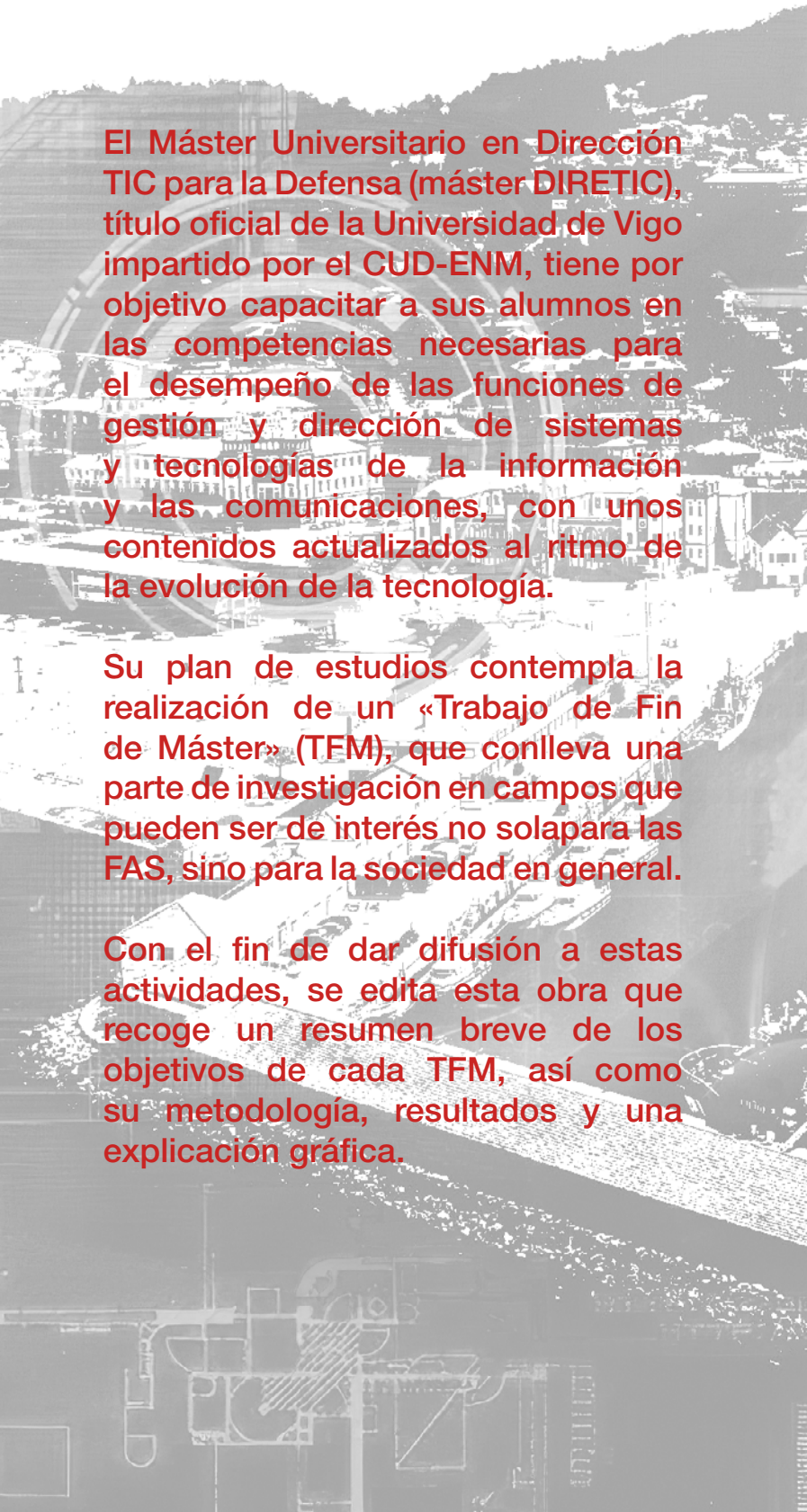
Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2020-2021

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 solapara 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 2020-2021

Resúmenes extendidos

Centro Universitario de la Defensa en la Escuela Naval Militar

MINISTERIO DE DEFENSA

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

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

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edición científica: Milagros Fernández Gavilanes y José María Núñez Ortuño

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-22-310-9 (impresión bajo demanda)
ISBN 978-84-9091-722-0 (impresión bajo demanda)

NIPO 083-22-309-6 (edición en línea)

Fecha de edición: diciembre 2022
Maqueta e imprime: Imprenta Ministerio de Defensa

IBERDROLA

En esta edición se ha utilizado papel 100% libre de cloro procedente de bosques gestionados de forma sostenible.

Prólogo

El Centro Universitario de la Defensa en la Escuela Naval Militar (CUD-ENM), es un centro universitario público del Ministerio de Defensa (MINISDEF), adscrito a la Universidad de Vigo, que comenzó su actividad en el curso académico 2010-2011, en virtud de lo dispuesto en el Real Decreto 1723/2008, de 24 de octubre, por el que se crea el sistema de centros universitarios de la defensa. Su finalidad principal es la impartición de las enseñanzas universitarias que acuerde el MINISDEF, en función de las necesidades de la defensa nacional y las exigencias del ejercicio profesional de las Fuerzas Armadas. Su objetivo prioritario es la impartición del título de grado en Ingeniería Mecánica (intensificación en Tecnologías Navales), título oficial de dicha universidad, pero el propio R.D. contempla que se puedan impartir enseñanzas de posgrado, en las modalidades de máster y doctor.

La Orden DEF/2639/2015, de 13 de diciembre, sobre Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, señala la necesidad de hacer una revisión de los cursos de perfeccionamiento y de altos estudios de la Defensa Nacional, a fin de obtener un mejor aprovechamiento de las capacidades del personal en el ámbito CIS/TIC del MINISDEF. Como consecuencia de esta necesidad nace el curso en Gestión y dirección de sistemas y tecnologías de la información y las comunicaciones (STIC) y de seguridad de la información, cuyo plan de estudios contempla una carga lectiva (60 ECTS), asignada al CUD-ENM en forma de máster, más un periodo de prácticas presenciales (6 ECTS), cuya responsabilidad recae en el CESTIC. El curso comenzó su andadura en

septiembre de 2017, con el máster impartido como título propio, por estar en proceso de verificación la memoria correspondiente al título oficial. La verificación positiva del título se produjo en julio de 2019, año a partir del cual el máster es impartido como título oficial de la Universidad de Vigo, con la denominación de Máster Universitario en Dirección TIC para la Defensa (máster DIRETIC). En enero de 2021 se ha producido el egreso de la primera promoción de este máster.

El plan de estudios del máster DIRETIC contempla la realización de un trabajo de fin de máster (TFM) dirigido por profesores del mismo, que conlleva una parte de investigación en campos que pueden ser de interés no solo para las FAS, sino para la sociedad en general. Con el fin de dar difusión a estas actividades, se edita el presente volumen que recoge, para cada TFM realizado durante el curso académico 2020-2021, un resumen de sus objetivos, metodología empleada y resultados obtenidos, así como una explicación esquemática en forma gráfica. Todos los resúmenes, así como los trabajos completos cuya difusión ha sido autorizada, se encuentran accesibles en el siguiente repositorio del centro: http://calderon.cud.uvigo.es, al que se puede acceder libremente.

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

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

Índice de contenidos

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

http://calderon.cud.uvigo.es/handle/123456789/482

Índice de contenidos

Especialidad en sistemas y tecnologías de la telecomunicación

Índice por autores

Trabajos Fin de Máster

Especialidad en sistemas y tecnologías de información

Especialidad en sistemas y tecnologías de la telecomunicación

Trabajos Fin de Máster

Especialidad en sistemas y tecnologías de información

Implantación de tecnologías de contenedores en una organización

Autor: Alonso Batuecas, Francisco (fab@interior.es)
Directores: Suárez Lorenzo, Fernando (externo.fernandosuarez@cud.uvigo.es)
Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – El contenido de este trabajo de fin de máster, versa sobre la implantación de tecnologías tipo contenedores, dentro de las infraestructuras de sistemas y comunicaciones de una organización, desde el punto de vista de un director de infraestructura con la experiencia de años en este campo y contextualizada en la fecha de realización del mismo.

Se pretende describir en qué consiste este tipo de tecnología, profundizando en los diferentes componentes que la forman, cómo se relacionan entre sí, qué funciones realizan y sobre qué tipos de servidores y sistemas de comunicaciones se pueden desplegar.

Analizar las diferentes posibilidades existentes a la hora de su implantación, productos comerciales y de software libre, así como abordar su despliegue, necesidades y consideraciones a tener en cuenta.

Por otro lado, se trata de introducir la metodología DevOps y su integración dentro de la infraestructura dockerizada, exponiendo en qué consiste la integración continua.

Por último, se pretende abordar la securización o retos de seguridad en estas plataformas y las claves para poder aplicar buenas prácticas de cara a una configuración segura de la plataforma.

Para finalizar, se presentan las conclusiones en función de todo lo desarrollado durante el TFM, que permitan tomar una decisión a la hora de abordar una implantación o cambio tecnológico dentro de una organización, en función de las diferentes posibilidades existentes.

Palabras clave – Docker, infraestructura, administración, seguridad, desarrollo, contenedores.

1. Introducción

Los *contenedores* no son un concepto nuevo, los primeros pasos se dieron sobre el sistema operativo Unix unos pocos años antes del 1979, año en el que comienza a darse sobre los sistemas operativos Linux. Desde entonces, esta tecnología no ha parado de evolucionar, para llegar a la situación actual que se prevé que no sea la final y siga con la constante evolución, a continuación, se muestra en la figura 1-1 una línea de tiempo de dicha evolución.

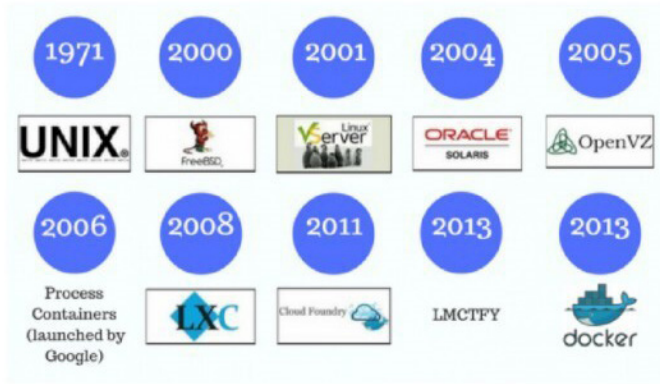


Figura 1-1 Historia contenedores (Fuente: [1])

En los inicios, los esfuerzos sobre esta tecnología se centraban en mejorar el aislamiento de los contendores, lo que dio origen a *Solaris Containers*, tecnología que aprovechó la función mejorada del Sistema Operativo Solaris llamada *Zones* para aislar aún más los contenedores.

Como siguiente hito, destacan las contribuciones de Google que aportaron como resultado la creación de varias arquitecturas de contenedores en el año 2006. Estas tenían la capacidad de particionar y asignar recursos de hardware, almacenamiento y red a los contenedores creados, proporcionando a los gestores mayor control y granularidad sobre los mismos y a su vez, tener mayor visibilidad sobre cómo podían influir en la seguridad.

Estas mejoras, poco a poco, se fueron incorporando en los sistemas operativos Linux, lo cual impulsó la evolución de las *tecnologías de virtualización* basada en *contenedores* conocidas actualmente. Destacándose las conocidas como *LXC*, *LMCTFY* de Google, que luego derivaron en *Kubernetes*, y *Docker*.

1.1. Introducción a la problemática

Para poder entender mejor, por qué se da el salto a una arquitectura de contendores, tenemos que conocer cuál es el estado del arte en el desarrollo de software y la gestión de la infraestructura en la cual se despliegan esos desarrollos.

Los retos o problemas a los que nos enfrentamos los podemos clasificar, en función de la fase en la que se producen, en tres categorías:

- Problemas durante la construcción del software.
  - Dependencias de desarrollo.
  - Versiones de entornos de ejecución.
  - Equivalencia de entornos de desarrollo.
  - Equivalencia de entornos de producción.
  - Versiones / compatibilidad con terceras partes.
- Problemas durante la distribución del software.
  - Generaciones de entregables (*builds*) diferentes.
  - Acceso a servidores de producción.
  - Ejecución nativa vs. ejecución distribuida.
- Problemas para la ejecución del software.
  - Dependencias de aplicación
  - Compatibilidad de sistema operativo
  - Disponibilidad de servicios externos
  - Recursos hardware

1.2. Soluciones adoptadas

Se suele abordar la respuesta a estos problemas, con entornos preproductivos, intentando mantenerlos nivelados con los entornos de producción. Haciendo uso de metodologías y procedimientos para el desarrollo de software y despliegue de aplicaciones, o utilizando las ventajas de la virtualización para conseguir distribuir entornos y acercarlos al desarrollador con la idea de atajar los problemas mencionados.

Con la virtualización, se pasó a una sencillez y flexibilidad que antes era impensable, simplemente con una platilla bien configurada era posible replicar servidores y crear un entorno preproductivo igual que el productivo, facilitando la labor a los responsables de infraestructura.

Pero el mundo de la tecnología no para de evolucionar y fijándose en el sector del transporte y las mercancías, parece que ha encontrado una solución muy optimizada para los problemas mencionados. A la fecha de redacción de este trabajo el estado del arte pasa por la infraestructura de contenedores y los desarrollos orientados a microservicios que aprovechen las bondades de dichas plataformas, tal como se mencionan en numerosos artículos especializados [2][3].

Ahora, extrapolado al mundo tecnológico, las soluciones basadas en contenedores, lo que prometen es que se pueda construir, distribuir y ejecutar el código desarrollado en cualquier lugar sin tener problemas del entorno en el cual se ejecutan, dentro de estas, *Docker* constituye una de las más extendidas en la industria.

Solomon Hykes comenzó *Docker* como un proyecto interno dentro dotCloud, empresa enfocada a una plataforma como servicio (PaaS), con las contribuciones iniciales de otros ingenieros de dotCloud, incluyendo Andrea Luzzardi y Francois-Xavier Bourlet. Jeff Lindsay también participó como colaborador independiente. *Docker* representa una evolución de la tecnología patentada de dotCloud, que es a su vez construida sobre proyectos de código abierto anteriores como Cloudlets [4].

Desde entonces hasta ahora *Docker*, ha conseguido ser el referente en cuanto a plataformas de contenedores se refiere, aunque le están surgiendo otros competidores como Kubernetes u OpenShift.

Kubernetes (K8s) que nació en 2014 como una plataforma de código abierto para automatizar la implementación, el escalado y la administración de aplicaciones en contenedores. Kubernetes agrupa los contenedores que conforman una aplicación en unidades lógicas para una fácil administración y descubrimiento [5].

Red Hat OpenShift es la plataforma de nube híbrida con el respaldo de la empresa Red Hat: que para infraestructuras empresariales cuenta con el soporte del propio Red Hat, ofreciendo características similares al resto [6].

En la figura 1-2, se puede ver la evolución del uso de la solución *Docker,* y como en los años 2016 y 2017, experimenta una subida exponencial.

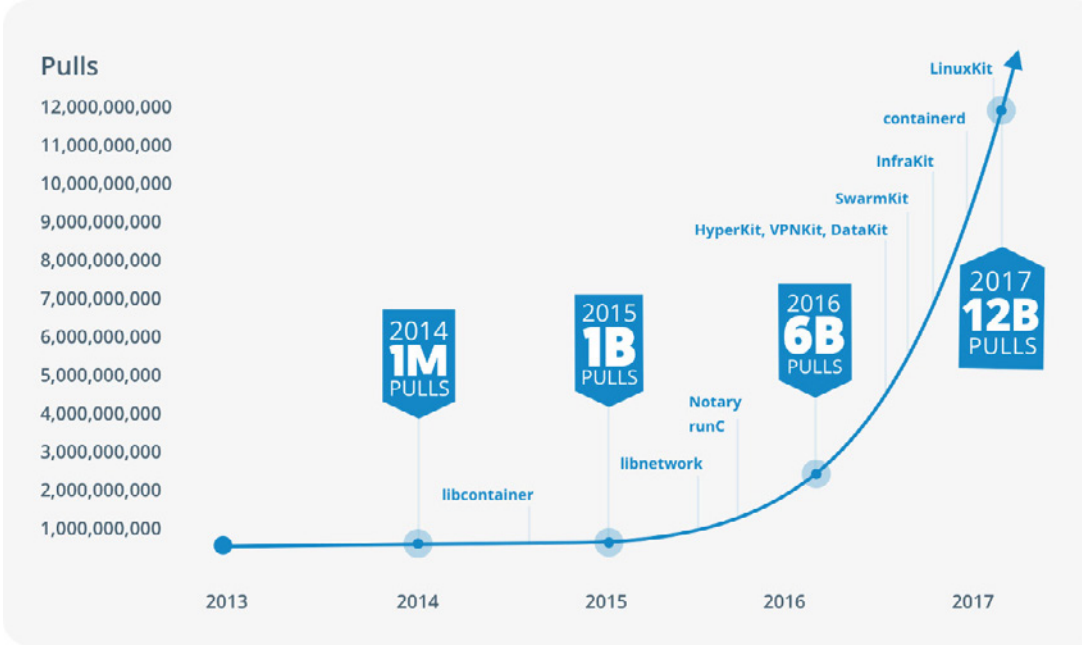


Figura 1-2 Evolución contenedores (Fuente: [7])

2. Desarrollo

La *Containarization*, también conocida como virtualización basada en contenedores, es una modalidad de virtualización a nivel de sistema operativo, que nos permite desplegar y ejecutar aplicaciones sin necesidad de contar con una máquina virtual completa, con su S.O. y asignación de recursos.

En su lugar, se puede montar uno o varios sistemas aislados denominados contenedores. Estos sistemas pueden ser ejecutados sobre un único servidor huésped *host* y acceden al mismo núcleo (*kernel*), que el de su servidor alojador, por lo cual comparten el mismo S.O. sin necesidad de montar uno para cada contenedor, a diferencia de las máquinas virtuales, que además requieren de un hipervisor para la gestión de los recursos del *host*, que consume recursos del mismo y conforman una infraestructura más pesada que la de contenedores.

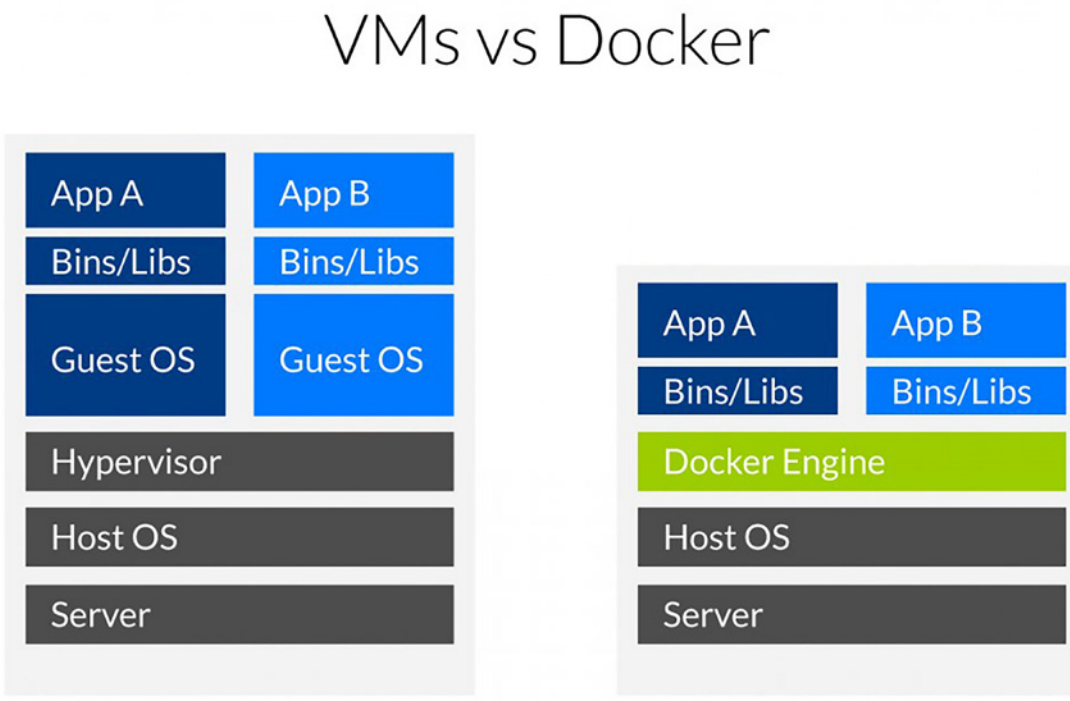


Figura 2-1 VMs vs. Docker (Fuente: [8])

En la siguiente tabla, se pueden ver las características de la *containarizacion* y la virtualización, al objeto de poder comprender de una forma más clara las diferencias entre estas dos tecnologías.

Containarization	Virtualización
Virtualización basada en S.O. Múltiples contenedores sobre el mismo O.S.	**Virtualización basada en hardware** Múltiples S.O. comparten los recursos del *host*
Ligero Servicios de aplicaciones compartiendo recursos del S.O.	**Pesado** S.O. adicionales gestionando recursos para cada *guest*
Aprovisionamiento en tiempo real De forma sencilla, en el momento en el que se comienzan a ejecutar nuevos servicios de aplicaciones	**Aprovisionamiento lento** Requiere inicialización del *guest*, más el tiempo de arranque del S.O.
Ejecución nativa Acceso directo a los recursos del hardware	**Ejecución limitada** Acceso a los recursos del hardware por medio de la capa de virtualización
Menos seguridad Aislamiento únicamente a nivel de procesos	**Alta seguridad** Aislamiento total

Tabla 1. Características de *containarization* y virtualización

2.1. Contenedor

El contenedor es la pieza fundamental sobre la que se apoya la infraestructura de contenedores, básicamente es un proceso o agrupación de procesos, en función de la complejidad del mismo, que solo pueden ejecutarse en el propio contexto del contenedor. Es decir, los procesos están aislados y solamente pueden usar los recursos definidos en el contenedor.

En el caso de *Docker*, los procesos corren de forma nativa en máquinas Linux, lo único que se comparte es el *kernel*, por eso en ambientes productivos se usa *Docker* instalado sobre Linux.

Para ello Linux aísla los contenedores utilizando los conceptos de *Chroot*, *Cgroups* y *Namespaces*.

2.2. Docker

Docker surge como un proyecto de código abierto basado en contenedores de Linux. Se puede definir como un *motor de contenedores*, para ello utiliza las características del núcleo de Linux que se han explicado

en el apartado anterior, permitiéndole crear los contenedores por encima del S.O. sin necesidad de montar un S.O. por cada contenedor, a diferencia de las M.V.

A continuación, se muestra un resumen de los componentes más importantes de *Docker*

Componente	Función
Servidor	Proceso lanzado mediante el comando, *dockerd*
Rest API	Interfaz de comunicación entre los programas y el demonio de *Docker*
Cliente	Consola de línea de comandos (*CLI*)
Imágenes de *Docker* (*Docker Images)*	Plantilla en modo solo lectura, con toda la configuración de un contenedor en el fichero de manifiesto (*Docker file*)
Registros de *Docker* (*Docker Registries)*	Componente utilizado para la distribución, define los repositorios de imágenes.
Contenedores de *Docker* (Docker Containers)	Componente con todo lo necesario para ejecutar las aplicaciones o servicios
Docker Swarm	Componente para la creación y gestión de *Clusters*
Docker Machine	Herramienta para el despliegue de contenedores en servidores virtuales
Docker Compose	Herramienta de gestión en infraestructuras con elevado número de contenedores

Tabla 2. Resumen Componentes *Docker*.

2.3. Aspectos de seguridad en *Docker*

A continuación, se muestran recomendaciones para bastionar nuestra infraestructura de contenedores, en función del componente que estemos configurando:

Componente	Función
Host	Chequear la partición de instalación Gestionar los permisos de los usuarios con gestión sobre la plataforma Auditar los ficheros y directorios de la instalación de *Docker*
Docker Daemon	Limitar el tráfico entre contendores Verificar la autorización de uso de la CLI Realizar una buena gestión de registros (*logs*) Configurar los permisos de acceso a los ficheros del Daemon.
Imágenes de *Docker* (*Docker Images*)	Revisar los permisos de ejecución (root) Uso del *Content Trust* para revisar la integridad de las imágenes Vigilar que no queden almacenados secretos
Contenedores de *Docker* (*Docker Containers*)	Restringir los protocolos de uso Configurar una política de limitación de uso de recursos

Tabla 3. Buenas prácticas de seguridad

3. Resultados y discusión

Como objetivos para la realización de este trabajo, se planteaban identificar las cuestiones que un director de infraestructura debe tener en cuenta, a la hora de abordar la implantación de una plataforma basada en contendores, por lo que a continuación se muestran los resultados obtenidos:

- Perfil de organización: No siempre encajan en nuestra organización, ni tampoco son sustitutivas de la virtualización, incluso pueden ser complementarias.
  Si el negocio tecnológico de la organización se limita al uso de los sistemas de información comerciales, puede ser que no sea el perfil ideal para dar el salto a los contendores, ya que en muchas ocasiones los paquetes comerciales de aplicaciones, no están desarrollados para ser desplegados sobre contendores y sí sobre máquinas virtuales, en este caso la optimización que se persigue con una estrategia de contenedores es inviable.
  En el caso de que la organización se dedique al desarrollo de sistemas de información, y cuente con el conocimiento necesario, sí es una opción, pero siempre y cuando los sistemas a desarrollar estén basados en microservicios, o productos atomizados, que son los que obtendrán mejores resultados en el despliegue en contendores.
- Elección de plataformas: Se han analizado durante el trabajo las plataformas *Docker*, *OpenShift*, *Kubernetes* y *Rocket*, pero no son las únicas, ya que también existen plataformas de contendores como servicio (CaaS), donde se consume el servicio desde una nube especializada en esta materia.
  En función de las preferencias de la organización y el tipo de sensibilidad de la información que maneje, tocará abordar esta cuestión al igual que cualquier servicio de la nube, con las ventajas y desventajas de los mismos.
  Si la organización maneja información sensible, lo normal es que opte por plataformas en sus propias instalaciones.
- Tipo de implantación: En el caso de que el servicio exija una disponibilidad elevada, existen los *cluster* de contenedores, pero si estamos pensando en servicios 24x7x365, y con la posibilidad de un buen plan de continuidad de negocio apoyándose en otros CPD o en una infraestructura de nube híbrida, quizá sea interesante un planteamiento tomando como base la virtualización con un hipervisor.

4. Conclusiones

La tecnología de contenedores ha venido para quedarse, igual que ya lo hizo la virtualización.

Docker está orientado para fusiones de los equipos de Dev y Ops en DevOps, aportando mayor agilidad para las operaciones, la seguridad y mejorar los tiempos en los desarrollos, también permitir en una misma infraestructura el despliegue de aplicaciones con diferentes leguajes y filosofías, para que puedan interoperar entre ellas.

Esto permite aumentar la productividad de los equipos y reducir los tiempos de entrega.

En el ámbito de las metodologías para el desarrollo, de la mano de los contenedores llegan las metodologías de integración continua y distribución continua. Esto promete mejorar los tiempos de desarrollo, ya que se acortan las esperas para pruebas y validaciones.

Tendremos que realizar un análisis previo en el que se considere los equipos de desarrollo e infraestructura que tenemos, el uso que le vamos a dar a esta nueva plataforma, es decir, qué sistemas de información se van a desplegar en la misma para elegir las diferentes opciones que tenemos. Queda reflejado, que, para entornos empresariales, siempre que sea posible se aconseja alguna de las soluciones comerciales frente a las soluciones de comunidad.

Habrá que estar pendiente de las nuevas actualizaciones de las plataformas, ya que constantemente están surgiendo nuevas herramientas para interoperar con los contenedores.

Agradecimientos

Me gustaría mostrar mi agradecimiento al profesorado y alumnado del máster, que pese a las particularidades que durante este curso hemos sufrido por la Covid19 han conseguido llevar a buen puerto este máster.

Una mención especial para mi familia, Amalia, Ángel y Mario, por acompañarme durante la realización del máster, y por aceptar con agrado mi falta de tiempo para ellos.

Referencias

[1] Tienda ReDIGIT Informática Circular, (2019) «Tecnología de virtualización basada en contenedores», tienda ReDIGIT Informática Circular.

[2] D. Russell, «https://cepymenews.es/predicciones-tecnologia-2020/» cepymenews.es, no. https://cepymenews.es/predicciones-tecnologia-2020/2020.

[3] E. Flo, (2021) «Teletrabajo, nube, contenedores y ciberseguridad protagonizarán 2021». computerworld, no. https://www.computerworld.es/tendencias/teletrabajo-nube-contenedores-y-ciberseguridad-protagonizaran-2021.

[4] Proyectos Wikimedia, «https://es.wikipedia.org/ 15 diciembre 2020. [Online]. Disponible: https://es.wikipedia.org/wiki/Docker_(software).

[5] L. a. d. Kubernetes, «https://kubernetes.io/», [Online]. Disponible: https://kubernetes.io/es/

[6] Copyright © 2020 Red Hat, Inc, «https://www.openshift.com/», [Online]. Disponible: https://www.openshift.com/

[7] A. E. Amri, «An Overall View On Docker Ecosystem — Containers, Moby, Swarm, Linuxkit, containerd & Kubernetes», 11 junio 2018. [Online]. Disponible: https://medium.com/faun/an-overall-view-on-docker-ecosystem-containers-moby-swarm-linuxkit-containerd-kubernetes-5e4972a6a1e8

[8] Erwin, «https://www.lomasnuevo.net/», 15 agosto 2016. [Online]. Disponible: https://www.lomasnuevo.net/cloud/maquinas-virtuales-vs-contenedores/

Implantación de Tecnologías de Contenedores en una Organización

Autor: Francisco Alonso Batuecas
Director/es: Fernando Suárez Lorenzo y Norberto Fernández García

Introducción

Se pretende describir en qué consiste este tipo de tecnología, profundizando en los diferentes componentes que la forman, cómo se relacionan entre sí y qué funciones realizan.

Analizar las diferentes posibilidades existentes a la hora de su implantación, así como abordar las consideraciones a tener en cuenta.

Por último, se pretende abordar la securización o retos de seguridad en estas plataformas y las claves para poder aplicar buenas prácticas de cara a una configuración segura de la plataforma.

Resultados

- Conocimiento de este tipo de tecnología.
- Puntos a tener en cuenta a la hora de implantarla.
- Comparativa de las diferentes plataformas.
- Buenas prácticas de seguridad en estas infraestructuras.
- Tipos de implementación.

Variedad de elección

Conclusiones

- La tecnología de contenedores ha venido para quedarse.
- Docker está orientado para fusiones de los equipos de Dev y Ops en DevOps.
- Esto permite aumentar la productividad de los equipos y reducir los tiempos de entrega.
- De la mano de loscontenedores llegan las metodologías de integración continua y distribución continua.
- Es evidente que seguirán evolucionando, ya que son las plataformas más utilizadas en tecnología tipo nube y se están extendiendo al resto de sectores

Agradecimientos

Al profesorado y alumnado del Máster, que pese a las particularidades que durante este curso hemos sufrido por la Covid19 han conseguido llevar a buen puerto este Máster.

De forma muy especial a mi familia, Amalia, Ángel y Mario, por acompañarme durante la realización del Master, y por aceptar con agrado mi falta de tiempo para ellos.
.

Metodología de gobierno, dirección y gestión TIC para la transformación digital en el Ministerio de Defensa de España: Guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS)

Autor: Alonso Pradillo, José Luis (jlpradillo@oc.mde.es)
Director/es: Ares Tarrío, Miguel Ángel (externo.miguelares@cud.uvigo.es)
y Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – Con el título Metodología de gobierno, dirección y gestión CIS/TIC para la transformación digital en el Ministerio de Defensa de España: Guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS). Este trabajo se sitúa en el ámbito del proceso de transformación digital de las organizaciones; el gobierno, dirección y gestión de los servicios CIS/TIC; la gestión por procesos; la gestión de los datos, de la información y del conocimiento; y la gestión del cambio para cerrar la brecha existente entre negocio y tecnología con un enfoque ágil que permita a equipos multidisciplinares desarrollar e implementar aplicaciones de forma rápida, segura y de calidad en un marco global e integral de arquitectura empresarial y gobierno corporativo.

El objetivo principal de este proyecto es realizar una metodología para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS) en el marco de la transformación digital del Ministerio de Defensa de España.

Para ello, y como guía de esta investigación se propone un modelo multidimensional en estrella basado en las cinco dimensiones de la transformación digital del Ministerio de Defensa: organización y personas, procesos de negocio, productos de información, servicios CIS/TIC y seguridad de la información.

El autor, tras realizar una revisión sistemática de la literatura que contextualiza el tema, recorre las dimensiones de este modelo en estrella para conformar el marco teórico y el estado del arte. Asimismo, durante este recorrido recoge a modo de resumen las ideas y aprendizaje adquirido para construir una guía metodológica práctica que sintetiza e integra todo este conocimiento.

Esta guía metodológica puede servir de referencia a organizaciones públicas o privadas para abordar el proceso de transformación digital.

Palabras clave – COBIT, BPM, datos, información y conocimiento, metodología ágil, SOA, transformación digital, arquitectura empresarial.

1. Introducción

El desarrollo de una metodología de gobierno, dirección y gestión CIS/TIC es una herramienta fundamental para abordar con éxito el proceso de transformación digital en el Ministerio de Defensa.

Este proceso se apoya en tres pilares fundamentales: los procesos de negocio, los productos de información y los servicios CIS/TIC, que junto a la organización y las personas y a la seguridad de la información conforman las cinco dimensiones en las que la segunda parte del Plan de acción del Ministerio de Defensa para la transformación digital (PATD-2) [1] agrupa y estructura sus actuaciones, encaminadas a cerrar la brecha actualmente existente entre negocio y tecnología.

Hoy nadie duda de la necesidad de implementar este proceso de transformación digital en sus organizaciones para ser más competitivos o incluso subsistir en un mundo incierto, cambiante y turbulento en el que nos ha tocado vivir, y donde la gestión del cambio y la tecnología están siendo uno de los factores más decisivos y fundamentales para alcanzar el éxito en este proceso que requiere un cambio cultural en las personas y en las organizaciones, no solamente en la tecnología.

En este sentido, el autor ha encontrado una excelente oportunidad para sumar sinergias desde el ámbito formativo y profesional para abordar este proyecto de investigación enfocado a crear una guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS) desde una perspectiva orientada a procesos que combina y compila las ideas más importantes del aprendizaje adquirido tras analizar la información relevante recopilada en el estado del arte.

Por todo ello, el proyecto lleva por título: Metodología de gobierno, dirección y gestión CIS/TIC para la transformación digital en el Ministerio de Defensa de España: Guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS). Se espera que este proyecto sea de utilidad para abordar con éxito el proceso de transformación digital del Ministerio de Defensa, además de poder servir de referencia a organizaciones y empresas tanto públicas como privadas.

2. Desarrollo y resultados

Tomando como base los estándares, mejores prácticas y marcos de referencia y usando COBIT® 2019 [2] como *marco paraguas* este pro yecto busca una metodología para el gobierno, dirección y gestión CIS/TIC sobre una estructura y distribución de responsabilidades que permita tomar decisiones y cierre la brecha actualmente existente entre negocio y TI para lograr los objetivos estratégicos marcados por el MDEF y monitorizar su control y seguimiento para facilitar la toma de decisiones.

Tras la contextualización del tema y del enfoque del proyecto dentro del ámbito normativo, académico y profesional en el momento actual

Tras la contextualización del tema y del enfoque del proyecto dentro del ámbito normativo, académico y profesional en el momento actual y partiendo del PATD-2 [1] del MDEF, se realiza un recorrido guiado utilizando el modelo METRO elaborado para analizar y recoger en una tabla resumen las ideas, lecciones aprendidas y buenas prácticas más significativas fruto de los estándares, marcos de referencia y revisión sistemática de la literatura, de los fundamentos teóricos y prácticos adquiridos en el máster DIRETIC y de la experiencia laboral y profesional del autor para elaborar una guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS) objetivo principal de este trabajo.

La guía práctica propuesta en el punto 3 de la memoria, identifica y orquesta los procesos, actividades, tareas, eventos, datos, metadatos, productos de información, servicios, roles, técnicas y herramientas necesarios para abordar de una forma ágil, rápida y flexible la gestión del cambio en el proceso de transformación digital del departamento. Alineada con los principios y directrices generales de la política CIS/TIC del Ministerio de Defensa (política CIS/TIC) [3] y apoyada en el marco técnico de referencia de una arquitectura empresarial o arquitectura global CIS/TIC del Ministerio de Defensa (AG CIS/TIC) [4] permite que equipos de trabajo multidisciplinares, formados por personal de negocio y tecnología, satisfagan las necesidades de los usuarios finales a través del desarrollo de aplicaciones basadas en procesos como servicio (BPMaaS), en el menor tiempo posible y sin renunciar a la seguridad ni a la calidad. Este nuevo paradigma de desarrollo de software es el motor principal del Plan de acción del Ministerio de Defensa para la transformación digital (PATD) y de este proyecto, permite trasvasar el conocimiento tácito en poder de las personas a conocimiento explícito para la organización a través del modelado y automatización de los flujos de trabajo que implementan la lógica de negocio.

Para facilitar el seguimiento y control de los objetivos específicos y conseguir el objetivo general de desarrollar una metodología completa y coherente con el PATD del MDEF, en este trabajo se crea un modelo multidimensional en estrella compuesto por la dimensión tiempo más las cinco dimensiones en las que el PATD-2 agrupa sus actuaciones: organización y personas, procesos de negocio, productos de información, seguridad de la información y servicios CIS/TIC. Esta dimensión tiempo recoge el instante en el que se registra un hecho o evento en el modelo y facilita el análisis de datos sobre la línea del tiempo.

La figura 1 representa el modelo multidimensional en estrella para la transformación digital de la organización (modelo METRO) que con una visión holística guía el método de trabajo para el desarrollo de la metodología de gobierno, dirección y gestión CIS/TIC aplicada al desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS), objetivo general de este proyecto.

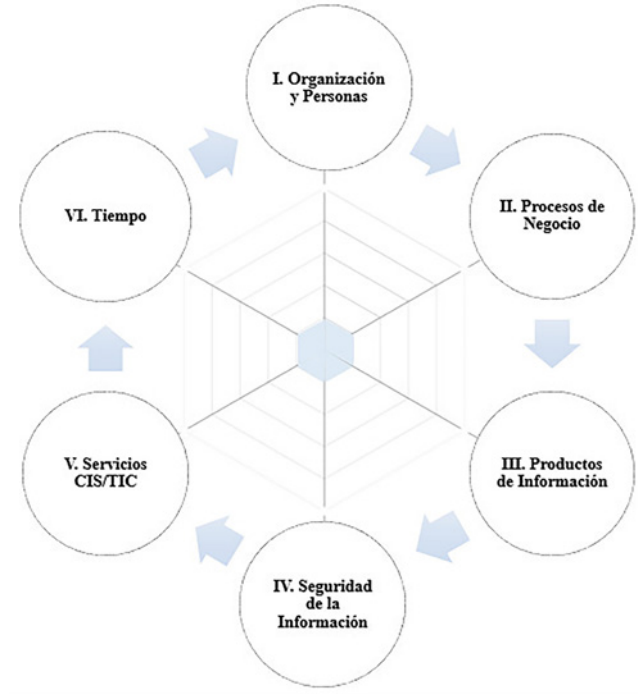


Figura 1. Modelo METRO

Desde esta visión multidimensional, el modelo METRO permite registrar en tablas resumen todos los hechos y eventos relacionados con la dinámica de aprendizaje y buenas prácticas de utilidad para la metodología propuesta. Asimismo, permite abstraer la complejidad técnica y unifica en un único punto de vista distintos enfoques de otros modelos empleados en el marco de la arquitectura empresarial sin perder la trazabilidad hacia ellos, por lo que es una buena herramienta para comunicar, controlar y seguir el grado de avance del proceso de transformación digital del Ministerio de Defensa (MDEF).

El proyecto analiza diversos temas de interés relacionados con el proceso de transformación digital que deben abordar las organizaciones y empresas tanto públicas como privadas y que afectan a la sociedad en su conjunto. Conceptos como arquitectura empresarial (AE), gobierno CIS/TIC, liderazgo, gestión por procesos de negocio (BPM, por sus siglas en inglés de *Business Process Management*), gestión de los datos, la información y el conocimiento (GIC), gestión de los servicios CIS/TIC, gestión de la seguridad de la información (SEGINFO), gestión de proyectos en el ámbito CIS/TIC, entre otros.

Asimismo, destaca la importancia que tienen en este nuevo paradigma de desarrollo de software basado en procesos como servicio los conceptos de interoperabilidad y de arquitectura orientada a servicios (SOA por sus siglas en inglés), ya que junto con la gestión por procesos (GpP o BPM

por sus siglas en inglés) forman un tándem perfecto para integrar los sistemas de información y aplicaciones legados actualmente existentes en las organizaciones, silos de información aún en producción y de cuyas funcionalidades no se puede prescindir a corto plazo.

Además, en el ámbito de la administración electrónica la Ley 39/2015, del Procedimiento Administrativo Común (LPAC) [5] y la Ley 40/2015, de Régimen Jurídico del Sector Público (LRJSP) [6] exigen a la Administración General del Estado (AGE) implementar una correcta gestión de documentos electrónicos. Por ello, el Ministerio de Defensa ha elaborado su política de gestión de documentos electrónicos (PGDE-MDEF) [7] y su esquema de metadatos para la gestión del documento electrónico (eEMGDE-MDEF) [8], herramienta fundamental para implementar una eficaz gestión de los activos de información a lo largo de todo el ciclo de vida.

Para el ciclo de vida de la información, incluido en la dimensión III del modelo METRO, la metodología usa de referencia las 11 guías de aplicación para la implantación de la política de gestión de documentos electrónicos de la AGE [9] y las buenas prácticas en la gestión de datos de DAMA DMBOK versión 2 [10], teniendo en cuenta sus orientaciones y requisitos básicos para integrarlos en la guía práctica para el desarrollo ágil de las aplicaciones basadas en procesos como servicio (BPMaaS, por su siglas en inglés) objeto de este proyecto.

El planteamiento de este proyecto nace de la necesidad de abordar la actuación II.1 del PATD-2 [1]: «Definir una metodología para la identificación, modelado, mejora y optimización de los procesos». Se fundamenta en los estándares, buenas prácticas, normas y trabajos de investigación similares existentes en el estado del arte; en las competencias adquiridas durante la realización del máster universitario en Dirección TIC para la Defensa por la Universidad de Vigo (máster DIRETIC) [11] y en la experiencia profesional y laboral del autor en relación con este tema durante los últimos cinco años.

Por último, se repasan los trabajos realizados y los resultados obtenidos del estado del arte para validar y probar que tanto el objetivo general como los objetivos específicos se han alcanzado.

3. Conclusiones

A modo de conclusión, se puede afirmar que se ha alcanzado el objetivo general de este proyecto cuyo producto se recoge en el punto 3 de la memoria, en concreto una guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS) en el marco de la transformación digital del Ministerio de Defensa.

Esta guía práctica permitirá una gestión de la información y de la tecnología relacionada (I&T) más eficaz y eficiente en las organizaciones para abordar la gestión del cambio desde un punto de vista de gobierno corporativo, sin

distinguir entre negocio y TI. Información y tecnología relacionada (I&T) que permita a las organizaciones centrarse en el conocimiento y ofrecer a través de los datos y la información el combustible necesario para que en un futuro agentes inteligentes infieran conocimiento sin necesidad de intervención humana.

Como líneas futuras a este trabajo de fin de máster, se propone utilizar la guía práctica propuesta en la memoria para desarrollar las aplicaciones BPMaaS de los procesos internos del CESTIC como proveedor de servicios único del MDEF, de forma progresiva y conforme a los procesos relacionados con las dimensiones de servicios CIS/TIC y seguridad del modelo METRO según procesos definidos en COBIT® 2019 [12].

Agradecimientos

A D. Miguel Ángel Ares Tarrío por su inestimable orientación y apoyo.

A Miriam y a Raúl, que junto al autor lideraron el grupo de trabajo encargado de elaborar la segunda parte del Plan de acción del Ministerio de Defensa para la transformación digital (PATD-2), pilares fundamentales de la transformación digital del departamento como son los procesos, los productos de información y los servicios.

A mi esposa Lola y a mi hijo José Luis por su complicidad y paciencia.

A mis padres por su esfuerzo, apoyo y generosidad en labrar un camino que hoy es mi vida.

A la Armada española a la que tanto debo.

Referencias

[1] Ministerio de Defensa de España, (2020). Instrucción 14/2020, de 15 de abril, del Secretario de Estado de Defensa, por la que se aprueba la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital. Instrucción.

[2] ISACA, (2018) Marco de referencia COBIT® 2019: Introducción y metodología.

[3] Ministerio de Defensa de España, (2015). Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. Orden DEF, pp. 116486–116499.

[4] Ministerio de Defensa de España, (2016). Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa. Instrucción.

[5] Jefatura del Estado, (2015) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común. Ley, pp. 1–72.

[6] Jefatura del Estado, (2015) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Ley, pp. 1–115.

[7] Ministerio de Defensa de España, (2017). Orden Ministerial 5/2017, de 9 de febrero, por la que se aprueba la Política de gestión de documentos electrónicos del Ministerio de Defensa. Orden Ministerial, pp. 1–181.

[8] Ministerio de Defensa de España, (2018). Resolución 420/17058/2018, de 7 de noviembre, de la Secretaría General

Técnica, por la que se da publicidad al Esquema de Metadatos para la Gestión del Documento Electrónico en el ámbito del Ministerio de Defensa. Resolución, pp. 1–213.

[9] Ministerio de Hacienda, (2015). «Guías de aplicación de la política de gestión de documentos electrónicos», [Online]. Disponible: https://www.hacienda.gob.es/Documentacion/Publico/SGT/POLITICA DE GESTION DE DOCUMENTOS MINHAP/GUIAS_PGDE.pdf.

[10] DAMA International Technics, (2017). DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition, Second Edi. Technics Publications.

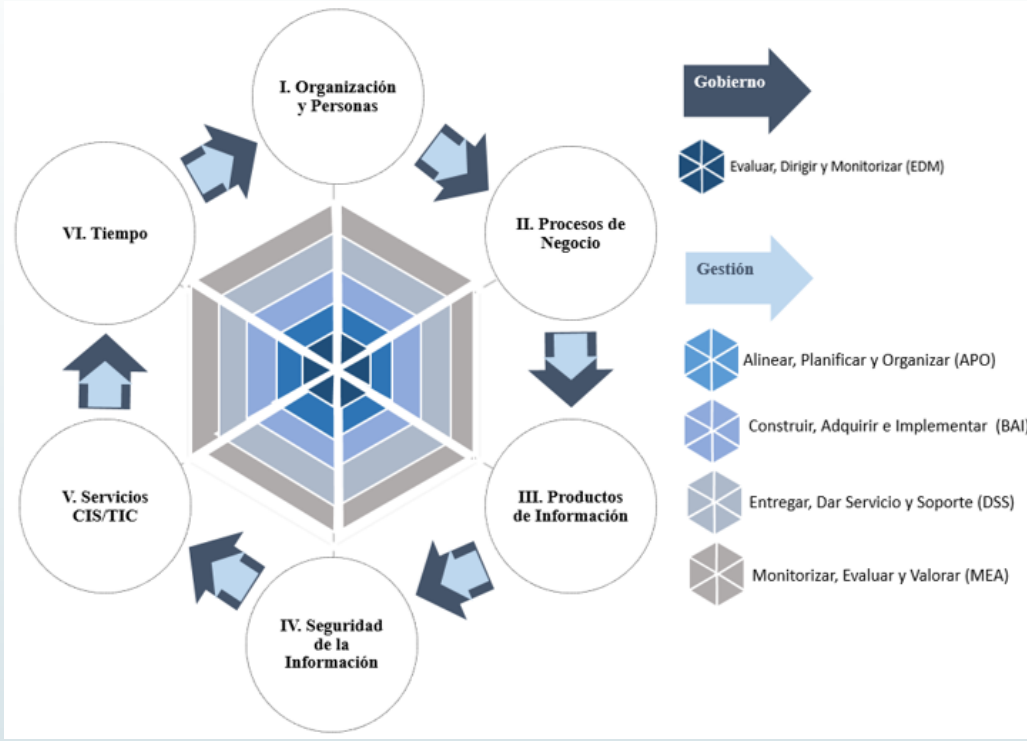
[11] Centro Universitario de la Defensa en la Escuela Naval Militar de Marín, (2019). «Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC)». https://cud.uvigo.es/index.php?option=com_content&view=article&id=2613&Itemid=322 [Último acceso: 16 de agosto de 2020).

[12] ISACA, (2018). Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión.

Universidad de Vigo

Metodología de gobierno, dirección y gestión TIC para la transformación digital en el Ministerio de Defensa de España: Guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS)

Autor: José Luis Alonso Pradillo
Directores: Miguel Ángel Ares Tarrío y Francisco Javier Rodríguez Rodríguez



El autor crea a modo de "rosa de los vientos" un modelo multidimensional para recorrer a lo largo del proyecto las dimensiones del Plan de Acción del Ministerio de Defensa para la Transformación Digital (PATD). Tras recoger a modo de resumen las ideas y aprendizaje adquirido, termina construyendo **una guía práctica para el desarrollo ágil de aplicaciones basadas en procesos como servicio (BPMaaS)** que sintetiza e integra todo este conocimiento.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2020/2021

Estudio de datos poblacionales de Galicia

Autor: Cuesta Calvo, Roberto (rcuesta@guardiacivil.es)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – Se ha pretendido establecer un estudio sobre la posibilidad de encontrar determinadas *características* cuantitativas, objetivas y medibles que pueden predecir, en cierta manera, el comportamiento de una *población* desde el punto de vista de la transgresión de leyes.

Dichas *características* se han intentado provisionar, a partir de información tanto de entidades y organismos públicos como de información privada y reservada correspondiente con otros entes u organizaciones, con el objeto de analizar el grado de relación existente respecto del hecho final que se quiere medir.

El estudio se ha limitado a la comunidad autónoma de Galicia con el objeto de analizar si esas características pueden adivinar patrones conductuales desde el punto de vista de conjunto, *población*, en cuanto a la trasgresión administrativa desde dos puntos de vista totalmente diferentes:

En el primero, intentando predecir todo aquello que esté relacionado con la violencia de género y en el segundo con todas aquellas infracciones que no tengan este carácter.

Palabras clave: Población, Galicia, violencia de género, no violencia de género, predecir.

1. Introducción

1.1. Objetivo

Establecer unos cimientos fuertes y suficientemente genéricos para poder recopilar información de distintos tipos y fuentes adoptando la misma en un futuro cercano por la correspondiente *organización*.

Esta recopilación de información, la mayor posible, servirá como base para la realización de un estudio poblacional por municipio, centrado en la comunidad autónoma de Galicia. Con este estudio se pretende poder establecer el pertinente conocimiento de cada municipio para poder tomar decisiones futuras en base a ello.

Este estudio finalmente intenta prever, en base al conocimiento de la *población*, variables o características, la transgresión de leyes que se va a realizar desde dos puntos de vista, *clase*, como son los siguientes:

- Infracciones cometidas que tengan relación con la violencia de género (VG).
- Infracciones cometidas que no guarden relación con la violencia de género (nVG).

1.2. Características o variables poblacionales.

Esta información ha sido obtenida tanto de fuentes públicas [1][2][3] (online, mediante *crawlers* generados, y *off line*) como de fuentes privadas.

El estudio de los datos está basado en el año 2016.

1.3. Medios.

Tanto la recolección de datos, como el proceso de tratamiento y estudio de los datos, mediante el lanzamiento de experimentos ha sido realizado con tecnología *Phyton* en diferentes cuadernos *Jupyter Notebook*.

No existen más requerimientos software ni hardware puesto que el proceso es lanzado en un portátil de gama media.

2. Desarrollo.

Así pues, se va a intentar predecir las clases definidas (normal y normalizada) mediante la generación de experimentos que se ejecutarán bajo una regresión lineal, Lasso [6][7], y se analizará su conveniencia en función del porcentaje de ajuste que tenga el conjunto de datos escogido frente a los datos esperados, haciéndose esto mediante el método r2_score [11].

2.1. Ejecución del proceso.

La imagen de la figura 1 muestra el proceso de generación del estudio seguido de una manera más visual. No obstante, a continuación, se detallan las fases del mismo.

El hilo o proceso principal está guardado en el cuaderno fMain, desde donde se referencian todas las librerías necesarias para su ejecución, así como las distintas clases (.py) y demás cuadernos necesarios, para realizar las distintas tareas:

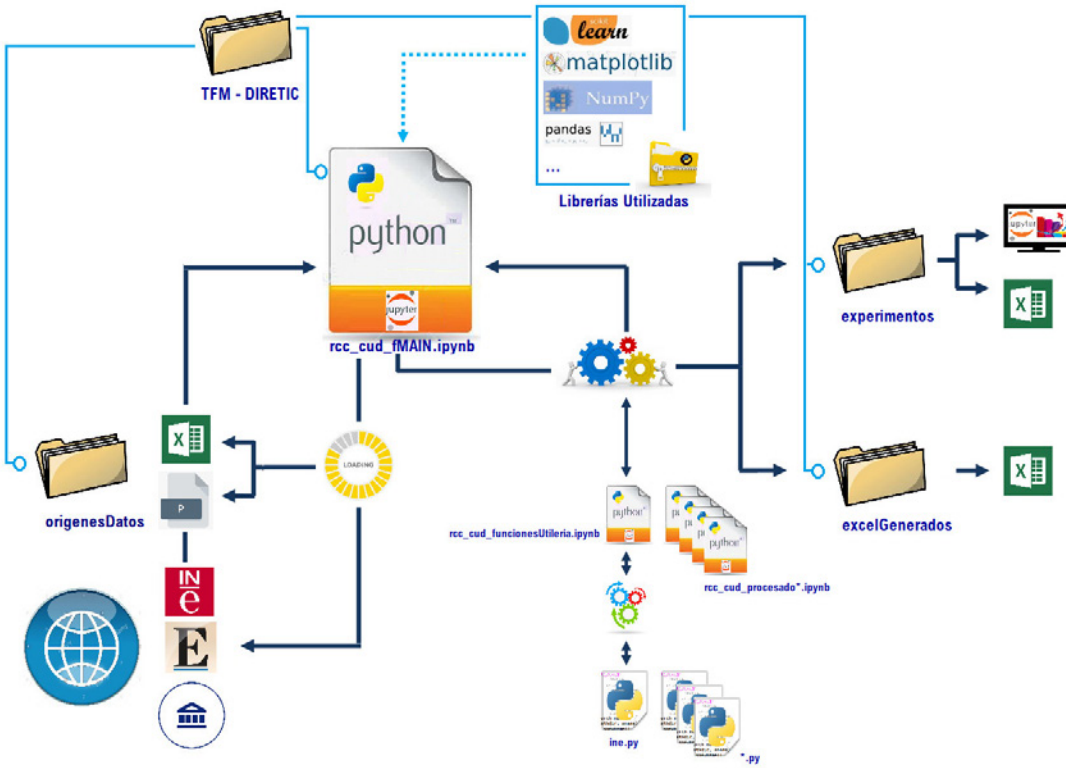


Figura 1. Ejecución proceso TFM – Estudio de datos poblacionales de Galicia

1) Recolección datos: En esta parte del proceso se recolecta todos los datos existentes de las distintas fuentes, tanto los previamente descargados como los que se hacen de manera online. Se trae información relativa a:

   a) Datos estadísticos de la población.

   b) Deuda del municipio.

   c) Información relativa al número de empresas.

   d) Número de contratos establecidos.

   e) Referencia a la actividad de la población por sectores.

f) Números relativos al paro.

g) Turismo.

h) Información relativa a las armas y licencias.

2) Tratamiento de la información: Una vez descargados se hacen distintas tareas de tratamiento de datos para poderlos convertir en información que sea fácilmente integrada dentro del estudio.

a) Generación del código INE para la posterior fusión.

b) Obtención de datos cuantificables objetivos en mismas unidades.

c) Normalización, refiriendo este concepto a referir la variable medida en relación a la cantidad de población total del municipio.

3) Generación de los experimentos: Con la información dispuesta (variables y clase) se van conformando los distintos experimentos que van surgiendo de distintas combinaciones posibles entre las variables existentes a la vez que se va midiendo el resultado de cada una de las predicciones lo que va determinando que conjuntos de valores son por los que se va apostando en las combinaciones. Se realizan un total de 75 experimentos por clase.

4) Visualización de los vesultados: Posteriormente se pasa a la realización de un análisis.

3. Resultados y discusión

Inicialmente se llega a un Accuracy máximo para VG de 0,322759 y para nVG de 0,427409987.

Se procede a analizar los datos obtenidos. Tal y como se muestra en la figura 2, existen valores que están bastante desproporcionados.

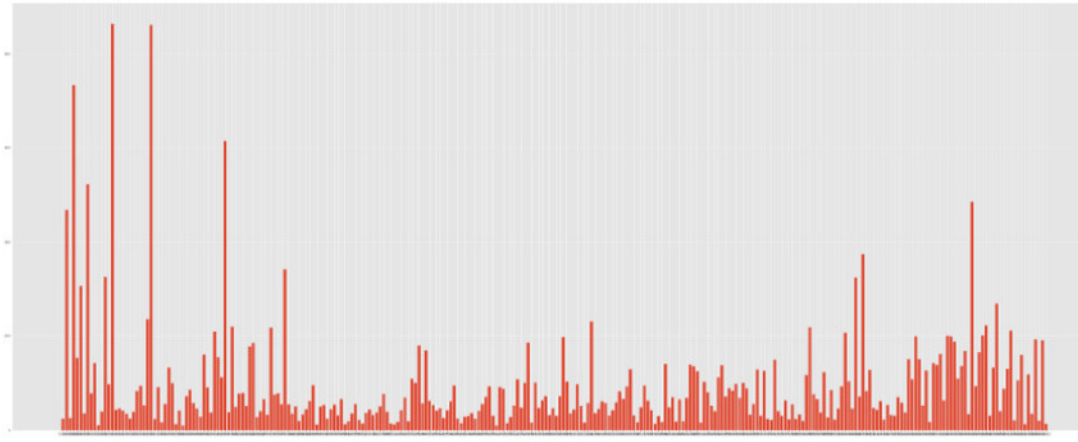


Figura 2. Gráfica de resultados pertenecientes a la diferencia entre el valor real y el predicho

Tras analizar estos datos se llega a la conclusión de que algunos desfases se producen en municipios donde existe otra Fuerza y Cuerpo de Seguridad del Estado de la que no se poseen datos y los mismos no son los totales. Así pues, se realizó una nueva generación de experimentos filtrando estos municipios. Los resultados obtenidos tras este experimento se muestran en la tabla 1.

N.º	Características	Clase	Observaciones	Accuracy
63	df_INE_2,df_Armas,df_numeroEstablecimientos	VG	% Armas	0,321656
101	df_experimento_63	VG	df_experimento_101	0,321656
201	df_experimento_101	VG	experimento_201	0,371829
63	df_INE_2,df_Armas,df_numeroEstablecimientos	NVG	% Armas	0,42741
101	df_experimento_63	NVG	df_experimento_101	0,42741
201	df_experimento_101	NVG	experimento_201	0,439763

Tabla 1. Resultados experimento filtrado FFCCSE

Se sigue analizando los datos que tienen menos relación y se observa que esto tiene que ver con los municipios que poseen Policías Locales. Se analiza y se afina al hecho de que existe una relación con las que poseen en plantilla más de 15 vacantes. Así pues, se procede a su filtrado y se vuelve a generar un nuevo experimento que cuyos resultados se pueden apreciar en la tabla 2.

N.º	Características	Clase	Observaciones	Accuracy
202	df_experimento_201	VG	experimento_202	0,382096
202	df_experimento_201	NVG	experimento_202	0,504904

Tabla 2. Resultados experimento filtrado Policía Local

4. Conclusiones

A continuación, en la tabla 3 se van a mostrar los experimentos que mejor puntuación han obtenido prediciendo las distintas clases.

N.º	Características	Clase	Observaciones	Accuracy
202	df_experimento_201	VG	experimento_202	0,382096
201	df_experimento_101	VG	experimento_201	0,371829
21	df_INE_2,df_Armas	VG	Suma de todas las Armas	0,322759
22	df_INE_2,df_Armas	VG	Solo con Suma de todas las Armas	0,322759
51	df_INE_2,df_Armas,df_Licencias	VG	suma Armas y % Licencias	0,322759
202	df_experimento_201	NVG	experimento_202	0,504904
201	df_experimento_101	NVG	experimento_201	0,439763
16	df_INE_2,df_numeroHoteles	NVG	Ninguna	0,42741
63	df_INE_2,df_Armas,df_numeroEstablecimientos	NVG	% Armas	0,42741
102	df_experimento_16	NVG	df_experimento_16	0,42741

Tabla 3. Resultados con mejor Accuracy

Se podría afirmar, dentro del prisma del estudio actual, y a tenor de los resultados obtenidos que:

1) Se puede observar que los mejores resultados obtenidos se producen cuando van asociados a los conjuntos de datos relacionados tanto del turismo como los relativos a la posesión de armas y/o licencias.

2) Incluso se puede contribuir, tras el estudio realizado dentro del mismo, a intentar romper con sesgos tradicionales de la población o estereotipos puesto que:

   a) Se ha observado que, aunque los porcentajes de población extranjera en Galicia, no son importantes, no existe una relación que determine la clase.

   b) Además se ha comprobado que el número de infracciones no se relaciona con las variables económicas.

Referencias

[1] «Web del Instituto Nacional de Estadística, INE» [En línea]. Disponible: http://www.ine.es. [Último acceso: 19 enero 2021].

[2] «Datos económicos de Expansión.com» [En línea]. Disponible: https://datosmacro.expansion.com/paro/espana/municipios/... [Último acceso: 21 enero 2021].

[3] «Datos de deuda» [En línea]. Disponible: https://www.hacienda.gob.es/. [Último acceso: 21 enero 2021].

[4] «Informe Telefónica sobre IA» [En línea]. Disponible: https://empresas.blogthinkbig.com/matematicas-del-machine-learning/. [Último acceso: 21 enero 2021].

[5] «PirámidedeInformación» [En línea]. Disponible: https://soulimproveledge.com/piramide-del-conocimiento/#:~:text=B%C3%A1sicamente%2C%20la%20Pir%C3%A1mide%20del%20Conocimiento,alta%2C%20o%20de%20m%C3%A1s%20valor.&text=Un%20concepto%20algo%20m%C3%A1s%20dif%C3%ADcil,grado%20m%C3%A1s%20elevado%20del%20conocimiento%E2%80%9D. [Último acceso: 21 enero 2021].

[6] «Método Lasso» [En línea]. Disponible: https://www.cienciadedatos.net/documentos/31_seleccion_de_predictores_subset_selection_ridge_lasso_dimension_reduction. [Último acceso: 21 enero 2021].

[7] «Método Lasso» [En línea]. Disponible: https://es.wikipedia.org/wiki/LASSO_(estadística). [Último acceso: 19 enero 2021].

[8] «Dudas Python y su implementación» [En línea]. Disponible: https://es.stackoverflow.com/. [Último acceso: 21 enero 2021].

[9] «Documentación y dudas sobre Pandas y su implementación» [En línea]. Disponible: https://pandas.pydata.org. [Último acceso: 21 enero 2021].

[10] «Documentación y dudas Numpy y su implementación» [En línea]. Disponible: https://numpy.org/. [Último acceso: 21 enero 2021].

[11] «Librería y dudas sobre Modulo de IA y su implementación» [En línea]. Disponible: https://scikit-learn.org/stable/. [Último acceso: 21 enero 2021].

[12] «Informe Gartner» [En línea]. Disponible: https://www.gartner.com/en. [Último acceso: 21 enero 2021].

[13] «Jupyter Notebook» [En línea]. Disponible: https://jupyter.org/. [Último acceso: 21 enero 2021].

[14] «Python» [En línea]. Disponible: https://www.python.org/. [Último acceso: 21 enero 2021].

[15] «Cross Val Predict» [En línea]. Disponible: https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.cross_val_predict.html. [Último acceso: 21 enero 2021].

Estudio de Datos Poblacionales de Galicia

Autor: Roberto Cuesta Calvo
Director: Miguel Rodero Lacruz
Universidade Vigo

Introducción

Establecer unos cimientos fuertes y suficientemente genéricos para poder recopilar información de distintos tipos y fuentes adoptando la misma en un futuro cercano por la correspondiente Organización.
Esta recopilación de información, la mayor posible, servirá como base para la realización de un estudio poblacional por municipio, centrado en la Comunidad Autónoma de Galicia. Con este estudio se pretende poder establecer el pertinente conocimiento de cada municipio para poder tomar decisiones futuras en base a ello. Este estudio finalmente intenta prever, en base al conocimiento de la Población, variables o características, la transgresión de leyes que se va a realizar desde dos puntos de vista, Clase, como son los siguientes:
•Infracciones cometidas que tengan relación con la violencia de género (VG).
•Infracciones cometidas que no guarden relación con la violencia de género (nVG).

Metodología

El hilo o proceso principal está guardado en el cuaderno de Jupyter fMain, desde donde se referencian todas las librerías necesarias para su ejecución (Python) así como las distintas clases (.py) y demás cuadernos necesarios, para realizar las distintas tareas:

1. *Recolección datos*: En esta parte del proceso se recolecta todos los datos existentes de las distintas fuentes, tanto los previamente descargados como los que se hacen de manera online. Se trae información relativa Datos estadísticos de la Población, Deuda del Municipio, Información relativa al número de empresas, Número de contratos establecidos, Referencia a la Actividad de la Población por sectores, Números relativos al Paro, Turismo, Información relativa a las armas y licencias.
2. *Tratamiento de la Información*:
   a. *Generación del Código INE*
   b. *Obtención ddatos cuantificables objetivos.*
   c. *Normalización.*
3. *Generación de los Experimentos*: Con la información dispuesta (variables y dase) se van confirmando los distintos experimentos que van surgiendo de distintas combinaciones posibles entre las variables existentes a la vez que se va midiendo el resultado de cada una de las predicciones lo que va determinando que conjuntos de valores son por los que se va apostando en las combinaciones. Se realizan un total de 75 experimentos por clase.
4. *Visualización de los Resultados*: Existen 4 clases (VG, nVG, normalizado VG y normalizado nVG) que dan 300 experimentos.

Resultados

Se ha llegado al final a tener un porcentaje de acierto para VG del **0,382096** y para nVG del **0,504904**.

Nº	Características	Clase	Observaciones	Accuracy
202	Población, Armas, Turismo	VG	experimento_202, filtrado_2	0,382096
201	Población, Armas, Turismo	VG	experimento_201, filtrado_1	0,371829
21	Población, Armas	VG	Suma de todas las Armas	0,322759
22	Población, Armas	VG	Solo con Suma de todas las Armas	0,322759
51	Población, Armas, Turismo	VG	suma Armas y % Licencias	0,322759
202	df_experimento_201	NVG	filtrado_2,filtrado_1	0,504904
201	df_experimento_101	NVG	Población, Armas, Turismo	0,439763
16	Población, Turismo	NVG	Ninguna	0,42741
63	Población, Armas, Turismo	NVG	% Armas	0,42741
101	Población, Armas, Turismo	NVG	df_experimento_16	0,42741

Conclusiones

Dentro del prisma del estudio actual, y a tenor de los resultados obtenidos que:
• Los mejores resultados obtenidos se producen cuando van asociados a los conjuntos de datos relacionados tanto con el Turismo como los relativos a la posesión de Armas y/o Licencias.
• Se puede contribuir, tras el estudio realizado dentro del mismo, a intentar romper con sesgos tradicionales de la Población o estereotipos puesto que:
• Se ha observado que aunque los porcentajes de población extranjera en Galicia, no son importantes, no existe una relación que determine la Clase.
Además se ha comprobado que el número de infracciones no se relaciona con las variables económicas.
No existiendo tampoco relación con el tipo de actividad.

DevOps qué es y cómo puede mejorar la gestión de TI en el Ministerio de Defensa

Autor: Escalante Martínez, Francisco (fescal@et.mde.es)
Director/es: Ares Tarrío, Miguel Ángel (externo.miguelares@cud.uvigo.es)
y Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – Las empresas y las organizaciones se desenvuelven hoy en día en unos ambientes caracterizados por su complejidad, con un elevado grado de incertidumbre y sujetos a cambios cada vez más rápidos, intensos y profundos, lo que dificulta el proceso de toma de decisiones y de ejecución y control de acciones. Su capacidad para adaptarse continuamente al entorno y a los requisitos que este exige mediante respuestas rápidas, reconfigurándose y transformándose con flexibilidad en caso necesario, constituye un objetivo estratégico fundamental.

En estas circunstancias la información disponible, interna y externa, así como la posesión de unos mecanismos que aseguren su buena gestión y su transformación en conocimiento útil para la toma de decisiones, se convierten en factores claves para asegurar la supervivencia, el éxito y el progreso constantes de cualquier entidad. Aquí adquieren un papel clave los servicios ofrecidos por las TIC y, en especial, el software específico que soporta los procesos y la gestión de datos de la organización. Por eso las organizaciones, incluyendo a las administraciones públicas en general y al Ministerio de Defensa (MINISDEF) y las Fuerzas Armadas (FAS) en particular, han tomado conciencia de la necesidad de modernizarse acometiendo procesos de transformación digital. El ministerio, en esta transformación, debe ser capaz de dotarse de aplicaciones de una forma ágil y continua.

Para ello el mundo tecnológico actual ofrece la adopción de la cultura DevOps, que preconiza el establecimiento de una mentalidad y el empleo de herramientas y técnicas avanzadas que favorecen el establecimiento de un flujo continuo, rápido y seguro de desarrollo y despliegue de aplicaciones de calidad.

Este trabajo pretende mostrar cuál es la situación actual en el ministerio en el sector del desarrollo y despliegue de aplicaciones y cómo este mejoraría al adoptar DevOps.

Palabras clave: DevOps, cultura, ágil, software, automatización.

1. Introducción

Hoy en día podemos considerar que la información es el recurso clave de cualquier organización. El sistema de información se constituye en el elemento coordinador y director del resto de sistemas. La obtención de datos y su trasformación en conocimiento e inteligencia útil es lo que va a permitir a una entidad sobrevivir, progresar y perdurar en ambientes cada vez más indefinidos y competitivos. Son los sistemas creados para tratar esa información, las aplicaciones informáticas como conjunto de software que se utiliza para tratarla y gestionarla, los que constituyen los elementos que en muchos casos van a determinar el éxito o fracaso de una entidad y de sus actividades. El ser capaz de proveerse de un software útil y de calidad, con capacidad de cambio y adaptación constante a las necesidades y al entorno altamente variable y competitivo en el que las organizaciones se desenvuelven hoy en día, es, por tanto, uno de los objetivos estratégicos fundamentales que, en la actualidad y en el futuro, siempre debería contemplarse.

El MINISDEF y las FAS no pueden ser ajenos a esta premisa que está implícita en el camino de transformación digital que han emprendido. El conjunto del ministerio, tanto para el funcionamiento en su vertiente administrativa, como organización que cuenta con un gran número de personal y de recursos materiales que gestionar, como para su funcionamiento operativo, en la ejecución de misiones militares, debe dotarse de software de calidad de forma ágil y de manera que pueda mantener una alta capacidad de adaptación, asegurándose el éxito en el cumplimiento de sus objetivos.

¿Cómo se proveen las organizaciones de un software adecuado? La tendencia actual es la adopción de paradigmas para el desarrollo de aplicaciones denominados ágiles y de las buenas prácticas definidas por DevOps para su implementación durante el ciclo de vida del software. DevOps es un acrónimo, compuesto por las palabras inglesas *development* y *operations*, que hace referencia a los equipos que intervienen a lo largo del ciclo de vida del software: los de desarrollo, que lo diseñan y producen; y los de operaciones, dedicados a la gestión y mantenimiento de las infraestructuras y plataformas asociadas a las tecnologías de la información y las comunicaciones (TI, TIC o CIS, según la terminología civil o militar empleada). DevOps describe, en esencia, una filosofía que pretende extender las prácticas ágiles, empleadas normalmente solo por los equipos de desarrollo, a todo el ciclo de vida de las aplicaciones y al resto de equipos que intervienen en el proceso de su puesta en explotación, rompiendo las barreras de comunicación existentes tradicionalmente entre *desarrollo* y *operaciones*.

2. Desarrollo

El desarrollo del software se inició de una forma creativa y artesanal, como ha sucedido en muchos campos de la evolución tecnológica, a

mediados del siglo XX. A medida que el uso de los programas informáticos se iba expandiendo y generalizando, a la vez que se consolidaba la cultura científica asociada a su desarrollo, creció también la necesidad de aplicar y repetir las técnicas productivas que mejor funcionaban. Surge así la ingeniería del software con el objetivo fundamental de crear programas que resulten útiles y fiables, con un enfoque sistemático y disciplinado, aplicando los principios básicos de cualquier ingeniería.

En tres décadas la parte más importante del esfuerzo en costes y recursos dedicados a los sistemas informáticos varía desde estar destinado inicialmente al hardware a pasar luego a centrarse en el proceso de desarrollo, hasta que, a finales de siglo, se acaba focalizando en las tareas de mantenimiento. Un determinado software es valorado positivamente por los usuarios si satisface los requisitos establecidos inicialmente, pero lo que realmente marca la diferencia es que el usuario perciba que puede cambiar esos requisitos, no solo durante el desarrollo inicial, sino también durante la fase de explotación. Y que, además, los cambios se producen de una forma rápida y eficaz. De esta forma su sistema de información se convierte en una herramienta ágil y útil en su papel fundamental de orquestador de todos los procesos que se desarrollen en la empresa u organización.

2.1. Desde los paradigmas clásicos de desarrollo de software hasta los paradigmas ágiles

Las fases generales a seguir en la resolución de problemas y, por tanto, la esencia en la práctica de la ingeniería del software para el desarrollo de aplicaciones son entender el problema, planear la solución, ejecutar el plan y examinar la exactitud del resultado [1]. Estas fases determinan y agrupan, en términos generales, un conjunto de tareas y actividades que hay que realizar para obtener el producto final deseado, esto es, una aplicación útil y confiable. No obstante, el flujo de ejecución de este proceso creativo del software puede ser variable. Esta variabilidad es lo que nos determina la existencia de los diferentes modelos de desarrollo o de ciclo de vida del software existentes. Entre los ciclos de vida más utilizados podemos citar, entre otros, el clásico, en «V», prototipado, en espiral y el orientado a objetos.

Desde el inicial ciclo de vida clásico, los diferentes modelos de desarrollo de software han intentado lidiar con una serie de problemas que lastraban a las organizaciones que los utilizaban. Se tenía una confianza excesiva en las especificaciones iniciales y se era poco flexible con las necesidades expresadas por el usuario una vez iniciado el proyecto, lo que provocaba, en muchos casos, insatisfacción con los productos finales. Se tendía a generar productos monolíticos, poco propensos a cambios y actividades de mantenimiento. Los retrasos y la imposibilidad de realizar una estimación de tiempos adecuada se incrementaban con la complejidad de los proyectos.

Se producía un gran volumen de documentación, que consumía mucho tiempo y recursos, sin que se apreciase claramente el beneficio de esta actividad en la obtención de un software útil y de calidad.

En la búsqueda de una solución a todo esto surge el concepto de desarrollo ágil (*Agile* en su denominación en inglés) a principios del siglo XXI. En general, estas metodologías de producción de software pueden considerarse como variaciones del ciclo de vida en espiral en las que se enfatiza la sencillez, rapidez, iteración y agilidad en la creación de aplicaciones. El objetivo es poder entregar código utilizable en intervalos que se miden en unas pocas semanas. Entre estos paradigmas pueden citarse, entre otros, *programación extrema* (XP), *Kanban* y *Scrum*, que es quizás el más extendido hoy en día.

2.2. DevOps

La adopción de metodologías ágiles por los equipos de desarrollo en su búsqueda para satisfacer a los usuarios, crear valor añadido de forma continua y resultar altamente competitivos, lleva a que se incremente de forma considerable la rapidez en la producción de software por parte de estos equipos. Las funcionalidades ofrecidas por las aplicaciones no se ven como algo dogmático e inamovible, sino que pueden y deben modificarse continuamente adaptándose a nuevos requerimientos que, a su vez, son volátiles y limitados en el tiempo. No obstante, su capacidad para responder a las necesidades de los usuarios de modificación y mejora continuas en cortos periodos de tiempo encuentra un significativo cuello de botella en la puesta en explotación. Los equipos de operaciones y otros, como los de aseguramiento de la calidad y los de seguridad, no sienten la necesidad de cambio continuo y rápido en las aplicaciones; por el contrario, su mundo ideal es el de la estabilidad y seguridad que se consigue con largos procesos de comprobación, configuración y puesta en explotación.

Es en este contexto donde, a principios de la segunda década del siglo XXI, nace DevOps. DevOps es mucho más que un paradigma de desarrollo de software y podría definirse como toda una *cultura*, una forma de entender y vivir la producción y entrega del software, que busca la eliminación de barreras y compartimentos estancos, como los que tradicionalmente surgen entre los equipos de desarrollo y operaciones. También se pretende la consecución de un flujo continuo de desarrollo, entrega y despliegue de software que resulte ágil y lo más automatizado posible. Agilidad y automatización que deben estar presentes no solo durante el diseño y entrega inicial sino también durante el ciclo de vida completo hasta la retirada del producto. DevOps tiene una parte cultural, la más importante, y una parte tecnológica, de apoyo a la anterior y más variable en función del estado del arte y de las preferencias y posibilidades económicas y técnicas de la organización.

El paradigma cultural necesita ser apoyado desde los niveles altos de dirección y se define por el uso de metodologías ágiles en el desarrollo y, a ser posible, en el resto de fases asociadas al ciclo de vida del software, por la ruptura de los compartimentos aislados (*silos* en la terminología inglesa), por focalizarse en satisfacer al usuario, por la importancia dada a la realimentación y la monitorización en todo momento, por el impulso a la iniciativa y la pérdida del miedo al error, por la importancia de la formación, y por el intercambio de conocimientos y el trabajo colaborativo.

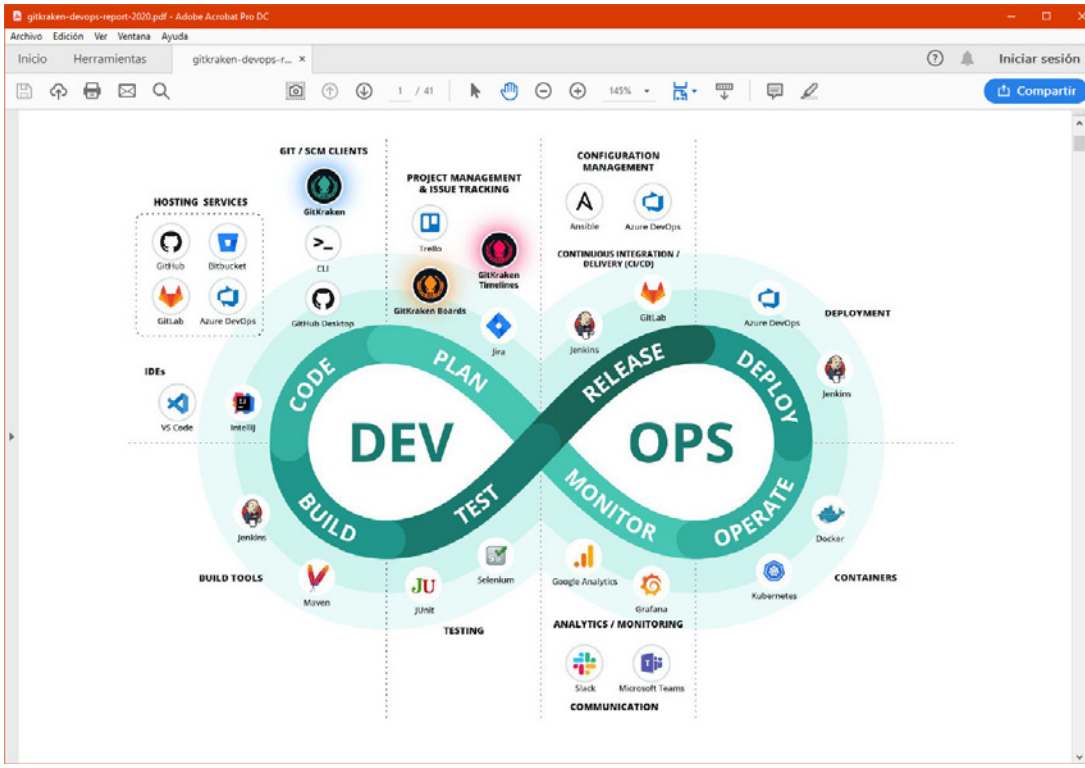


Figura 1. Ciclo DevOps y ejemplo de herramientas utilizadas (tomado de [2])

El uso de herramientas tecnológicas que faciliten la consecución de un ciclo continuo de desarrollo, entrega y mejora viene representado en el ejemplo de la figura 1. La continuidad del ciclo se visualiza componiendo las fases mediante el símbolo matemático de infinito, donde cada fragmento del código de un programa puede encontrarse en diferente fase y donde las fases se suceden hasta el final de la vida del producto. Las herramientas permiten que las tareas realizadas en cada fase se ejecuten de la forma más automática posible, liberando a los equipos de realizar actividades repetitivas y disminuyendo la ratio de errores, posibilitando que las fases se enlacen sin necesidad de intervención humana.

¿Cuáles son los principales problemas para adoptar DevOps? Además del esfuerzo inversor necesario para dotarse del conjunto de herramientas

adecuado para obtener una cadena altamente automatizada de creación y entrega de software, las principales dificultades giran en torno a las personas y los procesos internos. Puede destacarse la falta de unos roles y responsabilidades claramente definidos entre el personal de desarrollo y operaciones que favorezcan la interacción entre ellos y la creación de equipos orientados a conseguir un ciclo de vida de las aplicaciones ágil y seguro. También podemos encontrarnos con una carencia de formación técnica y, sobre todo, de mentalidad, que ayude al desarrollo y entrega ágil de software. En los puestos directivos no suelen apreciarse las ventajas y beneficios que puedan obtenerse al adoptar DevOps, ya que no se tiene una visión clara de qué es ni se realizan análisis de casos de estudio o estudios de prospectiva que orienten en este sentido. La falta del impulso desde arriba, fundamental para el necesario esfuerzo inversor y de cambio organizativo, dificulta su implementación. Y, por último, puede señalarse que el diseño de la propia organización suele resultar complejo y es difícil de cambiar, en caso de que se considere necesario, condicionando asimismo el diseño de los procesos, que en muchas ocasiones no se encuentran suficientemente analizados ni documentados.

En relación a la gestión de servicios TI podemos considerar que un modelo como el de ITIL puede existir en una organización sin implementar la cultura DevOps. Pero también DevOps puede adoptarse en una organización dedicada a la producción de software sin tener por qué considerar a ITIL. En este último caso se perdería la visión holística y las posibilidades de dirección y gobernanza que sobre el conjunto de los servicios TI nos ofrece ITIL. Por tanto, bajo mi punto de vista, puede concluirse que ITIL y DevOps no solo pueden convivir, sino que resulta muy ventajoso que lo hagan, sobre todo en grandes organizaciones como puede ser el MINISDEF donde un amplio conjunto de servicios TI son necesarios. Tan solo hay que considerar que las altas frecuencias de despliegue asociadas a DevOps no deben ser entorpecidas, por lo que los procesos de ITIL relacionados con el cambio, la configuración y la entrega de productos deberían automatizarse y agilizarse al máximo.

3. Resultados y discusión

Tanto la estrategia TIC de la AGE como la propia estrategia y política CIS/TIC del MINISDEF obligan al ministerio a su transformación digital como una necesidad para alinearse con el resto de administraciones en el ámbito funcional y de relaciones con los ciudadanos. Esta transformación también está obligada desde el punto de vista de las operaciones militares, dado el contexto actual en el que estas se desarrollan, para poder obtener y mantener la superioridad sobre el adversario, alcanzar los objetivos que se marquen y enfrentar con éxito cualquier posible amenaza. Esta transformación digital se basa en pasar de una organización sistémica a una organización orientada a procesos funcionales y operativos, centrada

en los datos y en los productos de información, y sostenido todo ello por unos servicios CIS/TIC avanzados y eficaces. El desarrollo de aplicaciones es una de las principales formas de proveerse de estos servicios por lo que cabe concluir que encontrar la mejor forma de hacerlo, adoptando las mejores y más avanzadas costumbres y usos, metodologías y tecnologías que puedan encontrarse en el ámbito de la ingeniería del software es fundamental para que uno de los objetivos estratégicos y pilar de la transformación sea alcanzable y lo más sólido posible.

Vistas las necesidades estratégicas de transformación digital, DevOps sería la cultura ideal a adoptar por el MINISDEF para dotarse del conjunto de prácticas y herramientas necesarias para obtener el modelo de desarrollo de aplicaciones que el ministerio requiere, moderno y eficaz, orientado a satisfacer de forma rápida y flexible las necesidades de los usuarios en la ejecución de procesos y gestión de la información.

3.1. Situación actual. Malas prácticas frente a DevOps

La primera y más evidente es el muro existente entre los equipos de desarrollo y el de operaciones. Prácticamente no existen relaciones. Las aplicaciones son creadas en entornos aislados, *lanzadas* al equipo de operaciones para su puesta en explotación y, de facto, olvidadas por el equipo de desarrollo. Esta situación fue precisamente el origen de DevOps. Además, la organización y dispersión de órganos TI refleja la propia realidad del ministerio como entidad compleja y es un contexto difícil de cambiar, lo que dificulta la implantación de DevOps y favorece la creación de compartimentos estancos.

No se han implantado modelos ágiles y los plazos de desarrollo o de mantenimiento evolutivo se miden en años y semestres. Además, las auditorías de seguridad suponen un cuello de botella significativo que retarda en exceso el despliegue de las aplicaciones. Esta falta de agilidad provoca que los usuarios vean las aplicaciones como recursos inmodificables que en función de cómo evolucionen sus propias necesidades se convierten más en una carga que en una herramienta eficaz de apoyo.

Los productos que se generan, a pesar de utilizar la arquitectura SOA y el diseño en forma de aplicaciones web, tienen los defectos propios de las aplicaciones monolíticas. Hay una confianza excesiva en los requisitos iniciales y hay poca flexibilidad ante cambios o nuevas necesidades expresadas por los usuarios una vez iniciado el proyecto o con el software en producción. El desarrollo de software se concibe como un proyecto, como una tarea que hay que completar generando un buen producto final, pero sin centrar el foco en la creación de valor para el usuario.

Los flujos de información de izquierda a derecha (desarrollo-operaciones-usuarios) se interrumpen y solo fluyen localmente en cada grupo. El

flujo de información de realimentación de derecha a izquierda (usuarios-operaciones-desarrollo) sencillamente no existe. No se tiene información de lo que funciona mejor o peor, no se crea conocimiento que mejore la calidad de los procesos y productos, no se generan nuevos objetivos comunes ni iniciativas de mejora y valor añadido, y no se comparten experiencias, positivas o negativas, ni lecciones aprendidas.

La asignación de recursos de infraestructura TI y su configuración no puede ser la más eficiente y óptima ya que la falta de comunicación entre los equipos de desarrollo y operaciones, así como el uso de procedimientos manuales, lleva al empleo de asignaciones estandarizadas, que solo se modifican en caso necesario ante fallos.

3.2. Situación actual. Buenas prácticas frente a DevOps

Los equipos de desarrollo disponen de herramientas de automatización suficientes y las utilizan de forma adecuada en el entorno de desarrollo. Esto significa que están preparados para implantar un flujo automatizado de CI/CD. Están en proceso de adoptar metodologías ágiles de desarrollo y pretenden adoptar la tecnología de virtualización en contenedores, alineándose en esta última iniciativa al equipo de operaciones.

El personal de operaciones cuenta con un buen bagaje formativo, de experiencias y conocimiento. Los avances tecnológicos que se pretenden adoptar, como servicios en la nube y tecnología de contenedores, coinciden con las iniciativas de los equipos de desarrollo y favorecen la adopción de DevOps al ayudar a la automatización de tareas, la autoprovisión de servicios y al aumento en la modularidad de las aplicaciones.

4. Conclusiones

El MINISDEF está empeñado en su transformación digital, tanto en el ámbito de propósito general, para equipararse al resto de la Administración General del Estado, como en el ámbito operativo, donde se pretenden conseguir unas Fuerzas Armadas ágiles y decisivas, tecnológicamente avanzadas, capaces de obtener la superioridad de la información, acortando sus ciclos de decisión e incrementando el ritmo de sus acciones. El poder disponer de las aplicaciones específicas que en todo momento satisfagan las necesidades de los usuarios, dando el soporte adecuado y automatizando los procesos y la gestión de la información de la organización, es, en mi opinión, uno de los elementos esenciales para alcanzar el éxito en la transformación digital.

El mundo actual surgido con el nuevo siglo está dominado por la tecnología TIC en todos sus ámbitos y se caracteriza por la rápida evolución y transformación en entornos cargados de incertidumbres. En este contexto podemos afirmar, sin riesgo a equivocarnos, que lo que

verdaderamente valoran los clientes y usuarios de las aplicaciones que dan soporte a los procesos de las empresas y organizaciones hoy en día no es que el software específico satisfaga unos requerimientos iniciales, comportándose como un producto COTS, sino que sea una herramienta adaptable, capaz de satisfacer unos requisitos variables y volátiles que deben responder a un entorno cada vez más competitivo, indefinido y cambiante. Es decir, los usuarios demandan que las aplicaciones ofrezcan valor añadido constantemente y que, además, lo hagan de forma ágil y rápida.

La mejor forma de proveerse de la capacidad, que es demandada hoy en día por la transformación digital, de desarrollo y mantenimiento ágil de las aplicaciones es adoptando la cultura DevOps. Las estrategias para adoptar esta cultura son muy variadas, pero, en esencia, conllevan una serie de cambios de mentalidad, que son los más importantes y quizás los más difíciles de acometer, así como la introducción de nuevas tecnologías. En la tabla 1 puede verse una propuesta de prácticas o acciones a emprender en el ámbito del MINISDEF para favorecer esta adopción.

Nivel en la organización	Mejores prácticas para DevOps
A nivel organización	Proceso de gestión del cambio ágil Paradigmas ágiles Arquitectura de muy bajo acoplamiento Legibilidad y mantenibilidad de código
A nivel equipo	Desarrollo concurrente con repositorios (Git) Test automatizados Integración continua (CI) Despliegue automatizado (CD) Infraestructura como código (IaC) Monitorización
A nivel organización y equipos	Cultura centrada en satisfacer al usuario Ruptura de compartimentos aislados Uso de servicios en la nube Uso de virtualización con contenedores Pruebas de recuperación ante desastres Formación e intercambio de conocimientos

Tabla 1. Algunas de las mejores prácticas para adoptar DevOps (tomado de [3] y modificado)

En síntesis, los ejes en los que debe centrarse el ministerio para implantar DevOps son realizar un esfuerzo en el cambio de mentalidad, en la adquisición de herramientas y en el cambio de modelos lógicos, como las metodologías ágiles y las arquitecturas de muy bajo acoplamiento (microservicios), y físicos, como la virtualización con contenedores o la infraestructura como código (IaC).

La ventaja más evidente en la adopción de una cultura DevOps es el de producir valor para el cliente, que en el caso del MINISDEF es la propia organización, de forma ágil y continua. Lo importante no es que se

disponga de buenos productos, sino que se va a poder poner a disposición del usuario de forma rápida el producto que necesita en cada momento. El soporte de los procesos y de la gestión de la información del ministerio se podrá realizar con aplicaciones de calidad que se adaptarán rápidamente a las necesidades que en cada momento requieran los usuarios en un mundo en constante cambio.

Con la automatización y las nuevas tecnologías también se van a emplear de forma más eficiente tanto los recursos humanos especializados en TIC, que verán cómo aumenta su productividad, como los recursos materiales TIC, cuyas capacidades serán mejor aprovechadas y se incrementarán sus niveles de fiabilidad y estabilidad. Con DevOps se consiguen la cooperación, comunicación y compartición de conocimientos y experiencias que hacen posible la mejora continua en el proceso de creación de software y, por extensión, en el conjunto de los procesos de la organización soportados por este software.

Agradecimientos

Al comandante Arroyo de la Jefatura CIS y AT del ET (JCISAT) y al teniente coronel Rodríguez del CESTIC por atenderme, dedicarme parte de su escaso tiempo, y proporcionarme la visión actual de los equipos de desarrollo y la de los equipos de operaciones sobre el ciclo de vida de las aplicaciones creadas en el MINISDEF.

Referencias

[1] R. S. Pressman, (2010). Ingeniería del Software. Un enfoque práctico (7.ª edición), México: McGraw-Hill.

[2] GitKraken, (2020) «DevOps Tools Report 2020». [En línea]. Disponible: https://www.gitkraken.com/resources/devops-report-2020. [Último acceso: 13 diciembre 2020].

[3] N. Forsgren, D. Smith, J. Humble y J. Frazelle, «Accelerate State of DevOps 2019» [En línea]. Disponible: https://services.google.com/fh/files/misc/state-of-devops-2019.pdf. [Último acceso: 9 diciembre 2020].

DevOps qué es y cómo puede mejorar la Gestión de TI en el Ministerio de Defensa

Autor: Francisco Escalante Martínez

Director/es: Miguel Ángel Ares Tarrío y José María Núñez Ortuño

Universidad de Vigo

Introducción

Las empresas y las organizaciones se desenvuelven hoy en día en unos ambientes caracterizados por su complejidad, con un elevado grado de incertidumbre y sujetos a cambios cada vez más rápidos, intensos y profundos, lo que dificulta el proceso de toma de decisiones y de ejecución y control de acciones.

Disponer de la capacidad de proveerse de forma ágil de aplicaciones, pudiendo modificar estas de forma muy dinámica según las necesidades, es esencial para la supervivencia y el éxito.

El MINISDEF y las FAS no pueden ser ajenos a estas circunstancias en su proceso de transformación digital.

Metodología

En este trabajo se sigue el método científico de resolución de problemas.

La hipótesis planteada es que la implantación de DevOps puede mejorar e impulsar la transformación digital del MINISDEF al conseguir que el proceso de producción de software específico se dinamice y responda continuamente a las necesidades reales de los usuarios.

Para comprobar su validez se analizan las tendencias actuales en ingeniería de software relacionadas con el desarrollo de aplicaciones y se estudia cómo se lleva a cabo actualmente este proceso en el ámbito del MINISDEF y cómo podría cambiar con DevOps. Este último análisis se realiza mediante entrevistas con representantes de los principales equipos intervinientes en el desarrollo y explotación de aplicaciones, los de desarrollo y los de operaciones. Finalmente se valida la hipótesis, como resultado de las conclusiones de los análisis, y se proponen una serie de acciones genéricas a ejecutar como estrategia que favorecería la implantación de la cultura DevOps en el MINISDEF.

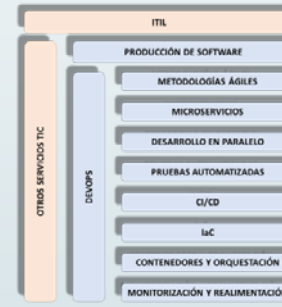
El ciclo de vida DevOps de aplicaciones

Resultados

La transformación digital es una imposición y una necesidad en el ámbito del MINISDEF y de las FAS. Esta transformación implica, entre otras cosas, el reconocimiento de la importancia de los servicios TIC, entre los que el desarrollo de aplicaciones específicas es fundamental.

DevOps es, en esencia, una cultura, una forma de pensar y actuar, con orígenes en las metodologías ágiles, que preconiza la ruptura de compartimentos estancos en las organizaciones para conseguir un ciclo de desarrollo de software continuo, dinámico y adaptado a los usuarios. También implica el uso extensivo de herramientas de automatización. Es la cultura que está siendo adoptada hoy en día por todas las organizaciones de éxito.

El actual proceso de desarrollo de aplicaciones en el MINISDEF resulta paradigmático en relación a las causas y problemas que motivaron el surgimiento de DevOps. No obstante, se aprecian potencialidades de mejora que se alinean con las buenas prácticas preconizadas por esta cultura.



Un modelo de prácticas y tecnologías DevOps

Conclusiones

El MINISDEF, dentro de su proceso de transformación digital y en el ámbito de los servicios TIC, necesita proveerse de los mecanismos que le permitan obtener y explotar aplicaciones específicas con calidad y de forma ágil.

Actualmente no dispone de esta capacidad. Para lograrla debería emprender la adopción de la cultura DevOps, modificando sus hábitos y su concepción del desarrollo de software, y realizando un esfuerzo tecnológico para la automatización del proceso.

La ciberseguridad en las infraestructuras críticas

Autor: Francoso Figueredo, Alberto (aff@interior.es)
Director/es: Vales Alonso, Javier (externo.jvales@cud.uvigo.es)
y Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – Con este trabajo se pretende dar a conocer la importancia de la ciberseguridad en la protección de las infraestructuras críticas españolas, así como el marco normativo que la regula en este ámbito y los nuevos proyectos en los que se está trabajando para la mejora de la misma.

Para ello, se hace un repaso por la normativa más importante que regula esta materia a nivel europeo y nacional y por los estándares internacionales más importantes en seguridad de la información. Además, se realiza un somero estudio sobre la problemática de la aplicación de la normativa sectorial en distintos sectores con marcadas diferencias entre ellos.

Se realiza un estudio del caso de transposición de la 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 (en adelante, Directiva NIS), a la legislación española, mediante la reutilización de estructuras y procedimientos previamente establecidos y en vigor, como es la normativa relacionada con la protección de las infraestructuras críticas o normativa PIC.

En el siguiente apartado se pone en contexto la ciberseguridad con el marco estratégico establecido por la Ley de Seguridad Nacional y se citan y estudian los documentos y actores más importantes recogidos en dicha ley.

Así mismo, se hace un repaso por las agencias estatales de ciberseguridad y cómo se relacionan entre ellas a partir del nuevo marco de actuación definido a raíz de la transposición de la Directiva NIS.

Por último, se analizan los nuevos retos a los que habrá que afrontar a medio y largo plazo, haciendo especial mención a la lucha contra la criminalidad.

Palabras clave: Infraestructura crítica, ciberseguridad, protección, normativa, gobernanza, cibercriminalidad.

1. Introducción

A raíz de una serie de atentados terroristas ocurridos en los primeros años de la década de los 2000, como el atentado contra las Torres Gemelas ocurrido en Nueva York el 11 de septiembre de 2001 o el ocurrido en Madrid el 11 de marzo de 2004, la Unión Europea se ve en la necesidad de proteger las infraestructuras críticas europeas, entendiendo como tales, «Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas».

Con esta finalidad, se publica la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, mediante el establecimiento de un procedimiento de identificación y designación de infraestructuras críticas europeas y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras, con el fin de contribuir a la protección de la población.

El 28 de abril de 2001, se publica en España la Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas (en adelante, Ley PIC), e inmediatamente después, el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (en adelante, Reglamento PIC). Con dicha ley y su reglamento de desarrollo, se establecen los instrumentos de planificación del sistema de protección de infraestructuras críticas y constituyen los elementos esenciales para garantizar la protección de las infraestructuras críticas y, por tanto, los servicios esenciales provistos por estas. En esta normativa, además de la creación del Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC), se contempla la elaboración de unos planes de actuación por parte de los operadores críticos, que conforman el conjunto de medidas de seguridad integral para elevar al máximo nivel de capacidad en la protección de las infraestructuras críticas, comprendiendo tanto aspectos estratégicos como tácticos.

De forma paralela, en el 2010 se publica el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Dicho esquema (en adelante ENS), aunque regula un ámbito distinto, como es el de la Administración Pública, para la que es de obligado cumplimiento, inspirará en materia de ciberseguridad el enfoque futuro de la protección de las infraestructuras críticas, destacando la consideración de sus dimensiones de seguridad, o la división de las medidas de seguridad en tres marcos definidos como son el organizativo, operacional y de protección.

Con la entrada en vigor de la 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 (en adelante, Directiva NIS), cambia radicalmente el panorama de la ciberseguridad, no sólo en España, sino en toda Europa.

Pese a ser una directiva con un marcado carácter económico, tal y como se recoge en su articulado: «La presente Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior», ha establecido obligaciones en ciberseguridad en sectores tradicionalmente híperregulados en esta materia como es el sector financiero, así como en sectores muy regulados en el ámbito físico pero sin regulación específica en el ámbito cibernético, como por ejemplo el subsector del transporte aéreo.

En abril del pasado 2019, se aprobó el 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 que refuerza las funciones de la Agencia de la Unión Europea para la ciberseguridad (ENISA) e intenta poner orden la hora de la certificación de productos, sistemas y procesos de la ciberseguridad, en un panorama caótico donde cada estado miembro posee sus propios esquemas de certificación, o utiliza estándares internacionales.

2. Estado del arte

Se hace un breve repaso por el estado del arte de la ciberseguridad, su regulación e iniciativas.

3. Marco normativo

3.1. Leyes europeas

Se analizan las distintas normas europeas que regulan en esta materia, como la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, la 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 o el 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.

3.2. Leyes españolas

En este apartado se hace un estudio sobre las normas españolas como la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Desarrollo reglamentario pendiente de publicación o el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3.3. Normativa sectorial

Se analizan las peculiaridades de los sectores estratégicos más significativos por su nivel de desarrollo en normativa o por otras cuestiones. En particular se analizan el sector financiero, sector transportes-subsector aéreo, sector industria nuclear y el sector energía-subsector eléctrico.

3.4. Estándares internacionales

Se hace referencia a los estándares internacionales más significativos en ciberseguridad de nuestro entorno como son el ISO/IEC 27001. Sistema de gestión de seguridad de la información, la serie NIST 800 o los *criterios comunes* para la evaluación de la Seguridad de la tecnología de la información (Common Criteria).

4. La convergencia de los servicios esenciales

Se analiza el caso concreto de cómo se ha abordado la transposición de la Directiva NIS en la normativa española.

5. La gobernanza de la ciberseguridad

Se repasa la gobernanza en ciberseguridad española, haciendo mención a la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al Consejo Nacional de Ciberseguridad y a la Estrategia Nacional de Ciberseguridad.

6. Ciberactores principales

Se mencionan los principales actores de la ciberseguridad gubernamentales y sus cometidos, como son el Centro Nacional de Protección de Infraestructuras Críticas, la Oficina de Coordinación de la Ciberseguridad, el Centro Criptológico Nacional, el Instituto Nacional de Ciberseguridad y el Mando Conjunto del Ciberespacio.

7. Conclusiones y líneas futuras de actuación

7.1. Tiempos desacompasados

Los próximos retos en ciberseguridad a los que se tendrán que enfrentar la Unión Europea en su conjunto, y España de manera particular, están caracterizados por un dinamismo y una velocidad que no se ajustan a los tiempos de producción regulatoria para la resolución de los problemas que vayan surgiendo, que son mucho más lentos.

Esto implica que necesariamente la regulación normativa relativa a estos aspectos, necesariamente irá retrasada con la necesidad de solución de los problemas, existiendo una percepción en la ciudadanía de que no se abordan los problemas de manera diligente.

Las autoridades europeas y españolas, habrán de realizar un esfuerzo para dinamizar los trámites legislativos y acortar los tiempos si quieren reaccionar a las cuestiones de la ciberseguridad en unos tiempos razonables.

7.2 La armonización normativa

La producción normativa en ciberseguridad se ha producido de manera desigual en la Unión Europea.

Países como Reino Unido, Alemania o España, abordaron la legislación en esta materia de manera temprana, lo que les ha permitido tener una normativa muy cohesionada en ciberseguridad. Esto ha ocasionado una colisión con las normas europeas que a posteriori se han publicado, por lo que es necesaria la armonización entre las complejas estructuras normativas de estos países y las europeas.

Dentro del propio seno de la Unión, autoridades centrales como la del Banco Central Europeo o ENISA, han ido emitiendo numerosas normas sectoriales a lo largo del tiempo para regular el marco de sus competencias. La necesidad de transversalidad de la ciberseguridad y la uniformidad en todos los países, ha provocado la publicación de normas generalistas como la Directiva NIS, el Reglamento de ciberseguridad europeo, o el Reglamento eIDAS.

En este momento, se están revelando incoherencias con la normativa sectorial que está motivando que se prioricen estas normas específicas sobre las generalistas, lo que está debilitando el carácter uniformador con el que fueron creadas estas últimas. Ejemplo de ello son las diferentes taxonomías de los incidentes de seguridad entre las distintas autoridades. Esta disfunción permite clasificar de manera distinta un mismo incidente, según lo interprete una autoridad u otra, y consecuentemente, se exige un distinto tratamiento a la hora de aplicar procedimientos o de cumplimentar

tiempos de resolución del incidente, todo ello agravado porque, en la mayoría de los casos, su incumplimiento conlleva sanciones económicas.

Los Estados miembros de la Unión que carecían de legislación sobre ciberseguridad en el momento de la publicación de las normas europeas, han tenido mucho más fácil la adecuación a dicha normativa.

7.3. La certificación en ciberseguridad

La existencia en los Estados miembros de la Unión Europea de innumerables certificaciones en ciberseguridad, ya sea de procesos, esquemas o elementos de software o hardware regulados por las autoridades competentes locales, sumados a las certificaciones exigidas por las autoridades de la Unión, más las distintas certificaciones de organismos privados reconocidos internacionalmente, presentan un panorama muy complicado a la hora de obtener certificaciones por parte de los operadores, ya que para operar en determinados sectores, necesitan según sea la autoridad competente, varios certificados en ciberseguridad con el consiguiente gasto, y donde además, se exigen los mismos controles.

El Reglamento de Ciberseguridad Europeo de 2019 ha publicado en un intento de poner orden en esta materia y crear certificaciones únicas en todo el territorio para simplificar el proceso de certificación.

No obstante, el panorama actual es que los operadores disponen de distintas certificaciones en ciberseguridad, que no son reconocidas por las autoridades y que en el ámbito privado tampoco pueden ser aprovechadas debido a que los niveles de certificación no son homogéneos.

Por parte del sector bancario, uno de los más activos en estas cuestiones, se ha creado un grupo de trabajo para la realización de una matriz de correspondencias entre los distintos certificados de su sector, que permita la racionalización en el uso de los certificados en beneficio de los operadores.

Por último, está el problema de la recertificación. Para la obtención de cualquier certificado en ciberseguridad, se han de realizar determinadas acciones para garantizar que el sistema en cuestión es seguro. Ello pasa necesariamente por estudios de laboratorio si son productos, o por auditorías si son procesos o esquemas. Dichas acciones suponen un coste en dinero y en tiempo.

El problema se presenta cuando, debido al dinamismo propio de la ciberseguridad, se han de actualizar versiones, o rediseñar procesos. Estas acciones que son necesarias para el mantenimiento de los sistemas y para garantizar un determinado nivel de seguridad, provoca que las certificaciones dejen de tener validez por la modificación del alcance objeto de la certificación.

La agilización de los procesos de certificación, su menor coste, así como la flexibilización en el reconocimiento de variación de versiones, es la única manera de que se puedan abordar las recertificaciones como una exigencia en ciberseguridad.

7.4. La lucha contra el cibercrimen

El uso de las tecnologías de la información y la comunicación se ha hecho presente como un aspecto más de nuestra vida cotidiana. Cualquier actividad va estrechamente ligada de una forma o de otra a estas tecnologías.

Esta normalidad tecnológica está siendo aprovechada por la delincuencia para cometer hechos delictivos a través de estas mismas tecnologías debido especialmente a los beneficios que les supone comparados con la comisión de los mismos por los métodos tradicionales, como son la dificultad de atribución, el escaso riesgo y los enormes beneficios que se pueden obtener con su comisión.

La globalización de los movimientos terroristas, ha favorecido su presencia en las redes para publicidad de sus actuaciones y sus postulados, además de para el uso de Internet como una herramienta más para atacar sus objetivos.

Nuevos delitos relacionados con las redes, motivados por prácticas de riesgo como el *sexting*, o por actividades delictivas, como por ejemplo el *grooming* o el intercambio de material pedófilo, han sufrido también un importante incremento.

En el estudio de la cibercriminalidad de 2019 publicado por el Ministerio del Interior, se observa como nuestro país ha sufrido un fortísimo incremento de la cibercriminalidad, produciéndose entre los años 2018 a 2019 un incremento del 41 %, y un total, desde que se comenzaron estos registros en el año 2015, de un incremento del 210 %.

El 10 % del total de delitos que se cometen en España son ciberdelitos y la cifra continúa subiendo año tras año.

La Estrategia Nacional de Ciberseguridad considera a la cibercriminalidad como una amenaza a la Seguridad Nacional, estableciendo en la línea de acción tercera la responsabilidad al Estado de «Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio», mediante el reforzamiento del marco jurídico, el fomento de la colaboración y participación ciudadana, potenciando las capacidades de investigación, reforzando la comunicación con los órganos judiciales y fomentando el intercambio de información entre las unidades policiales de inteligencia tanto nacionales como internacionales.

Para dar cumplimiento a esta línea de acción, el Ministerio del Interior está elaborando el Plan Estratégico contra la cibercriminalidad, donde recoge cada una de las acciones de la Estrategia Nacional y las desarrolla en planes de actuación específicos que habrán de ejecutar las Fuerzas y Cuerpos de Seguridad del Estado.

Actualmente existe un encendido debate sobre si la ciberseguridad es la parte preventiva del ciclo de la cibercriminalidad, compuesto por la prevención, la investigación y persecución de los autores y el auxilio a la víctima. El argumento es que, si la ciberseguridad cumple su función de proteger de los ciberataques, no se producirían hechos delictivos.

Por otro lado, están los que opinan que la ciberseguridad es un concepto más amplio que sobrepasa ampliamente el ámbito de la cibercriminalidad.

Una tercera corriente opina que son dos ámbitos diferentes con ciertos elementos comunes como la prevención o los ciberataques y aspectos exclusivos de cada uno de ellos como la investigación de los autores en el ámbito de la cibercriminalidad o las malas praxis en el de la ciberseguridad. En cualquier caso, el debate está servido.

La mejora en la eficacia de lucha contra la criminalidad pasa por la aplicación de determinadas medidas recogidas en el borrador del Plan Estratégico contra la Cibercriminalidad 2020 del Ministerio del Interior, como son:

- Fomentar el conocimiento y la información a los usuarios y público en general para incrementar la prevención y la autoprotección.
- Incrementar las capacidades operativas y de inteligencia de las unidades policiales y las competencias y habilidades de los agentes que las integran.
- Compartir información para generar inteligencia.
- Impulsar la coordinación nacional y la cooperación internacional.
- Promover un marco jurídico eficaz.
- Establecer líneas de colaboración y asociación con la industria, con las universidades y demás actores relevantes en este ámbito.

Agradecimientos

Quiero expresar mi especial agradecimiento a los directores de este trabajo fin de máster: Javier Alonso Vales y Norberto Fernández García por el tiempo que han dedicado a proponer ideas y sugerencias para mejorar este trabajo.

También me gustaría agradecer al director del Centro Nacional de Protección de Infraestructuras Críticas, teniente coronel de la Guardia Civil D. Fernando José Sánchez Gómez y al jefe de la Oficina de Coordinación de Ciberseguridad, comisario del Cuerpo Nacional de Policía D. Juan Carlos López Madera por todo lo que me han enseñado en estos años de trabajo en la Secretaría de Estado de Seguridad del Ministerio del Interior.

Por último, me gustaría agradecer a todos los compañeros del Máster Universitario en Dirección TIC para la Defensa en su edición 2019/2020 por su compañerismo y atención demostrada, y a los profesores del Centro Universitario de la Defensa y de la Universidad de Vigo por su profesionalidad, compromiso y buen hacer en la impartición de las distintas asignaturas.

Referencias

Norma europea	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 en 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 Europea,* n.º. 151, de 7 de junio de 2019, pp. 15-65.
Norma europea	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* L 194/1, 19 de julio de 2016, pp. 1-30.
Norma europea	Directiva (CE) 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de mejorar su protección. *Diario Oficial de la Unión Europea* n.º 345, de 23 de diciembre de 2008, pp. 75-82.

Norma española	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. *Boletín Oficial del Estado*, de 29 de abril de 201, n.º 1092, pp. 71548-71586.
Norma española	Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. *Boletín Oficial del Estado,* de fecha 21 de mayo de 2011, n.º 121, pp. 50808-50826.
Norma española	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica Boletín Oficial del Estado, de 29 de enero de 2010, n.º 25, pp. 8089-8138.
Norma española	Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Boletín Oficial del Estado, de 8 de septiembre de 2018, n.º 218, pp. 87675-87696.
Norma española	Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. *Boletín Oficial del Estado*, de 18 de septiembre de 2015, n.º 224, pp. 82405-82425.
Norma española	Instrucción 3/2015 de la Secretaría de Estado de Seguridad por la que se actualiza el Plan de Prevención y Protección Antiterrorista.
Norma española	Consejo de Seguridad Nacional. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. *Boletín Oficial del Estado,* de 30 de abril de 2019, n.º 103, pp. 43437-43455.
Norma española	CNPIC-CCN-DSN. Guía Nacional de Notificación y Gestión de Ciberincidentes
Norma española	CNPIC. Guía de Buenas Prácticas Plan de Seguridad del Operador, de 8 de septiembre de 2015.
Norma española	CNPIC. Guía de Buenas Prácticas Plan de Protección Específico, de 8 de septiembre de 2015.
Estándar	ISO 27001 Sistema de gestión de seguridad de la información.
Estándar	ISO 27002 Código de prácticas para los controles de seguridad de la información.
Norma EEUU.	NIST SP 800-82 Guía para la Seguridad de los Sistemas de Control Industrial (ICS).

NOMBRE DEL RECURSO	FECHA DE CONSULTA	URL
Departamento de Seguridad Nacional	24/10/2020	https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciber-seguridad-nacional
INCIBE	20/12/2020	https://www.incibe-cert.es/blog/diferencias-ti-to
normaiso27001.es	13/10/2020	https://normaiso27001.es
National Institute of Standars and Technology USA	27/12/2020	https://csrc.nist.gov/publications/sp800

La ciberseguridad en las infraestructuras críticas

Universidad de Vigo
Autor: Alberto Francoso Figueredo
Directores: Javier Vales Alonso y Norberto Fernández García

Introducción

Este trabajo pretende dar a conocer la importancia de la ciberseguridad en la protección de las infraestructuras críticas españolas, su marco normativo y los proyectos actuales.
Además, pone en contexto el marco estratégico de la ciberseguridad y hace un repaso por las agencias estatales de ciberseguridad españolas y cómo se relacionan entre ellas.
Por último analiza los nuevos retos y sus posibles soluciones.

Metodología

La metodología del trabajo, ha sido la siguiente:

- Identificación de las fuentes
- Análisis y síntesis de la información
- Análisis de la interrelación entre normas
- Identificación de otros factores
- Identificación de actores
- Prospectiva de la problemática futura

Resultados

- Tiempos desacompasados
- Armonización normativa
- Certificación en ciberseguridad
- Lucha contra la cibercriminalidad

Conclusiones

- Se necesita más agilidad normativa para evitar vacíos legales
- La UE debe dirigir sus esfuerzos a armonizar la numerosa y dispersa normativa en ciberseguridad
- Se deben establecer equivalencias entre las numerosas certificaciones en tanto se implanta la nueva normativa de certificación europea
- La lucha contra la cibercriminalidad se debe abordar desde distintas perspectivas e implicando a diferentes actores, pero dentro del marco de la ciberseguridad.

Generación y caracterización de secuencias PRN

Autor: Hernández González, Abel (ahdezg@ea.mde.es)
Director: Gómez Pérez, Paula (master.diretic@cud.uvigo.es)

Resumen – En este trabajo se ha llevado a cabo un estudio riguroso y exhaustivo de las secuencias PRN (*Pseudo-Random Noise*), que pretende ofrecer una base para el diseño o el análisis de sistemas de telecomunicación o, incluso, de información.

Las secuencias PRN (*Pseudo-Random Noise*) tienen características asimilables al ruido, cualidad esta que las hace muy atractivas para determinadas aplicaciones civiles y militares.

Dada la variedad de estas secuencias, se ha pretendido cubrir con el estudio un ambicioso rango de secuencias PRN, incluyendo los principales tipos: caóticas, de longitud máxima, de *Kasami* y *Gold*.

Entre las conclusiones más destacadas que se alcanzan, hay que mencionar que todas ellas logran un gran reparto en banda de la potencia, muy deseable en sistemas de espectro ensanchado, que las proporciona propiedades inmunidad frente al ruido y la interferencia.

Salvando lo anterior, se concluye que, de las secuencias analizadas, las que presentan una mejor autocorrelación son las caóticas y las secuencias PN (*Pseudo-Noise*) de longitud máxima, dado que las de *Kasami* y las *Gold* presentan un rizado de la función para desplazamientos mayores de un chip.

Desafortunadamente, las secuencias PN de longitud máxima presentan, salvo grupos muy reducidos, una mala correlación cruzada, que las descarta para aplicaciones de acceso compartido al medio. Por su parte, las secuencias de *Kasami* y de *Gold* consiguen proporcionar grandes familias de secuencias con buenas propiedades de correlación cruzada.

Palabras clave: secuencia, chip, autocorrelación, correlación, potencia, pseudoaleatorio.

1. Introducción

Este trabajo pretende ser un estudio riguroso y exhaustivo de las secuencias PRN (*Pseudo-Random Noise*) que pueda servir de base para el diseño o el análisis de sistemas de telecomunicación o, incluso, de sistemas de información.

Por consiguiente, el trabajo presenta dos vertientes diferenciadas, aunque interrelacionadas: la generación de las secuencias y la caracterización de las mismas.

A su vez, se ha pretendido ofrecer una amplia panorámica, extendiendo los análisis a los principales tipos de secuencias PRN: caóticas, de longitud máxima, de *Kasami* y *Gold*.

Estos códigos han sido empleados tradicionalmente en sistemas de telecomunicación de espectro ensanchado de uso militar, dada su robustez frente al ruido y las interferencias. La propiedad de baja correlación cruzada de algunos tipos de secuencias ha impulsado su extensión al ámbito civil, generalizándose su uso en sistemas de acceso múltiple al medio (además de en GPS, entre otros).

Las secuencias pseudoaleatorias serán, generalmente, señales digitales binarias +/-V, es decir, polares. En el marco de las comunicaciones de espectro ensanchado, para diferenciar la secuencia pseudoaleatoria de la señal de información, los bits de la secuencia pseudoaleatoria se designan como chips.

La criptografía, la ciberseguridad y las tecnologías de la información, en general, constituyen hoy día ámbitos de aplicación de las mismas poco explorados, con mucho potencial, donde las capacidades de cómputo actuales y la ingeniería de servicios pueden despertar el interés por ellas en cualquier momento.

2. Desarrollo

En la vertiente más teórica se explica el proceso de generación de los cuatro tipos de secuencias PRN consideradas: caóticas, de longitud máxima, de *Kasami* y *Gold*. Se incluyen diversos desarrollos matemáticos para explicar algunas de las propiedades.

En la vertiente experimental se efectúan una infinidad de simulaciones en Matlab. En el capítulo 4 y en los apéndices se incluye un extracto de las simulaciones y análisis realizados.

Del análisis de las gráficas (visual y cuantitativo) y del de las distintas tablas confeccionadas se alcanzan las conclusiones relacionadas a continuación, que incluyen también consideraciones relativas a la simulación.

3. Conclusiones

Conclusiones generales de las secuencias PRN.

- En ausencia de ruido, a los efectos de obtener gráficamente la función de autocorrelación de señales digitales o la correlación cruzada de una pareja de ellas, estas pueden ser muestreadas empleando una única muestra por chip.
- Si se desea obtener el valor de las propiedades de correlación para desplazamientos distintos de los múltiplos enteros de un periodo de chip, será necesario tomar varias muestras de la secuencia por cada chip.
- La autocorrelación de secuencias digitales es una función simétrica, es decir: R_c [τ]= R_c [-τ].
- El máximo de la función autocorrelación coincide con la potencia media de la señal.
- Presentan muy baja autocorrelación para cualquier desplazamiento τ que diste más de un chip del máximo de la función (y de sus infinitas réplicas, en el caso de ser periódica).
- La función de correlación cruzada de una pareja de secuencias, tomadas en un determinado orden, muestra simetría especular respecto de la función resultante en el caso de que las secuencias se tomasen en orden inverso: R_(c_1 c_2) [τ]= R_(c_2 c_1) [-τ].
- Las secuencias PRN logran un buen reparto en banda de la potencia de señal, propiedad necesaria en aplicaciones de espectro ensanchado.
- Tienen un espectro de tipo *sinc cuadrado*, estando concentrada la mayor parte de la potencia en el lóbulo principal, es decir, en frecuencias inferiores al régimen de chip.

Conclusiones específicas de las secuencias caóticas.

- Las secuencias generadas por un sistema caótico a partir de dos estados iniciales cuyo valor difiera muy poco tienden a ser incorreladas al poco tiempo.
- La función de autocorrelación de secuencias caóticas indefinidas tiende a ser plana, de valor nulo, para desplazamientos mayores de un chip.
- La función de correlación cruzada de secuencias caóticas indefinidas tiende a cero para cualquier desplazamiento t. En todo caso, la amplitud de la correlación parcial queda acotada en un rango más pequeño a medida que aumenta la longitud de la pareja de subsecuencias correladas.

- Trabajando con secuencias de longitud finita aparecen picos secundarios en la autocorrelación parcial. Por tanto, su aplicación a sistemas de acceso múltiple al medio requerirá el empleo de códigos lo suficientemente largos.
- El promedio de un determinado número de autocorrelaciones parciales, a partir de la extracción de subsecuencias no solapadas en el tiempo, constituye una mejor aproximación a la autocorrelación de la secuencia caótica indefinida que la del promedio de una sucesión de subsecuencias desplazadas chip a chip.
- El mecanismo de promediado de subsecuencias consecutivas no solapadas constituye, en definitiva, una muy buena aproximación a la autocorrelación de la secuencia caótica indefinida, permitiendo aproximarla con un número relativamente reducido de chips.
- Los picos secundarios de la autocorrelación parcial se cancelan o compensan en la gráfica de la autocorrelación promedio. Esta afirmación lleva implícita que no se tomen subsecuencias solapadas a la hora de calcular la aproximación a la autocorrelación de la secuencia caótica indefinida.
- Por lo general, al aumentar la longitud de las subsecuencias caóticas mejoran sus propiedades de correlación cruzada. Esta consideración habrá que tenerla en cuenta a la hora de establecer el tamaño de los códigos empleados en entornos de acceso múltiple al medio.

Conclusiones específicas de las secuencias PN de longitud máxima.

- Son secuencias periódicas, cuyo periodo tiene una longitud de 2N – 1 chips, donde N es el número de registros del generador linealmente realimentado.
- Cada ciclo tiene 2N / 2 ‘unos’.
- La autocorrelación de una secuencia PN indefinida es una función periódica de periodo L chips, al igual que el de la secuencia. Por tanto, los máximos de la función se encuentran posicionados en los desplazamientos múltiplos enteros del periodo.
- La función de autocorrelación de la secuencia indefinida muestra un pedestal o suelo de autocorrelación, que tiende a cero a medida que aumenta la longitud del periodo de la secuencia.
- Para obtener, mediante simulación, una buena aproximación de las funciones de autocorrelación o de correlación cruzada de secuencias indefinidas, no resulta suficiente con considerar un único periodo de las secuencias, sino que ha de ser un número suficientemente grande de ciclos, debiéndose acotar la observación a la región central de las funciones.

- El suelo de la autocorrelación parcial se suaviza al aumentar el número de periodos de la ventana de correlación de las simulaciones.
- La correlación cruzada de secuencias PN indefinidas es una función periódica de periodo L chips.
- Por lo general, no presentan buenas propiedades de correlación cruzada, salvo determinadas parejas de secuencias, denominadas preferentes, cuya función de correlación presenta únicamente tres valores característicos.
- La separación entre componentes espectrales es R chip /L, de tal modo que en cada lóbulo hay L-1 componentes, siendo L el periodo de la secuencia expresado en chips.
- La envolvente de potencia espectral disminuye conforme aumenta la longitud del periodo de la secuencia, al quedar repartida la misma potencia de señal entre un mayor número de componentes.

Conclusiones específicas de las secuencias de *Kasami*

- Una familia de secuencias de *Kasami* proporciona un conjunto de secuencias con buenas propiedades de correlacion cruzada, mayor que los conjuntos preferentes que pueden obtenerse de secuencias PN de longitud máxima, para una misma longitud de periodo.
- El número de secuencias de *Kasami* que integran una familia varía dependiendo de la secuencia PN de longitud máxima que se tome de base.
- Todas las secuencias de una familia de *Kasami* son periódicas, de igual longitud de periodo que la secuencia PN de longitud máxima en que se basen.
- Su función de autocorrelación presenta un rizado para desplazamientos mayores de un chip respecto de los máximos absolutos de la función.
- El rizado de la autocorrelación queda determinado por tres valores característicos, tendiendo a ser simétrico a medida que aumenta la longitud de la secuencia.
- El rizado de la autocorrelación disminuye a medida que aumenta la longitud del periodo de la secuencia.
- La función de correlación cruzada de secuencias de la misma familia presenta el mismo rizado que la función de autocorrelación de las secuencias.
- Las parejas de secuencias de una misma familia presentan mejores propiedades de correlación cruzada que las parejas preferentes de

secuencias PN, tendiendo a ser el rizado en el primer caso la mitad que, en el segundo, a medida que aumenta la longitud del periodo.

Conclusiones específicas de las secuencias *Gold*

- El número de secuencias *Gold* que integra una familia es muy grande, siendo: M= 2^N+1. Este número resulta muy superior al número de secuencias que integra una familia de *Kasami*.
- Todas las secuencias de una familia *Gold* son periódicas, de periodo de 2N – 1 chips, al igual que el de las secuencias preferentes en que se basan.
- No todas las secuencias *Gold* tienen 2N / 2 unos, existiendo en cada familia tres posibilidades distintas en cuanto al número de unos.
- Su función de autocorrelación presenta un rizado para desplazamientos mayores de un chip respecto de los máximos absolutos de la función.
- El rizado de la autocorrelación queda determinado por tres valores característicos, tendiendo a ser simétrico a medida que aumenta la longitud de la secuencia. No obstante, para longitudes de periodo bajas se encuentran algunas secuencias para las que desaparece el valor extremo inferior.
- El rizado de la autocorrelación disminuye a medida que aumenta la longitud del periodo de la secuencia.
- El rizado de la autocorrelación coincide con el de las parejas preferentes de secuencias PN de la misma longitud de periodo.
- La función de correlación cruzada de secuencias de la misma familia presenta el mismo rizado que la función de autocorrelación las secuencias.
- No todas las parejas de la familia muestran los tres valores característicos de correlación, encontrándose algunas parejas en las que desaparece la cota extrema inferior, para longitudes de periodo bajas.
- Las secuencias GPS que identifican los satélites de la red tienen un periodo de 1023 chips, de los cuales 512 son unos.
- El rizado de las funciones de autocorrelación y correlación cruzada de las secuencias GPS presentan ambas cotas extremas características, positiva y negativa.

Agradecimientos

A los miembros de mi familia, sin cuya comprensión, paciencia y ánimo no habría podido culminar este estudio. Soy consciente de las muchas facilidades que me han prestado, disculpándome siempre del tiempo de dedicación del que les he privado.

A mi directora de TFM, por los ánimos y colaboración que me ha brindado en todo momento.

Referencias

[1] Savo Glisic y Branka Vucetic, (1997). Spread Spectrum CDMA Systems for Wireless Communications. Artech House.

[2] José M. Hernando, (1997) Comunicaciones Móviles. Centro de Estudios Ramón Areces.

[3] Robert B. Ward (diciembre 1965) «Acquisition of Pseudonoise Signals by Sequential Estimation», IEEE Transactions on Communication Technology, vol. COM-13, pp. 475-483.

[4] Andreas Polydoros y Charles L. Weber, (diciembre 1965) «A Unified Approach to Serial Search Spread-Spectrum Code Acquisitión-Part II: A Matched-Filter Receiver», IEEE Transactions on Communications, vol. COM-32, n.º 5, pp. 550-551.

[5] J.-F. Beaumont (septiembre de 2004) «RTL Design of a Generic Pseudonoise Generator», Defence R&D 2004 176, Ottawa (Canadá).

[6] M. Gulotta (verano 2002). «HDL Coding for Pseudo-Random Noise Generators», Xcell Journal, Nº35, pp. 43-45.

[7] New Wave Instruments (septiembre de 2001). «LRS-200 Family Spread Spectrum Generators». (http://www.newwaveinstruments.com/literature/documents/pdf/LRS-200_brochure.pdf).

[8] S. Azou, G. Burel y C. Pistre (octubre 2002). «A Chaotic Direct-Sequence Spread-Spectrum System for Underwater Communication», IEEE-Oceans'2002, vol. 4, pp. 2409-2415.

[9] G. Heidari-Bateni y C. D. McGillem (1994). «A Chaotic Direct-Sequence Spread Spectrum Communication System», IEEE Transactions on Communications, vol. 42, n.º 2, pp. 1524-152.

[10]https://es.wikipedia.org/wiki/GPS#Evolución_del_sistema_GPS.

[11] M. Carmen Pérez Rubio (2009). «Generación y Correlación Eficiente de Códigos Binarios Derivados de Conjuntos de Secuencias Complementarias para Sistemas Ultrasónicos», Escuela Politécnica Superior de la Universidad de Alcalá.

Generación y Caracterización de Secuencias PRN

Autor: Abel Hernández González
Director/es: Paula Gómez Pérez
Universidad de Vigo

Introducción

En este trabajo se ha llevado a cabo un estudio riguroso y exhaustivo de las secuencias PRN (Pseudo-Random Noise), que pretende ofrecer una base para el diseño o el análisis de sistemas de tecomunicación o, incluso, de información.

Metodología

El estudio se ha llevado a cabo sobre la base de una infinidad de simulaciones en Matlab.
Las gráficas obtenidas han sido analizadas minuciosamente, tanto a nivel visual, como a nivel cuantitativo.
También se han confeccionado numerosas tablas de resultados, contribuyendo a la extracción de las conclusiones.

Resultados

En la vertiente más teórica se explica el proceso de generación de los cuatro tipos de secuencias PRN consideradas: caóticas, de longitud máxima, de Kasami y Gold. Se incluyen diversos desarrollos matemáticos para explicar algunas de las propiedades.

En la vertiente experimental se efectúan una infinidad de simulaciones en Matlab. En el capítulo 4 y en los Apéndices se incluye un extracto de las simulaciones y análisis realizados.

Conclusiones

Entre las conclusiones más destacadas que se alcanzan, hay que mencionar que todas ellas logran un gran reparto en banda de la potencia, muy deseable en sistemas de espectro ensanchado, que las proporciona propiedades inmunidad frente al ruido y la interferencia.

Salvando lo anterior, se concluye que, de las secuencias analizadas, las que presentan una mejor autocorrelación son las caóticas y las secuencias PN (Pseudo-Noise) de longitud máxima, dado que las de Kasami y las Gold presentan un rizado de la función para desplazamientos mayores de un chip.

Desafortunadamente, las secuencias PN de longitud máxima presentan, salvo grupos muy reducidos, una mala correlación cruzada, que las descarta para aplicaciones de acceso compartido al medio. Por su parte, las secuencias de Kasami y de Gold consiguen proporcionar grandes familias de secuencias con buenas propiedades de correlación cruzada.

Algoritmos de detección de anomalías y sus aplicaciones en el ámbito marítimo

Autor: Lasso Mula, Alberto (alberto_lasso@hotmail.com)
Director: Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – En los últimos años una de las principales tecnologías que se ha desarrollado exponencialmente posibilitando la trasformación digital del mundo es la *inteligencia artificial*, la cual tiene una de sus principales aplicaciones en la detección de anomalías.

La detección de anomalías presenta la utilidad de alertar de comportamientos que se salen de lo normal y que pueden presentar un problema, en el caso concreto del ámbito marítimo se pretende con ello detectar los comportamientos ilícitos y las situaciones de riesgo de las embarcaciones.

Este trabajo hace un extenso análisis del estado del arte de la detección de anomalías en el tráfico marítimo, comparando y clasificando un importante número de estudios relevantes.

Se valoran todos los aspectos concernientes a un sistema de este tipo:

- Las fuentes de información que se pueden utilizar como entrada al algoritmo, las que se analizan detalladamente y de las que el sistema de comunicaciones AIS es la más relevante.
- Se estudian muchas de las diferentes metodologías que se pueden aplicar en el algoritmo de detección de anomalías.
- La presentación de los resultados, es importante facilitar la interpretación de las alertas que se obtengan.

A partir de todos ellos se señalan las principales características y posibles dificultades a los que se tendrán que enfrentar los diseñadores de los sistemas de detección de anomalías en el ámbito marítimo. Con el fin de que las conozcan desde el principio, capacitándoles para tomar todas las decisiones que sean conveniente en el diseño de una buena solución a este problema.

Palabras clave: detección de anomalías, rutas marítimas, navegación, predicción de trayectorias, inteligencia artificial.

1. Introducción

1.1. Contexto

El transporte marítimo a lo largo de la historia ha sido un motor de progreso, desarrollo y prosperidad. En nuestros días sigue siendo fundamental para el avance de la economía, habiendo tomado más relevancia aún ante el proceso de globalización que se ha producido en las últimas décadas a nivel mundial.

La importancia para la humanidad de tráfico marítimo es evidente y con el fin de que se desarrolle de la manera más eficiente y segura, en 2002 se desarrolla un sistema de identificación automática de embarcaciones denominado AIS de obligada implantación en numerosas embarcaciones.

La expansión del sistema AIS, ha puesto a disposición de las autoridades competentes una fuente más de información para supervisar el tránsito marítimo, prever las situaciones de riesgo y combatir las actividades ilegales que se desarrollan en los mares.

1.2. Objetivo

El principal objetivo del trabajo es estudiar la viabilidad de aplicar sistemas automatizados basados en inteligencia artificial para la detección de anomalías en el tráfico marítimo que permitan identificar las actividades ilegales que se llevan a cabo.

Pretende aglutinar todos principales factores que sean de especial aplicación en este ámbito concreto, los cuales no deberían pasarse por alto en el diseño de los futuros sistemas de detección de anomalías, salvo que así se decida por motivos justificados.

2. Resultados y discusión

El diseño de un sistema que detecta anomalías en el tráfico marítimo es un proceso complejo en el que hay que tener en cuenta múltiples y muy diferentes opciones. Por ello se ha llevado a cabo un amplio estado del arte en que se han incluido los principales y más relevantes trabajos sobre este ámbito.

Estos trabajos se han clasificado en dos grandes grupos, muy diferenciados entre sí, de acercamientos a la hora de definir la solución con que resolver la detección de anomalías en el tráfico marítimo.

El primero de ellos se centra en detectar patrones definidos por expertos en navegación marítima que denotan comportamientos ilícitos o situaciones de riesgo, mientras que el segundo en vez de centrarse en casos concretos, busca los comportamientos que se alejan de los frecuentes y más habituales que son los que se considerarían anómalos.

En la tabla 1 se muestran todos los estudios incluidos en el estado del arte clasificados en estos dos grandes grupos, comparando sus principales características.

TRABAJO		CLASIFICACIÓN	SUPERVISADO	ENTRENAMIENTO	PARAMETRICO	DIMENSIONES	METODOLOGIA	TIEMPO REAL
TÍTULO	REFERENCIA							
Vessel Trajectories Outliers	3	Detección de Eventos	No supervisado	SI	SI	Varias	Rules	SI
Loitering with intent—Catching the outlier vessels at sea	4		Supervisado	SI	SI	Varias	Probability Model	SI
Extracting rules from expert operators to support situation awareness in maritime surveillance	21		Supervisado	SI	NO	Varias	Queries/Rules	SI
Maritime anomaly detection and threat assessment	12		Supervisado	SI	NO	Varias	Probability Model	NO
Crisis: Integrating ais and ocean data streams using semantic web standards for event detection	8		Supervisado	SI	NO	Varias	Queries/Rules	SI
Abstracting and reasoning over ship trajectories and web data with the Simple Event Model (SEM)	7		Supervisado	SI	NO	Varias	Queries/Rules	SI
Event Recognition for Maritime Surveillance	10		Supervisado	SI	NO	Varias	Queries/Rules	SI
Mining maritime traffic conflict trajectories from a massive AIS data	23		No supervisado	NO	SI	Varias	Clustering	NO
Online Event Recognition from Moving Vessel Trajectories	11		Supervisado	SI	NO	Varias	Queries/Rules	SI
Semantic modelling of ship behavior in harbor based on ontology and dynamic bayesian network	13		Supervisado	SI	NO	Varias	Probability Model	NO
Open data for anomaly detection in maritime surveillance	9		Supervisado	SI	NO	Varias	Queries/Rules	SI
A complex event processing approach to detect abnormal behaviours in the marine environment	5		Supervisado	SI	NO	Varias	Rules	SI
Detecting search and rescue missions from ais data	6		No supervisado	NO	NO	Varias	Rules	SI
A multi-task deep learning architecture for maritime surveillance using ais data streams	19	Detección de Anomalías	No Supervisado	SI	NO	Varias	Neural Network	SI
Valor atipico por cuartiles - Four Techniques for Outlier Detection	2		No Supervisado	No	SI	Una	Statistical	NO APLICA
Z-Score - Four Techniques for Outlier Detection	2		No Supervisado	SI	SI	Varias	Gaussian Model	NO APLICA
DBSCAN - Four Techniques for Outlier Detection	2		No Supervisado	SI	SI	Varias	Clustering	NO APLICA
Isolation forrest - Four Techniques for Outlier Detection	2		No Supervisado	NO	SI	Varias	Rules	NO APLICA
Seafaring TRansport ANomaly Detection, STRAND	1		No Supervisado	SI	NO	Varias	Rules	SI
A network abstraction of multi-vessel trajectory data for detecting anomalies	22		No Supervisado	SI	SI	Varias	Clustering	SI
Statistical analysis of motion patterns in data: Anomaly detection and motion prediction	14		No Supervisado	SI	NO	Varias	KDE	SI
Maritime anomaly detection using gaussian process active learning	15		Supervisado	SI	NO	Varias	Gaussian Model	NO
Improving maritime anomaly detection and situation awareness through interactive visualization	16		Supervisado	SI	NO	Varias	Gaussian Mixture Model (GMM)	NO
Anomaly detection in maritime data based on geometrical analysis of trajectories	17		No Supervisado	NO	SI	Varias	Rules	SI
Associative learning of vessel motion patterns for maritime situation awareness	18		No Supervisado	SI	NO	Varias	Neural Network	SI
Vessel pattern knowledge discovery from ais data: A framework for anomaly detection and route prediction	20		No Supervisado	NO	NO	Varias	Clustering + Probability Model	SI

Figura 1. Tabla comparativa de los diferentes trabajos incluidos en el estado del arte

De todos ellos se extraen numerosos aspectos fundamentales que no deberían pasarse por alto en el desarrollo de un sistema de detección de anomalías en el tráfico marítimo.

2.1. Fuentes de información

El primer aspecto a analizar es la cantidad y calidad de fuentes de información disponibles, siendo algunas de las más representativas; señalización AIS, información meteorológica, información portuaria, cartografía e información geográfica, información de rutas marítimas, imágenes de drones, satélite, información aduanera.

Antes de seleccionar las fuentes a utilizar hay que tener en cuenta que cada una de las que se incluya en el sistema aumenta las dimensiones a tratar y con ello, la complejidad del mismo.

2.1.1. Sistema AIS

Representa una base muy sólida, por no decir fundamental para analizar el comportamiento de las embarcaciones gracias a que facilita registros periódicos con su geolocalización, además de más parámetros cinemáticos y de otra naturaleza.

Pero este sistema de comunicaciones, ni es infalible, ni toda la información que aporta se puede considerar igual de válida, pudiendo llegar parte de ella a generar confusión. Algunos de los campos remitidos en la señalización AIS deben ser actualizados a mano por los tripulantes, como es el caso del *status*, el cual no es fiable, un número muy elevado de tripulaciones no lo actualizan durante la travesía.

2.1.2. Información meteorológica

La información meteorológica es otra de las fuentes de información que puede tener más sentido tener en cuenta ya que puede ejercer una importante influencia en la navegación de las embarcaciones.

2.1.3. Imágenes

El importante desarrollo que tiene la IA en lo correspondiente al tratamiento de imágenes en otros ámbitos sería fácilmente extrapolable al tránsito marítimo en cuanto exista una forma de obtener imágenes de manera económica y fluida.

2.2. Transformación, preprocesado y filtrado de la información

Una vez se hayan seleccionado las fuentes de información para el sistema de detección de anomalías hay que analizar el formato de los datos, porque es bastante posible que requieran de un procesado o transformación previa a su utilización.

2.3. Sistemas basados en la detección de eventos y patrones de comportamiento

De los dos grandes bloques de metodologías comentados al inicio del capítulo, este es el primero de ellos, el que se basa en el reconocimiento de patrones predefinidos por expertos como sospechosos de delatar comportamientos ilícitos o ilegales. Los principales patrones que incluyen los trabajos revisados son:

- Pérdida señal AIS: pérdida intencionada o no intencionada de la señalización AIS de una embarcación.
- Detención de un barco un tiempo largo.
- Si una embarcación hace un giro repentino sin justificación.
- Dos barcos se detienen en alta mar muy próximos entre sí.
- Si un barco tiene un encuentro con un barco de menor tamaño.
- Dos barcos que van en paralelo (o navegan muy próximos) al menos una cierta distancia y/o tiempo.
- Más aún si un barco que navega próximo a otro durante un tiempo y justo después de estar lo más próximos entre sí uno cambia de dirección significativamente.
- Dos buques que van uno hacia el otro y tras el encuentro uno o los dos realiza un giro.
- Si una embarcación navega a velocidades muy elevadas.
- Una embarcación que transite a una velocidad muy reducida.
- Una embarcación que abandone una ruta habitual para adentrarse a una zona en la que habitualmente no hay tráfico.
- Si una embarcación que habitualmente navega entre dos puertos, de repente va a un tercero al que no iba antes.
- Si un barco no ha dejado registros AIS abandonando o entrando en puerto, pero sí figura en los registros portuarios correspondientes.
- Si un barco que figura en los registros de un puerto como que está atracado en él, deja registros AIS en otra localización.
- Si el destino de una embarcación indicado en el sistema AIS, no está registrado en la agenda del puerto.
- Si un barco entra en puerto sin haberle informado previamente.
- Si en vez de entrar a puerto un barco en un horario previsto, entra otro justo en ese intervalo.
- Si una embarcación no ha dejado señalización dentro de puerto, pero sí figura que haya solicitado un práctico.
- Si el tiempo estimado de llegada registrado en las comunicaciones AIS, no coincide con el real de llegada a puerto.

Bastantes de las metodologías de este tipo, detección de eventos, optan por dividir la región marítima que van a tratar en múltiples celdas con objeto de subdividir las trayectorias de las embarcaciones en trozos más cortos sobre los que buscar anomalías con mayor facilidad

o bien para aplicar patrones concretos característicos de cada zona concreta.

Queda demostrado que las dimensiones concretas que se elijan para estas celdas afecta directamente a la capacidad de detección de los algoritmos.

2.4. Sistemas basados en la detección de comportamientos anómalos

El segundo grupo de trabajos incluidos en el estado del arte es el que tiene que ver con detectar las embarcaciones que se salen del comportamiento normal, las que tienen algo diferenciador respecto a la mayoría en su comportamiento. Se da por sentado que el gran grueso de las embarcaciones no está inmerso en actividades ilegales y se pretende detectar las que realizan esas actividades justo por las diferencias que tendrá su navegación frente a las que llevan a cabo las tareas habituales y cotidianas.

Los trabajos recopilados en el estado del arte abordan la detección de comportamientos anómalos con una variedad de técnicas diferentes, distribuciones de Gauss, *Kernel Density Estimation*, redes neuronales, agrupamiento, etc.

Siendo la carencia de datos etiquetados una de las principales dificultades a las que se enfrentan y que intentan solventar de diferente forma.

- Retroalimentando el sistema a través de visualizaciones interactivas que validen las detecciones de forma que el sistema se vaya refinando constantemente.
- Que un grupo de expertos etiquete la información manualmente, lo que resultaría extraordinariamente lento y caro por la dificultad que presenta.
- Mediante aplicaciones en Internet que permiten a los propios tripulantes subir las navegaciones que efectúen y etiquetarlas, de forma que se genere una base de datos de información etiquetada con la que trabajar.
- A través de aprendizaje por transferencia, esto es, a partir de unos pocos ejemplos etiquetados, generar y etiquetar otros.

Otra de las singularidades que hay que tener en cuenta es que cierto tipo de embarcaciones se desenvuelven en el mar de diferente manera, por ello algunos estudios se centran en algún tipo de barco concreto o aplican el mismo modelo de forma separada según la naturaleza de estos.

Son de especial interés los trabajos que utilizan redes neuronales para predecir las trayectorias futuras de las embarcaciones además de detectar anomalías. A partir de modelar los comportamientos habituales

de los barcos con estos sistemas se puede detectar cuando alguno se aleja de ellos incluso predecir su trayectoria futura.

Una limitación de la gran mayoría de trabajos de este ámbito es que analizan principalmente el comportamiento individual de las embarcaciones, aunque algunas anomalías solo pueden detectarse al analizar un grupo de embarcaciones. Comprender los patrones de movimiento colectivo de los barcos puede ser una tarea más fácil que analizar los comportamientos individuales, tarea que no se está explotando en exceso.

Por último, pero no menos importante, estos sistemas de detección de anomalías se enfrentan también a la baja interpretabilidad de los resultados que obtienen. Debe de procurarse añadir a los sistemas capacidades de visualización y procesamiento de datos relevantes involucrados en las alarmas que detecten, para facilitar a los agentes marítimos la interpretación de las mismas. En estos casos sistemas de retroalimentación, como los que se han comentado antes, podrían ser de utilidad.

3. Conclusiones

La detección de anomalías en el tráfico marítimo es un problema complejo que se puede abordar de muy diferentes formas, siendo cada una de ellas más o menos eficaz según sean los objetivos que se pretendan cubrir y los recursos disponibles para ello.

Aunque la señalización de las comunicaciones AIS no es la única fuente de información, se ha comprobado que es la principal siendo utilizada en todos los sistemas analizados. Aunque no todos sus campos tienen la misma fiabilidad, se ha demostrado que no existe garantía de que las tripulaciones actualicen convenientemente los que deben modificarse manualmente.

El crecimiento de la actividad marítima junto con el desarrollo de la tecnología AIS ha resultado en la generación de grandes volúmenes de datos todos los días. Se dispone de una gran cantidad de datos, pero su problema radica en que no están etiquetados, dificultando su utilización en algoritmos de aprendizaje supervisado.

Por lo que una gran parte de los trabajos existentes no aprenden de los datos, sino que se basan en el establecimiento de reglas o umbrales definidos de antemano que son indicativos de un conjunto restringido de actividades presuntamente ilícitas que desarrollan las embarcaciones. La definición de esas reglas o patrones requiere de la implicación de especialistas, lo que es muy costoso tanto en términos económicos, como de tiempo. Además, puede resultar en la introducción del sesgo humano.

En cambio, las principales dificultades a las que enfrentan los sistemas no supervisados son de diferente índole, como estar limitados al análisis de unas pocas variables o características por la complejidad y necesidades de cómputo que exige aumentar su número, o que se estudie principalmente el comportamiento individual de las embarcaciones y no en su conjunto que es fundamental para la detección de algunas anomalías.

Además, los sistemas no supervisados presentan un problema importante, la dificultad en la interpretabilidad de sus detecciones, con la desconfianza que esto genera en los resultados que presentan estos sistemas ante el personal que los explota. Llegar a entender qué está pasando detrás de una anomalía detectada por un sistema de detección de anomalías llega a ser un desafío para los operadores.

Así que hay que, aunque en todos los sistemas de información de detección de anomalías es importante entregar la información de forma ordenada, clasificada y con representaciones visuales que ayuden a interpretar las alarmas que produzcan, en el caso de los no supervisados es fundamental.

Referencias

[1] «Design and Implementation of Maritime Traffic Modeling and Anomaly Detection Method» [En línea]. Disponible: https://www.diva-portal.org/smash/get/diva2:833998/FULLTEXT01.pdf [Último acceso: 7 diciembre 2021]

[2] «Four Techniques For Outlier Detection» [En línea]. Disponible: https://www.knime.com/blog/four-techniques-for-outlier-detection [Último acceso: 25 noviembre 2020] Autor/Autores: Maarit Widmann & Moritz Heine [Publicado: 1 de octubre del 2018]

[3] «Vessel Trajectories Outliers» [En línea]. Disponible: https://easychair.org/publications/preprint_open/FbMB [Último acceso: 15 noviembre 2020] Autor/Autores: Tomas Machado, Rui Maia, Pedro Santos and João Ferreira [Publicado: 24 de mayo 2018]

[4] «Loitering with intent—Catching the outliervessels at sea» [En línea]. Disponible: https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0200189&type=printable [Último acceso: 17 noviembre 2020] Autor/Autotes: Jessica H. Ford, David Peel, Britta Denise Hardesty, Uwe Rosebrock, Chris Wilcox [Publicado: 12 de julio 2018]

[5] Fernando Terroso-Saenz, Mercedes Valdes-Vela, and Antonio F Skarmeta-Gomez. A complex event processing approach to detect abnormal behaviours in the marine environment. Editorial: Information Systems Frontiers, 18(4):765–780, 2016 [En línea]. Disponible: https: https://www.researchgate.net/publication/276532092_A_complex_event_processing_approach_to_detect_abnormal_behaviours_in_the_marine_environment

[6] «Detecting search and rescue missions from ais data» [En línea]. Disponible: https: http://www.master-project-h2020.eu/wp-content/uploads/2018/09/ICDE-Tserpes-et-al.pdf [Último acceso: 8 diciembre 2020]

[7] «Abstracting and reasoning over ship trajectories and web data with the Simple Event Model (SEM)» [En línea]. Disponible: https://link.springer.com/article/10.1007/s11042-010-0680-2 [Último acceso: 8 diciembre 2020]

[8] «Crisis: Integrating ais and ocean data streams using semantic web standards for event detection» [En línea]. Disponible: https://www.researchgate.net/publication/335935262_CRISIS_Integrating_AIS_and_Ocean_Data_Streams_Using_Semantic_Web_Standards_for_Event_Detection [Último acceso: 5 diciembre 2020]

[9] «Open data for anomaly detection in maritime surveillance» [En línea]. Disponible: https: https://www.diva-portal.org/smash/get/diva2:832155/FULLTEXT01.pdf [Último acceso: 7 diciembre 2020]

[10] «Event Recognition for Maritime Surveillance» [En línea]. Disponible: http://openproceedings.org/2015/conf/edbt/paper-364.pdf [Último acceso: 2 diciembre 2020]

[11] «Online Event Recognition from Moving Vessel Trajectories» [En línea]. Disponible: https://arxiv.org/pdf/1601.06041.pdf [Último acceso: 2 diciembre 2020]

[12] «Maritime anomaly detection and threat assessment» [En línea]. Disponible: https://www.researchgate.net/publication/224218677_Maritime_anomaly_detection_and_threat_assessment [Último acceso: 8 diciembre 2020]

[13] «Semantic modelling of ship behavior in harbor based on ontology and dynamic bayesian network» [En línea]. Disponible: https://www.mdpi.com/2220-9964/8/3/107 [Último acceso: 09 diciembre 2020]

[14] «Statistical analysis of motion patterns in data: Anomaly detection and motion prediction» [En línea]. Disponible: https://www.researchgate.net/publication/4370120_Statistical_Analysis_of_Motion_Patterns_in_AIS_Data_Anomaly_Detection_and_Motion_Prediction [Último acceso: 10 diciembre 2020]

[15] «Maritime anomaly detection using gaussian process active learning» [En línea]. Disponible: https://www.researchgate.net/publication/261308815_Maritime_anomaly_detection_using_Gaussian_Process_active_learning [Último acceso: 10 diciembre 2020]

[16] «Improving maritime anomaly detection and situation awareness through interactive visualization» [En línea]. Disponible: https://www.researchgate.net/publication/4370119_Improving_maritime_anomaly_detection_and_situation_awareness_through_interactive_visualization [Último acceso: 10 diciembre 2020]

[17] «Anomaly detection in maritime data based on geometrical analysis of trajectories» [En línea]. Disponible:https://c4i.gmu.edu/~pcosta/F15/data/fileserver/file/472181/filename/Paper_1570106169.pdf [Último acceso: 9 diciembre 2020]

[18] «Associative learning of vessel motion patterns for maritime situation awareness» [En línea]. Disponible: https: http://fusion.isif.org/proceedings/fusion06CD/Papers/234.pdf [Último acceso: 5 diciembre 2020]

[19] «A multi-task deep learning architecture for maritime surveillance using ais data streams» [En línea]. Disponible: https://arxiv.org/pdf/1806.03972.pdf [Último acceso: 11 diciembre 2020]

[20] «Vessel pattern knowledge discovery from ais data: A framework for anomaly detection and route prediction» [En línea]. Disponible: https://www.mdpi.com/1099-4300/15/6/2218 [Último acceso: 12 diciembre 2020]

[21] «Extracting rules from expert operators to support situation awareness in maritime surveillance» [En línea]. Disponible: http://fusion.isif.org/proceedings/fusion08CD/papers/1569106719.pdf [Último acceso: 12 diciembre 2020]

[22] «A network abstraction of multi-vessel trajectory data for detecting anomalies» [En línea]. Disponible: https://zenodo.org/record/2649606#.X9PWTthKg2w [Último acceso: 2 diciembre 2020]

[23] «Mining maritime traffic conflict trajectories from a massive AIS data» [En línea]. Disponible: https://www.researchgate.net/publication/331945393_Mining_maritime_traffic_conflict_trajectories_from_a_massive_AIS_data [Último acceso: 26 noviembre 2020].

ALGORITMOS DE DETECCIÓN DE ANOMALÍAS Y SUS APLICACIONES EN EL ÁMBITO MARÍTIMO

Autor: Alberto Lasso Mula

Director/es: Norberto Fernández García

Universidad de Vigo

Introducción

La expansión del Sistema de Identificación Automática (AIS) por las diferentes embarcaciones ha puesto a disposición de las autoridades competentes una fuente de información fundamental para supervisar el tránsito marítimo, prever las situaciones de riesgo y combatir las actividades ilegales que se desarrollan en los mares. Pero el volumen ingente de información que se genera cada día hace que la Inteligencia Artificial sea imprescindible en su análisis.

Metodología

Se lleva a cabo un profundo estudio del estado del arte, para partir de él, tanto enumerar todos los factores que no deberían pasarse por alto en el diseño de los futuros sistemas de detección de anomalías, como clasificar los trabajos más relevantes en dos grandes grupos.

- Los que buscan patrones definidos por expertos susceptibles de indicar que se estaban produciendo comportamientos ilícitos o situaciones de riesgo.
- Los que buscan comportamientos diferentes a los habituales.

Resultados

TRABAJO		CLASIFICACIÓN	SUPERVISADO	ENTRENAMIENTO	PARAMETRICO	DIMENSIONES	METODOLOGIA	TIEMPO REAL
TÍTULO	REFERENCIA							
Vessel Trajectories Outliers	28	Detección de Eventos	No supervisado	SI	SI	Varias	Rules	SI
Loitering with intent—Catching the outlier vessels at sea	30		Supervisado	SI	SI	Varias	Probability Model	SI
Extracting rules from expert operators to support situation awareness in maritime surveillance	52		Supervisado	SI	NO	Varias	Queries/Rules	SI
Maritime anomaly detection and threat assessment	42		Supervisado	SI	NO	Varias	Probability Model	NO
Crisis: Integrating ais and ocean data streams using semantic web standards for event detection	38		Supervisado	SI	NO	Varias	Queries/Rules	SI
Abstracting and reasoning over ship trajectories and web data with the Simple Event Model (SEM)	37		Supervisado	SI	NO	Varias	Queries/Rules	SI
Event Recognition for Maritime Surveillance	40		Supervisado	SI	NO	Varias	Queries/Rules	SI
Mining maritime traffic conflict trajectories from a massive AIS data	76		No supervisado	NO	SI	Varias	Clustering	NO
Online Event Recognition from Moving Vessel Trajectories	41		Supervisado	SI	NO	Varias	Queries/Rules	SI
Semantic modelling of ship behavior in harbor based on ontology and dynamic bayesian network	43		Supervisado	SI	NO	Varias	Probability Model	NO
Open data for anomaly detection in maritime surveillance	39		Supervisado	SI	NO	Varias	Queries/Rules	SI
A complex event processing approach to detect abnormal behaviours in the marine environment	35		Supervisado	SI	NO	Varias	Rules	SI
Detecting search and rescue missions from ais data	36		No supervisado	NO	NO	Varias	Rules	SI
A multi-task deep learning architecture for maritime surveillance using ais data streams	49	Detección de Anomalías	No Supervisado	SI	NO	Varias	Neural Network	SI
Valor atipico por cuartiles - Four Techniques for Outlier Detection	27		No Supervisado	No	SI	Una	Statistical	NO APLICA
Z-Score - Four Techniques for Outlier Detection	27		No Supervisado	SI	SI	Varias	Gaussian Model	NO APLICA
DBSCAN - Four Techniques for Outlier Detection	27		No Supervisado	SI	SI	Varias	Clustering	NO APLICA
Isolation forrest - Four Techniques for Outlier Detection	27		No Supervisado	NO	SI	Varias	Rules	NO APLICA
Seafaring TRansport ANomaly Detection, STRAND	11		No Supervisado	SI	NO	Varias	Rules	SI
A network abstraction of multi-vessel trajectory data for detecting anomalies	53		No Supervisado	SI	SI	Varias	Clustering	SI
Statistical analysis of motion patterns in data: Anomaly detection and motion prediction	44		No Supervisado	SI	NO	Varias	KDE	SI
Maritime anomaly detection using gaussian process active learning	45		Supervisado	SI	NO	Varias	Gaussian Model	NO
Improving maritime anomaly detection and situation awareness through interactive visualization	46		Supervisado	SI	NO	Varias	Gaussian Mixture Model (GMM)	NO
Anomaly detection in maritime data based on geometrical analysis of trajectories	47		No Supervisado	NO	SI	Varias	Rules	SI
Associative learning of vessel motion patterns for maritime situation awareness	48		No Supervisado	SI	NO	Varias	Neural Network	SI
Vessel pattern knowledge discovery from ais data: A framework for anomaly detection and route prediction	51		No Supervisado	NO	NO	Varias	Clustering + Probability Model	SI

Conclusiones

- La detección de anomalías en este ámbito marítimo se debe abordar en función de los objetivos definidos y los recursos disponibles.
- La señalización de las comunicaciones AIS es la principal fuente para ello.
- La definición de patrones por expertos que puedan indicar comportamientos ilegales es muy costosa.
- Aunque existen formas de mitigarlo, la carencia de datos etiquetados dificulta la utilización de la IA en la detección de comportamientos anómalos.
- No siendo el único, ya que otro reto al que tienen que hacer frente es la escasa interpretabilidad que presentan.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2020/2021

Presente y futuro de los nodos desplegables. Estudio de la viabilidad de la tecnología HCI para albergar servicios clasificados/no clasificados de la OTAN a los nodos de misión desplegables

Autor: Liaño Núñez, Fernando (flianun@fn.mde.es)
Directora: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – Con este documento, el autor se ha planteado el objetivo de analizar, desde un punto de vista de gestión y dirección TIC, cómo los avances tecnológicos en virtualización e hiperconvergencia pueden mejorar las capacidades actuales de los nodos desplegables DCIS de la OTAN.

Para ello, el autor ha realizado un estudio somero de un concepto que se encuentra en boga, mundialmente conocido dentro del ámbito TIC, y que se ha convertido en uno de los pilares fundamentales de la transformación digital. Este concepto es la infraestructura en la nube y por consecuencia la hiperconvergencia (HCI) como tecnología subyacente de esta infraestructura. Previo a este análisis será necesario abordar el tema de virtualización, como base inicial y fundamental para comprender las posibilidades del HCI.

En lo que respecta al cliente, en nuestro documento la OTAN, el autor llevará a cabo un estudio de las capacidades actuales de los medios DCIS de la OTAN y pretende demostrar que, aunque en su momento cumplieron eficazmente su objetivo, la realidad es que se han quedado obsoletos en comparación con la tecnología actual existente.

De una manera breve y concisa, el autor presentará la capacidad FMN como elemento esencial para la interoperabilidad e intercambio de información de los sistemas de información OTAN con el resto de países aliados o *afiliados*, dentro de una operación o ejercicio en el ámbito de la Alianza.

Por último, después de analizar las diferentes arquitecturas hiperconvergentes de los principales fabricantes y estudiar sus principales características, el autor presentará dos de ellas (NetApp

y CISCO) como potenciales opciones que se podrían adaptar a los requerimientos de la OTAN.

Palabras clave: DCIS OTAN, hiperconvergencia, virtualización, integración e interoperabilidad.

1. Introducción

1.1. Antecedentes

Los cambios experimentados por la Organización del Tratado del Atlántico Norte (OTAN) en los últimos años han sido significativos. Estos cambios han tenido una especial repercusión en lo referente a los sistemas de comunicaciones e información (CIS), no sólo en lo concerniente al mantenimiento de esta capacidad, sino también en lo relativo a futuros programas de desarrollo, como es el caso de medios CIS desplegables.

La fuerza de respuesta de la OTAN (NRF) es una fuerza conjunta y combinada de alta disponibilidad, capaz de realizar misiones autónomamente, así como de participar en una operación como parte de una fuerza mayor, o incluso servir como una fuerza de entrada que prepara el teatro de operaciones para fuerzas posteriores (*Follow On Forces*). La NRF proporciona una fuerza creíble y de despliegue rápido para la defensa colectiva y las operaciones de respuesta a crisis.

Los medios DCIS deben proporcionar a la NRF y otras fuerzas expedicionarias una capacidad segura, modular, escalable, desplegable y sostenible, que proporcione los servicios de comunicación entre los propios elementos desplegados y sus mandos en los *cuarteles generales estáticos*.

1.2. Objetivo

Con este trabajo se pretende analizar en qué sentido los avances tecnológicos actuales en virtualización e hiperconvergencia pueden mejorar y optimizar los nodos desplegables de comunicaciones e información (DCIS) con los que cuenta la OTAN.

En definitiva, este trabajo se ha realizado desde la perspectiva de este máster, es decir, desde el punto de vista de gestión y dirección. Para ello, su desarrollo se ha centrado en el análisis de las capacidades [1], sus ventajas e inconvenientes, posible *casos de uso* [2] y *estado del arte* [3], aportando en determinados apartados información más detallada y de carácter técnico.

2. Desarrollo

2.1. Hiperconvergencia y virtualización

Actualmente, la mayoría de las organizaciones se basan en el modelo de infraestructura convergente tradicional basadas en las arquitecturas específicas de tres niveles [4] incluidas en servidores: procesamiento, almacenamiento y elementos de red, tal y como se observa en la figura

2.1. Aunque estas arquitecturas han sido eficaces durante muchos años, resultan costosas de implementar, complejas de administrar, difíciles de escalar e incapaces de responder con la suficiente agilidad a las demandas de las aplicaciones actuales.

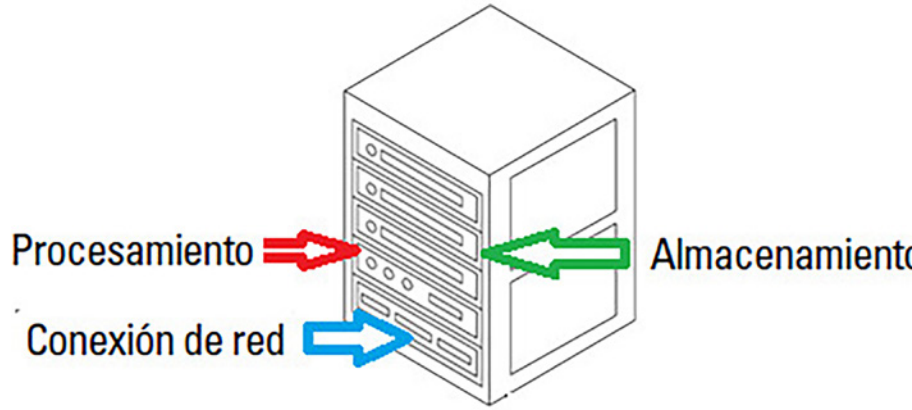


Figura 2.1: Infraestructura convergente tradicional (extraído de [1])

Esta falta de agilidad es la razón por la que la mayoría de las organizaciones/empresas están considerando cada vez más, disponer de sus servicios en la nube pública y no tener que esperar a que su infraestructura de telecomunicaciones e información se modernice o adapte para dar respaldo a las nuevas aplicaciones y sus requisitos asociados.

Con la infraestructura HCI, las organizaciones/empresas están experimentando significativas reducciones de gasto en formación del personal, licencias, mantenimiento y adquisiciones de SW (conocido con el término OPEX), así como en los costes de inversión en adquisiciones de nuevo HW (conocido con el término CAPEX) al sustituirlos únicamente por servidores x86. Con todos estos componentes convergiendo en el servidor, las operaciones resultan mucho más sencillas, requieren menos tiempo de configuración y menos experiencia del personal en las tareas rutinarias.

Asimismo, la arquitectura HCI permite tener el hardware en funcionamiento y simultáneamente, sin interrupciones y en pocas horas disponer de la capacidad de aumentar la carga o repartirla/equilibrarla de una manera ágil y dinámica.

Por debajo de la arquitectura HCI, subyace la virtualización como elemento crítico y motor principal de esta arquitectura, la posibilidad de enmascarar los recursos hardware a los usuarios y eliminar la dependencia del mismo, ha permitido optimizar los recursos disponibles y mejorar significativamente su rendimiento. La posibilidad de converger

el procesamiento, el almacenamiento y la red proporciona al sistema una flexibilidad hasta ahora inimaginable.

La OTAN, al igual que las grandes empresas, está optando por la implementación del modelo *On-Cloud* que traerá consigo múltiples ventajas respecto a los modelos tradicionales del CPD de respaldo *On Premise*. Entre estas ventajas podemos reseñar:

- Una considerable disminución de los riesgos operativos y de seguridad de la información.
- Una mayor facilidad del escalado, ampliación y traslado de las cargas de trabajo y las capacidades a la nube en caso de su requerimiento.
- Unos menores tiempos de despliegue de la infraestructura y las aplicaciones, de semanas a días e incluso horas.
- Una mayor disponibilidad y potencia de los sistemas, para mejorar la productividad y la satisfacción de sus usuarios.
- Una menor carga de trabajo del departamento de TI en la administración y gestión tecnológica permitiría a este personal centrarse en la innovación y consecuentemente incrementar el valor de la organización.

2.2 DCIS OTAN en la actualidad

Por su carácter clasificado como *Nato Restricted* este apartado estará únicamente disponible en la memoria final del trabajo fin de máster, la persona interesada deberá demostrar ante los depositarios, ser conocedor de sus responsabilidades y tener la necesidad de conocer la información para el desempeño de sus cometidos oficiales.

2.3 FMN: Federación de redes de misión

La capacidad *Federated Mission Networking* (FMN), marcará, si no lo ha hecho ya, las operaciones de la OTAN en un futuro y la manera en la que sus aliados comparten la información y se comunican con sus sistemas de mando y control (C2). Hasta tal extremo que, en un futuro no muy lejano, no tendrán cabida en las operaciones lideradas por la OTAN, aquellos países que no hayan implementado esta capacidad.

La capacidad FMN se obtiene llevando a cabo unos procedimientos, doctrina y capacidades que permiten su implementación, denominada en FMN, como instanciación, desde sus orígenes, en cualquier lugar y en un tiempo mínimo, de una red de comunicaciones e intercambio de información totalmente interoperables entre sí. Para ello, es necesario que previamente a su despliegue los procedimientos, adiestramiento y capacidades hayan sido diseñados, definidos, obtenidos, verificados, validados y probados.

FMN la conforman sus *afiliados* y no las naciones, como se pudiera pensar. El motivo es que existen naciones y organizaciones miembros de este exclusivo círculo que la componen. Actualmente existen 36 afiliados, entre los que se encuentra la OTAN como un afiliado más e incluye 6 naciones que no son miembros de la Alianza. FMN está en constante crecimiento y existen otras naciones interesadas en adherirse y que actualmente se hallan en trámite para ello. Entre estos últimos se incluye la Unión Europea como organización.

Figura 2 2: Federated Mission Network (extraído de [2])

Básicamente, ser afiliado de FMN implica el compromiso de desarrollar y mantener las capacidades FMN que se hayan acordado para desplegar o instanciar las conocidas como redes de misión y al mismo tiempo operar haciendo uso de ellas. Los afiliados deben garantizar el cumplimiento de los requisitos de adiestramiento, seguridad e interoperabilidad mediante su participación en eventos de verificación, validación, evaluaciones de seguridad y acreditación que se llevan a cabo durante diferentes pruebas y ejercicios.

3. Resultados y discusión

3.1 Inconvenientes presente DCIS OTAN

Ídem apartado 2.2.

3.2 Futuro DCIS OTAN

La OTAN se encuentra inmersa en un planeamiento de diseño y modernización de sus sistemas DCIS con el objeto de afrontar de manera

más eficaz los desafíos impuestos por el entorno actual de seguridad global. El fin primordial consiste en disponer de un DCIS que sea más ágil, menos complejo y con un coste total de la propiedad (TCO) más bajo del que posee en la actualidad.

Las nuevas amenazas a las que se enfrenta la Alianza, sumado al dinamismo del mundo actual, exigen que la OTAN reaccione de una manera más eficaz y eficiente a las diferentes misiones que se le encomienden y adaptarse de una manera ágil a los diferentes requisitos de servicios para cada misión.

Para prepararse para estas *misiones a medida*, la OTAN necesita un DCIS desplegable que permita cubrir con mayor agilidad sus necesidades de adiestramiento acorde a los numerosos ejercicios que organiza de manera periódica y al mismo tiempo respaldar las operaciones reales que surjan, con tiempos de activación más reducidos. Además, el DCIS debe estar optimizado para poder operar con comunicaciones degradadas y al mismo tiempo ser compatible con *Federated Mission Networking* (FMN), todo esto con el TCO más bajo.

Desde el punto de vista técnico, el nuevo DCIS debe de ser lo suficientemente flexible para poder implementar fácilmente los servicios desplegables necesarios y del mismo modo cambiarlos rápidamente si fuera necesario. Debe tener una *huella logística* mínima de manera que su transporte y funcionamiento en zona sean reducidos y al mismo tiempo que no sean necesarios ingenieros altamente cualificados para poder operarlos una vez desplegados. Por último, debe disponer de una alta capacidad de recuperación en caso de fallos en el sistema.

4. Prueba

4.2.1 Antecedentes

El autor ha optado por seleccionar la aproximación en hiperconvergencia de dos empresas tecnológicas de prestigio que, a su modo de ver, considera se puedan adaptar mejor a los requerimientos de la OTAN.

Indudablemente existen otras muchas opciones similares y de calidad en el mercado, que no han sido objeto de un estudio en profundidad en este trabajo y que deben ser consideradas con el objeto de obtener un resultado final idóneo.

4.2.2 Opción NetApp

Tras un estudio exhaustivo de las capacidades del sistema HCI NetApp y a modo resumen, podemos destacar lo siguiente:

- Experiencia de almacenamiento en la nube y tratamiento de los *Snapshots* para reestablecer configuraciones anteriores.
- Eficiencia de los datos de almacenamiento en lo referente a la deduplicación y compresión de los datos con su sistema operativo ONTAP.
- Flexibilidad en el escalado de nodos de cómputo y almacenamiento, de una manera totalmente independiente con el ahorro que esto supone en equipamiento y licencias.
- Simplificación en el despliegue de sus nodos y posibilidad de integrarlos con nodos de almacenamiento de otros fabricantes.
- Gestión sencilla e intuitiva desde su plataforma NDE, que no requiere de muchos conocimientos técnicos.
- Optimizado para infraestructura VDI mediante integración de adaptadores de GPU de alto rendimiento.
- Estrategia más *abierta* que sus competidores y en cierto modo agnóstica en lo referente a la implementación en la nube de aplicaciones nativas de una manera eficiente. Posibilidad de adaptarse a otras arquitecturas referenciadas como Redhat, Openstack o KVM.
- Gestión en tiempo real y de forma centralizada de los recursos IOPS para una asignación de recursos más precisa garantizando el rendimiento de las VM más sensibles.
- Dispone API *VMware vRealize Orchestrator* de acceso al portal específico de catálogo de autoservicios y que proporciona cierto automatismo a la hora de realizar las tradicionales gestiones de *ticketing*, tareas operativas y tareas de gestión, que normalmente suponen una carga de trabajo adicional al personal IT.
- Posibilidad de trabajar con plataformas de contenedores software tipo *Kubernetes* o *Dockers* mediante la herramienta *Trident* que además de ser de código abierto está especialmente diseñada para satisfacer la persistencia necesaria de este tipo de aplicaciones.

4.2.3 Opción Cisco

En lo que respecta a Cisco HyperFlex, como plataforma de gestión de su infraestructura HCI, estas son las principales características que podemos mencionar:

- Facilidad de uso de la plataforma Cisco HyperFlex que no implica grandes conocimientos específicos de cada uno de sus componentes.
- Protección y confiabilidad en los datos, el sistema HyperFlex está optimizado para la tolerancia a fallos y recuperación ante desastres.

- Variedad de opciones de despliegue en base a las necesidades de los usuarios, tanto en cómputo como almacenamiento, donde la gestión se realiza de manera sencilla y centralizada mediante su plataforma.
- Incluye Cisco Intersight como plataforma de asistencia remota en casos de necesidad. Esta herramienta permite desplegar, administrar, monitorizar los registros, cambiar la configuración e incluso trabajar con el centro de asistencia técnica de Cisco cuando exista algún problema.
- La arquitectura Cisco HyperFlex contempla el soporte a las unidades de procesamiento gráfico (GPU) tanto en la parte convergente, como de procesamiento lo que permite a los usuarios mejorar su experiencia en los despliegues con VDI.
- La plataforma de Cisco también incluye el soporte para múltiples hipervisores, lo que supone que esta arquitectura no esté vinculada a una única solución de hipervisor.
- Contempla el soporte para aplicaciones de datos persistentes con contenedores tipo *Docker* administrados por *Kubernetes*, administración de datos en forma de replicación, compresión en línea, soporte de clones y *Snapshots*.

5. Conclusiones

A lo largo del análisis del inventario DCIS OTAN, hemos podido comprobar que su función principal es facilitar a los comandantes de la NRF y VJTF realizar el mando y control (C2) con sus unidades subordinada y al mismo tiempo recibir directivas de sus mandos desde los cuarteles generales estáticos.

En el trabajo se ha podido constatar que los medios actuales DCIS con los que cuenta la OTAN son voluminosos, pesados y no son acordes a las necesidades actuales de la Alianza. Del mismo modo, se ha comprobado que previo al despliegue, el proceso de instalación y configuración del actual DCIS es lento y complejo, además de requerir demasiado personal especializado e ingenieros civiles, tanto para su mantenimiento como para su alistamiento, lo que obliga a depender de personal muy técnico en las zonas de operaciones.

El futuro DCIS OTAN deberá simplificar significativamente la huella logística y los medios necesarios para su despliegue, el proceso de instalación y configuración previo al despliegue, debe ser rápido, ágil y sencillo de manera que pueda adaptarse rápidamente de un modelo operacional a otro de adiestramiento y viceversa. El DCIS OTAN debe permitir a sus elementos despegables ejecutar eficazmente las operaciones que se le asignen en un entorno altamente dinámico e interoperable con naciones aliadas y otros organismos desplegados en la zona de operaciones.

Los futuros nodos desplegables de la OTAN deben mejorar la eficiencia en el uso de los recursos mediante la consolidación de servidores, redes y almacenamiento, tal y como nos proporciona la hiperconvergencia. Esta tecnología permitirá facilitar las tareas de administración y seguridad y al mismo tiempo aislar los diferentes entornos como son el desarrollo y la producción de los mismos.

El próximo DCIS, debe contemplar la posibilidad de adaptarse al limitado ancho de banda disponible, en muchas ocasiones en zonas de operaciones, como resultado de un entorno electromagnético saturado y una alta dependencia de las comunicaciones SATCOM y conexión inalámbrica terrestre desplegable. Tanto su conectividad como movilidad deben ser las ideales, basados en un DCIS definido por software basado una infraestructura en la nube modelo *Infraestructura como Servicio (IaaS)* de una manera orquestada que permita automatizar en gran medida sus tareas más rutinarias descargando de estos cometidos a sus administradores.

El nuevo modelo debe capturar todos los requisitos de federación de redes FMN tanto en arquitectura, implementación, así como verificación y validación.

En lo que respecta a seguridad debería estar implementada por diseño y adaptada a un escenario actual y realista, aplicando el concepto de utilizar las mismas habilidades que un adversario emplearía contra la Alianza, es decir, *piensa como un hacker*. Asimismo, la arquitectura debe ser *Multi-Tenancy* y contemplando la jerarquía de usuarios en materia de seguridad y necesidad de conocer.

Las dos opciones que se han analizado en este trabajo podrían adaptarse a las necesidades de la OTAN, ambas presentan ventajas e inconvenientes respecto a sus competidores, la decisión final de estas y otras posibles opciones estará influenciada principalmente por las necesidades de los usuarios finales, en nuestro caso la *comunidad operativa* de la OTAN y por grupos de trabajo formado por especialistas militares en materia TIC, la propia NCIA y representantes de las diferentes grandes compañías tecnológicas.

Conviene recalcar, que este documento debiera ser constantemente actualizado y de alguna manera estar *vivo*, ya que los avances y desarrollos que están llevando los diferentes fabricantes, en materia de hiperconvergencia, es constante y es muy probable que a corto plazo surjan nuevos desarrollos que se puedan adaptar mejor a las necesidades de la OTAN.

En base a lo anterior, considero que sería una buena opción que la OTAN no se decidiera por una única aproximación, en su lugar debería abordar la situación de una manera colectiva, procurando realizar un estudio de manera conjunta donde los distintos fabricantes pudieran aportar ideas, así como lo mejor de sus tecnologías, con el objeto que el resultado final sea un nodo desplegable idóneo y adaptado a la tecnología más vanguardista existente hasta la fecha.

Referencias:

[1] G. C. Piella, (2020) «Lecciones identificadas y nuevos condicionantes para el planeamiento de la Defensa Nacional,» Revista General de Marina, pp. 799-810.

[2] Wikipedia, «Diagrama de casos de uso,» 24 10 2020. [En línea]. Disponible: https://es.wikipedia.org/wiki/Diagrama_de_casos_de_uso. [Último acceso: 05 01 2021]

[3] Wikipedia, «Estado del arte» 7 mayo 2020. [En línea]. Disponible: https://es.wikipedia.org/wiki/Estado_del_arte. [Último acceso: 05 01 2021]

[4] M. Haag, (2018). Infraestructura hiperconvergente para Dummies, New Jersey: Wiley.

[5] NATO Federated Mission Networking Implementation Plan Vol. I, 2015.

Presente y Futuro de los Nodos Desplegables.

Estudio de la viabilidad de la tecnología HCI para albergar servicios clasificados/no clasificados de la OTAN a los nodos de misión desplegables

Autor: Fernando Liaño Núñez

Director/es: Milagros Fernández Gavilanes

Los cambios que ha experimentado la Organización del Tratado del Atlántico Norte (OTAN) en los últimos años han sido significativos, estos cambios han tenido un especial impacto en lo referente a los Sistemas de Comunicaciones e Información (CIS), no solo en lo concerniente al mantenimiento de esta capacidad sino también, en lo relativo a futuros programas de desarrollo, como es el caso de medios CIS desplegables (DCIS).

Los medios DCIS deben proporcionar a la NRF y otras fuerzas expedicionarias aliadas de una capacidad segura, modular, escalable, desplegable y sostenible, que proporcione los servicios de información entre los mismos elementos desplegados y las redes estratégicas de los Cuarteles Generales estáticos .

Los avances tecnológicos en virtualización e hiperconvergencia, pueden convertirse en la mejor opción para obtener esta capacidad DCIS, acordes a las nuevas amenazas y nuevos retos a los que se enfrenta la Alianza en una situación geopolítica global dinámica y cambiante.

Dentro de las diferentes infraestructuras hiperconvergentes desarrolladas por los diferentes fabricantes tecnológicos reconocidos, NetApp y CISCO, han demostrado ser dos soluciones factibles para esa modernización necesaria en los medios DCIS de la OTAN.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2020/2021

Simulación de un ataque de *ingeniería social* para el robo de credenciales mediante *Social Engineer Toolkit*

Autor: Maíllo Fernández, Juan Andrés (jmaifer@et.mde.es)
Director/es: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – La ciberdelincuencia gana peso año tras año en el volumen total de infracciones que se cometen, tanto en España como en el resto del mundo. La gran revolución que han supuesto las TIC en el mundo actual en el que vivimos, unido a las facilidades que les han proporcionado a los delincuentes, han creado el caldo de cultivo perfecto para que hoy en día tengamos que ser más precavidos ante un robo en Internet que cuando salimos a la calle.

Y dentro de este escenario, los delitos más comunes son los relacionados con los fraudes informáticos, especialmente aquellos que tienen que ver con los robos de credenciales de los usuarios en los servicios *on-line*, aquello que denominamos *Phishing*.

Es sumamente importante que tanto los responsables de seguridad como los propios usuarios estén familiarizados con este tipo de ataques, su *modus operandi* y sus consecuencias, para que sean capaces de detectarlos antes de llegar a ser víctimas de ellos.

A lo largo de este trabajo se abordarán cuestiones relativas a la ciberseguridad en el ámbito de los ataques mediante *ingeniería social*, proporcionando al lector una visión global del problema que suponen y estudiando el funcionamiento de los mismos mediante una simulación de ataque con *Social Engineer Toolkit*, de modo que consiga adquirir las capacidades necesarias para saber cuándo está siendo objetivo de un intento de fraude.

Palabras clave: seguridad de la información, ingeniería social, robo de credenciales, *Social Engineer Toolkit, Phishing*

1. Introducción

1.1. Motivación y objetivos

La aparición y la gran expansión que han experimentado las TIC en el mundo actual durante los últimos años han producido grandes cambios en nuestra vida diaria, tanto en el ámbito laboral como en el personal. Pero a pesar de habernos aportado grandes ventajas, también han traído consigo bajo el brazo nuevas amenazas a las que debemos hacer frente para salvaguardar nuestra seguridad.

Los delincuentes también han sabido aprovechar las nuevas tecnologías para cometer sus crímenes, y se han adaptado con rapidez a este nuevo paradigma al darse cuenta de las enormes posibilidades que les ofrecían.

Esta circunstancia obliga a empresas y organismos a invertir gran cantidad de recursos en la seguridad de sus sistemas digitales que los hace cada vez más resistentes a posibles acciones malintencionadas. Pero hay un elemento dentro de todo el conjunto que sigue siendo el más débil, y por lo tanto uno de lo más explotados: las personas.

Ante esta situación, se hace tremendamente importante conocer el modo de actuación que siguen los cibercriminales en este tipo de ataques, de modo que tanto los usuarios como los administradores de los sistemas de información sean conscientes de los graves riesgos a los que están expuestos y tengan la capacidad de protegerse.

Para ello, los objetivos que se persiguen en el presente trabajo fin de máster son los siguientes:

- Estudiar la situación actual de la ciberdelincuencia en España, incluyendo los tipos de ataques más habituales que se producen.
- Introducirnos en los ataques de *ingeniería social*, especialmente en aquellos que tienen como propósito el robo de credenciales de usuarios.
- Conocer las capacidades y funcionamiento de la herramienta SET (*Social Engineer Toolkit*), y profundizar en las opciones que ofrece para realizar el tipo de ataques que estamos estudiando.
- Realizar una simulación de un ataque, dentro de un entorno controlado, explicando el proceso del mismo.
- Analizar los resultados obtenidos, extrayendo de los mismos las conclusiones principales que nos aporten.
- Estudiar las posibles aplicaciones que podría tener este trabajo en el entorno del Ministerio de Defensa.

1.2. Situación de la ciberdelincuencia en España

Tal y como puede comprobarse en la figura 1, el porcentaje que supone los crímenes de tipo cibernético dentro del total de las acciones delictivas cometidas en España aumenta año tras año.

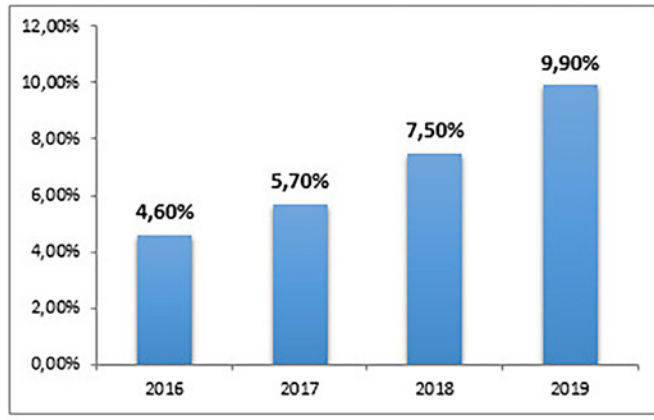


Figura 1. Evolución del porcentaje que representa la cibercriminalidad sobre el total de infracciones penales en España [1]

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	**92.716**	**117.399**	**160.729**	**218.302**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

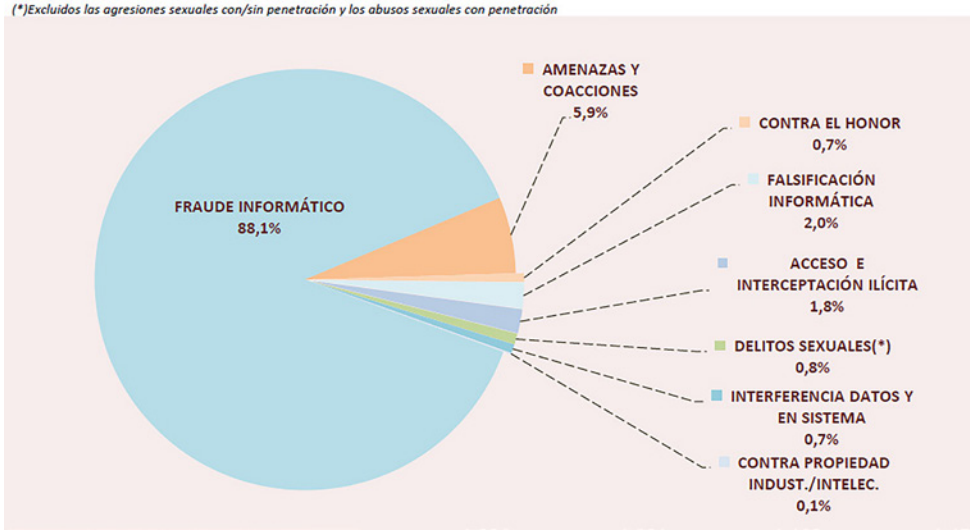


Figura 2. Evolución de hechos conocidos por categorías delictivas. Imagen extraída del estudio sobre la cibercriminalidad en España de la Secretaría de Estado de Seguridad [1]

Y de entre todos ellos, sin lugar a dudas el más común de todos ellos es el fraude informático, que como se puede comprobar en la figura 2 supuso casi un 90 % del total en 2019, experimentando un aumento del 50 % respecto al año anterior.

Uno de los métodos más extendidos para llevar a cabo este tipo de ataques consiste en el robo de las credenciales de acceso a los sistemas de los usuarios. Y para ello los delincuentes cuentan con una disciplina que les aporta grandes resultados en este sentido: la *ingeniería social*.

1.3. Introducción a la ingeniería social

Se puede definir la ingeniería social como el arte de obtener información de personas sin que estas sean conscientes de lo que están haciendo, para lo cual se recurre a engaños, técnicas psicológicas y habilidades sociales. Un atacante con buenas dotes para esta disciplina puede obtener gran cantidad de información de un usuario sin que este sea consciente de lo que está sucediendo en realidad.

El padre de la ingeniería social, Kevin Mitnick, enumera cuatro principios básicos innatos al ser humanos en los que se basa cualquier acción de ingeniería social para lograr sus objetivos [2]:

- Todos queremos ayudar.
- El primer impulso hacia alguien que no conocemos es de confianza hacia él.
- A nadie le gustar decir no.
- A todos nos gusta que nos adulen.

Para ello se pondrán en práctica diferentes técnicas que actúan sobre el propio comportamiento humano, llevadas a cabo por el propio atacante como el *pretexting*, el *quid pro quo* o el *tailgating* (entre otros), o con ayuda de herramientas digitales como sucede en el caso que vamos a estudiar para un ataque de *Phishing* [3].

2. Desarrollo

Para comprobar la eficacia de este tipo de ataques, y comprender mejor el funcionamiento de los mismos, se llevará a cabo una simulación de un robo de credenciales [4], utilizando para ello una plataforma virtualizada mediante VirtualBox [5] donde desplegaremos una máquina virtual con Kali Linux [6] (distribución orientada a pruebas de *pentesting*) que hará las veces de atacante, y utilizando el sistema anfitrión con Microsoft Windows 10 como víctima.

Dentro de la máquina con Kali Linux, se recurre a la herramienta *Social-Engineer Toolkit* [7], una completa suite desarrollada con Phyton que nos ofrece múltiples funcionalidades para automatizar ataques mediante ingeniería social.

En nuestro caso vamos a emplear una opción que nos permitirá llevar a cabo un ataque de *Web Spoofing* de un modo muy sencillo [8] y [9], creando una copia idéntica de una web de login a la que haremos llegar a nuestra víctima para que intente acceder al servicio.

Una vez el usuario haya introducido sus credenciales, estas serán recogidas automáticamente en SET dentro de Kali Linux (véase figura 3) y la víctima será redirigida a la página real que ha sido clonada.

Figura 3. Resultado del robo de credenciales en la simulación del ataque de phishing

De este modo es muy posible que piense que se ha producido un fallo en el proceso de autenticación y vuelva a meter su nombre de usuario y su contraseña, accediendo esta vez sí al servicio y (muy probablemente) sin ser consciente en ningún momento de haber sido víctima de un ataque de *phishing*.

3. Resultados y discusión

Después de llevar a cabo la simulación, somos conscientes de lo sencillo que puede resultar a un cibercriminal poner en práctica esta técnica para intentar hacerse con las credenciales de acceso de los usuarios de los servicios web. En tan solo unos pasos, y apoyándose en herramientas como SET, se puede crear un clon idéntico del sistema a suplantar para lanzar el ataque.

Afortunadamente para los usuarios, estas herramientas no son perfectas, y si prestamos un poco de atención a los detalles podremos ser capaces de detectar en muchas ocasiones que el sitio web al que nos han enviado no es el real y estamos siendo víctimas de un *phishing*. Pero de todos modos no debemos bajar la guardia, ya que los atacantes cada vez perfeccionan más sus acciones y resulta más complicado detectarlas.

Métodos como los ataques homográficos para conseguir que la URL del sitio clonado se parezca a la real, la incorporación de certificados digitales para implementar la web con protocolo HTTPS, o la distribución de enlaces a nuestro *website* malicioso con pretextos bien diseñados y técnicas de suplantación de remitentes, nos dificultarán la labor de detección de este tipo de fraudes.

4. Conclusiones

Las implicaciones que un robo de credenciales puede tener en la seguridad de nuestros sistemas es más que evidente. Si alguien

no autorizado consigue tener acceso a un determinado servicio, las consecuencias pueden ir desde un robo en la cuenta de banca *on-line* de un usuario, hasta la revelación de información clasificada en el caso de los sistemas del Ministerio de Defensa.

Teniendo en cuenta la gran proliferación que existe actualmente de este tipo de ataques, se hace completamente necesario invertir mayores esfuerzos en protegernos contra ellos [10] y [11], para lo cual se establecen las siguientes líneas futuras de trabajo:

- Securización de las aplicaciones, exigiendo la implementación de la autenticación por doble factor, aumentado de este modo la seguridad en los procesos de login de los servicios web.
- Despliegue de sistemas contra intrusiones en nuestra infraestructura de red (IDS, IPS y/o SIEM), que dificultarán el acceso de personas no autorizadas a la misma y nos avisará en caso de que llegue a producirse para poder minimizar daños.
- Establecimiento de políticas robustas de cambio de contraseñas, obligando a los usuarios al cambio de las mismas cada cierto tiempo, de modo que si un atacante consigue robar sus credenciales únicamente le sean de utilidad hasta el siguiente cambio.
- Implementar una campaña de información y concienciación entre los usuarios de los sistemas de nuestra organización, dando a conocer los métodos de ataques más habituales y los riesgos que pueden correr en caso de ser víctimas de uno de ellos.

Referencias

[1] «Web del Ministerio del Interior» [En línea]. Disponible: http://www.interior.gob.es. [Último acceso: 16 de noviembre de 2020]

[2] K. Mitnick, (2017). El arte de la intrusión, Editorial Ra-Ma.

[3] A. Ramos, C. A. Barbero, D. Marugán e I. González, (2015). Hacking con Ingeniería Social. Técnicas para hackear humanos, Editorial Ra-Ma.

[4] P. González, (2015). Ethical Hacking. Teoría y práctica para la realización de un pentesting, Editorial OxWORD.

[5] «Web de Oracle VM Virtual Box» [En línea]. Disponible: https://www.virtualbox.org. [Último acceso: 19 de noviembre de 2020]

[6] «Web de Kali Linux,» [En línea]. Disponible: https://www.kali.org. [Último acceso: 19 de noviembre de 2020]

[7] «Web de Social Engineering Toolkit» [En línea]. Disponible: https://github.com/trustedsec/social-engineer-toolkit. [Último acceso: 24 de noviembre de 2020]

[8] P. González, G. Sánchez y J. M. Soriano, (2015). Pentesting con Kali 2.0, Editorial OxWORD.

[9] M. A. Caballero y D. Cilleros, (2018) El libro del hacker. Edición 2018, Ediciones Anaya Multimedia.

[10] «Web de la Oficina de Seguridad del Internauta» [En línea]. Disponible: https://www.osi.es. [Último acceso: 17 de diciembre de 2020]

[11] «Web del Instituto Nacional de Ciberseguridad» [En línea]. Disponible: https://www.incibe.es. [Último acceso: 17 de diciembre de 2020]

Simulación de un ataque de ingeniería social para el robo de credenciales mediante SOCIAL ENGINEER TOOLKIT

Autor: Juan Andrés Maíllo Fernández
Director/es: Miguel Rodelgo Lacruz

Universidad de Vigo

La aparición y gran éxito que han tenido las TIC en los últimos años han cambiado el mundo tal y como lo conocíamos hasta ahora. Nos relacionamos, trabajamos y nos entretenemos de un modo diferente a como lo hacían nuestros padres y abuelos.

Los métodos usados por los criminales para cometer sus delitos también ha mutado a lo largo de estos años, y nos vemos sometidos a nuevas amenazas que hace un tiempo no éramos capaces ni de imaginar.

Uno de los tipos más comunes de ciberdelitos es el conocido como Phishing, que mediante el uso de la Ingeniería Social busca que la víctima realice una determinada acción sin ser consciente de ello.

Debemos estar lo más protegidos posible ante este tipo de ataques, para lo cual es imprescindible conocer cómo funcionan.

Pongámonos en la mente de estos criminales, y comprendamos su forma de pensar y actuar para aprender a esquivarlos.

Gestión de la seguridad de la información manejada en un centro de trabajo

Autor: Martinez Tamargo, Vanesa (vmtamargo@fn.mde.es)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – La Jefatura de Sistemas Satelitales y Ciberdefensa se encuadra en la Subdirección General de Programas de la Dirección General de Armamento y Material del Ministerio de Defensa. Se crea en febrero de 2020 con el fin de impulsar, realizar un seguimiento y controlar la gestión, realizada por las Oficinas de Programa (OOPP) y en colaboración con las FAS, de los programas de obtención, de modernización y de sostenimiento común de sistemas satelitales y de ciberdefensa, asegurando su necesaria uniformidad e interoperabilidad. No obstante, dada la transversalidad la jefatura, surge una nueva necesidad como apoyo al resto de jefaturas de la SDG programas, y otros organismos que se determinen, en la consideración de aspectos relativos a ciberdefensa en los programas de sus ámbitos de competencia.

Ante la creación de la misma, se hace necesaria la implementación de unos procedimientos de trabajo con el fin de asegurar la trazabilidad de la documentación manejada en el mismo y para securizar dicha información. Mediante el presente trabajo de fin de máster se pretende cubrir este reto.

El centro de trabajo tendrá unos requisitos mínimos de seguridad que se desarrollarán en diferentes entornos de seguridad.

Los entornos de seguridad serán:

- Entorno global de seguridad del centro de trabajo.
- Entorno local de seguridad del centro de trabajo.
- Entorno electrónico de seguridad del centro de trabajo.

Además de las medidas de seguridad de un edificio, cada entorno de seguridad tendrá unas medidas particularizadas que se desarrollarán en función de unos riesgos particularizados.

Una vez estos riesgos sean gestionados, se establecerán una serie de procedimientos de seguridad básicos, los cuales podrán ser ampliados según las necesidades tanto de la documentación como del entorno de seguridad en sí mismo.

Los procedimientos básicos que se tratarán en este trabajo son los siguientes:

- Procedimiento de alta y baja de usuarios.
- Procedimiento de medidas de seguridad a adoptar por el personal no usuarios del sistema clasificado.
- Procedimiento de seguridad documental del sistema clasificado.
- Procedimiento de seguridad TIC.
- Procedimiento de gestión de incidentes de seguridad.
- Procedimiento de auditoria y gestión interna de la seguridad.

Palabras clave: seguridad, información, riesgos, incidente, medidas.

1. Introducción

En febrero de 2020 se crea la Jefatura de Sistemas Satelitales y Ciberdefensa (JSSAT&CIBER) con un cometido principal que es común a todas las jefaturas de los programas de armamento y material, enfocado en este caso a los sistemas satelitales y de ciberdefensa: «Impulso, seguimiento y control de la gestión, realizada por las Oficinas de Programa (OOPP) y en colaboración con las FAS, de los programas de obtención, de modernización y de sostenimiento común de sistemas satelitales y de ciberdefensa, asegurando su necesaria uniformidad e interoperabilidad«.

No obstante, dada la transversalidad de la ciberdefensa, se consideró conveniente añadir un segundo cometido, definido como «apoyo al resto de Jefaturas de la SDG de Programas, y otros organismos que se determinen, en la consideración de aspectos relativos a ciberdefensa en los programas de sus ámbitos de competencia». Señaló, así mismo, que esta segunda misión no estaba oficializada todavía, al no figurar en la Instrucción de Organización de la DGAM.

El objetivo principal de este trabajo es la descripción de los diferentes entornos reales de seguridad en un centro de trabajo en el que se maneja información con diferentes grados de clasificación, los requisitos y medidas de seguridad requeridas para su protección.

Por ello se hace necesario establecer una metodología de trabajo además de una serie de procedimientos para el manejo de la información con un nivel determinado de clasificación al tratarse de sistemas de armas, en este caso se generaliza, aunque los sistemas de armas en los que se incluye contenido para la *ciberdefensa* se puede decir que su contenido si cabe se puede clasificar como *altamente sensible*.

Con este fin se proponen los siguientes objetivos específicos:

- Estudio de la normativa actual y su aplicabilidad.
- Análisis de los siguientes condicionantes:

    1. Identificación de los requisitos de seguridad necesarios de acuerdo a la normativa aplicable.
    2. Identificación de los entornos de seguridad.
    3. Identificación de medidas de seguridad a implantar.
    4. Identificación y autentificación.
    5. Registros.
    6. Salvaguarda de la información y datos.
    7. Salvaguarda de la integridad y disponibilidad.
    8. Salvaguarda sobre el HW y SW.

9. Salvaguarda sobre las comunicaciones.
10. Salvaguarda sobre la reutilización de elementos.
11. Auditorias.
12. Administración de la seguridad.

Estos condicionantes nos dan lugar a la redacción de una serie de procedimientos de acuerdo a cumplir los requisitos específicos de cada uno de ellos, estos serán los siguientes:

- Procedimiento de alta y baja de usuarios.
- Procedimiento de medidas de seguridad a adoptar por el personal no usuarios del sistema clasificado.
- Procedimiento de seguridad documental del sistema clasificado.
- Procedimiento de seguridad TIC.
- Procedimiento de gestión de incidentes de seguridad.
- Procedimiento de auditoria y gestión interna de la seguridad.

2. Desarrollo

El trabajo incluye el análisis de:

- El centro de trabajo, el cual estará compuesto tanto de estaciones de trabajo, servidores dedicados, aplicaciones SW, periféricos y equipamiento de red tanto local como externa y WAN-PG, soportada por los sistemas de telecomunicaciones del Ministerio de Defensa.

— Descripción de los niveles de clasificación de la información.

— Tipos de usuarios del centro de trabajo, estos deberán estar en posesión de la Habilitación Personal Seguridad (HPS) de acuerdo a la información que han de manejar.

— Requisitos mínimos de seguridad del centro de trabajo.

— Análisis de las posibles amenazas y vulnerabilidades asociadas a diversos factores.

- Los diferentes entornos de seguridad, catalogándolos de acuerdo a la información que se va a manejar y dónde se va archivar.

Como resultado se establecerán:

- Medidas de seguridad del entorno perimetral teniendo en cuenta el control de accesos. En función de los riegos detectados, se decretarán e implantarán distintos controles asociados a dichos riesgos.
- Medidas para identificar y autentificar a los usuarios del sistema de acuerdo a los riesgos identificados.

- Un registro de las acciones derivadas del manejo de la información de acuerdo a los riesgos reconocidos.
- La salvaguarda de la información y datos de acuerdo a los riesgos identificados.
- Una garantía de la integridad y disponibilidad de la información de acuerdo a los riesgos detectados.
- Las salvaguardas adecuadas asociadas a HW y SW.
- Una serie de salvaguardas de las comunicaciones en los diferentes entornos de seguridad.
- Una serie de salvaguardas sobre la reutilización de elementos.
- Una serie de auditorías periódicas del sistema.
- Procedimientos para la administración del sistema.
- Un procedimiento con el fin de controlar la altas y bajas de los usuarios.
- Un procedimiento con el fin de establecer la seguridad documental necesaria para un sistema clasificado.
- Un procedimiento con el fin de asegurar la seguridad de las TIC.
- Un procedimiento de gestión de los posibles incidentes de seguridad.
- Un procedimiento de auditorías tanto internas como externas.

3. Resultados y discusión

Los resultados del presente trabajo se pueden aplicar en cualquier centro de trabajo real que maneje información con diferentes grados de clasificación.

No obstante, cada uno de ellos se particularizará para la Jefatura de Sistemas Satelitales y Ciberdefensa.

De esta manera se cubre el objetivo de asegurar la trazabilidad de la documentación manejada en el mismo y para securizar la información que se maneja en el centro de trabajo.

Estos procedimientos son los mínimos a aplicar, pudiendo en un futuro ampliarlos conforme sea necesario y requerido.

4. Conclusiones

Con el presente trabajo se cubren los objetivos iniciales que se planteaban:

— Se han identificación de los requisitos de seguridad necesarios de acuerdo a la normativa aplicable.

— Se han identificado y analizado los diferentes entornos de seguridad.

— Se han definido y procedimentado las medidas de seguridad a implantar.

- Se ha definido y procedimentado el proceso de autentificación.
- Se han definido y procedimentado los registros mínimos.
- Se ha definido y procedimentado la salvaguarda de la información y datos.
- Se ha definido y procedimentado la salvaguarda de la integridad y disponibilidad.
- Se ha definido y procedimentado la salvaguarda sobre el HW y SW.
- Se ha definido y procedimentado la salvaguarda sobre las comunicaciones.
- Se ha definido y procedimentado la salvaguarda sobre la reutilización de elementos.
- Se ha definido y procedimentado auditorías.
- Se ha definido y procedimentado como se ha de administrar la seguridad.

De esta manera se ha cumplido el objetivo de establecer una metodología de trabajo a partir de una serie de procedimientos para el manejo de la información con un nivel determinado de clasificación asegurando la trazabilidad de la documentación manejada con el fin de securizarla a través de la delimitación los diferentes entornos de seguridad que se pueden dar en un centro de trabajo. Se han identificación de los posibles riesgos que se pueden dar anulándolos o mitigándolos y se han analizado y aplicado la normativa actual vigente.

Agradecimientos

A Miguel Rodelgo por su eterna comprensión al aceptar ser tutor de este trabajo.

A mi familia, por todo el tiempo que no les he dedicado, su paciencia y colaboración aliviando las tareas cotidianas, siempre o casi siempre, con una sonrisa.

Al profesorado del máster; nos ha tocado vivir un curso inusual debido a esta pandemia, han intentado sacar siempre lo mejor de todo el alumnado, tratando de colaborar y apoyar en situaciones complicadas tanto a nivel personal, laboral o académicas con el mejor talante y dedicación.

A mis compañeros del máster, hemos hecho de un grupo de gente independiente de muy diversa índole y procedencia, un grupo de amigos.

Referencias

[1] Norma CCN-STIC-001 - Seguridad de las Tecnologías de la Información y las Comunicaciones que maneja Información Clasificada en la Administración.

[2] Norma CCN-STIC-152-Evaluación y Clasificación de Zoning Locales (DL) (clasificada).

[3] Norma CCN-STIC-202-Estructura y Contenido Declaración de Requisitos Seguridad.

[4] Norma CCN-STIC-301-Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados.

[5] Norma CCN-STIC-305-Destrucción y sanitización de soportes informáticos.

[6] Norma CCN-STIC-403-Gestión Incidentes de Seguridad.

[7] Norma CCN-STIC-404-Control de soportes informáticos.

[8] Norma CCN-STIC-430-Herramientas de Seguridad.

[9] Riesgos de los Sistemas de Información (MAGERIT I, II y III).

Gestión de la Seguridad de la información manejada en un centro de trabajo

Autor: Vanesa MartÍnez Tamargo
Director: Miguel Rodelgo Lacruz

Introducción

La Jefatura de Sistemas Satelitales y Ciberdefensa encuadrada en la Subdirección General de Programas de la Dirección General de Armamento y Material del Ministerio de Defensa se crea en febrero de 2020 con el fin de impulsar, realizar un seguimiento y controlar la gestión, realizada por las Oficinas de Programa (OOPP) y en colaboración con las FAS, de los programas de obtención, de modernización y de sostenimiento común de sistemas satelitales y de ciberdefensa. Ante la creación de la misma, se hace necesaria la implementación de unos procedimientos de trabajo con el fin de asegurar la trazabilidad de la documentación manejada en el mismo y para securizar dicha información

Metodología

El Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo, basándonos en la normativa establecida como autoridad nacional se crean los procedimientos básicos para el manejo de información clasificada en un centro de trabajo tipo.

Agradecimientos

A Miguel Rodelgo por su eterna comprensión al aceptar ser tutor de este trabajo.
A mi familia, por todo el tiempo que no les he dedicado, su paciencia y colaboración aliviando las tareas cotidianas, siempre o casi siempre, con una sonrisa.
Al profesorado del Máster; nos ha tocado vivir un curso inusual debido a esta pandemia, han intentado sacar siempre lo mejor de todo el alumnado, tratando de colaborar y apoyar en situaciones complicadas tanto a nivel personal, laboral o académicas con el mejor talante y dedicación.
A mis compañeros del Máster, hemos hecho de un grupo de gente independiente de muy diversa índole y procedencia, un grupo de amigos.

Resultados

Se han gestionado los posibles riesgos a los que centro se puede someter y se han establecido una serie de procedimientos de seguridad básicos, los cuales podrán ser ampliados según las necesidades tanto de la documentación como del entorno de seguridad en sí mismo, los cuales son:.

- Entorno Global de seguridad del centro de trabajo.
- Entorno Local de seguridad del centro de trabajo.
- Entorno Electrónico de seguridad del centro de trabajo.

Conclusiones

Con el presente trabajo se cubren los objetivos iniciales que se planteaban:

- Se han identificación de los requisitos de seguridad necesarios de acuerdo a la normativa aplicable.
- Se han identificado y analizado los diferentes entornos de seguridad.
- Se han definido y procedimentado las medidas de seguridad a implantar.
- Se ha definido y procedimentado el proceso de autentificación.
- Se han definido y procedimentado los registros mínimos.
- Se ha definido y procedimentado la salvaguarda de la información y datos.
- Se ha definido y procedimentado la salvaguarda de la integridad y disponibilidad.
- Se ha definido y procedimentado la salvaguarda sobre el HW y SW.
- Se ha definido y procedimentado la salvaguarda sobre las comunicaciones.
- Se ha definido y procedimentado la salvaguarda sobre la reutilización de elementos.
- Se ha definido y procedimentado auditorías.
- Se ha definido y procedimentado cómo se ha de administrar la seguridad.

Arquitectura de referencia única para la gestión de la información y el conocimiento en el Ministerio de Defensa (AR GIC)

Autor: Peña Ramos, Rubén de la, (rdelram@fn.mde.es)
Director: Álvarez Sabucedo, Luis (externo.lsabucedo@cud.uvigo.es)

Resumen – El presente trabajo de fin de máster (TFM) propone una arquitectura de referencia única para la Gestión de la Información y del Conocimiento (AR GIC) en el Ministerio de Defensa, centrándose en el desarrollo de los aspectos principales de una arquitectura, con especial énfasis en las capacidades tecnológicas y en los servicios que las soportan.

Por su naturaleza de arquitectura de referencia, la AR GIC desarrolla las capacidades CIS/TIC identificadas en la AG CIS/TIC y ofrece las guías y especificaciones para el desarrollo de las arquitecturas objetivo del nivel inferior. Para ello, identifica y describe los sistemas CIS/TIC necesarios para proporcionar dichas capacidades CIS/TIC.

Además, la AR GIC desarrolla cada una de las 11 áreas que deben cubrirse para gestionar apropiadamente el ciclo de vida de los datos, información y conocimiento dentro del MDEF. Dichas áreas se basan en las Áreas de Conocimiento definidas en el modelo de referencia de gestión de datos DAMA-DMBOK2, adaptadas y ampliadas a la casuística y particularidades del MDEF.

La AR GIC propuesta tiene como referente técnico la arquitectura de referencia del NIST (*National Institute of Standards and Technology*) conocida como NIST *Big Data Reference Architecture* (NBDRA), la cual ha sido elaborada por el NIST *Big Data Public Working Group* (NBD-PWG) *Reference Architecture Subgroup.*

Para la elaboración de la AR GIC, y tal y como recoge la política CIS/TIC en su artículo 7.3.a), se ha adoptado el modelo homologado de arquitecturas de la OTAN en vigor, NATO *Architecture Framework Version 4* (NAFv4).

Palabras clave: arquitectura de referencia, gestión de la información y del conocimiento, I3D, NAF, DAMA.

1. Introducción

El objeto del presente trabajo de fin de máster (TFM) es proponer la arquitectura de referencia única para la Gestión de la Información y del Conocimiento (AR GIC) en el Ministerio de Defensa, centrándose en el desarrollo de los aspectos principales de una arquitectura, con especial énfasis en las capacidades tecnológicas y en los servicios que las soportan, empleando el marco metodológico del NATO *Architecture Framework, versión 4* (NAFv4) [6].

El objetivo final será la definición de una arquitectura que dará soporte a un sistema estratégico, consistente, integral y único de gestión de la información y conocimiento en el ámbito de la infraestructura integral de información para la Defensa (SGIC I3D) en el que estarán integradas el conjunto de herramientas necesarias para gestionar la información a través del empleo del modelo de datos oportuno, proporcionando a su vez los servicios CIS/TIC de seguridad y control de acceso a la información y las aplicaciones necesarios para su correcta gestión y explotación.

Para ello, esta arquitectura de referencia deberá cumplir los siguientes objetivos:

- Desarrollar las capacidades CIS/TIC necesarias para la GIC.
- Identificar y describir los servicios CIS/TIC necesarios para proporcionar dichas capacidades CIS/TIC.
- Identificar y describir los nodos lógicos (elementos de capacidad), actividades e intercambios de recursos/información necesarios para levar a cabo tanto las misiones operativas como los procesos de negocio del MDEF.
- Identificar y describir los recursos físicos que contribuyen al desarrollo de las capacidades GIC, a través de la implementación de los servicios GIC y de los nodos lógicos.
- Ofrecer guías y especificaciones para el desarrollo de las arquitecturas objetivo del nivel inferior.
- Servir de referencia para el desarrollo de la coordinación en materia GIC, y para alcanzar los objetivos y medidas de la estrategia de la información corporativa.

Para la obtención de la arquitectura se seguirá un enfoque basado en las siguientes premisas:

- Alineamiento con la política CIS/TIC [5], la arquitectura global CIS/TIC [1] el Plan estratégico de los sistemas y tecnologías de la información y las comunicaciones (PECIS) [7] y la Política de seguridad de la información del Ministerio de Defensa [8], extrayendo de estos los requisitos de alto nivel y profundizando en la definición de sus conceptos tecnológicos cuando se considere necesario para los propósitos de este documento.

- Desarrollo de la estrategia de la información del Ministerio de Defensa [9], y elaboración regida por las directrices de la instrucción para la coordinación de la gestión de la información y del conocimiento en el Ministerio de Defensa [10].
- Análisis de los requisitos y capacidades operativas que espera satisfacer la arquitectura propuesta a partir de las áreas de conocimiento de DAMA-DMBOK2 [2].
- Identificación y caracterización de las capacidades tecnológicas, los servicios, los nodos lógicos y los recursos físicos, y sus relaciones y estructura, requeridos para satisfacer los requisitos y capacidades operativas, a partir de los establecido en la arquitectura de referencia del NIST (NBDRA, NIST *Big Data Reference Architecture)* [3].
- Adopción del NATO *Architecture Framework Version 4* (NAFv4) [6] para el modelado de la arquitectura, tal y como se establece en el artículo 7.3.a) de la política CIS/TIC [5].

2. Desarrollo

A continuación, se presentan los componentes que forman parte del presente TFM:

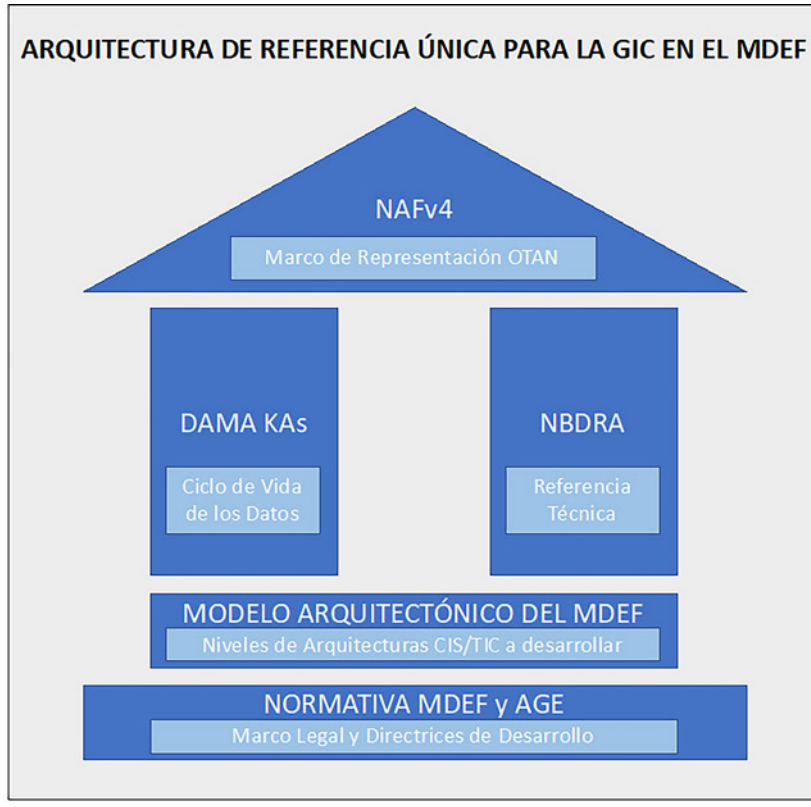


Figura 1. Componentes de la AR GIC

- La base la compone el resumen normativo en el ámbito GIC (Ministerio de Defensa y Administración General del Estado), encargado de definir el marco legal y establecer directrices en el desarrollo de la AR GIC.
- Un escalón por encima se situaría el modelo arquitectónico del Ministerio de Defensa, que define y describe los niveles de arquitecturas CIS/TIC a desarrollar.
- Los dos pilares que llenan de contenido el TFM son las áreas de conocimiento de DAMA [2] que deben contemplarse para gestionar apropiadamente el ciclo de vida de los datos, información y conocimiento dentro del MDEF y la arquitectura de referencia del NIST (NBDRA) [3], principal referente técnico del TFM.
- Por último, el marco de presentación de la AR GIC viene dado por el *framework* arquitectónico OTAN NAFv4 [6].

La siguiente imagen representa la importancia de cada una de estas piezas en el producto final:

3. Propuesta de arquitectura

La política CIS/TIC [5] establece en su artículo 7.3.a) que se utilizará el modelo homologado de arquitecturas de la OTAN para el desarrollo de arquitecturas CIS/TIC. Para la elaboración de la arquitectura de referencia única para la gestión de la información y del conocimiento (AR GIC) se empleará el modelo en vigor, NATO *Architecture Framework Version 4* (NAFv4) [6].

NAFv4 estructura los *viewpoints* (puntos de vista de la arquitectura, donde cada uno de ellos puede ser modelado a través de diferentes vistas) en una rejilla o *grid*, donde las filas representan las *dimensiones* de interés de la arquitectura y las columnas los *aspectos*. De esta forma, cada uno de los *viewpoints* queda definido por la intersección de la fila y la columna correspondiente.

NAFv4 proporciona un conjunto estandarizado de *viewpoints* (*grid*) a considerar en la elaboración de arquitecturas desarrolladas bajo este *framework*. No obstante, para cada caso particular podrá contemplar un subconjunto de dichos *viewpoints*, o incluso definir algunos adicionales.

En la siguiente figura se resaltan los *viewpoints* del *grid* de NAFv4 desarrollados para la AR GIC:

La siguiente tabla muestra información de los tipos de vistas o dimensiones de la arquitectura:

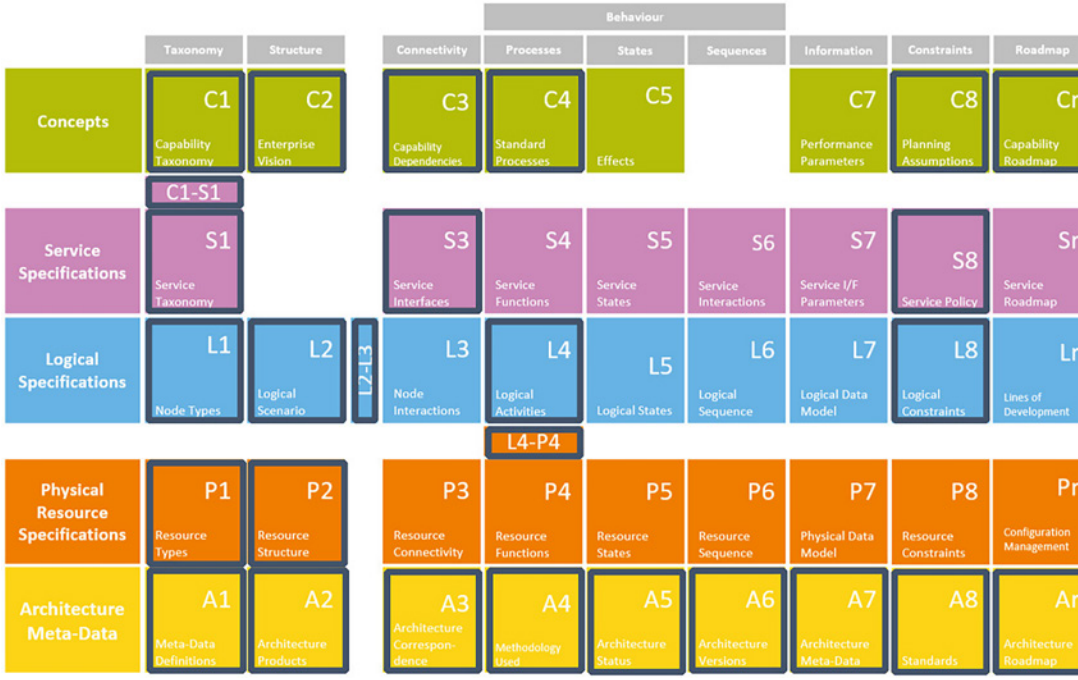


Figura 2. Grid NAFv4 de la AR GIC

VISTA	DESCRIPCIÓN
Conceptos	Descripción del proceso de análisis y optimización de la entrega de capacidades, en línea con el propósito estratégico de la organización.
Especificación de servicios	Descripción de los servicios independientemente de su implementación o utilización. Se considera un servicio en su sentido más amplio, como el suministro desde un proveedor de un resultado útil a un consumidor.
Especificación lógica	Descripción de los nodos lógicos (elementos de capacidad), actividades e intercambios de recursos/información necesarios para cumplir misiones. Las misiones incluyen tanto misiones operativas como procesos de negocio.
Especificación de recursos físicos	Descripción de la estructura, conectividad y comportamiento de los diferentes tipos de recursos (personas, organizaciones, artefactos, software y combinaciones de los mismos).
Metadatos de arquitectura	Descripción de los aspectos administrativos de la arquitectura.

Tabla 1. Dimensiones de arquitectura NAFv4

Cada una de estas vistas se desarrollará bajo distintos puntos de vista (*viewpoints* o aspectos) de arquitectura:

ASPECTO	DESCRIPCIÓN
Taxonomía	Especialización jerárquica de elemento de arquitectura.
Estructura	Descripción la composición de los elementos de arquitectura, incluyendo las interacciones entre los elementos.
Conectividad	Descripción de la conexión entre elementos de arquitectura, desde dependencias de alto nivel entre capacidades a detallada conexión entre sistemas.
Comportamiento	Descripción funcional de los elementos de la arquitectura: - Procesos: flujos de procesos y su descomposición. - Estados: transiciones de estado permitidas. - Secuencias: cómo interactúan los elementos y en qué orden.
Información	Descripción de los aspectos administrativos de la arquitectura.
Restricciones	Descripción y estructura de la información/datos empleada.
Hoja de ruta	Descripción de los hitos temporales de proyecto que afectan a los elementos de arquitectura.

Tabla 2. Aspectos de arquitectura NAFv4

Por último, la siguiente tabla recoge el resumen de los *viewpoints* que se han elaborado en la presente arquitectura, cuyo detalle puede consultarse en la memoria del TFM:

VIEWPOINTS	DESCRIPCIÓN
CONCEPTOS	
C1	Identificación de capacidades y su organización jerárquica (taxonomía).
C2	Descripción del ámbito de la arquitectura y el contexto estratégico de las capacidades descritas.
C3	Dependencias entre capacidades y su composición lógica (agrupaciones de capacidades).
C4	Actividades estándar (doctrinales) y su posible trazabilidad con las capacidades identificadas.
C8	Descripción de los supuestos que se han tenido en cuenta para la implementación de las capacidades.
Cr	Planificación estimada para la disponibilidad de las capacidades incluyendo los programas/proyectos necesarios para su entrega.
SERVICIOS	
S1	Revisión y ampliación de la taxonomía de servicios de la arquitectura global.
S3	Ofrece una vista de la naturaleza de los interfaces que deben proporcionar los principales bloques de servicio.

VIEWPOINTS	DESCRIPCIÓN
S8	Modela los principios de diseño y métricas operativas a contemplar durante la fase de diseño de las arquitecturas objetivo.
C1-S1	Proporciona el mapeo entre capacidades y servicios.
LÓGICA	
L1	Descripción de los diferentes tipos de nodos que estarán presentes dentro de la infraestructura de información del Ministerio de Defensa.
L2	Descripción de las interacciones entre los nodos identificados.
L2-L3	Proporciona una visión ejecutiva del propósito, alcance y contenido de la presente arquitectura de referencia.
L4	Descripción de las actividades lógicas de alto nivel que se aplicarán sobre la infraestructura de información del Ministerio de Defensa.
L8	Identificación de reglas/restricciones operacionales.
RECURSOS FÍSICOS	
P1	Descripción de los tipos de recursos relevantes para la arquitectura identificando las tecnologías y competencias requeridas.
P2	Descripción de la composición e interacción de alto nivel de los recursos.
L4-P4	Descripción de las funciones de recursos físicos y las funciones de servicios y las actividades lógicas que implementan.
METADATOS	
A1	Conjunto de metadatos empleados en la descripción de la arquitectura.
A2	Conjunto de productos/vistas que componen la arquitectura.
A3	Dependencias a alto nivel entre la arquitectura global y las distintas arquitecturas de referencia que componen la I3D.
A4	Metodología empleada en la elaboración de la arquitectura.
A5	Descripción del estado actual de la arquitectura.
A6	Descripción de las de las versiones previas de la arquitectura.
A7	Descripción de los tipos de vistas o dimensiones de la arquitectura.
A8	Conjunto de estándares, reglas, políticas y guías aplicables en la arquitectura.
Ar	Descripción de la línea temporal y planificación a futuro de nuevas versiones de la arquitectura.

Tabla 3. *Viewpoints* de la AR GIC

4. Conclusiones y líneas futuras

A la vista del trabajo realizado se puede concluir:

1) Se han establecido y desarrollado las capacidades CIS/TIC necesarias para la GIC.

2) Se han identificado y desarrollado los servicios CIS/TIC necesarios para proporcionar dichas capacidades CIS/TIC.

3) Se han identificado y desarrollado los nodos lógicos necesarios para llevar a cabo tanto las misiones operativas como los procesos de negocio del MDEF.

4) Se han identificado y desarrollado los recursos físicos que contribuyen al desarrollo de las capacidades GIC, a través de la implementación de los servicios GIC y de los nodos lógicos.

5) Se han ofrecido guías y especificaciones para el desarrollo de las arquitecturas objetivo del nivel inferior.

6) Se ha establecido una referencia para el desarrollo de la coordinación en materia GIC, y para alcanzar los objetivos y medidas de la estrategia de la información corporativa.

7) Se ha alineado el trabajo realizado con la política CIS/TIC [5], la AG CIS/TIC [1] el PECIS [7] y la política de seguridad de la información del Ministerio de Defensa [8].

8) Se ha establecido el desarrollo de la estrategia de la información del Ministerio de Defensa [9], y la elaboración ha estado regida por las directrices de la instrucción para la coordinación de la gestión de la información y del conocimiento en el Ministerio de Defensa [10].

9) Se ha realizado el análisis de los requisitos y capacidades operativas que espera satisfacer la arquitectura propuesta a partir de las áreas de conocimiento de DAMA-DMBOK2 [2].

10) Se han identificado y caracterizado las capacidades tecnológicas, los servicios, los nodos lógicos y los recursos físicos, y sus relaciones y estructura, requeridos para satisfacer los requisitos y capacidades operativas, a partir de los establecido en la arquitectura de referencia del NIST (NBDRA, NIST *Big Data Reference Architecture*) [3].

11) Se ha empleado NATO *Architecture Framework Version 4* (NAFv4) [6] para el modelado de la Arquitectura, tal y como se establece en el artículo 7.3.a) de la política CIS/TIC [5].

En base a lo anterior, puede afirmarse que se ha cumplido el objetivo del TFM, consistente en «la definición de una arquitectura que dará soporte

a un Sistema estratégico, consistente, integral y único de Gestión de la Información y Conocimiento en el ámbito de la Infraestructura Integral de Información para la Defensa (SGIC I3D)».

A partir del trabajo realizado se establecen las siguientes líneas futuras:

1) Elaborar el Plan de Acción GIC complementario a la AR GIC y que definirá en detalle las actividades para la consecución de los objetivos en cada una de las áreas GIC en todo aquello relativo a los plazos de consecución y recursos humanos y materiales requeridos.

2) Elaborar las arquitecturas objetivo derivadas de la AR GIC que deberán desarrollar en detalle los sistemas y subsistemas identificados en la AR GIC, ofreciendo la descripción de la solución prevista y las guías para su consecución sin perder de vista todos los factores de las capacidades CIS/TIC a alcanzar, especialmente los relativos al personal y su formación, operación y mantenimiento de los sistemas y a la provisión de los servicios.

3) Aprovechar la experiencia acumulada en NAFv4 para elaborar el resto de arquitecturas de referencia, y establecer una base de datos de conocimiento de modelado de arquitecturas, en la que participen integrantes del CESTIC, del EMAD y de los ámbitos con el objetivo de compartir y obtener conocimiento arquitectónico.

Referencias

[1] Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa.

[2] DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition, Technics Publications, 2017.

[3] «NIST Big Data Interoperability Framework (NBDIF): Volume 6, Reference Architecture» [Online]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-6r2.pdf. [Consultato il giorno 03 agosto 2020].

[4] «NIST Big Data Public Working Group (NBD-PWG),» [Online]. Disponible: https://bigdatawg.nist.gov/home.php. [Consultato il giorno 03 agosto 2020].

[5] Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

[6] «Nato Architecture Framework Version 4» [Online]. Disponible: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_12/20191203_191203-NAFv4_2019.10_print.pdf. [Consultato il giorno 03 agosto 2020].

[7] Instrucción 33 /2018, de 6 de junio, del secretario de Estado de Defensa, por la que se aprueba el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa.

[8] Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la Política de Seguridad de la Información del Ministerio de Defensa.

[9] Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa.

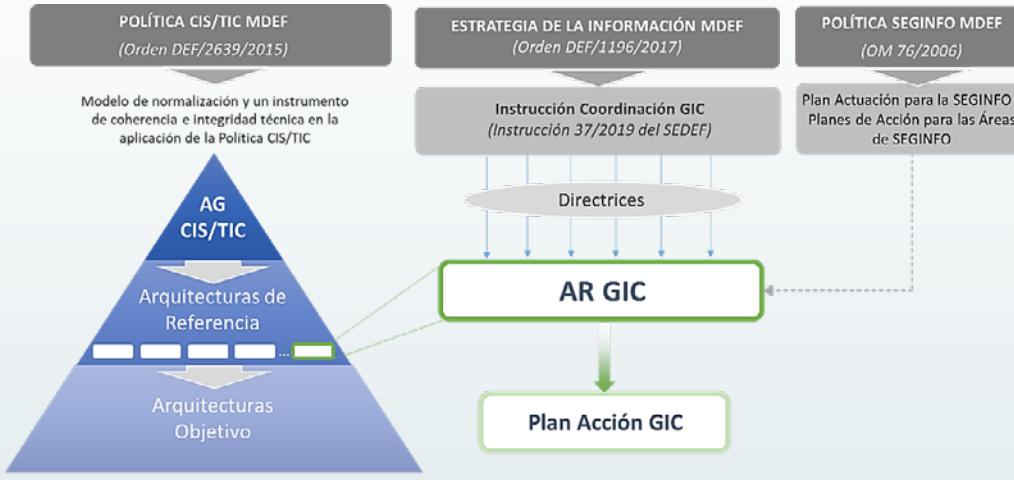
[10] Instrucción 37/2019, de 9 de julio, del secretario de Estado de Defensa, para la Coordinación de la Gestión de la Información y del Conocimiento en el Ministerio de Defensa.

Arquitectura de Referencia única para la Gestión de la Información y del Conocimiento en el Ministerio de Defensa (AR GIC)

Autor: TN CIA-EOF Rubén de la Peña Ramos
Director/es: Luis Álvarez Sabucedo

Objetivo

Proponer una arquitectura para soportar un **Sistema estratégico, consistente, integral y único para la Gestión de la Información y del Conocimiento en el ámbito de la Infraestructura Integral de Información para la Defensa** (SGIC I3D). La **AR GIC** es una de las Arquitecturas de Referencia recogidas en la **AG CIS/TIC**, desarrollo de la **Política CIS/TIC MDEF**. Su elaboración se sustenta en la **Instrucción de Coordinación GIC**, desarrollo de la **Estrategia de la Información MDEF**.



Modelo de la Arquitectura de Referencia única para la GIC en el MDEF

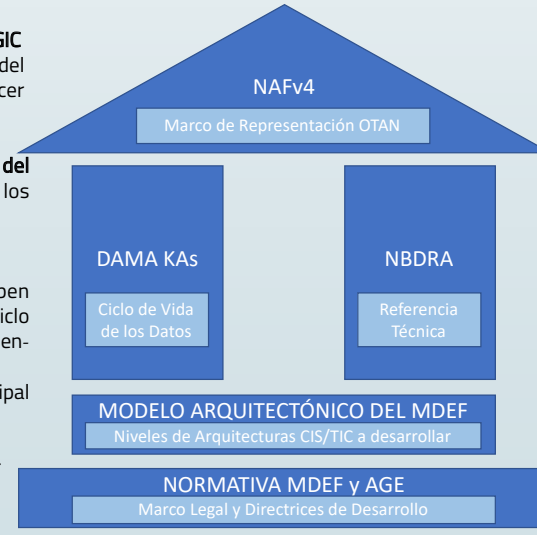
Base formada por el **resumen normativo en el ámbito GIC** (Ministerio de Defensa y Administración General del Estado), encargado de definir el marco legal y establecer directrices en el desarrollo de la AR GIC.

Sobre ella se apoya el **Modelo Arquitectónico del Ministerio de Defensa**, que define y describe los niveles de Arquitecturas CIS/TIC a desarrollar.

Los dos pilares sobre los que se asienta son:

- **Áreas de Conocimiento de DAMA** que deben contemplarse para gestionar apropiadamente el ciclo de vida de los datos, información y conocimiento dentro del MDEF.
- **Arquitectura de Referencia del NIST** (NBDRA), principal referente técnico de la AR GIC.

El marco de presentación de la AR GIC viene dado por el framework arquitectónico OTAN **NAFv4**.



Interoperabilidad entre los diferentes sistemas europeos en el ámbito de la justicia y los asuntos de interior

Autor: Rodríguez Olmos, Juan Jesús (jro@interior.es)
Directora: Gómez Pérez, Paula (master.diretic@cud.uvigo.es)

Resumen – El contenido del TFM intenta reflejar como se está abordando la interoperabilidad entre los diferentes sistemas de información de la Unión Europea, explicando el punto de partida con los sistemas existentes, ya sean centralizados o no, los motivos para un avance hacia una integración de la información en la mayor parte de los sistemas y los condicionantes legales que han de cumplir.

Además de los sistemas existentes, se han identificado nuevos sistemas que fueron concebidos para cubrir los gaps en los sistemas de información actuales, que están en fase de creación y los gaps y problemas que quedan sin resolver respetando en todo momento los requisitos de protección de datos y derechos fundamentales.

En este trabajo se contemplan los sistemas para afrontar los retos de seguridad y migratorios que son muy complejos y están interconectados para: llevar una gestión eficaz de las fronteras como parte integrante de la arquitectura de seguridad de la UE, hacer frente a la inmigración ilegal, el terrorismo y la delincuencia y apoyar la seguridad interior. Para todo ello, se necesita que los sistemas de la Unión Europea estén debidamente alimentados y sean utilizados por las autoridades nacionales competentes de manera intensiva, teniendo en cuenta que calidad de la información que se comparte es tan importante como la cantidad.

En lo relativo al consumo de la información, la interoperabilidad tratada en este trabajo hace referencia principalmente a una interfaz de búsqueda única (*European Search Portal*, ESP) y a la consulta automatizada de un sistema por otro sistema. Una interfaz de búsqueda única es el mayor avance para los usuarios de los diferentes sistemas.

Palabras clave: interoperabilidad, sistemas existentes, normativa, gap, nuevos sistemas.

1. Introducción

La situación de extrema gravedad e inseguridad que existía en Europa en 2016 hizo replantearse los recursos de los que disponían las fuerzas policiales y de inteligencia europeas con el fin de poder reaccionar de manera adecuada y, si era posible, adelantarse y prevenirlos, ser proactivos en todo lo posible, evitando los atentados que se estaban llevando a cabo en esos días. Este trabajo pretende explorar como se afrontó desde el punto de vista de la tecnología (aún no se han culminado los trabajos) y exponer los puntos que aún podrían requerir mejoras.

En junio de 2016 se creó un grupo denominado *high-level expert group on information systems and interoperability*, para realizar un estudio de las fortalezas, debilidades y posibles puntos de mejora de los sistemas de información existentes a nivel europeo y de aquellos gaps que se debían cubrir dado el aumento de los cruces de fronteras irregulares hacia la Unión Europea que suponían una amenaza para la seguridad interna, como demostraron las series de atentados que iban evolucionando y que eran cada vez más usuales y más cercanos al ciudadano de a pie.

El informe final del grupo de expertos de alto nivel se publicó en mayo de 2018 [1] llegando a la conclusión de que era necesario y técnicamente factible trabajar en pro de soluciones prácticas para la interoperabilidad entre los sistemas, que podían aportar beneficios operacionales y respetarse los requisitos de protección de datos y crear aquellos en los que se identificaron como necesarios para cubrir la falta de información que quedó patente de su estudio.

Los objetivos específicos de la propuesta eran:

1) Garantizar que los usuarios finales, en particular los policías de fronteras, los funcionarios encargados de hacer cumplir la ley, los funcionarios de inmigración y las autoridades judiciales tengan un acceso rápido, sin fisuras, sistemático y controlado a la información que necesitan para desempeñar sus tareas.

2) Ofrecer una solución para detectar múltiples identidades vinculadas a un mismo conjunto de datos biométricos, con el doble propósito de garantizar la correcta identificación de las personas de buena fe y combatir el fraude de identidad.

3) Facilitar los controles de identidad de los nacionales de terceros países, en el territorio de un Estado miembro, por parte de las autoridades policiales.

4) Facilitar y racionalizar el acceso de las autoridades encargadas de hacer cumplir la ley a los sistemas de información no relacionados con la aplicación de la ley en el ámbito de la UE, cuando sea necesario para la prevención, la investigación, la detección o el enjuiciamiento de los delitos graves y el terrorismo.

Adicionalmente contribuir a:

- Facilitar la implementación técnica y operativa por los Estados miembros de los sistemas de información tanto existentes como futuros.
- Fortalecer y racionalizar las condiciones de seguridad y protección de datos que rigen los respectivos sistemas.
- Mejorar y armonizar los requisitos de calidad de los datos de los respectivos sistemas.

2. Desarrollo

Los sistemas existentes a nivel europeo aún son islas (cada uno de ellos están concebidos para dar solución a unos objetivos concretos y no se compartirá información hasta la entrada en operación de los elementos comunes que se han definido para hacerlo posible).

2.1. Sistemas actuales

Los sistemas con los que se cuenta actualmente son el Sistema de Información de Schengen (SIS), el Sistema de Información de Visados (VIS), el sistema EURODAC, el Sistema Europeo de Información de Antecedentes Penales (ECRIS), el intercambio de información en el ámbito Prum y los Sistemas de información de las Agencias Europeas Europol y Frontex. A continuación, se realizará una breve descripción de cada uno de ellos.

El Sistema de Información de Schengen (SIS) [2] es el sistema por el que se comparte información más utilizado y con más volumen, utilizado para la seguridad interior y exterior y la gestión de las fronteras en Europa cuyo propósito es hacer que Europa sea más segura. El sistema ayuda a las autoridades competentes de Europa a preservar la seguridad interna en ausencia de controles en las fronteras internas.

El SIS permite a las autoridades nacionales competentes, como las policías (de ámbito nacional o territorial) y las policías de fronteras, introducir y consultar alertas sobre personas u objetos.

Una alerta del SIS no sólo contiene información sobre una persona u objeto determinado, sino también instrucciones para las autoridades sobre lo que deben hacer cuando se encuentra la persona u objeto.

Debido al uso intensivo de este sistema por las fuerzas policiales la mayoría de los Estados miembros tienen una copia técnica sincronizada al momento de los datos del para evitar problemas de disponibilidad del sistema central y optimización de recursos.

El Sistema de Información de Visados (VIS) permite a los Estados miembros del espacio Schengen intercambiar datos sobre visados (el visado

para estancias de corta duración que permite a un ciudadano no europeo permanecer un máximo de 90 días, dentro de un periodo de 180 días). El sistema procesa los datos y las decisiones relativas a las solicitudes de visados de corta duración para visitar o transitar por el espacio Schengen. El sistema realiza comparaciones biométricas con fines de identificación y verificación.

EURODAC [3] facilita a los Estados de la UE la determinación de la responsabilidad del examen de una solicitud de asilo (determina a quien le corresponde realizarla) mediante la comparación de conjuntos de datos de huellas dactilares conforme a lo establecido en el Reglamento de Dublín.

El Sistema Europeo de Información de Antecedentes Penales ECRIS, (*European Criminal Records Information System*) utilizado para compartir condenas anteriores dictadas en otros Estados miembros.

El intercambio de información policial [4] en el ámbito Prüm que tiene como objetivo el acceso automatizado a perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos y de forma menos usual para compartir relacionados con acontecimientos importantes, suministro de información con el fin de prevenir atentados terroristas u otras medidas para intensificar la cooperación policial transfronteriza.

Sistemas de información de las Agencias Europeas Europol y Frontex por el que se intercambia información sobre actividades delictivas.

2.2. Protocolos de intercambio de información

Para cada uno de los sistemas existen unas reglas definidas para el intercambio de información dentro de su ecosistema, podemos encontrar:

- Uso de colas de mensajes.
- Uso del correo electrónico.
- Servicios Web.
- Aplicaciones Web.

Si bien, la mayoría de los mensajes usan XML para definir el formato, en ninguno de los sistemas se utiliza un estándar la mayoría usan etiquetas diferentes que para referir lo mismo y casos con distinto tipo o tamaño. Además, EURODAC solo contiene datos biométricos para la identificación de personas, sin datos biográficos, lo que dificulta la identificación de problemas de calidad, duplicidades o la propia interoperabilidad.

2.3. Nuevos sistemas

Otro de los aspectos significativos es la existencia de gaps en los sistemas europeos para una gestión integral de la seguridad, que se

intentan solucionar con la creación de nuevos sistemas, entre los que se cuentan los siguientes:

Sistema de entrada/salida (EES) para registrar los datos de entrada y salida —y los datos de denegación de entrada— de los nacionales de terceros países que cruzan las fronteras exteriores del espacio Schengen y determinar las condiciones de acceso al sistema a efectos de la aplicación de la ley. En su concepción se prevé que sea interoperable con el Sistema de Información de Visados (VIS), a fin de lograr que los controles fronterizos fuesen más eficaces y rápidos.

Sistema europeo de información y autorización de viajes (ETIAS). Todos los nacionales de terceros países exentos de visado que planeen viajar al espacio Schengen, requieren una autorización antes de realizar el viaje. La información permitirá verificar con antelación los posibles riesgos para la seguridad o la migración irregular. ETIAS está diseñado para ser interoperable tanto con los sistemas existentes como con los sistemas nuevos previstos.

Sistema europeo de información de antecedentes penales para nacionales de terceros países (ECRIS-TCN), con el que se amplía el sistema ECRIS de intercambio de información de antecedentes penales a fin de incluir la información sobre los nacionales de terceros países condenados y los apátridas que se encuentran repartidas por los sistemas procesales de todos los Estados miembros y hacen muy complejo su acceso en un sistema central y compartido.

2.4. Interoperabilidad entre los sistemas

Para la interoperabilidad entre los sistemas se necesita que se reformen los sistemas actuales, tanto desde el punto de vista legislativo como el técnico para hacerla posible y que ambos, los sistemas nuevos y actuales, utilicen los mismos estándares para compartir información, protocolos de intercambio, estructura y calidad.

El elemento común de todos los sistemas son las personas, que independientemente del sistema al que pertenezcan tienen unas características comunes:

1. Datos biográficos.
2. Datos biométricos.
3. Resto de información o información de contexto que la liga de alguna manera a ese sistema.

Desde el punto de vista técnico, se puede pensar en uno o dos repositorios comunes para todos los sistemas, en el que se almacenen los datos biográficos y los biométricos, independientemente de los datos necesa-

rios que enriquece y complementan al sistema y pudiesen enlazarse con los sistemas dónde residiría el resto de información de contexto.

Con un repositorio único nos podríamos asegurar que se usan los mismos parámetros de calidad independientemente del sistema que se quiera alimentar y que no nos encontraremos con criterios diferentes dependiendo del sistema, evitando inconsistencias entre los datos de las mismas personas distribuidas en los diferentes sistemas o duplicidades innecesarias.

No obstante, el resultado no se limitó sólo al aspecto técnico, sino que fue necesario tener en cuenta todos los aspectos legales de proporcionalidad, el ámbito de aplicación y objeto de cada uno de los sistemas, antes de su tramitación por la comisión y posterior pase por el parlamento europeo. No se consideró modificar lo suficiente los instrumentos legales para que pudiese considerarse proporcional crear un repositorio único. Como desde el punto de vista técnico era de esperar (con las copias distribuidas que se consideren necesarias) y basándose en las aportaciones de los departamentos de la Comisión de protección de datos y derechos fundamentales se creó la estructura siguiente:

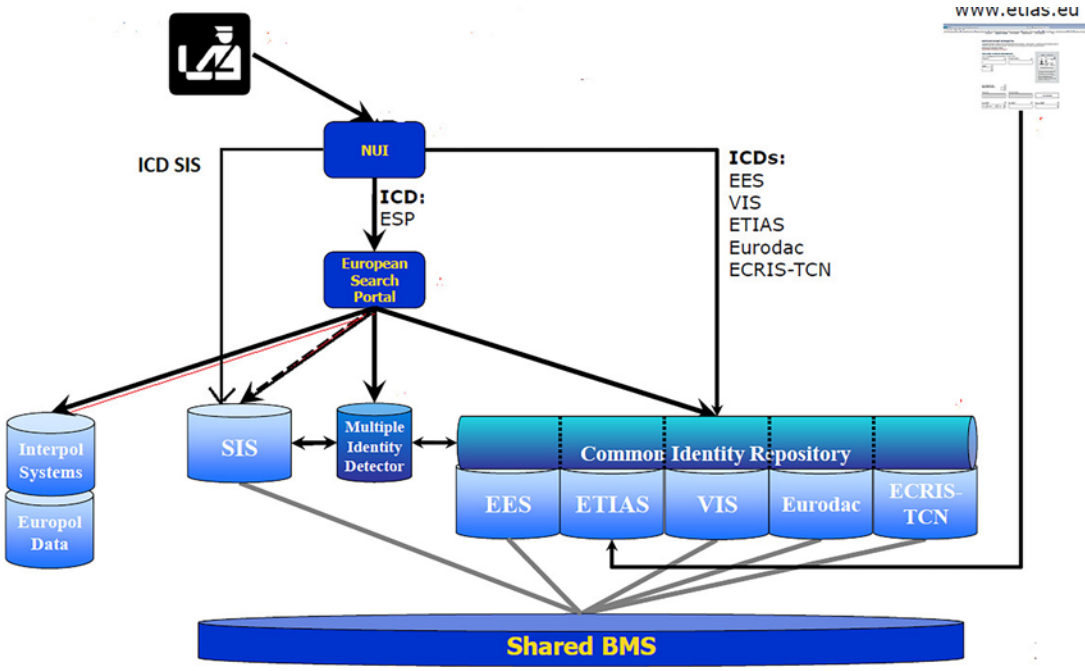


Figura 1. Representación conjunta de los sistemas.
Fuente: Comisión Europea (con alguna adaptación)

Como se puede observar la estructura es complicada y se incorporan elementos que tratarán información común que permitirán la interoperabilidad de los sistemas, y que se describen brevemente a continuación:

- NUI

Elemento que conecta a un Estado miembro a la red europea, tiene todos los elementos de conectividad y seguridad exigidos por los sistemas y sus instrumentos legales. No aporta elementos a discutir en cuanto a la interoperabilidad entre los sistemas más allá de la conexión segura.

- ESP

El portal de búsqueda europeo (ESP) ofrecerá los interfaces que permitirán realizar consultas entre los sistemas de información de la UE, los componentes del marco de interoperabilidad, los datos de Europol y las bases de datos de Interpol. Con un único punto de entrada se podrá consultar a todos los sistemas y componentes de interoperabilidad.

- MID

Detector de Identidad Múltiple (MID) permitirá la creación de vínculos (links) entre los datos de dos o más sistemas de información de la UE.

Cada uno de los links implicará datos de dos sistemas de información diferentes de la UE y no si hay datos diferentes en el mismo sistema.

El MID se conectará al Sistema de Información de Schengen (SIS), al Depósito Común de Identidad (CIR) y al Portal de Búsqueda Europeo (ESP).

El MID se basa en el sBMS (sistema con los templates de los biométricos) para la comparación biométrica de los datos contenidos en EES, VIS, SIS y ECRIS-TCN y Eurodac en cuanto se consolide la actualización de sus instrumentos legales y en el CIR para la comparación biográfica de los datos contenidos en EES, VIS, ETIAS y ECRIS-TCN y Eurodac (con la misma restricción de actualización) y, mediante el uso de la ESP de los datos biográficos contenidos en el SIS.

- SBMS

El BMS compartido contendrá plantillas biométricas (sin imágenes) y además *etiquetadas* con el sistema central propietario de esos datos.

El principal objetivo del BMS compartido es facilitar la identificación de una persona que pueda estar registrada en diferentes bases de datos, cotejando sus datos biométricos en diferentes sistemas y basándose en un único componente tecnológico en lugar de cinco diferentes en cada uno de los sistemas subyacentes.

3. Resultados y discusión

El resultado de *interoperabilidad* entre los diferentes sistemas europeos es un avance muy importante en cuanto a su interconexión, compartir información y que esta sea de calidad, pero no es total porque han pesado

más las restricciones legales impuestas por protección de datos y derechos fundamentales que las meramente técnicas que llevarían al dato único y de calidad y una mayor flexibilidad en cuanto a los accesos a los datos muy restringidos mediante uso de roles por la definición de proporcionalidad, definida en su sentido más restrictivo, que se ha mantenido en los sistemas.

Se ha asegurado el intercambio de información sin que dependa del factor humano, se han unificado los estándares en cuanto al formato de los mensajes (todos serán UMF *Universal Message Format*) con etiquetas unificadas para los mismos objetos (no tendrán un nombre diferente en cada sistema) y un mismo conjunto de etiquetas para los mismos objetivos, se han asegurado mediante la definición de los roles adecuados que las diferentes autoridades de cada Estado miembro tenga el acceso adecuado y de manera uniforme en todos los Estados miembros.

En lo relativo a los protocolos de intercambio de información, no están completamente definidos y aunque en la mayoría de los casos se usarán servicios web es seguro que se mantendrán colas de mensajes y correo electrónico.

Con relación a los gaps, se han cubierto la mayoría que tienen que ver con los ciudadanos de terceros países, pero quedan algunos sin cubrir en lo relativo a ciudadanos de la Unión y el uso de la información que se genera después de su uso.

Por último, queda por definir y acordar como interoperar los sistemas europeos con los no europeos, como Interpol, para completar la información que se requiere para cumplir con unos parámetros adecuados de seguridad, tanto interior como en frontera.

4. Conclusiones

Los objetivos del TFM se han alcanzado explicando el estado actual de los sistemas europeos, su aislamiento y las soluciones que se están implementando.

La implantación de los nuevos sistemas y la modificación de los existentes afrontan un importante reto de interconexión entre ellos y de trasformación digital de procesos que hasta la fecha son manuales, como por ejemplo todo el cruce de fronteras, dónde la anotación en el pasaporte y registros de entrada y salida pasan a ser completamente digitales.

Del estudio de la situación futura es notorio que los sistemas no son completamente interoperables y podría ser, desde el punto de vista técnico, más eficaces y eficientes.

Agradecimientos

Quiero mostrar mi agradecimiento a todo el profesorado y alumnado del máster, que, a pesar de los inconvenientes en la realización del curso por las consecuencias de la pandemia siempre han estado ahí y nos han apoyado en todo lo posible.

Referencias

[1]https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_proposal_regulation_on_establishing_framework_for_interoperability_between_eu_information_systems_police_judicial_cooperation_asylum_migration_.

[2]https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en

[3]https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en

[4]https://eur-lex.europa.eu/legal-content/ES.

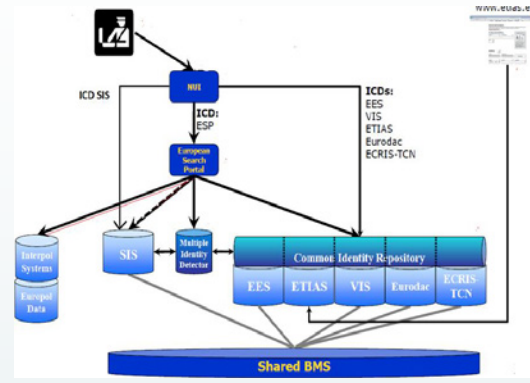
Interoperabilidad entre los diferentes sistemas europeos en el ámbito de la justicia y los asuntos de interior

Autor: Juan Jesús, Rodríguez, Olmos
Director/es: Paula, Gómez, Pérez
Universidad de Vigo

Introducción

El trabajo refleja el replanteamiento de los recursos disponibles por las fuerzas policiales y de inteligencia europeas debido a la situación de extrema gravedad e inseguridad que existía en Europa en 2016, con el fin de poder reaccionar de manera adecuada y, si era posible, adelantarse y prevenirlos, siendo proactivos en todo lo posible evitando los atentados que se estaban llevando a cabo en esos días. Este documento pretende explorar como se afrontó desde el punto de vista de la tecnología (aún no se han culminado los trabajos) y los puntos que aún podrían requerir mejoras.

Resultados



Metodología

Metodología cuantitativa basada en la documentación existente en la Comisión Europea, Agencias Europeas relacionadas con la Interoperabilidad y grupos de trabajo creados ad hoc, orientada a los resultados reales obtenidos revisando los pasos dados hasta llegar a su conclusión.

Conclusiones

Se presenta el estado actual y previsiones de futuro de los sistemas Europeos, su aislamiento y las soluciones que se están implementando.

Se han explicado los hechos que pusieron de manifiesto la falta de eficacia del diseño actual, como se identificaron los problemas y las soluciones que se han comenzado a implementar y que tienen previsto finalizar en 2023

La implantación de los nuevos sistemas y la modificación de los existentes afrontan un importante reto de interconexión entre ellos y de trasformación digital de procesos que hasta la fecha son manuales, como ejemplo, todos los procesos relacionados con el cruce de fronteras dónde la anotación en el pasaporte y registros de entrada y salida pasan a ser completamente digitales.

Agradecimientos

Quiero mostrar mi agradecimiento a todo el profesorado y alumnado del Máster, que, a pesar de los inconvenientes en la realización del curso por las consecuencias de la pandemia siempre han estado ahí y nos han apoyado en todo lo posible.

Soluciones para protección frente a ataques DoS. Implementación para el Ministerio de Defensa y posible evolución

Autor: Rodríguez Ortega, Juan José
(jrodort@fn.mde.es; juanjo1972ad@gmail.com)
Director/es: Zamorano Pinal, Carlos (externo.czamorano@cud.uvigo.es)
y Álvarez Sabucedo, Luis (externo.lsabucedo@cud.uvigo.es)

Resumen – El objetivo del trabajo es proporcionar un acercamiento a los ataques tipo denegación de servicios comúnmente conocidos por su acrónimo de inglés *Denial of Services DoS*, como podemos protegernos frente a ellos y cuál es el estado del arte actualmente en cuanto a medidas de protección existentes.

A través de la *taxonomia* de referencia desarrollada por el CCN, se introduce en los diferentes tipos de que ataque DoS/DDoS que podemos encontrarnos, lo que nos ayudará a entender mejor las distintas formas en las que se puede producir un ataque de denegación de servicios y como protegernos frente a estas amenazas.

Se realizará un recorrido por el estado del arte, en cuanto a medios y medidas de protección frente a estos ataques disponibles en el mercado actual, así como las herramientas que el CCN-CERT pone a disposición de las AA. PP. y empresas que quieren cumplir con los estándares del ENS.

Dar una visión de la estrategia que emplea en Ministerio de Defensa (MINISDEF) para hacer frente a ataques del tipo DoS. Solución implementada en ámbito del MINISDEF para defenderse de estos ataques, que mecanismos y procedimientos operativos se emplean en el MINISDEF a día de hoy para luchar contra ellos.

Para finalizar se detallarán las conclusiones a que nos ha llevado este trabajo en lo referente a protección frente a DoS y específicamente en el ámbito del Ministerio de Defensa.

Palabras clave: DoS, DDoS, denegación de servicios, ataque, tráfico legítimo, *spoofing*, *flood*.

1. Introducción

1.1. Introducción

Existen múltiples tipos de amenaza en el ciberespacio, algunas de ellas van encaminadas al robo de información, otras a la escalada de privilegios para sabotear un sistema o tomar su control, otras van dirigidas a la destrucción de la información o los sistemas de información, etc.

La denegación de servicios más conocida por sus siglas en inglés DoS (*Denial of Services*), es un tipo de ataque dirigido a la fuente de la información o al canal de transmisión, impidiendo el acceso a un recurso informático por parte de los usuarios legitimados para el acceso al sistema o la información que en él se almacena, la navegación web, realizar operaciones de banca, uso del correo electrónico, etc.

Cuando estos ataques en lugar de realizarse desde una única fuente se realizan desde múltiples fuentes en la misma o diferentes ubicaciones, nos estamos refiriendo entonces a ataques del tipo DDoS (*Distributed Denial of Services*) mucho más perjudiciales y peligrosos que los primeros, si bien el objetivo de estos sigue siendo el mismo, la interrupción de un servicio o lo que es lo mismo la denegación de este a los usuarios.

1.2. Atacantes potenciales o actores relacionados con los ciberataques.

Las tecnologías de la información han dado entrada a nuevas actividades y formas de negocio. De igual manera que el ciberespacio ha representado una oportunidad de expansión para la sociedad digital, también puede ser explotado con fines malintencionados o delictivos, debido a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación [1].

Como en cualquier otro tipo de ciberataques, en los DoS/DDoS podemos encontrarnos con múltiples agentes de muy diversa índole y con motivaciones de todo tipo [2]. En muchos casos la peligrosidad de estos agentes estará en función de los recursos a su disposición, lo podemos clasificarlos de la siguiente manera:

- Estados.
- Grupos terroristas.
- Organizaciones criminales.
- Hackativistas.
- Ciberdelincuentes.
- Insider.

1.3. Taxonomía de ataques de denegación de servicio propuesta por el CCN [3]

El Centro Criptológico Nacional (CCN) propone en su Guía sobre la Seguridad de las Tecnologías de la Información número 820 (CCN-STIC-820) una taxonomía genérica, que se ha adoptado en el ámbito del Ministerio de Defensa para clasificar y analizar las características de los ataques DoS.

Afrontar de forma eficaz un ataque de denegación de servicio ya sea distribuido o no, requiere entender sus características el objetivo, su origen, el impacto que genera, su método de propagación, las vulnerabilidades que explota, etc. Los ataques DoS pueden afectar a diferentes capas del modelo de referencia OSI y hacerlo de formas diversas.

1.4. Categorías de ataques DoS

Como norma general y para poder facilitar la categorización de los distintos tipos de ataques DoS, podemos distinguir entre tres tipos distintos de categoría de ataque DoS.

1) Volumétricos o por inundación [4], que tienen como objetivo principal el consumo del ancho de banda de la víctima.

2) Ataques reflexivos (DrDoS) [5] representa un 20 % del total de los casos de DDoS, se enfoca a debilidades en las capas de red (capa 3) y de transporte (capa 4) del modelo OSI. El ataque explota el proceso de protocolo de enlace o *handshake* del Protocolo de Control de Transmisión (TCP).

3) Agotamiento de recursos el atacante se dirige contra los recursos de un sistema, genera tráfico fragmentado o mal formado, peticiones inválidas o sin sentido, el servidor intenta resolver todas estas peticiones inútilmente.

1.5. Métodos más comunes para ejecutar un DoS

Algunos de los métodos más comúnmente empleados para desarrollar ataques de denegación de servicios son [6]:

1) Ping de la muerte [7]. El Ping de la muerte o *Ping of Death* se hizo famoso en la década de los 90, cuando un ataque a base de paquetes ICMP pesados conseguía bloquear el sistema. El atacante crea un paquete ICMP que supera el tamaño máximo permitido para estos paquetes de datos.

2) ICMP *Flood*. También conocido como *Ping Flood*, es un tipo de ataque en el que se intenta sobrecargar a la víctima con paquetes de peticiones

de echo ICMP, provocando que el objetivo se vuelva inaccesible para el tráfico lícito [4].

3) *Smurf* [8]. El atacante realiza peticiones ping (*echo-request*) a una o más redes de dispositivos, falsificando la dirección IP de la víctima (IP *spoofing*) los dispositivos que han recibido la solicitud de ping envían sus respuestas a la dirección IP de la víctima, amplificando el tráfico inicial del ataque.

4) *Buffer overflow* [9]. Este tipo de ataque consiste en enviar una cantidad de tráfico a los recursos de una red que exceda la capacidad por defecto de procesamiento del sistema, cargando el búfer con más datos de los que puede contener.

5) Ataque de fragmentación de paquetes IP [10]. Es un tipo de ataque en el que la víctima recibe un flujo de fragmentos de tamaño pequeño sin que ninguno de ellos tenga desplazamiento de cero, el objetivo podría colapsar al intentar reconstruir el datagrama a partir de los paquetes recibidos. Se pueden mitigar de diferentes formas, siendo en la mayoría de los casos, el asegurar que los paquetes maliciosos no lleguen nunca a su objetivo.

6) Ataques de amplificación [11]. En ellos se utiliza un factor de amplificación para aumentar el efecto del ataque cuando este se ejecuta con un número limitado de recursos. El DNS (*Domain Name Service*) *Amplificaton attack* es el más común de estos ataques.

7) *SYN attack* [4]. Es un ataque DDoS que explota parte del proceso denominado conexión en tres pasos el protocolo TCP para consumir recurso en la máquina objetivo con el fin de dejarla fuera de servicio.

8) *UDP Flood* [12]. Es un tipo de denegación de servicio que explota el *User Datagram Protocol* (UDP) enviando un elevado número de estos paquetes a la víctima con la intención de saturar la capacidad de proceso y respuesta de esta.

9) HTTP *Flood* [4]. Este ataque está diseñado para que la víctima destine el mayor número de recursos posible para hacer frente a las solicitudes que recibe, el atacante intenta saturar al objetivo con una inundación de cuantas más solicitudes de procesado intensivo como le sea posible.

10) *Mac Flood* [13]. A diferencia de otros ataques, el *MAC flood* no va dirigido contra *host* u otras máquinas que alojan distintos servicios, en su lugar va dirigido a comprometer la seguridad de los dispositivos de conmutación de red (*switch*).

11) *Slowloris* [4]. Este tipo de ataque utiliza solicitudes HTTP parciales para abrir una conexión con un servidor web y mantenerla abierta tanto tiempo como le sea posible con el fin de sobrecargar y ralentizar a la máquina objetivo.

12) NTP *Amplification* [12]. Se basa en un ataque volumétrico de reflexión, el atacante aprovecha el protocolo de tiempo *Network Time Protocol* (NTP) para desbordar a la víctima con una cantidad amplificada de tráfico UDP, lo que hace que el objetivo y su infraestructura circundante quede inaccesible al tráfico legítimo.

13) *Zero-day* DDoS *Attack* [14]. Generalmente el término *Zero-day* hace referencia a ataques que explotan una nueva vulnerabilidad del software de la cual la comunidad no tiene conocimientos aún. Puede pasar mucho tiempo desde que un atacante detecta este tipo de vulnerabilidades hasta que la comunidad la descubre y lanza una actualización para solucionar la vulnerabilidad.

1.6. *Mirai*, la red *Zombie*

En octubre de 2016 tuvo lugar un ciberataque contra Dyn, compañía estadounidense dedicada a soluciones DNS en direcciones IP dinámicas en Internet.

Se trató de un DDoS que colapsó los servicios de Dyn, fue un ataque masivo a la infraestructura básica de internet ejecutado por millones de dispositivos del Internet de las cosas (IoT).

Mirai es un *malware* de la familia de los *botnets*, destinado a infectar equipos del IoT, el objeto principal de este *malware* es la infección de routers y cámaras IP. Se cree que Mirai ha sido empleada para atacar a la web *Krebs on Security* y la francesa OVH *cloud-computing service* además de Dyn [15].

Mirai afectó a millones de usuarios, por más de dos horas provocó la imposibilidad de acceder a recursos de Internet tales como Twitter, CNN, ediciones digitales de periódicos de tirada nacional, Amazon, Reddit, Tumblr, PayPal, etc.

2. Desarrollo

A la hora de tomar medidas preventivas a los DoS/DDoS debemos tener en cuenta los distintos vectores que un atacante puede aprovechar para lanzar su ataque, quizás el primer vector que debemos contemplar al implementar las distintas capas de seguridad es nuestra infraestructura de red que nos dan conectividad hacia el exterior, otro vector lo conforman las infraestructuras que componen nuestra red interna (routers, *switches* y servidores) y un tercer vector lo componen nuestras aplicaciones web.

El CCN ofrece a la AGE y a las empresas que quieran cumplir con el ENS una solución, con el fin de incrementar el grado de protección de estos

organismos y su eficacia en la respuesta y mitigación de incidentes de seguridad. Podemos encontrar, desde el Sistema de Alerta Temprana de la red SARA, a herramientas de seguridad del tipo de LUCIA (gestión de incidentes de seguridad tipo RT-IR), o INES (para verificar el grado de cumplimiento de las organizaciones del ENS).

Existen en el mercado multitud de empresas y dispositivos dedicados a la protección anti-DoS, sus productos y soluciones están específicamente diseñadas para la prevención y mitigación de estos ataques.

2.1. Imperva [16]

Es una empresa de servicios y software de ciberseguridad, que ofrece protección a los datos y al software de aplicaciones de multitud de empresas y organizaciones gubernamentales. Por lo tanto, podemos encasillar a Imperva dentro del grupo de proveedores de servicios de seguridad. Imperva es líder mundial entre los proveedores de soluciones DDoS según informe de *Forrester Research*.

Imperva ofrece soluciones de protección contra ataques DDoS para sitios web, redes, servidores de aplicaciones, DNS e IPs individuales. Entre sus éxitos Imperva ha mitigado el ataque más grande producido hasta el momento, de forma inmediata y sin incurrir apenas en aumento de la latencia ni interfiriendo en el tráfico de usuarios legítimos. Las soluciones Imperva están diseñadas para encontrar las necesidades específicas del cliente, las opciones ofrecidas se ajustan a los clientes.

2.2. Netscout Arbor [10]

A diferencia de Imperva, Netscout Arbor, está centrada principalmente a la venta de soluciones de seguridad hardware y/o software, pero no proporciona servicios de protección contra incidentes.

La solución propuesta por Arbor, se basa en la inteligencia obtenida mediante el escaneo de la red del cliente y en la detección de anomalías en la gestión de amenazas de primera categoría, detectando así un posible agotamiento volumétrico, de estado de las conexiones TCP y por último a nivel de aplicación. Adicionalmente, Arbor dispone de ATLAS, una red global de inteligencia que nutre las bases de datos de *Arbor Network* en beneficio directo de sus productos de protección.

2.3. Neustar [17]

Neustar tiene una solución contra DDoS capaz de mitigar ataques que superen los 12 Tbps a través de una de las redes de depuración de datos más grandes del mundo.

Las soluciones Neustar ofrecen a sus clientes servicios 24/7, protección en las capas 3 a 7 del modelo OSI. Implantación sin necesidad de despliegue de hardware o software en las redes del cliente, años de experiencia en el sector.

2.4. ELK Stack [18].

Uso de *Machine Learning* asociado a la seguridad frente a DoS/DDoS, integrando plataformas como ELK *Stack*.

El *plugging* de *Machine Learning* del ELK, nos sirve para identificar patrones y ver anomalías en estos patrones, podemos ejecutar este *plugging* en nuestro sistema, para que aprenda cual es el funcionamiento normal del mismo a lo largo un periodo de tiempo, por ejemplo, así podrá distinguir cual es el volumen de tráfico, los eventos generados, las llamadas a los servicios que desplegamos, etc.

3. Resultados y discusión

En el tratamiento de un incidente DoS se establecen típicamente tres fases (Detección, Autorización y Mitigación). En CESTIC la gestión de un incidente DoS corresponde a la subunidad de Internet de la Unidad de Redes de la División de Operaciones (DIVOPER) y la operadora adjudicataria del contrato de servicios del nodo de interconexión.

El MINISDEF identifica como activos críticos a proteger frente a amenazas DoS Servicios y Redes, estableciendo unas prioridades en cuanto al nivel de protección.

CESTIC adopta una serie de medidas preventivas agrupada en tres aspectos diferenciados (Organización, Técnicos y Monitorización y Control) para luchar contra los ataques DoS.

La mitigación de los ataques DoS, se realiza activamente a través de las medidas reactivas y dentro del marco del contrato vigente con el operador de servicios, se solicita la provisión de un servicio de mitigación contra ataques DoS que incluye la inspección de todo el tráfico cursado por las líneas de acceso a Internet conectadas al MINISDEF en los centros principales y de respaldo.

Este servicio permite configurar una serie de alertas para que detecten la existencia de un ataque y dependiendo del tipo, iniciar de manera automática determinadas contramedidas. Es lo que se conoce como automitigación.

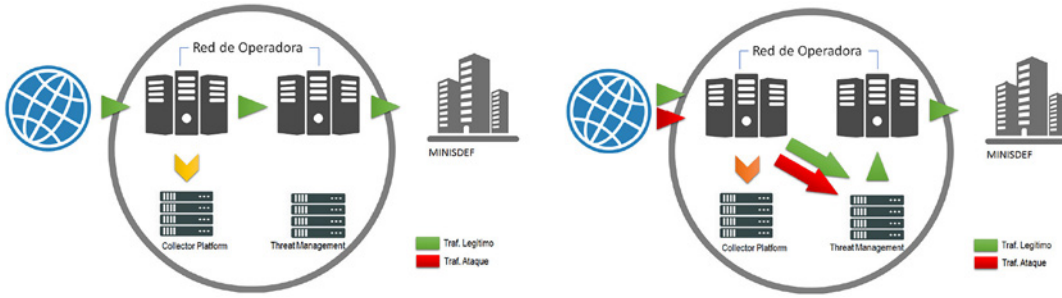


Figura 1. a) Tráfico normal b) Tráfico mitigado

Se define la siguiente operativa asociada frente a un ataque DoS:

- El sistema autónomo envía un resumen de 1/2000 paquetes del tráfico a la sonda colectora que monitoriza el servicio, este envío se realiza por SNMP.
- El servicio, comprueba si se está rebasando el consumo de ancho de banda habitual, más un tanto por ciento acordado (en previsión de noticias, campañas o actividades que puedan exceder el consumo habitual).
- Superado los valores establecidos, si este consumo anómalo se mantiene durante un tiempo preestablecido, se generan las alertas.
- Cada alerta generará automáticamente una notificación a los equipos de operación tanto en el C-SOC de la operadora, como al equipo que da soporte en las instalaciones del ministerio.
- Tras la alerta, ambos equipos de operación realizan un seguimiento de la alerta, pendientes de su evolución.
- Si el evento llega al umbral de *alarma*:
  - La operadora modificará el protocolo de *routing* (BGP) para hacer pasar el tráfico por las herramientas anti-DoS.
  - El TMS se intercalará entre el sistema autónomo de la operadora y el sistema autónomo del MINISDEF.
  - Se ejecutan las contramedidas automáticas acordadas.
  - Se registra una incidencia en el sistema ITSM SCAN.

- Si la automitigación no da resultado, los operadores del C-SOC solicitan autorización a los responsables del MINISDEF, la ejecución de contramedidas adicionales (estas medidas pueden afectar al tráfico legítimo, con la consiguiente pérdida de información).
- Finalizado el ataque, se restablece el servicio.

4. Conclusiones

El Ministerio de Defensa ha optado por una solución híbrida en cuanto a la defensa y prevención de ataques del tipo DoS/DDoS, dividiendo la carga

de la gestión frente a este tipo de incidentes entre las responsabilidades del ISP, mediante la adecuada contratación del servicio y el establecimiento de un SLA, que permita o garantice la continuidad del servicio del MINISDEF a sus usuarios aun estando siendo objeto de un ataque de denegación de servicios, y los equipos de defensa interna gestionados por el grupo de explotación de seguridad del CESTIC a través de la implementación de *Firewall*, IDS, IPS y configuraciones seguras en los distintos servicios que se han identificado como críticos.

La configuración adecuada de *firewall*, IDS, IPS y el establecimiento de *mailguard* que limiten o filtren el tráfico de correos recibidos y enviados, así como la limitación en el número de destinatarios posibles o limitar el número de direcciones de correo que puedan formar parte de una lista de distribución, limitar las conexiones a los servicios web tanto en el número como en el tiempo que se pueden mantener activas, etc., son medidas que deben implementarse por parte del MINISDEF.

La evolución de los sistemas de defensa contra DoS/DDoS pasa actualmente por un incremento en el desarrollo de técnicas de IA y *Machine Learning* en los distintos dispositivos empleados para la prevención de estos incidentes.

Agradecimientos

A mi esposa Alejandra y a mis hijas Rocío, Emma y Sofía, por apoyarme y aguantar mis malos ratos y padecer el tiempo que les he hurtado con alegría y buenas caras.

Sin vuestro cariño y apoyo no habría podido terminar este trabajo.

Referencias

[1] Estrategia de Seguridad Nacional 2017.

[2] Estrategia Nacional de Ciberseguriad 2019.

[3] Guía sobre la Seguridad de las Tecnologías de la Información n.º 820 (CCN-STIC-820).

[4] «Wikipedia,» [En línea]. Disponible: https://en.wikipedia.org/wiki/.

[5] «unaaldia.hispasec.com,» [En línea]. Disponible: https://unaaldia.hispasec.com/2018/03/hablemos-de-drdos.html.

[6] «Openwebinars.Net,» [En línea]. Disponible: https://openwebinars.net/blog/top-10-de-ataques-dos-denial-of-service-o-denegacion-de-servicios/.

[7] «Informática para tu negocio». [En línea]. Disponible: https://www.informaticaparatunegocio.com/blog/significa-ping-funciona/.

[8] «Kaspersky,» [En línea]. Disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack.

[9] «OWASP.ORG,» [En línea]. Disponible: https://owasp.org/www-community/attacks/Buffer_overflow_attack.

[10] «NETSCOUT,» [En línea]. Disponible: https://www.netscout.com/what-is-ddos/ip-icmp-fragmentation.

[11] «Centro de Gestión de Incidentes Informáticos,» [En línea]. Disponible: https://www.cgii.gob.bo/es/publicaciones/ataque-de-amplificacion-de-servidor-de-nombre-de-dominio-dns-recursivo.

[12] «Cloudflare,» [En línea]. Disponible: https://www.cloudflare.com/.

[13] «Interserver.Net,» [En línea]. Disponible: https://www.interserver.net/tips/kb/mac-flooding-prevent/.

[14] «INCIBE,» [En línea]. Disponible: https://www.incibe.es.

[15] «McAfee Labs Threats Report 2017».

[16] «Imperva». [En línea]. Disponible: https://www.imperva.com/.

[17] «Neustar». [En línea]. Disponible: https://www.home.neustar/.

[18] «Elastic». [En línea]. Disponible: https://www.elastic.co/.

Soluciones para protección frente a ataques DoS.

Implementación para el Ministerio de Defensa y posible evolución.

Universidad de Vigo

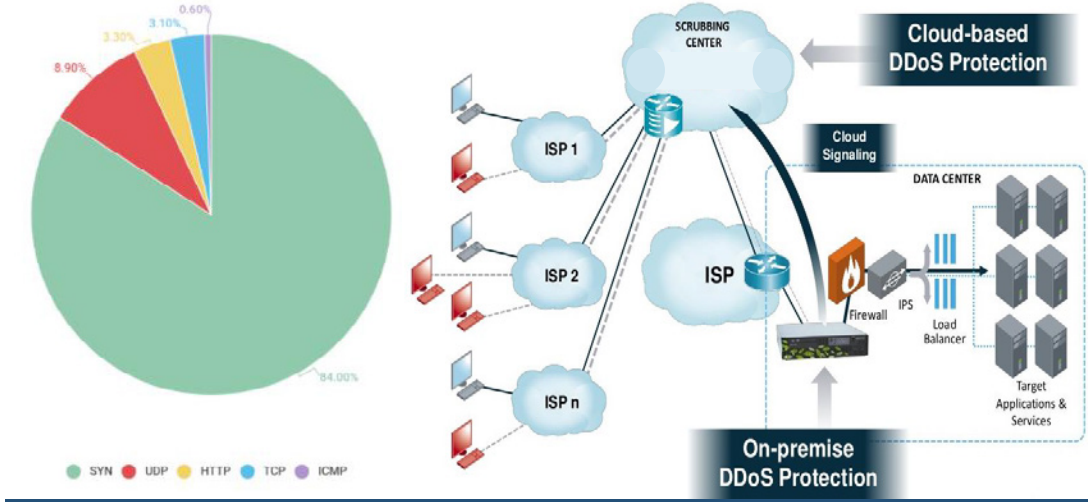
Autor: Juan José, Rodríguez Ortega

Director/es: Carlos, Zamorano Pinal y Luis, Álvarez Sabucedo

En el ámbito del MINISDEF un ataque DoS puede suponer, no sólo:

- **Perdida de conectividad, impidiendo normal funcionamiento del MINISDEF.**
- **Indisponibilidad prestación determinados servicios (Sede Electrónica,…)**

Sino que también, puede dañar gravemente la imagen del MINISDEF.



Empleo del sistema Talos para ayuda en situaciones de emergencia

Autor: Torre López, Andrés Ignacio (atorlop@fn.mde.es)
Directora: Gómez Pérez, Paula (master.diretic@cud.uvigo.es)

Resumen – La existencia de emergencias sanitarias como la causada por la enfermedad del COVID19 supone un enorme esfuerzo de coordinación de diferentes organismos estatales y el empleo de las Fuerzas y Cuerpos de Seguridad del Estado (FCS/FCSE) y las Fuerzas Armadas (FAS) para realizar actividades de control, presencia, reconocimiento, labores de desinfección, entrega de comida, transporte de mercancías, rastreo de contagios, etc.

El sistema TALOS (programa desarrollado por la empresa GMV para el mando táctico y técnico de unidades de apoyo de fuego de las FAS) tiene las características adecuadas para facilitar el mando y control de operaciones incluyendo el posicionamiento de unidades y el establecimiento y difusión de órdenes a las unidades implicadas en la ejecución de operaciones en el campo de batalla.

Durante la conducción de la Operación Balmis de apoyo al entorno civil se ha identificado la necesidad de disponer de una herramienta eficaz para la gestión y el control de las solicitudes de apoyos requeridas por las autoridades y organismos civiles.

El diseño de una arquitectura TIC que permita conducir eficientemente el apoyo a los organismos civiles durante situaciones similares al de la provocada por la pandemia del COVID19 proporcionaría información en tiempo real sobre las solicitudes de apoyo a los organismos civiles. Esta arquitectura TIC podría basarse en el empleo del programa TALOS combinado con el empleo de un portal WEB asociado a un servicio Web (WS, *Web Service*).

Palabras clave: sistema TALOS, coordinación de emergencias, Operaciones CIMIC.

1. Introducción

La crisis sanitaria de 2020 motivada por el Coronavirus SARS-CoV-2, causante de la enfermedad COVID-19, ha provocado un impacto sobre las infraestructuras sanitarias y los recursos humanos y logísticos a nivel mundial.

En España, el Ministerio de Sanidad (MNSD) lideró las acciones necesarias para dar respuesta al grave impacto de la enfermedad sobre la población y afrontar las exigentes condiciones laborales durante su evolución. Por su parte, el Ministerio de Interior (MINT) y el Ministerio de Defensa (MDEF) participaron activamente en la adopción de despliegues de unidades y apoyo a las autoridades civiles. La Operación Balmis, llevada a cabo entre los meses de marzo a junio de 2020, fue la respuesta del MDEF para aportar sus capacidades de personal y material en el desarrollo de la crisis del COVID-19. Esta operación estuvo vinculada al estado de alarma decretado en sucesivas ocasiones por la Presidencia del Gobierno. En concreto, la operación se inició el 15 de marzo y finalizó el 21 de junio tras 98 días de apoyo a las autoridades y organismos civiles.

El objetivo principal de la operación fue la de contribuir a los esfuerzos del gobierno para prevenir y contener la transmisión del virus y su impacto sanitario, social y económico. Para ello se aportaron las capacidades y medios para preservar la seguridad y el bienestar y garantizar la prestación de servicios, ordinarios o extraordinarios.

Los principales datos estadísticos de la operación se resumen en la participación de 188.713 militares en más de 20.000 actuaciones de desinfección de espacios, montaje de hospitales, ayuda a mayores y otras intervenciones de apoyo en 2.302 localidades en lo que se considera el mayor esfuerzo militar llevado a cabo en tiempo de paz en España [1].

Tras la finalización de la operación Balmis, durante el mes de agosto se produjo un aumento progresivo de rebrotes de infección del Coronavirus en la totalidad del territorio nacional (TN). La principal medida adoptada por la Presidencia del Gobierno para afrontar el control de los rebrotes de la epidemia fue la de poner a disposición de las comunidades autónomas (CC.AA.) 2.000 rastreadores militares del MDEF desde su anuncio el 25 de agosto.

El Mando de Operaciones (MOPS) hizo una gestión centralizada de las necesidades, coordinada con el MINT, basada en el empleo de paquetes de ofimática Office y Libre Office, según disponibilidad de licencias, por medio del empleo de hojas de cálculo para la gestión de necesidades y editores de texto para la gestión de la documentación operativa. El principal medio de intercambio de los archivos necesarios para la gestión documental y la ejecución de la operación fue el empleo del correo electrónico por parte de los organismos civiles públicos y privados y el correo electrónico gestionado

por la aplicación Outlook corporativo en el ámbito del MDEF a través de la red de propósito general WAN PG de uso oficial y en menor medida el empleo de otras formas de distribución de mensajes. El conjunto de medios TIC empleados para la gestión de las solicitudes de los organismos civiles adoleció de un uso excesivo de la mensajería y recursos humanos y una falta de eficacia a la hora de gestionar las solicitudes de apoyo y de notificar el estado de las propias solicitudes a sus peticionarios.

El empleo de una combinación de un sistema de información para el Mando y Control (TALOS) ya empleado en el MDEF junto con el desarrollo de un servicio web (WS, *Web Service*) que permita a los actores participantes en la operación la rápida gestión de las solicitudes de apoyo, permitiría mejorar en gran medida la eficacia en la gestión de la información y el control de la ejecución de la operación sin necesidad de implementar soluciones más costosas y que necesiten de un mayor desarrollo para su puesta en funcionamiento.

2. Desarrollo

2.1 Elementos de la arquitectura TIC

El diseño de arquitectura TIC propuesto en el TFM del mismo nombre se basa en dos pilares fundamentales:

- El primer pilar se apoya en el uso de un WS al cual se le ha denominado *solicitudes* (compuesto por un conjunto de servicios) para que cualquier actor participante autorizado, sea autoridad civil, ONG o representante de los FCS, pueda realizar una gestión rápida y sencilla de apoyo al MDEF. Este WS podría ser consumido directamente por parte de los actores civiles que así lo requieran, por medio de la publicación de sus funcionalidades, o indirectamente por medio del diseño de un portal web para su uso por aquellos organismos civiles que prefieran esta otra modalidad.
- El segundo pilar se basa en el empleo del sistema TALOS Táctico, empleado en la actualidad por parte del Ejército de Tierra (ET) y la Armada (AR), aprovechando sus capacidades de representación de unidades en su funcionalidad de representación geográfica (GIS, *Geographic Information System*), de gestión de acciones y de incorporación del posicionamiento de terminales móviles en un entorno de trabajo de la red de propósito general WANPG o corriendo por Internet con la seguridad del propio cifrado del TALOS (ambas posibilidades de trabajo adecuadas para la pseudo-clasificación *uso oficial* propia de este tipo de operaciones). Debido a las características específicas de este tipo de operaciones desarrolladas en TN y el carácter de las funcionalidades requeridas para su conducción, se

considera adecuado el nivel *sin clasificación* (SINCLAS) para este trabajo y para el sistema propuesto.

Adicionalmente, se considera recomendable la incorporación del posicionamiento de las unidades ejecutantes de las actividades de apoyo por medio del empleo de terminales de telefonía móvil para completar los dos pilares anteriores.

2.2 Esquema de la arquitectura TIC

En la figura 1 se representa el esquema de la arquitectura de integración de los componentes del sistema C2 para poder gestionar y controlar la solicitud y ejecución de apoyos militares a las autoridades y organismos civiles.

Bajo la denominación *SIST. C2 TALOS* de la figura 1 se puede identificar una estructura jerarquizada del MDEF formada por los diferentes escalones de mando que compondrían la organización operativa diseñada para la operación de apoyo a las autoridades y organismos civiles participantes. Como último peldaño de la organización operativa se encuentran las unidades ejecutantes de los apoyos solicitados, que llevarían a cabo la ejecución de las actividades por medio de las pequeñas patrullas representadas en la imagen como terminales de telefonía móvil bajo la etiqueta *actividades*.

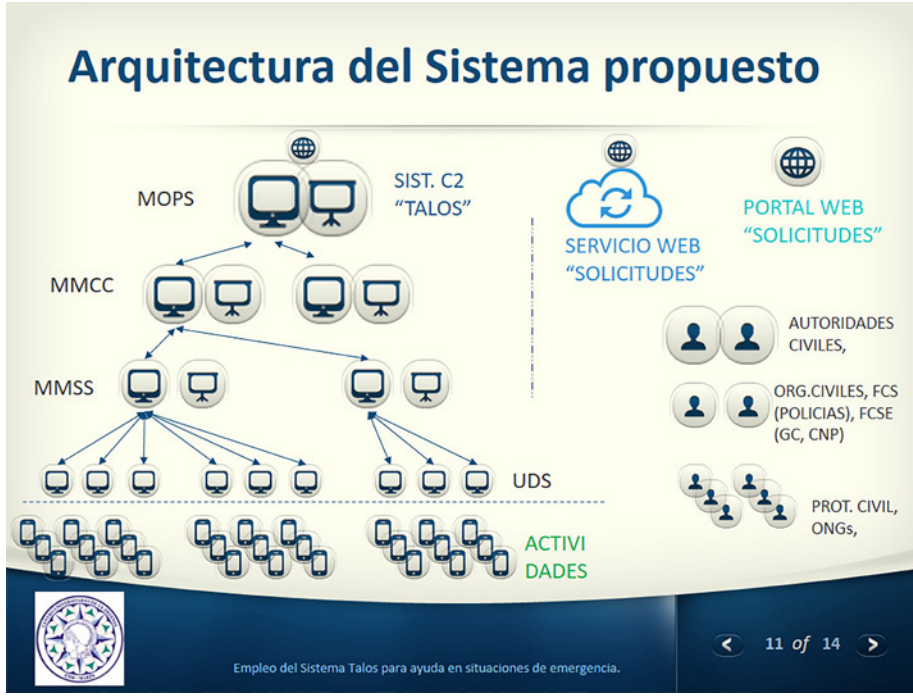


Figura 1. Esquema de la arquitectura TIC del sistema C2 para gestión y control de apoyos

A la derecha de la figura 1 se pueden identificar el resto de elementos integrantes del sistema compuestos por el WS y el portal WEB, ambos orientados a su uso o consumo por parte de las autoridades y organismos civiles para la gestión de las solicitudes.

2.3 Procesos involucrados en la gestión de solicitudes

Para el diseño del WS de gestión de solicitudes de las autoridades y organismos civiles se ha empleado el programa Bizagi Modeler que permite identificar los flujos de trabajo de cada una de las actividades solicitadas cubriendo todo el abanico de opciones. En concreto se ha dividido la gestión de los procesos en varias fases de solicitud, validación, aprobación, ejecución y finalización. En la figura 2 se muestra el esquema de la primera de las partes citadas.

2.4 Servicios asociados al WS *solicitudes* de la arquitectura TIC

Debido a la necesidad de disponer de una serie de funciones definidas como servicios independientes con interfaces invocables en secuencias definidas por el flujo de trabajo diseñado con anterioridad se consideró más adecuado el empleo de una Arquitectura Orientada a Servicios (SOA).

A la vista de los procesos de la gestión de apoyos a través del WS *solicitudes* se identificaron como necesarios los siguientes servicios:

- SVC1. Gestión de usuarios del WS.
- SVC2. Gestión de solicitudes de apoyo.
- SVC3. Gestión de modificaciones de la solicitud.
- SVC4. Asignación de recursos personales y materiales.
- SVC5. Gestión de los estados de las solicitudes.
- SVC6. Gestión de las anotaciones de las solicitudes.
- SVC7. Gestión de informes operativos.

Para cada uno de estos servicios se detalló su descripción, funcionalidades, variables, métodos, y el tratamiento de los datos.

Posteriormente se detalló la orquestación de los servicios constituyentes del WS de acuerdo a los estados por los que puede pasar cada una de las solicitudes de apoyo desde su petición inicial hasta su finalización.

2.5 Extensión de TALOS para el consumo del WS *solicitudes*.

Para el intercambio de información entre el programa TALOS y el WS *solicitudes* se requiere de una extensión del TALOS y la ampliación de dos

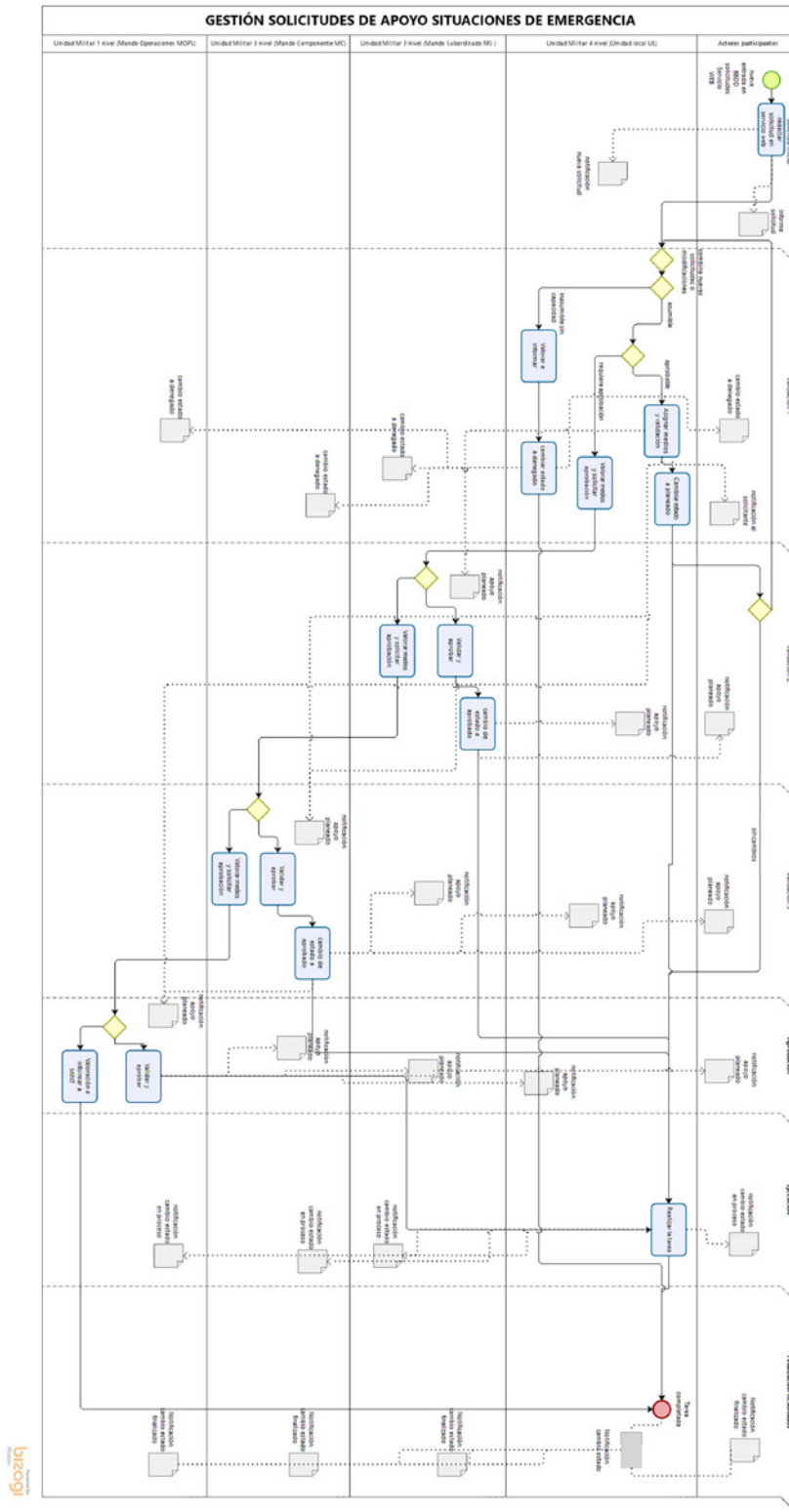


Figura 2. Detalle del flujo de trabajo en su fase de validación de primer nivel

de sus funcionalidades (*acciones* e *informes*). Estos pequeños cambios facilitarán la selección de las instalaciones objeto del apoyo a las autoridades civiles, así como automatizarán la elaboración de documentos e informes operativos necesarios para la conducción de las operaciones en el MDEF.

2.6 Empleo de terminales móviles para la ejecución de los apoyos.

Por último, para la visualización de las actividades y patrullas de apoyo en tiempo real por medio de terminales telefónicos móviles se requiere del uso de la ubicación de los terminales corporativos para la incorporación de las trazas de posicionamiento empleando un Servidor TCP externo para la grabación de los posicionamientos de los terminales móviles a través de una IP fija, una extensión ya implementada en TALOS y una aplicación móvil denominada APP Traccar Client para los terminales móviles, mientras no se desarrolle un SW específico del programa TALOS para los SO móviles (Android e iOS).

3. Resultados y discusión

Del estudio de la arquitectura TIC necesaria para mejorar el sistema de gestión de solicitudes de apoyo en situaciones de emergencia se ha obtenido como resultado la definición del alcance y los requisitos de la arquitectura. Se ha realizado la consulta a los ingenieros del Programa: DNO907 - TALOS sobre su viabilidad y estimación de tiempos y costes económicos para poder aportar una valoración aproximada de lo que supondría su ejecución, obteniendo las siguientes estimaciones:

- desarrollo del Portal/WS *solicitudes*: 9 meses / hombre
- desarrollo de la extensión de TALOS: 3 meses / hombre
- desarrollo de las versiones TALOS para SO móviles Android/iOS: 12 meses / hombre.

Adicionalmente sería necesaria la formación sobre funcionalidades TALOS para personal EA y UME, estimándose este requisito en un curso de 20 horas para un grupo de 60 personas centrado en el aprendizaje de las principales funcionalidades del programa (organización de unidades y jerarquía, empleo del GIS y la gestión de las acciones e informes).

La valoración del proyecto se estima en un coste aproximado de 24 meses/hombre y 230.000 € (coste horario de 60 € hora, 160 horas / mes).

4. Conclusiones

- Para mejorar la eficacia del apoyo proporcionado por las FAS y otras FCSE/FCS a los organismos civiles en situaciones de emergencia similar a la acaecida durante la crisis de la COVID-19 se requiere de un impulso en los medios de gestión de la información.

- En la actualidad las FAS disponen del programa TALOS que puede emplearse como sistema de información para facilitar el C2 de las organizaciones operativas diseñadas para el apoyo en emergencias.
- El empleo del TALOS junto a un WS para la gestión de solicitudes de apoyo procedentes de los organismos civiles sería una solución eficaz y económica para proporcionar el impulso necesario para mejorar la gestión, rapidez de respuesta y visibilidad de los procesos para todos los actores participantes.
- Para completar las funcionalidades aportadas por el programa TALOS y el WS de gestión de solicitudes de apoyo se considera recomendable el empleo del posicionamiento de las pequeñas unidades por medio del empleo de una extensión del TALOS ya desarrollada.
- Se ha establecido el diseño de la arquitectura TIC necesaria para el funcionamiento de todos los elementos implicados en un entorno de información adecuada para la clasificación *sin clasificar*, definiendo los servicios de un WS, la extensión necesaria en TALOS para su comunicación con WS y los requerimientos para integrar el posicionamiento de terminales móviles de los ejecutantes en el GIS de TALOS.

Agradecimientos

Todo mi agradecimiento para Francisco Pérez, Erica Benito y Víctor Molleda, ingenieros de GMV, por la ayuda recibida durante las prácticas realizadas en empresas para el desarrollo de este trabajo y a Paula Gómez Pérez, profesora ingeniera del CUD MARÍN por tutorizar este trabajo y estar siempre disponible para ayudarme.

Referencias

[1] «Onda cero noticias finaliza la operación Balmis», 21 junio 2020. [Online]. Disponible: https://www.ondacero.es/noticias/espana/finaliza-operacion-balmis-20000-intervenciones_202006215eef44d461045700001f91e6c.html#:~:text=La%20operaci%C3%B3n%20Balmis%20de%20las,el%20mayor%20n%C3%BAmero%20de%20vidas%22.. [Último acceso 29 Agosto 2020].

Empleo del Sistema Talos para ayuda en situaciones de emergencia

Autor: Andrés Ignacio Torre López
Directora: Paula Gómez Pérez

Introducción

Durante la crisis sanitaria de la pandemia del COVID19, el MDEF llevó a cabo la operación "BALMIS" para apoyar a las autoridades civiles en diversas actividades. Para ello se gestionaron, de forma centralizada, las necesidades de apoyo, empleando paquetes de ofimática Office y Libre Office y usando principalmente la red de propósito general WAN PG. El conjunto de medios TIC empleados para la gestión de las solicitudes de los organismos civiles adoleció de un uso excesivo de mensajería y recursos humanos, así como de una falta de eficacia a la hora de gestionar las solicitudes de apoyo y de notificar el estado de las propias solicitudes a sus peticionarios.

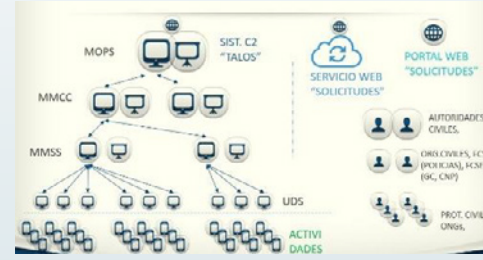
Metodología

Se empleó un enfoque cualitativo en el que primó la obtención de las Lecciones Aprendidas de la Operación en relación a la gestión de los apoyos y la observación privilegiada del autor del trabajo, jefe de Operaciones de una de las principales unidades participantes en la Operación "BALMIS" y de otros miembros claves.

Resultados

El empleo de una combinación de un sistema de información para el Mando y Control (TALOS), ya empleado en el MDEF, junto con el desarrollo de un servicio web (WS, Web Service) que dejase, a los actores participantes en la Operación, la rápida gestión de las solicitudes de apoyo, permitiría mejorar en gran medida la eficacia en la gestión de la información y el control de la ejecución de la Operación sin necesidad de implementar soluciones más costosas y que necesiten de un mayor desarrollo para su puesta en funcionamiento.

Para el desarrollo de este TFM, además del sistema TALOS, se empleó la herramienta BPM "Bizagi Modeller" para el diseño de los flujos de procesos para la gestión de solicitudes de apoyo y para la orquestación de los servicios del WS a través de la gestión de los estados de las solicitudes.



Conclusiones

El empleo de una arquitectura TIC sencilla, de fácil implementación y de impacto transversal en el ámbito interministerial podría permitir la mejora de la gestión de las peticiones de apoyo solicitadas por las autoridades y organismos civiles durante el desarrollo de situaciones de emergencia como la ocurrida en la pandemia del COVID19.

Agradecimientos

Todo mi agradecimiento para Francisco Pérez, Erica Benito y Víctor Molleda, ingenieros de GMV, por la ayuda recibida para el desarrollo de este trabajo y a Paula Gómez Pérez, profesora ingeniera del CUD MARÍN por tutorizar este trabajo y estar siempre disponible para ayudarme.

La atracción de talento mediante la marca clave de competitividad en las organizaciones: aplicación de TIC al ámbito de defensa

Autor: Vico Cardenete, Paulino (pviccar@et.mde.es)
Director: Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – En la actualidad, los futuros empleados para las empresas muestran unos criterios muy definidos a la hora de decidir en qué organización quieren formar parte. Estas deben cumplir una serie de requisitos que ya no están referidos a percibir una elevada cuantía económica en su salario.

En estos momentos, lo que buscan los futuros trabajadores de una compañía es pertenecer a una gran organización que sea competitiva en su sector y que cuente con los trabajadores del mayor talento del país. El poder formar parte de este equipo es lo más demandado. Es por ello, que se necesita ser una empresa competitiva para poder captar al mejor talento, pues es lo que demandan aquellos trabajadores con las mayores habilidades y destrezas.

Constituirse como organización competitiva, y poseer el mejor talento entre su personal, implica no solo atraerlo, sino también cumplir todo el ciclo de la gestión del talento: evaluación, desarrollo y retención del talento. Se trata de una labor que no es sencilla debido a la alta competitividad que existe hoy en día fruto de la globalización en la que vivimos.

El MINISDEF, como institución fundamental del Estado, para poder desarrollar todos sus cometidos que tiene asignados debe implicarse en esta competitividad organizacional para poder atraer al mejor talento de la sociedad. En este contexto, las TIC son unas herramientas que se alinean con este objetivo de obtención de una importante imagen de marca, pues su correcto empleo garantizaría el poder transmitirle a la sociedad el atractivo de la pertenencia al MINISDEF, como un grupo selecto de trabajadores con demostrado talento y capacidades.

Palabras clave: talento, competitividad, MINISDEF, empresas, captación, empleado, marca, sociedad.

1. Introducción

1.1 Motivación

Nuestra sociedad, marcada por una situación de constante cambio, volatilidad e incertidumbre, hace que nuestras Fuerzas Armadas deban estar preparadas para asumir los diferentes cometidos que le reclama la colectividad.

Un factor clave para poder asumir estos cometidos tan demandantes reside en la gestión del talento que tanto se ha puesto en práctica en las grandes empresas y otras tipologías de organizaciones. A través del análisis de la evaluación del desempeño y de los perfiles de competencias de las empresas somos capaces de conocer las técnicas del control del talento implantadas por dichas organizaciones para posteriormente poder adaptarlas a nuestras Fuerzas Armadas.

Nuestros ejércitos, debido a su elevado número de personal, son grandes gestores del valor humano; por ello, es creciente la importancia que está adquiriendo dentro las FAS. Se ha pasado de trabajar por paliar la escasez de recursos humanos que desde mucho tiempo atrás se ha acuciado dentro de nuestro ejército, a valorar la calidad humana de aquellos que visten el uniforme.

1.2 Objetivos

Mediante la realización de este trabajo de fin de máster (TFM) se pretende abordar la mejor estrategia a aplicar para lograr que nuestras FAS constituyan una imagen de referencia de la que todo el mundo desee formar parte. Ello derivará de la capacidad de poseer los profesionales de mayor talento, lo cual estará íntimamente relacionado con la aplicación de la herramienta denominada *employer branding* y que analizaremos posteriormente. Este instrumento, de amplio empleo en el ámbito empresarial, busca, mediante la adopción de una serie de medidas, conseguir para la organización una gran imagen de marca de empleador y así captar y retener talento. Por tanto, su empleo permitirá atraer y retener al personal que mejor se alinee con los objetivos de nuestros actuales ejércitos.

Asimismo, se pretende evaluar la posibilidad de aplicar ciertas medidas empleadas por las organizaciones de referencia al Ministerio de Defensa. Por tanto, se busca aportar propuestas de actuación que puedan ayudar de manera positiva, dentro de las limitaciones que existen tratándose de un contexto militar, para potenciar el empleo de las tecnologías de la información y las comunicaciones (TIC) en el *employer branding* referido al Ministerio de Defensa y detectar las ventajas que derivarían del empleo de sistemas y aplicaciones digitales para el desarrollo de una estrategia de *employer branding* en las Fuerzas Armadas (FAS), así como la gestión

del talento, de acuerdo con su constante afán de superación y de mejora continua.

2. Gestión del talento en las empresas

La gestión del talento se ha basado tradicionalmente en la atracción del talento, desarrollo y retención del mismo. Este procedimiento ha funcionado en las empresas hasta el momento de manera satisfactoria. En la actualidad son otras las necesidades las que se demandan en la gestión de las personas y que quedan definidas en cuatro procesos: desarrollo de capacidades, cultura del talento, formación de líderes y gestión del desempeño.

Con respecto al desarrollo de capacidades, la empresa crea sus procesos y estrategias dirigidos hacia el cliente, lo cual define su identidad como empresa en el mercado y que los hacen diferentes al resto. Cuando hablamos de Microsoft, nos referimos a sus capacidades tecnológicas, cuando hablamos de IKEA nos referimos a sus capacidades de competitividad en el ámbito de precios reducidos y cuando hablamos del Corte Inglés nos referimos a su gran capacidad para prestar un servicio de venta de gran calidad y garantías.

Con respecto al desempeño, la empresa debe contar con un modelo que le permita recompensar por el desempeño, así como identificar aspectos en los que el personal pueda desarrollarse en un futuro.

La cultura del talento es muy variada en las empresas debido a la gran diversidad de perfiles de empleados que se ve influenciada por las franjas de edades y generaciones existentes. Cada uno de ellos debe encontrar en la empresa la capacidad de poder desarrollarse en el ámbito de sus inquietudes y necesidades.

Con respecto al liderazgo, la empresa debe tener la capacidad de poder formar a su personal y desarrollar habilidades en su persona para que posteriormente puedan contar con líderes en sus correspondientes ámbitos. De esta forma, se conseguirá que estos líderes puedan formar con posterioridad al nuevo personal que entre a formar parte de la empresa. Es así como se consigue dar continuidad a la empresa a medio-largo plazo.

2.1 Entorno VUCA

En la actualidad, todas las instituciones se encuentran sometidas a un entorno muy turbulento donde existen multitud de variables que pueden cambiar radicalmente el futuro de nuestras empresas. Para ello se utilizó el término VUCA procedente de las siglas en inglés *volatile*, *uncertain*, *complex* y *ambiguous* para referirse a un mundo de discontinuidad y turbulencias que actualmente se encuentra referido en su totalidad

al mundo empresarial y educativo. Cabe destacar que este entorno se encuentra motivado en gran medida por la digitalización y la tecnología.

Figura 1. Entorno VUCA 2.0. [1]

2.2 Marca del empleador ME

Actualmente las empresas tienen dificultades para poder reclutar a gente con talento que puedan desempeñar cometidos específicos dentro de ella, esto se debe a que el talento escasea en general y este tipo de personas exigen mucho a la empresa por lo que si esta no cumple con las condiciones exigidas se marcha. Este personal es volátil y solo asume cometidos a corto plazo.

Las razones por las que surge la necesidad tan drástica en el mundo empresarial de crear la ME se basan principalmente en los cambios que están sucediendo y que nos afectan globalmente, mencionados anteriormente (entorno VUCA).

El *employer branding* es una estrategia a largo plazo para ser reconocidos como un empleador de referencia por parte de los futuros y actuales empleados de una empresa, y con el objetivo de ganar la guerra por el talento.

Esta estrategia debe llevarse a cabo de manera que se produzca un cambio cultural entre sus trabajadores, de forma que con posterioridad pueda reclutarse a aquel personal que pueda mejorar y adaptarse a esa cultura ya adquirida por las empresas. Este cambio no es algo que pueda producirse de modo inmediato, por lo que llevará consigo un tiempo de

trabajo continuo y constante para que ello se produzca. Una vez que se adquiere la cultura perseguida en la empresa es muy difícil que se pueda perder rápidamente.

3. Contribución de las TIC a la gestión del talento

En la actualidad, nos encontramos inmersos en la transformación digital en todos los aspectos de nuestra vida y, como no podía ser de otra manera, también está incluida en el mundo empresarial. Esta situación ha favorecido la revolución tecnológica en la que hoy en día vivimos. Dentro de las empresas, los departamentos de RR. HH. son una de las áreas que se han visto afectadas más si cabe.

Es un hecho que las TIC desempeñan un papel más importante en la gestión del talento en cada una de las empresas, por lo que las áreas de recursos humanos deben potenciar esta herramienta para poder lograr la sostenibilidad de la empresa en un futuro, así como tener unos empleados comprometidos con ella. En esta línea, las TIC deben detectar el talento, gestionarlo, identificar las capacidades y promover la gestión basada en méritos que den lugar al desarrollo de sus profesionales [2].

Para llevar a cabo esta transformación digital es necesario un cambio significativo en la mentalidad de todos los miembros de la empresa que permita una rápida adaptación a la digitalización de gran parte de los procesos, con ello se sostiene la necesidad, como ya se ha comentado anteriormente, de cambiar la cultura de la empresa.

Con la transformación digital se han creado nuevas herramientas tecnológicas que facilitan la labor de la gestión de los RR.HH. Con ello se ha podido lograr que las aplicaciones permitan crear los perfiles necesarios del personal que queremos que formen parte de la empresa. De forma que la captación del talento quede totalmente definida y vaya preorientada para poder cubrir las expectativas de la organización.

Son varias las herramientas digitales que hoy en día, a modo de propuesta, pueden tener cabida en la gestión del talento en las organizaciones [3], entre ellas se encuentra: *Big Data*, aplicaciones móviles, *digital employer branding*, tecnologías en la nube, gamificación, *People Analitycs*, *Dynamics 365 human resources*.

4. Las TIC y el talento en el MINISDEF

Existen diferentes herramientas tecnológicas que sirven para el reclutamiento del personal necesario que debe formar parte en una empresa. Dentro del MINISDEF, podrían tener aplicación también teniendo en cuenta que no serían los mismos procesos los aplicados al personal que llegará a ser militares de carrera a los procesos de selección aplicados a personal de tropa y marinería.

En el momento de iniciar la selección no se ha de tener en cuenta la persona, sino lo importante es el puesto de trabajo a desempeñar dentro de la organización, las herramientas tecnológicas existentes diferencian las pruebas que se deben realizar dependiendo de los empleos a ocupar. Todo ello supone un gran impacto a la nueva gestión de los RR.HH., y al propio MINISDEF si se logra implementar estas capacidades.

Este avance tecnológico debe ser de aplicación para crear un proceso de captación que proporcione garantías en la identificación de aptitudes de los futuros militares y ayudarles a que desarrollen su vida profesional dentro de las áreas donde están capacitados y poder trabajar de una forma más exitosa. Las tecnologías deben ser la herramienta principal para la selección de talento humano en las Fuerzas Armadas ya que estas, cada vez más, requieren que el personal que va a formar parte de ellas posea las máximas garantías para el desarrollo del puesto que va a desarrollar.

Es ya un hecho, y se ha descrito anteriormente, que las empresas más destacadas emplean diversas fuentes enmarcadas en las TIC para llevar a cabo sus procesos de selección, donde a través de estas tecnologías obtienen muchos datos de los candidatos para poder hacer algo de análisis a los potenciales trabajadores a contratar.

En la actualidad los criterios de selección del personal militar están muy poco orientados hacia los trabajos que, posteriormente, van a desarrollar dentro de la organización, por lo que da lugar a un número elevado de bajas indeseadas durante las fases académicas. Esto último está referido a los militares de carrera, donde hay constancia, en un porcentaje considerable, del abandono de la fase inicial de la carrera militar.

Hoy en día, cada vez más, las empresas utilizan múltiples procedimientos para evaluar a los posibles candidatos para formar parte de las empresas, todo ello en procesos de selección de personal donde se están implementando el uso de las TIC para poder llevarlo a cabo de manera exitosa y con garantías.

Dentro de las TIC también se están llevando a cabo el empleo de tecnologías para poder asegurar la confiabilidad de la información que los aspirantes muestran en las entrevistas personales, donde en muchas ocasiones no se ajustan las capacidades y destrezas que dicen poseer los candidatos con aquellas que realmente tienen. Estaríamos hablando de llevar a cabo un procedimiento para poder detectar posibles fraudes.

La gestión del talento dentro del MINISDEF es un proceso que no se debe basar únicamente en la captación para posteriormente no tratar su desarrollo y evaluación en la propia vacante asignada, por el contrario, se debe analizar continuamente el capital humano para poder observar si el personal militar está realizando los cometidos para lo que realmente tiene potencial, capacidades y le permite mantener su talento que finalmente garantizan su estabilidad laboral.

Las nuevas tecnologías han evolucionado enormemente en el campo de la selección del personal para ocupar determinados puestos que podrían ser de aplicación en el ámbito del MINISDEF, con ello queremos decir que existen aplicaciones informáticas para poder desarrollar todas las tareas referidas a los RR.HH. y, con ello, poder reclutar al personal más idóneo para poder desarrollar determinados puestos de trabajo. A continuación, se muestra una figura donde se muestra una comparativa de las necesidades de automatización más demandadas de aplicación a las FAS en el pasado 2020. Así mismo, se podría identificar el grado de riesgo que se puede observar al seleccionar a determinado personal para algunas vacantes específicas.

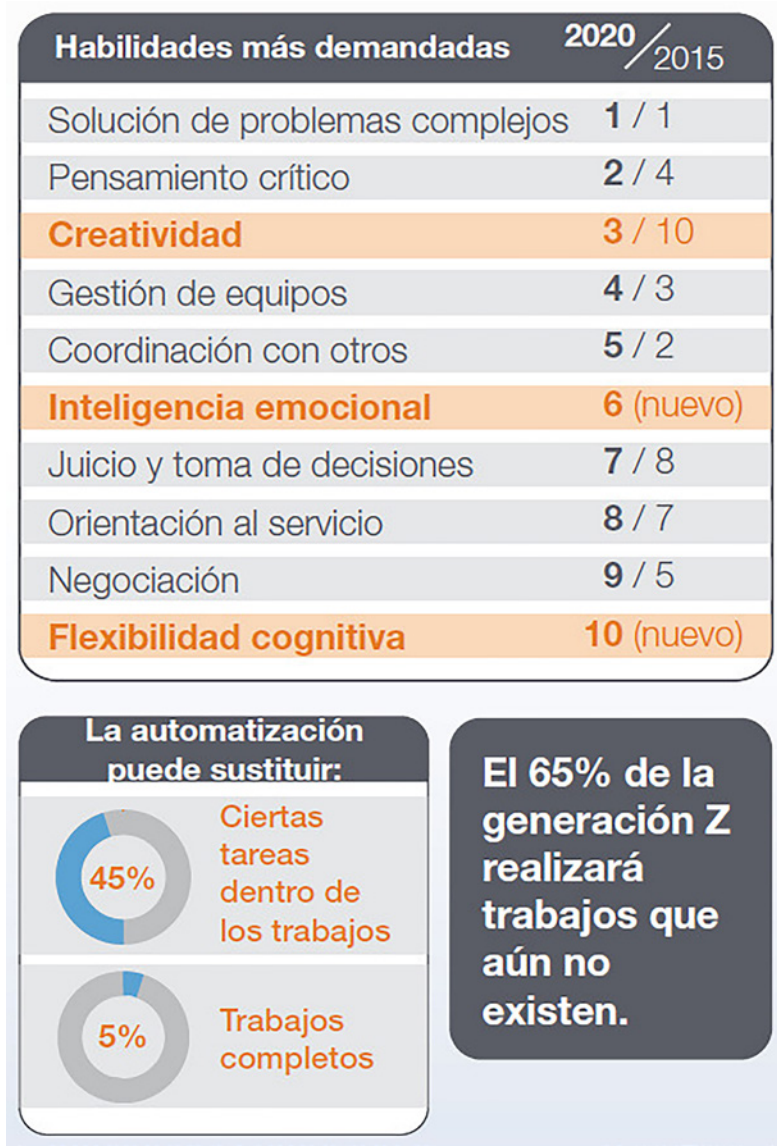


Figura 2. Automatización de posibles habilidades más demandadas para el MINISDEF [4]

4.1 Las redes sociales como marca de empleador y herramienta de selección

Las redes sociales pueden ser un elemento estratégico importante a la hora de lanzar advertencias a determinados perfiles de candidatos para poder atraerlos a las empresas. El empleo de las redes sociales es ya utilizado por un 79 % de las compañías punteras. Es por ello por lo que el MINISDEF debe seguir trabajando en esta vía de reclutamiento tan actual y exitosa para contar con los mejores candidatos dentro del ministerio. Además de esta finalidad, también motivará al personal militar para que no abandone el ejército, debido a que puedan ofrecerle un nuevo puesto desde otras empresas competitivas. Así mismo, también se tendrá una visión de la marca del empleador de empresas que demanden un perfil militar entre sus empleados (se va a conocer al enemigo). [5]

Así mismo, este canal puede ser utilizado como vía para difundir la cultura de defensa a todo aquel personal que está interesado en adquirir la condición de militar, así como aquellos que están desarrollando su actividad profesional e inicialmente no tienen pensado cambiar de empresa (posibles reservistas voluntarios). Por otra parte, el uso de las redes sociales también se considera una herramienta para constituir la marca como empleador propio (*employer branding*) que permite a las FAS establecer su estrategia para la captación del talento ya que es considerado como segundo factor clave en la búsqueda de talento.

5. Conclusiones

Es un hecho que las empresas continúan, como desde hace ya más de un siglo, con la guerra por la caza del talento, para contar con los mejores trabajadores entre su personal. Está demostrado que esta política de empresa logra que la organización se dirija en la dirección de la eficiencia y supervivencia en un entorno de continuos cambios.

Es aquí donde aparece la estrategia de desarrollo y captación de talento denominada la marca del empleador (ME) o *employer branding*, cuyo fin último es conseguir que las organizaciones sean referencia de calidad (atractivas) para aquellos futuros empleados que deseen trabajar en un equipo donde todos aporten a la organización, consiguiendo que esta captación sea dirigida hacia aquellos cuyo talento se encuentre más alineando a los objetivos de dicha organización. En este contexto, en el presente trabajo se han analizado los beneficios organizacionales inducidos por esta herramienta estratégica.

En este aspecto, el Ministerio de Defensa ha puesto en práctica estrategias como: las redes sociales, la continua formación entre sus cuadros de mando y la proyección a nivel empresarial fuera de la organización, que han logrado que el personal militar sea percibido ante la sociedad como personal con alto grado de capacidades y de talento que se muestra por su empleabilidad para ocupar gran diversidad de vacantes

que requieren diferentes tipos de capacidades. Dichas capacidades se adquieren con una cualificada preparación y capacidad de adaptación.

Así mismo, es un hecho que, las Fuerzas Armadas deben estar preparadas con grandes capacidades y talento para poder llevar a cabo cualquier tipo de cometidos que demande la sociedad, como es el caso más reciente del control de la pandemia Covid-19 mediante las operaciones Balmis y Baluarte, donde está quedando de manifiesto que el personal que forma el ejército posee el talento necesario para asumir nuevos cometidos para el beneficio de la sociedad.

Como herramienta fundamental para el avance y progresión de las empresas, se ha podido observar, mediante el desarrollo del presente trabajo, que es necesario el apoyo de las TIC. Por ello, consideramos que las Fuerzas Armadas deben tenerlas presentes para todo el proceso de gestión del talento entre su personal.

Por ello, el trabajo realizado permite definir y aportar un conjunto de líneas de acción encaminadas a la consecución de una excelente imagen de marca en las FAS, como paso previo imprescindible para la gestión del talento, materializada, principalmente, en la captación de los mejores candidatos disponibles en la sociedad.

Teniendo en cuenta lo presentado en este trabajo, se puede afirmar que el uso de Internet como canal de comunicaciones para redes clasificadas podría ser una solución versátil y segura para los despliegues militares fuera de territorio nacional. La solución técnica propuesta cumple con los estándares de seguridad exigidos por la normativa vigente para sistemas clasificados y cuenta con la enorme ventaja que tiene el despliegue mundial de Internet con su gran capilaridad, permitiendo un acceso a la red de transporte en cualquier parte de del mundo con un ancho de banda aceptable a un coste razonable.

El coste del equipamiento necesario en la solución técnica propuesta es casi cuatro veces más económico que las soluciones tradicionales y el precio por Mbps también es más ventajoso.

El gran hándicap de esta solución es la disponibilidad debido a la total dependencia de los proveedores de los servicios de Internet y al tiempo de aprovisionamiento, sumado a que en las zonas de operaciones suele haber conflictos que pueden degradar o inutilizar el acceso a Internet. Los servicios de las redes clasificadas se pueden ver interrumpidos o degradados sin previo aviso y la prioridad de su restablecimiento está fuera de las capacidades de las fuerzas desplegadas.

Ante estos hechos, se considera que la solución técnica propuesta es apropiada para el despliegue de unidades en zona de operaciones, pero debería tener como respaldo una solución tradicional, es decir, acceso a satélites gubernamentales o con varios proveedores de Internet diferentes que hicieran de *backup*.

Agradecimientos

En primer lugar, me gustaría agradecer a mi tutor, don Francisco Javier Rodríguez Rodríguez por la ayuda prestada en la realización de este TFM y por la atención puesta sobre mí en el transcurso del mismo.

Asimismo, me gustaría agradecer a mi familia por el apoyo mostrado durante todo este tiempo y ser mi principal sustento, especialmente a mis dos hijos Paulino y Ana, por ser el motor de mi vida y el aliciente a todos mis retos personales.

Por último, y no por ello menos importante, quisiera agradecer a mis compañeros de máster, que han promovido crear un clima de compañerismo, trabajo en equipo y camaradería en beneficio de alcanzar el máximo provecho a este año y medio de formación.

Referencias

[1] «VUCA, la tormenta perfecta y la formación como salvavidas». [En línea]. Disponible: https://medium.com/uxerschool/vuca-la-tormenta-perfecta-y-la-formaci%C3%B3n-como-salvavidas-de82221d6806. [Último acceso: 13 diciembre 2020].

[2] «La tecnología como aliada de los RRHH». [En línea]. Disponible: https://www.glocalthinking.com/la-tecnologia-como-aliada-de-los-recursos-humanos. [Último acceso: 20 noviembre 2020].

[3] «Sodexo». [En línea]. Disponible: ttps://www.sodexo.es/centro-conocimiento/nuevas-tecnologias-y-aplicacion-en-rrhh/. [Último acceso: 28 noviembre 2020].

[4] J. P. C. MANPOWERGROUP, (2020). «Automatización de posibles habilidades más demandadas».

[5] «Uso de las Redes Sociales en las FAS». [En línea]. Disponible: https://www.equiposytalento.com/talentstreet/noticias/2019/07/02/las-redes-sociales-herramienta-clave-para-el-exito-de-las-estrategias-de-seleccion/3457/. [Último acceso: 20 noviembre. 2020].

La atracción de talento mediante la marca clave de competitividad en las organizaciones: Aplicación de TIC al ámbito de Defensa.

Autor: Paulino Vico Cardenete

Directores: Francisco Javier Rodríguez Rodríguez

Identificación Talento

Atracción Talento

ENTORNO VUCA

Employer Branding

Desarrollo y Retención Talento

Máster Universitario en Dirección TIC para la Defensa, 2019/2020

Trabajos Fin de Máster

Especialidad en sistemas y tecnologías de la telecomunicación

Aproximación a la topología de la red de telecomunicaciones terrestres de la I3D del Ministerio de Defensa

Autor: Bargueño Díaz-Villarejo, Félix (fbardia@et.mde.es)
Directores: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – Con este trabajo se pretende realizar una primera aproximación a la Topología de la red de telecomunicaciones terrestres de la infraestructura integral de información para la defensa (I3D), partiendo de la infraestructura existente en la actualidad.

Los datos con los que se ha realizado este trabajo no son los reales, por razones de seguridad, dado que no se pretende definir exactamente la red, sino la posibilidad de utilización del algoritmo propuesto y sus bondades.

Los requisitos que se le van a pedir a la red, se centran en los siguientes parámetros:

- Capacidad de salida desde cada nodo.
- Redundancia de enlaces.
- Preferencia estricta de unos tipos de enlaces sobre otros.

El problema consiste en definir los enlaces necesarios entre nodos y las capacidades de los mismos que satisfagan los requisitos.

Estudiados diversos enfoques desde la teoría de grafos, dadas las preferencias estrictas de unos enlaces sobre otros, se opta por aplicar el algoritmo de Prim adaptado al problema, calculando posteriormente las capacidades necesarias de cada enlace para esa solución.

Para asegurar la supervivencia de los servicios en caso de caída de un enlace, se simula la caída uno a uno, volviendo a aplicar el algoritmo completo para hallar una nueva solución.

Finalmente se ha comprobado que el algoritmo propuesto es válido para ser utilizado con datos reales, identificando posibles cuellos de botella en la red, definiendo los enlaces necesarios y las capacidades de los mismos, para poder cumplir los requisitos.

Palabras clave – Topología de la red de telecomunicaciones terrestres de la I3D, requisitos, preferencia estricta, teoría de grafos, algoritmo de Prim.

1. Introducción

1.1. Situación

La situación de partida en las que coexisten diversidad de redes de telecomunicaciones, tal y como se observa en la figura 1, como pueden ser la WAN de propósito general, donde discurren los servicios administrativos, con una red para voz y otra para datos; y las diferentes redes de Mando y Control, conlleva la existencia de limitaciones en el acceso a la información, redundancias y dificultades para su gestión y planeamiento. Por lo tanto, se hace necesario la convergencia de las redes hacia una infraestructura única que integre a las mismas.

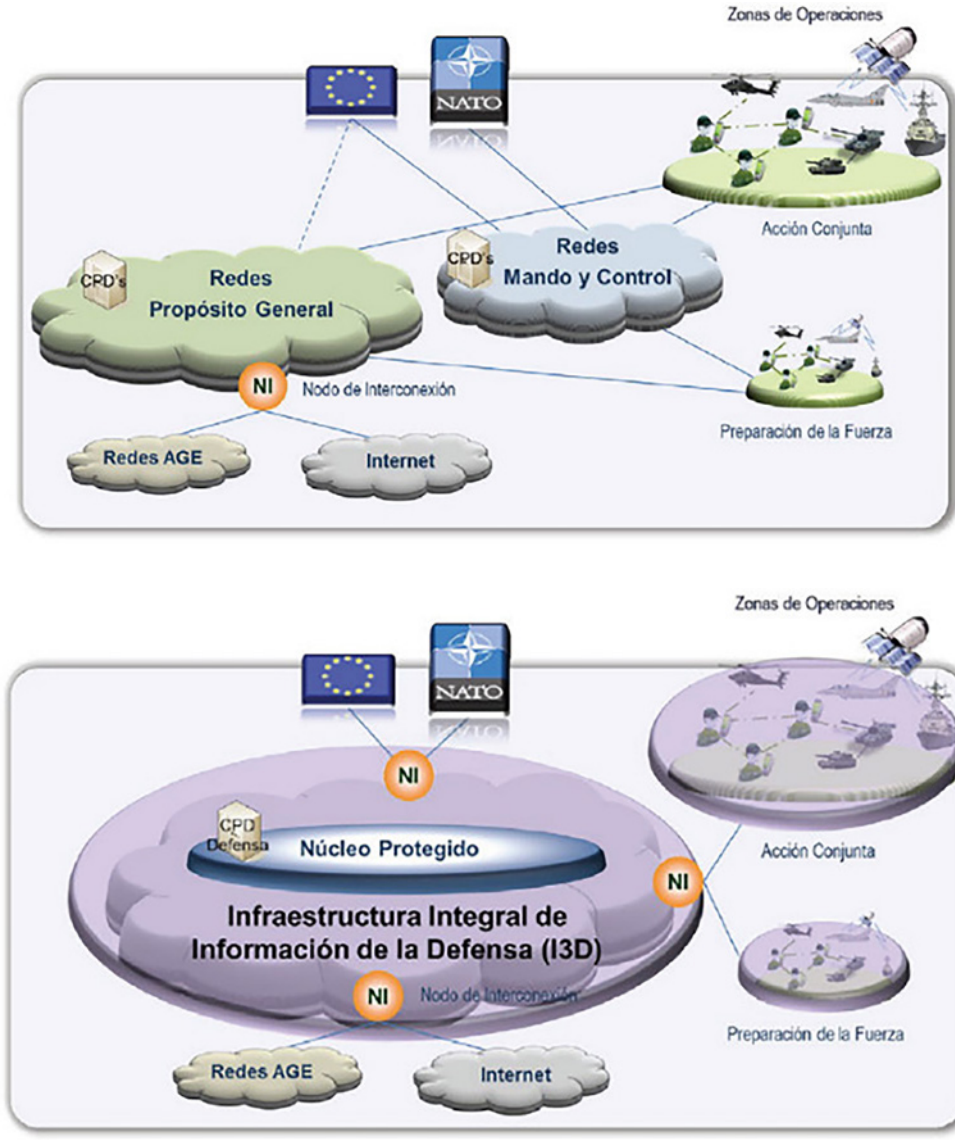


Figura 1. Situación de partida y final de la I3D tomadas de [1]

A consecuencia de lo marcado en el Plan de transformación digital de la Administración General del Estado (AGE) y sus Organismos Públicos [2], en 2020, las comunicaciones de los emplazamientos cuyos sistemas no afecten a la defensa o manejen información clasificada deberían ser suministradas por la AGE a través de la red SARA (Sistemas de Aplicaciones y Redes para las Administraciones). El resto de emplazamientos formarán parte del núcleo protegido de la I3D.

En la actualidad se está empezando a estudiar la unificación de la red de telecomunicaciones terrestres del Ministerio de Defensa para, partiendo de la infraestructura existente, definir una red de telecomunicaciones única, como se muestra en la situación final de la figura 1.

1.2. Objetivo

El objetivo es utilizar la teoría de grafos para diseñar un algoritmo que se pueda implementar para definir la topología de Red de Telecomunicaciones Terrestres para dar servicio a la WAN de la I3D, aprovechando la infraestructura existente.

2. Problema y solución

El primer problema encontrado es las diferencias entre las denominaciones e identificaciones de los nodos en las diferentes fuentes de información utilizadas, por lo que el trabajo de depuración de los datos ha sido arduo. Tras un primer intento de automatización, en la mayoría de los casos se ha debido realizar manualmente y en ocasiones incluso contrastar los datos con fuentes diferentes a los ficheros suministrados.

Finalmente, al tratar los datos, se observó la existencia de una zona con una alta densidad de enlaces formada por anillos de fibra óptica (FO). En esta zona se encuentran incluidos los Centros de Procesos de Datos (CPD), existiendo al menos dos tendidos de 64 fibras que une cada emplazamiento con otros, lo que supera ampliamente las capacidades requeridas. Todos los nodos de esta zona son considerados para el presente trabajo como un nodo *sumidero*, pues es capaz de absorber y reencaminar todo el tráfico entrante y se considera como origen o destino de todas las comunicaciones.

2.1. Requisitos necesarios

Aunque todavía se están fijando los requisitos por parte de las entidades involucradas, inicialmente se van a considerar dos tipos: capacidad o velocidad de transferencia de datos de salida necesaria en cada nodo o emplazamiento; y número de enlaces para asegurar la continuidad del servicio.

Respecto a la capacidad, el ancho de banda necesario para cada tipo de nodo para este trabajo es el que figura en la tabla 1 siguiente, correspondiéndose el tipo 5 o de tránsito, a un nodo que no necesite de capacidad adicional de la red de telecomunicaciones.

Tipo	Capacidad
1	10 Gbps
2	1 Gbps
3	400 Mbps
4	100 Mbps
5	Tránsito

Tabla 1. Tipo de nodo y capacidad requerida

Se parte de la hipótesis de que el número de enlaces necesario por nodo del núcleo protegido será de 2, de forma que en todo momento estará asegurado el servicio en caso de caída de un enlace.

Por otra parte, los enlaces de la Red de Telecomunicaciones Terrestre de la I3D se pueden clasificar en tres tipos:

- Fibra óptica en propiedad.
- Fibra óptica de terceros.
- Radioenlaces.

Esta clasificación es importante, porque a la hora de diseñar la red de telecomunicaciones terrestre va a existir una preferencia estricta entre los tipos de enlace, precisamente en el orden señalado anteriormente. Las razones para estas preferencias se centran en la mayor capacidad, fiabilidad y seguridad de la FO y el menor mantenimiento, pues los radioenlaces están generalmente ubicados en zonas altas de difícil acceso, donde es necesario mantener una infraestructura aislada que incluye los tendidos eléctricos, caminos, desbroce de maleza y seguridad perimetral, y ya sólo los gastos de desplazamiento, en caso de ser necesaria una actuación, se ven incrementados.

Aunque no se han marcado requisitos de latencia, cumpliendo con las preferencias anteriores, se intentará que el enlace tenga el menor número de saltos posible, lo que facilitará que se produzcan las menores latencias y pérdidas posibles.

2.2. Definición del problema

El problema consiste en definir los enlaces necesarios entre nodos y las capacidades de los mismos que satisfagan los requisitos.

Como se tiene que partir de la infraestructura existente, se podrían utilizar dos enfoques: considerar la red existente con todas sus

características, entre ellas la capacidad de los enlaces o considerar sólo los enlaces, sin la capacidad.

Considerando la red de telecomunicaciones terrestres existente con sus capacidades, se debería de tratar como un problema de flujo máximo. Este problema se podría resolver con el algoritmo de Ford-Fulkerson [3]. Sin embargo, este enfoque no se va a considerar y desarrollar por varios motivos entre los que destacan que los radioenlaces de los que se parte, son bastantes antiguos y los anchos de banda son a todas luces insuficientes para los requerimientos de los nuevos sistemas; y que considerando la capacidad se podrían llegar a utilizar varios enlaces entre dos nodos sumando las capacidades de los mismos, pero se intenta disminuir el número de enlaces necesarios, con la economía de medios que conlleva.

Al suponer la red de telecomunicaciones terrestres sin capacidades, solamente se considera el *esqueleto* de la infraestructura existente, es decir, la existencia o no de enlace entre dos emplazamientos o nodos. Además, se tiene en cuenta el tipo de enlace por los requisitos exigidos de preferencias de unos tipos de enlace sobre otros. Con este planteamiento, aunque seguramente sea necesario aumentar la capacidad de los enlaces utilizados, se reduce el número de enlaces necesarios, con el consiguiente ahorro en mantenimiento de infraestructuras no necesarias. Esta visión parece más adecuada estratégicamente, por lo que es la que se ha desarrollado.

Los problemas a los cuales será necesario dar solución serán, en primer lugar, determinar qué enlaces se van a utilizar y después calcular la capacidad requerida por cada uno de ellos.

2.3 Solución

2.3.1 Aproximación inicial

Planteada la problemática, y dado que inicialmente el número de nodos y aristas del grafo es de 280 y 361 respectivamente, y que la potencia de los ordenadores actuales es alta, tanto en procesamiento como en memoria, el problema de determinar el esqueleto inicial de la red se podría resolver utilizando casi cualquier algoritmo. Se comentan a continuación las principales alternativas.

Al considerar la red sin capacidades, esta se puede representar por un grafo en el que los emplazamientos son los nodos y los enlaces son las aristas. El problema resultante se puede afrontar desde dos perspectivas en teoría de grafos: problema del camino más corto o árbol de expansión mínima. En ambos es necesario determinar una métrica. La solución más sencilla es atribuir a todos los enlaces un coste o distancia unidad. Sin

embargo, adoptando esta solución no se cumpliría el criterio de preferencia de enlaces. Por tanto, para cumplir con el criterio de las preferencias bastaría con hacer que el coste de un tipo de enlaces sobre otro difiera en un orden de magