoperabilidad en todas sus dimensiones y desde el primer momento del despliegue, lo que redunda en el cumplimiento de las misiones OTAN en un escenario cada vez más complejo. Uno de los principales retos de FMN de cara al futuro es su adaptación al nuevo entorno operativo, donde la transformación digital iniciada hace ya años se une a unas operaciones multidominio que requieren mejorar el intercambio de información para optimizar el proceso de toma de decisiones.

La iniciativa FMN cuenta ya con una larga trayectoria y el número de participantes ha ido aumentando de forma paulatina. De los datos analizados en el TFM se puede confirmar que la mayoría de los afiliados han incrementado su participación y han mejorado su estatus FMN dentro los niveles de ambición que se habían marcado. Desde el punto de vista de la organización, el Marco FMN ha conseguido mantener una estructura más estable para monitorizar los procesos y trabajos en marcha, gracias al trabajo del Secretariado FMN. Los diferentes WG están dando mayor coherencia a los procesos del ciclo de vida de las espirales, con especial énfasis en el desarrollo de arquitecturas para poder alinear FMN con la implantación de DCS en las redes de misión.

El personal sigue siendo el recurso más valioso de la OTAN y también de FMN, por lo que se ha fomentado la participación de expertos de todos los ámbitos que contribuyan al desarrollo e implementación de las nuevas tecnologías emergentes y al análisis de posibles riesgos. Las reuniones del MG son de vital importancia para consolidar diferentes asuntos que son consensuados por los representantes nacionales, por lo que se requiere una priorización adecuada de los asuntos a tratar en dicho ámbito.

Como se describe en el trabajo, la mejora de la eficacia operativa también ha sido posible gracias a la disponibilidad de un portal web específico, donde se recogen todos los hitos y productos de cada organismo implicado. También el empleo de TIDEPEDIA permite a los participantes aportar soluciones o correcciones de cualquier asunto relacionado con FMN. El acceso a estos recursos facilita a los diferentes grupos de trabajo estar en contacto diario sobre los cambios y avances que afecten a FMN en general y a los eventos de su área de responsabilidad en particular.

En general se ha mejorado el Marco FMN para que los productos obtenidos en cada espiral estén perfectamente alineados, intentando dar mayor protagonismo a la fase de pruebas. España es una nación afiliada desde 2014 y ha participado de forma muy activa en la implantación de la capacidad FMN, realizando pruebas y ejercicios que le permiten evaluar de forma periódica cómo mejora la interoperabilidad de las diferentes herramientas que proporcionan los servicios a las redes de misión federadas.

En resumen, en este TFM se analiza cómo el Marco FMN es un auténtico potenciador de la eficacia operativa y permite contribuir a la consecución

de los objetivos de la OTAN a través de la interoperabilidad en sus tres dimensiones: personas, procesos y tecnología. El éxito futuro dependerá en gran medida de la voluntad de los afiliados para seguir contribuyendo a fortalecer la estructura FMN, aprovechando los recursos disponibles y fomentando la participación en todos los foros orientados a mejorar el despliegue de redes de misión federadas para ejercicios y operaciones.

Referencias

NATO. (2015). MCM-0038-2005/0032-2006, Development of a NATO Network-Enabled Capability (NNEC).

NATO. (2019). Enterprise C3 Interoperability Directive, AC/322-D (2019) 0031(INV). Portal web CoI FMN OTAN.

MADOC. (2019). Conceptos para el Combate 2035.

Ministerio de Defensa. (2018). PDC-01(A) Empleo de las Fuerzas Terrestres.

Martínez-Valera, G. (2022). El enfrentamiento avanzado, las operaciones multidominio. *Global Strategy Reports.*

Llopis Sánchez, S. (2021). Las telecomunicaciones tácticas militares: vanguardia de la transformación digital del campo de batalla. *ACAMI*.

NATO. (2023). PO 0191. NATO's Digital Transformation Implementation Plan Strategy.

NATO. (2012). Future Mission Network Concept, version 2.0.

NATO. (2018). SH/CCD J6/FMN/137/16-313769. Management Directive, Version 2.0. *Portal web CoI FMN.*

NATO. (2014). Federated Mission Networking Implementation Plan (NFIP) V.4.0. *Portal web CoI FMN OTAN*.

FMN. (2023). Spiral 5 Specification. Secretariado FMN.

El marco FMN como potenciador de la eficacia operativa de la OTAN y de las Naciones

Autor: Óscar Javier Gajete Molina
Director: José María Núñez Ortuño

Universidad de Vigo

Introducción

El concepto FMN (*Federated Mission Networking*) se deriva de la experiencia de la AMN (*Afghanistan Mission Network*) y fue desarrollado por la OTAN para asegurar la interoperabilidad entre sus afiliados.

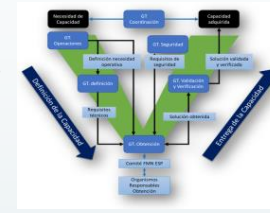
FMN engloba personas, procesos y tecnología y su misión es mejorar el Mando y Control (C2) y la toma de decisiones en operaciones y ejercicios, para conseguir una mayor eficacia y operatividad tanto en el presente como en el futuro.

Objetivo

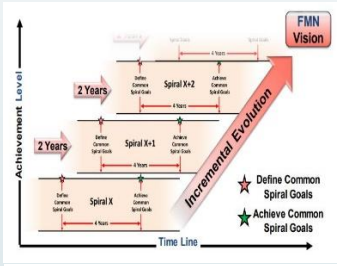
Posibilitar la acción conjunta de los participantes en una red de misión federada desde el primer momento del despliegue y contribuir a optimizar la toma de decisiones en tiempo real.

Metodología

- Revisión bibliográfica
- Entrevista con expertos
- Estadística
- Pruebas de validación



Resultados



CONFIANZA + IMPLICACIÓN

- GOBERNANZA ÓPTIMA
- GESTIÓN EFICIENTE
- VALIDACIÓN y VERIFICACIÓN EFICAZ

Conclusiones

- FMN se alinea con el Concepto Estratégico de OTAN y con la Agenda 2030, contribuyendo al éxito en las MDO
- INCREMENTO de la participación de afilados FMN para hacer frente a nuevos retos como DCS
- IMPULSO para la realización de más ejercicios y foros sobre interoperabilidad
- MEJORA de resultados con la utilización de herramientas colaborativas y participación de más expertos
- AUMENTO de la calidad de los productos FMN como referencia para el desarrollo de capacidades de los afiliados

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

Sistema de Comunicaciones Estratégico por Satélite

Autor: Herrero Santos, Carlos (cesticmaster.chs@gmail.com)
Director: Gil Castiñeira, Felipe (externo.felipegil@cud.uvigo.es)

Resumen – El presente TFM analiza teóricamente el caso de un posible proyecto de diseño y despliegue de un sistema de comunicaciones basado en satélites de órbita geoestacionaria para comunicaciones estratégicas, que podría ser de utilidad para el ámbito de defensa y seguridad.

Se ha realizado un recorrido por el estado del arte en este ámbito de la ingeniería para plantear la viabilidad técnica, basándose en datos, bien reales, bien típicos u obtenidos como resultados de cálculos y estimaciones.

Se han aplicado los procedimientos de cálculo empleados por las ingenierías especializadas en el diseño de redes de comunicaciones por satélite, para llevar a cabo un diseño que podría ser funcional en la práctica.

Las consideraciones de gestión y diseño abarcan desde la exposición de las fases de diseño y puesta en servicio de un sistema de comunicaciones por satélite, los elementos principales que podrían componer el sistema y la seguridad hasta la realización de un balance del enlace del sistema en las bandas de frecuencias de mayor interés en el ámbito del Ministerio de Defensa y organizaciones internacionales, como la EDA y la OTAN.

Palabras clave – Satélite, Enlace, Antena, Ciberseguridad, Geoestacionario, SECOMSAT.

1. Introducción

1.1 Los sistemas de comunicaciones por satélite en el ámbito de defensa

El Ministerio de Defensa explota, desde 1992, sistemas de comunicaciones militares por satélite (HISPASAT 1A y 1B), a través de la Misión Gubernamental de los satélites de comunicaciones militares (SATCOM).

En julio de 2001, el Ministerio de Defensa y las empresas HISDESAT e HISPASAT suscribieron un Acuerdo Marco para la Implantación de un Sistema de Comunicaciones Militares por Satélite, para la colaboración en la definición, implantación y explotación de la Misión Gubernamental.

1.2 El modelo del Sistema de Comunicaciones Militares Seguras por Satélite Español

La participación de la industria nacional ha sido esencial en el desarrollo del programa de comunicaciones para usos gubernamentales por satélite del Ministerio de Defensa español, que incluye dos satélites, al final de su vida útil en la actualidad, y otros dos en desarrollo de nueva generación, pensados para operar en parejas, uno principal y otro de respaldo que complementa la cobertura.

La capacidad total del sistema permite ofrecer servicios de comunicaciones seguras en bandas X, Ka y UHF militar a las Fuerzas Armadas españolas, instituciones españolas y también a Gobiernos de países amigos. La Organización del Tratado del Atlántico Norte (OTAN) también necesita servicios de comunicaciones seguras por satélite para su radio de cobertura de actuación.

El actual Paquete de Capacidad de Comunicaciones Militares por Satélite de la OTAN (CPA09130, de 2019 a 2034), en el que el Ministerio de Defensa español tiene interés por participar activamente, ha completado sus primeras fases de definición y asistencia técnica del proyecto.

La nueva generación de satélites del Sistema Español de Comunicaciones por Satélite (SECOMSAT), en desarrollo, tendrá las características necesarias para los ámbitos nacional, MILSATCOM de la OTAN, GOVSATCOM de la Agencia Europea de Armamento (EDA) y el entorno comercial internacional.

1.3 Objetivo del trabajo

El presente trabajo pretende mostrar las líneas generales más importantes del diseño de un sistema estratégico de comunicaciones por satélite que podría ser de utilidad para el SECOMSAT.

1.4 Principales contribuciones del trabajo

Este trabajo contribuye a:

- La divulgación de los logros realizados en el ámbito de defensa y la industria, destacando la empresa Hisdesat.
- La difusión de la historia de la tecnología espacial española en el ámbito de la defensa.
- Divulgar los componentes relevantes de un sistema de comunicaciones por satélite moderno.
- Exponer la razón por la cual se invierte en reservar posiciones orbitales ante la UIT.
- Conocer las fases de la obtención, implantación y puesta en operación de un sistema SATCOM.
- Exponer las características, elementos y posibilidades de los componentes del segmento espacial y del segmento terreno (Software Defined Radio-SDR, Ground Segment as a Service-GsaaS).
- Evaluar cuantitativamente características del enlace satélite en bandas de frecuencia de interés.
- Plantear líneas de investigación, destacando las relativas a robustez ante ciberataques, ataques no convencionales HANE (eventos nucleares a gran altitud) y la utilización de comunicaciones ópticas y láser entre el segmento terreno y el segmento espacial o entre nodos del segmento espacial.
- Aporta una variedad de referencias y recursos de información sobre el sector de SATCOM.

2. Estado del arte de los sistemas de comunicaciones por satélite

2.1 Qué son los satélites artificiales, historia y evolución en España

Un satélite artificial es una máquina construida por el hombre que orbita alrededor de un planeta, como la Tierra. El primero fue el Sputnik 1, lanzado por la U.R.S.S. en 1957.

El Minisat 01, lanzado el 21 de abril de 1997, fue el primer satélite de investigación y su diseño fue totalmente español.

El Hispasat 1A fue el primer satélite de comunicaciones del operador español Hispasat.

A principios de los noventa del siglo XX se creó el Sistema Español de Comunicaciones Militares por Satélite (SECOMSAT), una red militar española de comunicaciones militares a larga distancia vía satélite.

El XTAR-EUR, situado en la posición 29º Este, lanzado el 12 de febrero de 2005, es un satélite de comunicaciones desarrollado conjuntamente por España y Estados Unidos que pertenece a Hisdesat, al igual que el satélite SPAINSAT, en la órbita 30º Oeste, lanzado el 11 de marzo de 2006 y también dedicado a comunicaciones militares y gubernamentales.

2.2 Tecnologías incorporadas en los sistemas de comunicaciones por satélite

Destacan las siguientes tecnologías impulsoras:

- Transpondedores de potencia.
- Señales de frecuencias elevadas.
- Órbita geoestacionaria (GEO).
- Satélites definidos por *software*.
- Inteligencia artificial (IA).
- Enlaces ópticos.
- Comunicaciones 5G.

2.3 El futuro de los sistemas de comunicaciones por satélite en España

El programa SPAINSAT NG (Next Generation) de la empresa española Hisdesat, impulsado por el Ministerio de Defensa con financiación del Ministerio de Industria, Comercio y Turismo, comprenderá los satélites SPAINSAT NG I y SPAINSAT NG II, que se ubicarán en las posiciones 30º O y 29º E y operarán en las bandas X, Ka militar y UHF desde 2025.

2.4 Revisión de trabajos similares sobre diseño de sistemas de comunicaciones por satélite

Existen muchos trabajos y artículos sobre el diseño de sistemas de comunicaciones por satélite o sus componentes. En relación con los procesos de obtención de satélites en el ámbito de la Administración española, destaca el Plan Director de Sistemas Espaciales de la Dirección General de Armamento y Material (DGAM) y en el ámbito del Departamento de Defensa (DoD) de los Estados Unidos destaca el procedimiento del U.S. General Services Administration (GSA) sobre obtención de servicios SATCOM.

3. Desarrollo del TFM

3.1 Posiciones orbitales y gestión del espectro

3.1.1 *Las posiciones orbitales y gestión del espectro espacial.*

Las posiciones orbitales necesitan ser coordinadas internacionalmente según los procedimientos de la Unión Internacional de Telecomunicaciones (UIT), para permitir que las diferentes redes de comunicaciones por satélite puedan coexistir evitando la interferencia perjudicial entre ellas, esa tarea la realiza en el ámbito de defensa la Sección NARFA del EMACON.

3.2 Proyecto de un sistema de comunicaciones por satélite

El proceso de lanzamiento y puesta en órbita de un satélite de comunicaciones geoestacionario es una operación compleja y altamente especializada que implica las siguientes fases:

1) Fase 1: diseño y construcción del satélite.
2) Fase 2: planificación de la misión (ventana y trayectoria de lanzamiento).
3) Fase 3: integración del satélite en la carga útil (pruebas finales).
4) Fase 4: lanzamiento (encendido y separación de etapas del cohete, inyección en Órbita de Transferencia Geoestacionaria-GTO).
5) Fase 5: maniobras orbitales y entrada en órbita geoestacionaria.
6) Fase 6: pruebas y puesta en servicio (pruebas funcionales, calibración y alineación, puesta en servicio).

3.3. Geometría del enlace de comunicaciones por satélite en órbita GEO

3.3.1 Órbitas

La órbita geoestacionaria es una órbita circular ecuatorial sin inclinación a 35 786 km sobre la superficie de la Tierra, en la cual el periodo de revolución de los satélites situados en ella es igual al periodo sideral de rotación de la Tierra alrededor de su propio eje.

3.4 Elementos principales de un sistema de comunicaciones por satélite GEO

3.4.1 Segmento espacial

El segmento espacial proporcionará capacidad de comunicaciones en banda X, banda Ka militar y banda UHF para misiones gubernamentales.

3.4.1.1 Bus del satélite

Se propone la plataforma SSL1300, conocida por su capacidad para soportar cargas útiles grandes y complejas.

3.4.1.2 Subsistema de potencia y baterías de lón-Litio

El subsistema de potencia proporciona tensión continúa producida por dos conjuntos de paneles solares desplegados en dos alas con cinco paneles cada una que pueden generar más de 15 kW de potencia, utilizando baterías de tecnología de lon-Litio.

3.4.1.3 Subsistema de control de postura

La estabilización en órbita y el apuntamiento preciso de antenas se consiguen utilizando el subsistema de control de postura en órbita, basado en sensores de infrarrojos.

3.4.1.4 Subsistema de propulsión

Basado en un sistema bi-propelente, mezcla de dos componentes (hidracina y oxidante) que se usa principalmente en satélites medios o pesados.

3.4.1.5 Subsistema de control térmico

Su función principal es mantener a todo el satélite y a los equipos que lo componen dentro de los rangos de temperaturas de operación de cada uno para la misión del satélite.

3.4.1.6 Subsistema de tratamiento de datos de a bordo

El subsistema de tratamiento de datos de a bordo proporciona telemetría y mandos de control en banda base para los subsistemas del satélite.

3.4.1.7 Subsistema de comunicaciones

Es la carga de pago principal del satélite. En esta propuesta teórica, el satélite incorporará un sistema de comunicaciones en banda X, banda Ka, banda UHF y banda S (para telemetría y telecomando) tanto RHCP como LHCP. Los canales podrán ser conmutables de banda X a banda Ka o viceversa, mediante una matriz de conmutación.

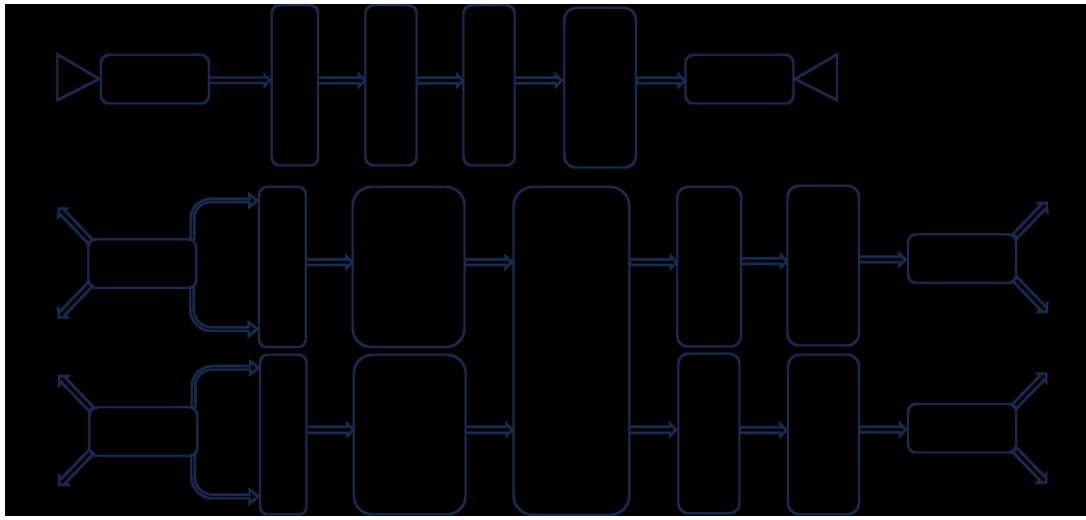


Figura 1. Esquema de la cadena de transmisión / recepción propuesto

Se usarán antenas parabólicas de cobertura global y regional para generar una huella de cobertura adecuada sobre la superficie terrestre.

3.4.2 Segmento terreno

3.4.2.1 Aspectos generales del segmento terreno

Aunque actualmente parece que la tecnología más popular en el entorno de las redes de comunicaciones por satélite son los terminales de usuario compactos de cobertura global, tanto en instalaciones fijas como móviles, esta tecnología es muy cambiante en función de las necesidades de los negocios en el ámbito civil y de la evolución de los conflictos como Ucrania, Siria o Gaza en el ámbito de defensa, lo que obliga a adaptar continuamente el *hardware* y el *software*, especialmente en este último entorno.

Figura 2. Diagrama aproximado de haz global (17º) sobre la posición 29º E (calculado con)

3.4.2.2 Arquitectura propuesta del segmento terreno

Arquitectura de segmento terreno para una red de satélites de comunicaciones:

A) Terminal de la Estación Terrena.
B) Centro de Operaciones de Misión (MOC).
C) Centro Técnico de Operaciones (TOC).
D) Red de comunicaciones local del segmento terreno y almacenamiento de datos
E) Infraestructuras de comunicación, que podrían ser:
   1) Directos a la Tierra (DTE), más habituales.
   2) Aumentados mediante retransmisión espacial.
F) Segmento terrestre como servicio (GSaaS):

Es un servicio administrado mediante un sistema de pago por uso de estaciones terrestres satelitales, habitualmente usado con satélites pequeños.

Figura 3. Diagrama de segmento terrestre como servicio (GSaaS)

4. Resultados y discusión

4.1 Cálculos de los enlaces de comunicaciones por satélite

A continuación se presentan los cálculos de balance del enlace satélite para las diferentes bandas consideradas. La posición del satélite que se va a considerar es la 29 E, con estaciones en Madrid y Beirut (Líbano) y los datos de las tablas 1 y 2.

Banda	Frecuencia enlace ascendente	Frecuencia enlace descendente	Ancho de banda canal	Modulación	Velocidad de la información	Tasa de error de bit en recepción (con FEC 3/4)
UHF	250 MHz	325,00 MHz	25 KHz	Q-PSK	16 Kbps	10^{-6}
X	8.028,00 MHz	7.228,00 MHz	2 MHz	Q-PSK	2048 Kbps	10^{-6}
Ka	24.528,00 MHz	23.028,00 MHz	40 MHz	Q-PSK	6.144 Kbps	10^{-6}
S	1.990,00 MHz	2.180,00 MHz	500 KHz	Q-PSK	512 Kbps	10^{-6}

Tabla 1. Plan de frecuencias

Banda	Densidad de flujo de potencia mínimo	Potencia isotrópica radiada equivalente de saturación	Relación ganancia a temperatura de ruido de recepción mínima	Intermodulación del transpondedor
UHF	-140 dBW/m^2	20 dBW	G/T = -13,5 dB/K G/T sistema = 12 dB/K	-37 dB/4 KHz
X	-70 dBW/m^2	30 dBW	G/T = -7 dB/K G/T sistema = 32 dB/K	-37 dB/4 KHz
Ka	-70dBW/m^2	32 dBW	G/T = -6 dB/K G/T sistema = 35 dB/K	-37 dB/4 KHz
S	-80 dBW/m^2	20 dBW	G/T = -8 dB/K G/T sistema = 25 dB/K	-37 dB/4 KHz

Tabla 2. Requisitos mínimos de los enlaces para las bandas de interés

4.1.1 Resultados de los cálculos del balance del enlace en bandas X, Ka, UHF y S

Los resultados indican que el enlace es viable con todas las frecuencias.

Banda	Potencia isotrópica radiada equivalente del satélite	Output Backoff	Input Backoff	Iluminación W (dBW/m^2)	BER
UHF	9,231 dBW	10,769 dB	13,769 dB	-153,769 dBW/m^2	$1{,}549 \cdot 10^{-7}$
X	11,753 dBW	18,247 dB	23,259 dB	-88,247 dBW/m^2	$< 10^{-6}$
Ka	29,678 dBW	2,022 dB	5,022 dB	-76,968 dBW/m^2	$< 10^{-6}$
S	-6,221 dBW	13,723 dB	16,723 dB	-96,723 dBW/m^2	despreciable

Tabla 3. Resultados de los cálculos

5. Conclusiones y líneas futuras

5.1 Conclusiones

Se ha resuelto, a nivel teórico, el diseño de un sistema de comunicaciones por satélite (segmento terreno y segmento espacial), cuyas líneas generales de diseño podrían satisfacer requisitos del SECOMSAT en las bandas UHF, S, X y Ka.

5.2 Líneas futuras

Se propone avanzar en el conocimiento del diseño de redes de sistemas de telecomunicaciones basados en constelaciones de satélites LEO para dar servicio de internet tipo «nube».

Profundizar en los aspectos de ciberoperaciones en el quinto dominio militar.

Estudiar las vulnerabilidades del sistema de cifrado de las comunicaciones (telecontrol y servicio de comunicaciones) en lo relativo a la computación y el cifrado cuánticos.

Otra línea futura de ampliación podría ser el estudio del mantenimiento de servicios de comunicaciones por satélite en entornos de riesgo de eventos nucleares a gran altitud (HANE).

Por último, el estudio de la aplicación de tecnologías de comunicaciones ópticas o láser tanto entre satélites en órbita, para realizar proceso y conmutación a bordo, así como para comunicaciones de muy alta velocidad entre el segmento terreno y el segmento espacial.

Referencias

Herrero Santos, C. (2019). Los sistemas espaciales de comunicaciones por satélite. *Memorial Ingenieros Politécnicos,* n.º 6, p. 23.

— Los sistemas espaciales de comunicaciones por satélite. *Memorial de Ingenieros Politécnicos*, n.º 6, p. 31.

G. Montaño, J. M. (2018). Sistemas espaciales para la Defensa. Revista Española de Defensa, enero 2018, p. 40.

Frąckiewicz, Marcin. (2023, 30 junio). La evolución de la comunicación por satélite: una breve historia. *TS2 SPACE*. LIM Center, XVI floor, Aleje Jerozolimskie 65/79, PL 00-697 Warsaw, Poland. [Consulta: 6 de enero 2024]. Disponible en: https://ts2.space/es/la-evolucion-de-la-comunicacion-por-satelite-una-breve-historia/

Hernández, María Jesús. (2021, 13 abril). El lanzamiento del satélite Minisat-01 desde Gran Canaria cumple 16 años. *La Provincia. Diario de Las Palmas*. [Consulta: 6 de enero 2024]. Disponible en: https://www.laprovincia.es/sociedad/2013/04/21/lanzamiento-satelite-minisat-01-gran-10446151.html

Hispasat. (2022, 13 septiembre). *Hispasat 1A: 30 años sin parar de sonar.* [Consulta: 6 de enero 2024]. Disponible en: https://blog.hispasat.com/es/articulo/116/hispasat-1a-30-anos-sin-parar-de-sonar

Infodefensa.com. (2019, 18 marzo). *Defensa adquirirá nuevos terminales satelitales sobre plataformas terrestres.* [Consulta: 6 de enero 2024]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3130310/defensa-adquirira-nuevos-terminales-satelitales-sobre-plataformas-terrestres

Wikipedia, La Enciclopedia libre. (2022, 4 mayo). *XTAR-EUR*. [Consulta: 6 de enero 2024]. Disponible en: https://es.wikipedia.org/wiki/XTAR-EUR

— (2023, 21 diciembre). *Spainsat*. [Consulta: 6 de enero 2024]. Disponible en: https://es.wikipedia.org/wiki/Spainsat

Morán, José Antonio y Mozo Sánchez, Carlos. (2023, 7 septiembre). El 5G por satélite: la nueva revolución en las telecomunicaciones. *Universidad Abierta de Cataluña (UOC),* [Consulta: 6 de enero 2024]. Disponible en: https://blogs.uoc.edu/informatica/5g-por-satelite-nueva-revolucion-telecomunicaciones/

HISDESAT (2023). *Programa Spainsat NG*. [Consulta: 6 de enero 2024]. Disponible en: https://www.hisdesat.es/c-seguras/programa-spainsat-ng/

Ministerio de Defensa. (2019). Plan Director de Sistemas Espaciales. Dirección General de Armamento y Material. Madrid, Imprenta Ministerio de Defensa.

U.S. General Services Administration. (2021, 27 abril). *How to Order Satellite Communications.* [Consulta: 14 de enero 2024]. Disponible en: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/telecommunications-and-network-services/satellite-communications/how-to-order

Naciones Unidas. (2024.). Unión Internacional de Telecomunicaciones. *Oficina de las Naciones Unidas en Ginebra*. [Consulta: 6 de enero 2024]. Disponible en: https://www.ungeneva.org/es/about/organizations /itu

Hernando Rábanos, José María. (1993). 6.4 Geometría del enlace por satélite. En: *Transmisión por Radio*. Escuela Técnica Superior de Ingenieros de Telecomunicación. Universidad Politécnica de Madrid. Madrid, Editorial Centro de Estudios Ramón Areces, p. 438.

Cloud Brain Think Tank. (2022, 21 febrero). *Características de desarrollo de la plataforma satelital SSL-1300 de Loral Systems de Estados Unidos*. [Consulta: 6 de enero 2024]. Disponible en: https://www.eet-china.com/mp/a112200.html

SatCatalog. (2024). *STD 16*. [Consulta: 6 de enero 2024]. Disponible en: https://www.satcatalog.com/component/std-16/

Cortés Borgmeyer, Susana. (2023). *Chemical Orbital Propulsion Module. Unified Propulsion Systems.* Ariane Group Orbital Propulsion TAUFKIRCHEN GERMANY. [Consulta: 6 de enero 2024]. Disponible en: https://space-propulsion.com/brochures/propulsion-systems/orbital-propulsion-module.pdf

Instituto Universitario de Microgravedad Ignacio da Riba. (2023). *UPM-Sat 2. Control Térmico.* Universidad Politécnica de Madrid. [Consulta: 6 de enero 2024]. Disponible en: https://www.idr.upm.es/index.php/es/upm-sat2?view=article&id=33:control-termico&catid=12

Satellite Signals Limited. (2013, 14 diciembre). Satellite beam design. Satellite Signals. [Consulta: 6 de enero 2024]. Disponible en: https://www.satsig.net/satellite/satellite-beam-design.htm

Amazon Web Services, Inc.(2023). *AWS Ground Station.* Disponible en: https://aws.amazon.com/es/ground-station/

Sistema de Comunicaciones Estratégico por Satélite

Autor: Carlos Herrero Santos
Director: Felipe Gil Castiñeira
Universidad de Vigo

Introducción

El trabajo muestra a nivel teórico los aspectos más importantes del diseño de un sistema de comunicaciones por satélite GEO que podría ser de utilidad para el SECOMSAT.
Para ello trata los siguientes temas:

- Geometría de los enlaces por satélite.
- Posiciones orbitales y gestión del espectro EM.
- Elementos principales del segmento espacial.
- Elementos principales del segmento terreno.
- Balance del enlace satélite.
- Ciberseguridad en los sistemas de comunicaciones por satélite.
- Aspectos generales de la gestión del proyecto.
- Conclusiones.

Metodología

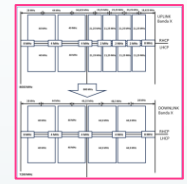
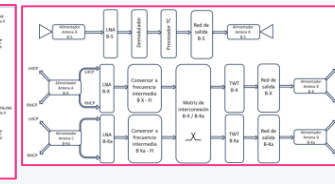
La metodología ha sido la investigación en la documentación académica disponible, la selección de fuentes bibliográficas y páginas Web de interés y la aplicación de métodos de cálculo específicos para averiguar las prestaciones teóricas de los enlaces satélite. Se han analizado:

- La gestión de las posiciones orbitales del NARFA-EMACON con la UIT.
- Las fases de un proyecto de un sistema de telecomunicaciones por satélite.
- Órbita GEO (geoestacionaria).
- Segmento espacial:
  - Subsistemas
  - Comunicaciones y antenas (parabólicas y array).


- Segmento terreno
  - Arquitectura, frecuencias, redes, balance de enlace.
  - Ground Segment as a Service (GSaaS).
  - Software Defined Radio (SDR).
- Cálculos de los enlaces de comunicaciones por satélite GEO:
  - Bandas UHF, S, X y Ka.,

Resultados

Se han planteado consideraciones válidas para el diseño de los segmentos terreno y espacial para cobertura en las bandas UHF, S, X y Ka con una BER mejor que 10^{-6}.

El resultado podría servir de referencia para un nodo de la nueva generación de satélites de Defensa SPAINSAR NG 1 y 2.

Conclusiones

Se ha expuesto las líneas generales de mayor importancia en el diseño de un sistema de comunicaciones por satélite GEO de posible utilidad para el SECOMSAT:



a. Geometría orbital GEO, en posición 29 E.
b. Gestión de recurso órbita-espectro.
c. Fases del proyecto de diseño e implantación.
d. Antenas parabólicas y en array de conformación electrónica del haz y orientables.
d. Verificación de la viabilidad del enlace en bandas UHF, S, X y Ka militar mediante cálculos.
e. Segmento terreno, SDR y computación en la nube como novedades.
f. Seguridad y ciberseguridad en sistemas satélite.

Agradecimientos

A mi esposa e hijos, por su paciencia y el tiempo que me han dado.

Megaconstelaciones de satélites en órbita LEO. Oportunidades, desafíos y riesgos en el ámbito de la defensa y seguridad

Autor: Magaz Villaverde, Francisco José (fmagaz.directic22.23@gmail.com)
Director: Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – La industria de los satélites está preparada para colocar en órbita terrestre baja LEO (Low Earth Orbit) en la próxima década más satélites pequeños, aquellos con una masa inferior a 600 kg, que todos los lanzados desde el comienzo de la carrera espacial. A medida que los avances tecnológicos han hecho que el uso del espacio sea más factible y económico, el número de satélites pequeños en el espacio exterior ha aumentado a un ritmo exponencial. La miniaturización de la tecnología también ha afectado la tecnología satelital y ha permitido que la industria espacial utilice satélites pequeños con capacidades que hace solo unos años habrían requerido satélites mucho más grandes. Estos satélites hacen posible el reciente lanzamiento y propuesta de megaconstelaciones, redes de más de cien satélites operando juntos en LEO.

La Estrategia Espacial de Seguridad Nacional de los EE. UU. reconoce que las operaciones espaciales son de vital importancia para la seguridad nacional. Para los Ejércitos de todo el mundo, estas megaconstelaciones propuestas brindan un potencial de ventajas inigualables sobre el escenario actual, pero también numerosos riesgos potenciales.

Este trabajo examina documentos disponibles públicamente, artículos de noticias, revistas, publicaciones académicas, informes gubernamentales, tratados internacionales, leyes y regulaciones, y otra información para evaluar el estado actual de la industria de las megaconstelaciones LEO, así como las tendencias que se están produciendo. Algunos de los aspectos discutidos se relacionan con actividades espaciales que incluyen el conocimiento de la situación espacial; ciberseguridad, inteligencia, reconocimiento y vigilancia, espionaje en órbita, interferencias de radio, desechos espaciales y armas antisatélite, por nombrar algunos.

Palabras clave – Defensa, Seguridad, LEO, Megaconstelación, Satélite.

1. Introducción

Estamos en la antesala de la próxima gran revolución de Internet, una revolución que proporcionará acceso rápido y de baja latencia a Internet en cualquier lugar del mundo, permitiendo una sociedad global verdaderamente conectada.

Hoy en día, si bien la conectividad a Internet se ha vuelto esencial en muchos aspectos de la vida cotidiana, todavía hay más de 3500 millones de personas sin acceso a internet, es decir, casi el 40 % de la población mundial. Incluso en los países más desarrollados, el acceso a internet no está disponible de manera uniforme, y algunas áreas sufren un acceso limitado, lento o nulo, incluidas ubicaciones rurales en las que puede no ser rentable conectarse.

Como resultado de los recientes avances tecnológicos, los satélites de órbita terrestre baja LEO de nueva generación tienen el potencial de ofrecer acceso a internet rápido y asequible en cualquier parte del mundo, en tierra, mar o aire.

El acceso a internet por satélite ha estado disponible desde hace más de veinticinco años desde satélites geoestacionarios en órbita terrestre alta GEO (Geosynchronous Equatorial Orbit). El desafío ha sido que los satélites que operan a esta altitud proporcionaran conexión a internet con una latencia mínima de 500 a 600 ms, lo cual es necesario para muchas aplicaciones. De hecho, la comunicación eficaz con estos satélites GEO suele requerir el uso de una gran antena parabólica fija o una señal relativamente potente.

Los satélites LEO, la última generación de satélites que proporcionan acceso a internet, son más pequeños, ligeros y menos costosos que los satélites GEO. Además, los satélites LEO se producen en masa y pueden costar tan solo siete mil euros cada uno, sin contar los costes de lanzamiento. Además, la disponibilidad de vehículos de lanzamiento reutilizables ha mejorado la economía en torno a la colocación de satélites en órbita terrestre baja, proporcionando la capacidad de poner hasta sesenta satélites LEO en órbita terrestre baja en un solo lanzamiento.

Uno de los inconvenientes de los satélites LEO es que operan a altitudes bajas, por lo que solo pueden cubrir áreas relativamente pequeñas. También se mueven rápidamente en el cielo, por lo que los proveedores de internet por satélite necesitar desplegar cientos o miles de satélites para proporcionar la conectividad que necesitan los usuarios en tierra. En el lado positivo, la baja altitud reduce la potencia necesaria para comunicarse con ellos, en comparación con los satélites GEO.

Para aumentar la resiliencia de estas megaconstelaciones de satélites LEO, algunos operadores de megaconstelaciones han equipado sus satélites con ISL (Inter-satellite link), comunicación satélite a satélite basada en

láser. Esto permite que los satélites de una constelación se comuniquen entre sí, proporcionando un servicio continuo incluso cuando algunos de ellos no tengan un enlace directo con una estación terrestre.

2. Desarrollo

2.1 Megaconstelaciones LEO

A fecha de 1 de enero de 2023, 5973 satélites LEO activos orbitan la Tierra, de los cuales más de cinco mil son de uso civil y el resto de uso militar o gubernamental. Históricamente, las comunicaciones por satélite implicaban naves en órbitas GEO, grandes sistemas que han adquirido más capacidades a lo largo de los años. Pero ahora las constelaciones de comunicaciones en órbita NGSO (Non-Geostationary Orbit), incluidos los satélites de órbita LEO y MEO (Medium Earth Orbit), están ganando protagonismo frente a las situadas en órbitas GSO (Geostationary Orbit) y su número pronto podría dispararse. Si las actuales propuestas de internet por satélite se hacen realidad, alrededor de cincuenta mil satélites activos orbitarán sobre la tierra dentro de diez años. Incluso si los planes más ambiciosos no se hacen realidad, los satélites se fabricarán y lanzarán a una escala sin precedentes.

Los nuevos conceptos de satélites LEO, que orbitan entre 180 km y 2000 de la Tierra, ofrecen comunicaciones más rápidas, con menor latencia y a menudo proporcionan un mayor ancho de banda por usuario que los satélites GEO, incluso más que el cable, el cobre y los sistemas inalámbricos anteriores a 5G. Estos conceptos requerirán cambios importantes en las operaciones de los satélites, incluida la fabricación y la cadena de suministro, ya que exigen más de un satélite y con una vida media más corta, estimada, por ejemplo, en unos cinco años en los satélites de la constelación Starlink.

2.2 Órbita terrestre baja

Una órbita terrestre baja es una órbita alrededor de la Tierra, entre la atmósfera y el cinturón de radiación de Van Allen, entre 180 km y 2000 km sobre su superficie, con un periodo de 128 minutos o menos, realizando al menos 11,25 órbitas por día, y una excentricidad inferior a 0,25.

La atracción de la gravedad en LEO es solo ligeramente menor que en la superficie de la Tierra. Esto se debe a que la distancia a LEO desde la superficie de la Tierra es mucho menor que el radio de la Tierra. Sin embargo, un objeto en órbita está en caída libre permanente alrededor de la Tierra, porque en órbita la fuerza gravitacional y la fuerza centrífuga se equilibran entre sí. Como resultado, las naves espaciales continúan en órbita, y las personas dentro o fuera de tales naves experimentan continuamente ingravidez.

Los objetos en LEO encuentran resistencia atmosférica proveniente de gases en la termosfera, aproximadamente a 80 km a 600 km de la superficie, o de la exosfera, a 600 km. Las órbitas de los satélites que alcanzan altitudes inferiores a 300 km se desintegran rápidamente debido a la resistencia atmosférica.

2.3 Ventajas de los satélites en órbita LEO

Costos de fabricación

Los satélites son mucho más baratos de fabricar que los satélites tradicionales de generaciones anteriores. En décadas anteriores, la fabricación de satélites normalmente llevaba varios años y costaba millones de dólares por satélite. Con el auge de los satélites pequeños y las megaconstelaciones, estos costos se están reduciendo considerablemente.

Tiempo de producción más rápido

De manera similar a la reducción de costos, los satélites pequeños tienen una reducción en el cronograma de producción debido a muchos factores, algunos de los cuales incluyen el uso de componentes COTS estandarizados y un factor de forma consistente que requiere menos personalización por satélite.

Costos de lanzamiento

Uno de los factores más importantes que impulsan el renacimiento de los satélites pequeños es la reducción del costo de lanzamiento y la mayor disponibilidad de lanzamiento. En la historia de la exploración espacial, los costos de lanzamiento siempre han representado una parte importante del gasto.

Latencia de comunicación

Una de las mayores capacidades que ofrecen los satélites pequeños en LEO sobre los satélites MEO y GEO tradicionales es un aumento en la velocidad de comunicación. Dado que la altitud de los satélites LEO es inferior al 5 % de la de los satélites GEO, el tiempo que tardan las señales de comunicación en llegar al satélite y regresar a la Tierra, latencia, se reduce significativamente.

Velocidad de comunicación y beneficios del sistema terrestre

5G es la generación actual de redes móviles y conectividad a internet con velocidades de conexión significativamente mayores, mayor ancho de banda y latencia reducida. La parte satelital de 5G, mediante megaconstelaciones LEO, tendrá la capacidad de complementar las redes 5G terrestres en momentos de desastres naturales y saturación de la red, pero también tendrá la capacidad de llevar cobertura a plataformas móviles, áreas remotas/rurales y partes del mundo que actualmente están desatendidas por proveedores de telefonía móvil e internet.

2.4 Megaconstelaciones satelitales

Iridium: La constelación consta de 66 satélites activos en órbita, necesarios para la cobertura global, y satélites de repuesto adicionales para servir en caso de fallo. Los satélites se colocan en órbita terrestre baja a una altura de 780 km y una inclinación de 86,4°.

Starlink: es un proyecto de megaconstelación de satélites en órbita LEO de la empresa SpaceX, para implementar un nuevo sistema de comunicación por Internet satelital. SpaceX ofrece velocidades de hasta 1 bit/s, con latencias entre 25 ms y 35 ms. A fecha de 16 de diciembre de 2023 se encuentran operativos en órbita 5168 satélites.

Kuiper: lanzará y operará el 50 % de sus satélites el 30 de julio de 2026, y deberá lanzar las restantes estaciones espaciales necesarias para completar su constelación de servicio autorizado, colocarlos en sus órbitas asignadas y operar cada uno de ellos de acuerdo con la autorización el 30 de julio de 2029. Kuiper ofrecerá servicios satelitales de alta velocidad y baja latencia mediante la puesta en órbita LEO de 3236 satélites en 98 planos orbitales agrupados en tres capas: a 590 km, 610 km y 630 km.

OneWeb: el sistema de satélites LEO OneWeb consta de 634 satélites operativos, a fecha de 20 de mayo de 2023, que operarán en doce planos a 1200 km de altitud, con una inclinación orbital casi polar, de 86,4°. Inicialmente se planearon 882 satélites, pero la capacidad mejorada de cobertura satelital permitió que esto se redujera a 588 satélites más algunos repuestos en órbita.

IRIS^2 (Infraestructura para la resiliencia, la interconectividad y la seguridad por satélite): es una constelación de Internet por satélite multiórbita planificada que la Unión Europea implementará en 2027. Su objetivo es proporcionar servicio a agencias gubernamentales, así como servicio comercial a entidades privadas.

2.5 Aspectos de defensa en las megaconstelaciones

El lanzamiento asequible y el desarrollo con una operación más precisa son algunos de los factores que están impulsando la demanda de operaciones espaciales en LEO. Las aplicaciones que ofrecen los satélites LEO casi están dejando de lado a los satélites más tradicionales y costosos en órbitas más altas.

Comunicaciones

Los Ejércitos utilizan una variedad de satélites SATCOM diferentes para satisfacer sus necesidades de comunicación, incluidos contratos comerciales SATCOM para ancho de banda en satélites de comunicaciones comerciales.

Según el general de división Peter Gallagher, director del equipo de red del Comando Futuros del Ejército, una alternativa LEO que pueda proporcionar «significativamente más rendimiento, más ancho de banda, más capacidad de su canal de transporte con menor latencia, por lo que los datos fluirán mucho más rápido de un extremo a otro».

Inteligencia, Vigilancia y Reconocimiento

Las megaconstelaciones ofrecen una alta tasa de revisita para aplicaciones ISR. En particular, la detección de cambios o el monitoreo casi continuo hacen posibles servicios militares.

Monitorización meteorológica

A través de una red de satélites, el Ejército puede crear una imagen del clima en cualquier punto de la Tierra y monitorear los cambios ambientales para proporcionar información valiosa para la planificación de operaciones militares. El clima puede afectar muchas partes de las operaciones militares; desde el clima específico del área objetivo, guía de armas, aviación y viajes navales seguros hasta reabastecimiento de combustible en el aire.

PNT

La obtención de información PNT (*Position, Navigation & Timing*) es, probablemente, la capacidad satelital militar más conocida.

Alerta temprana de misiles balísticos

Las megaconstelaciones LEO con capacidades de imágenes, radar o ELINT (Electronic Intelligence) serán beneficiosas para la alerta y la defensa contra misiles. Como las megaconstelaciones son capaces de proporcionar una cobertura casi continua de toda la Tierra, estas capacidades pueden utilizarse para proporcionar una cobertura continua de áreas conocidas de operación de misiles.

3. Resultados y discusión

El despegue de las megaconstelaciones LEO está impactando en la industria espacial tanto en el ámbito comercial como en el de defensa. Aproximadamente un tercio de los satélites activos en órbita son satélites Starlink. En la próxima década, hasta cincuenta mil satélites podrían orbitar la Tierra. La mayoría serán operados comercialmente, pero al menos unos cientos pertenecerán a los ejércitos de diferentes países y organizaciones gubernamentales.

El concepto de megaconstelación LEO no siempre fue bienvenido en la comunidad de defensa. Pero gracias a un cambio tecnológico fundamental en los últimos años, liderado por compañías espaciales comerciales, está impulsado la proliferación de las megaconstelaciones LEO.

El concepto de megaconstelación de satélites en órbita LEO no es nada nuevo, surgió en la década de los noventa, cuando varias empresas intentaron proporcionar conectividad global. Al final, sin embargo, redujeron o cancelaron sus megaconstelaciones previstas debido a los altos costos y la demanda limitada.

Sin embargo, muchas cosas han cambiado en los últimos veinte años. La tecnología satelital ha avanzado; la demanda de ancho de banda se ha disparado, sin que se vislumbre ninguna desaceleración; y las empresas han desarrollado modelos de negocio creativos para generar beneficios a partir de la conectividad. Además, tanto las empresas tecnológicas como los inversores cuentan ahora con reservas de capital mucho mayores para invertir, lo que les permite financiar grandes constelaciones.

4. Conclusiones

En un contexto geopolítico en el que las amenazas cibernéticas e híbridas se multiplican, las preocupaciones sobre la seguridad y la resiliencia aumentan y exigen una mejora cuantitativa y cualitativa de las capacidades gubernamentales de comunicaciones por satélite avanzando hacia soluciones de mayor seguridad, baja latencia y mayor ancho de banda.

El *boom* de las megaconstelaciones LEO ha comenzado. Estas megaconstelaciones por sí solas tienen el potencial de lanzar casi diez veces el número total de satélites jamás lanzados en la historia de la humanidad. El crecimiento de las megaconstelaciones de satélites pequeños y LEO en la próxima década tiene el potencial de crear una igualdad de acceso a Internet de alta velocidad en todo el mundo como nunca.

Actualmente, la industria se encuentra en un periodo de transición en el que se impone el modelo de arquitectura multicapa. Pero a medida que los sistemas se vuelven más pequeños y potentes, muchas de las capacidades que actualmente funcionan en GEO y en MEO pasarán en gran medida a LEO en los próximos diez a quince años.

Referencias

Miniwatts Marketing Group. (2023). *Internet Usage Statistics. The Internet Big Picture*. [En línea]. Disponible en: https://www.internetworldstats.com/stats.htm

Raj, A. (2022). Are low earth orbit satellites the future of internet connectivity? *Tech Wire Asia*. [En línea]. Disponible en: https://techwireasia.com/2022/04/are-low-earth-orbit-satellites-the-future-of-internet-connectivity/

Winick, E. (2019). SpaceX has launched the first 60 satellites of its space internet system. *MIT Technolgy Review*. [En línea]. Disponible en: https://www.technologyreview.com/2019/05/24/135223/spacex-has-launched-the-first-60-satellites-of-its-space-internet-system/

Nijhawan, A. (2022, 24 marzo). Inter-satellite Optical Links: A New Frontier for Communications Technology. *All about circuits*. [En línea]. Disponible en: https://www.allaboutcircuits.com/news/inter-satellite-optical-links-a-new-frontier-for-communications-technology/

Union of Concerned Scientists. (2023). *UCS-Satellite-Database-1-1-2023*. [En línea]. Disponible en: https://www.ucsusa.org/sites/default/files/2023-06/UCS-Satellite-Database-1-1-2023.xlsx

Malik, T. (2019, 15 noviembre). How to Spot SpaceX's 60 New Starlink Satellites in the Night Sky. *Space.com*. [En línea]. Disponible en: https://www.space.com/see-spacex-starlink-satellites-in-night-sky.html

NASA. (s.f.). *SCaN Glossary*. [En línea]. Disponible en: https://www.nasa.gov/directorates/heo/scan/definitions/glossary/index.html

Steering Group and Working Group 4. (2007, septiembre). *IADC Space Debris Mitigation Guidelines*. [En línea]. Disponible en: https://www.unoosa.org/documents/pdf/spacelaw/sd/IADC-2002-01-IADC-Space_Debris-Guidelines-Revision1.pdf

Segert, T. y Attara, S. (2019, 16 julio). Mass Manufacturing of Small Satellites, Gearing up for the Henry Ford Moment. Digital Commons. [En línea]. Available: https://digitalcommons.usu.edu/smallsat/2019/all2019/265/

Rayal, F. (2021, 7 julio). *Latency in LEO Satellites vs. Terrestrial Fiber*. [En lín ea]. Disponible en: https://frankrayal.com/2021/07/07/latency-in-leo-satellites-vs-terrestrial-fiber/

Hollington, J. (2023, 18 marzo). What is 5G? Speeds, coverage, comparisons, and more. *Digital Trends*. [En línea]. Disponible en: https://www.digitaltrends.com/mobile/what-is-5g/

Orbital ATK. (2015, 26 septiembre). *Iridium NEXT*. [En línea]. Disponible en: https://web.archive.org/web/20150926094943/https:/www.orbitalatk.com/space-systems/commercial-satellites/communications-satellites/docs/FS002_11_OA_3862 %20IridiumNEXT.pdf

SpaceX. (s.f.). *Starlink*. [En línea]. Disponible en: https://www.starlink.com/

McDowell, J. (2023, 4 noviembre). Starlink Statistics. *Jonathan's Space Pages*. Disponible en: Available: https://planet4589.org/space/con/star/stats.html

FCC. (2020, 30 julio). In the Matter of Kuiper Systems LLC Application for Authority to Deploy and Operate a Ka-band Non-Geostationary Satellite Orbit System. [En línea]. Disponible en: https://docs.fcc.gov/public/attachments/FCC-20-102A1.pdf

EutesatOneWeb. (2023, 20 mayo). *OneWeb confirms successful deployment of 16 satellites including next-generation JoeySat*. [En línea]. Disponible en: https://oneweb.net/resources/oneweb-confirms-successful-deployment-16-satellites-including-next-generation-joeysat

FCC. (2016, 28 abril). *OneWeb Non-Geostationary Satellite System*. [En línea]. Disponible en: https://forum.nasaspaceflight.com/index.php?action=dlattach;topic=37814.0;attach=1345367

Breton, T. (2022, 17 noviembre). Welcome to IRIS², Europe's new Infrastructure for Resilience, Interconnection & Security by Satellites. *European Commission*. [En línea]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_6999

Erwin, S. (2019, 15 octubre). Army eyes commercial megaconstellations to support its future battlefield network. *Spacenews*. [En línea]. Disponible en: https://spacenews.com/army-eyes-commercial-megaconstellations-to-support-its-future-battlefield-network/

Hallex, M. A. y Cottom, T. S. (2020, 31 marzo). Proliferated Commercial Satellite Constellations: Implications for National Security. *National Defense University Press*. [En línea]. Disponible en: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106495/proliferated-commercial-satellite-constellations-implications-for-national-secu/

Wood, L. (2000, 14 enero). Big LEO overview. [En línea]. Disponible en: http://personal.ee.surrey.ac.uk/Personal/L.Wood/constellations/tables/overview.html

Megaconstelaciones de satélites en órbita LEO. Oportunidades, desafíos y riesgos en el ámbito de la Defensa y Seguridad

Autor: Francisco José Magaz Villaverde
Director: José María Núñez Ortuño

Universidad de Vigo

Introducción

- El concepto de megaconstelación de satélites en órbita LEO no es nada nuevo, surgió en la década de los 90. Sin embargo, redujeron o cancelaron sus megaconstelaciones previstas debido a los altos costos y la demanda limitada.
- La tecnología satelital ha avanzado, la demanda de ancho de banda se ha disparado y las empresas han desarrollado modelos de negocio para generar beneficios a partir de la conectividad.
- Los nuevos conceptos de satélites LEO, que orbitan entre 180 km. y 2.000 de la Tierra, ofrecen comunicaciones más rápidas, con menor latencia y a menudo proporcionan un mayor ancho de banda por usuario que los satélites GEO, incluso más que el cable y los sistemas inalámbricos anteriores a 5G.

Capacidades en Defensa y Seguridad

- SATCOM.
- Inteligencia, Vigilancia y Reconocimiento.
- Monitorización meteorológica.
- PNT.
- Alerta temprana de misiles balísticos.
- Operaciones de disuasión nuclear.

Amenazas y Desafíos

- Amenazas cibernéticas.
- Acumulación de desechos espaciales en órbitas LEO.
- Interferencias del espectro radioeléctrico.
- Aspectos legales y regulatorios de las megaconstelaciones.
- *Anti-satellite Weapon.*

Megaconstelaciones

STARLINK

IRIS²

iridium connected

OneWeb

amazon | project kuiper

Conclusiones

- La revolución de los satélites en órbita LEO está en marcha, liderada principalmente por el sector privado. Las estructuras de Defensa deben buscar formas de aprovechar estas tendencias en su beneficio, tanto haciendo uso de proyectos comerciales como estudiando soluciones específicas para el ejército.
- En un contexto geopolítico en el que las amenazas cibernéticas e híbridas se multiplican, las preocupaciones sobre la seguridad exigen una de las capacidades de comunicaciones por satélite avanzando hacia soluciones de mayor seguridad, baja latencia y mayor ancho de banda.
- Serán una pieza importante para el de operaciones multidominio de cualquier Ejército en términos tanto de defensa como de ataque. Los satélites LEO ayudan a combinar esfuerzos en tierra, aire, agua y espacio.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2023/2024

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL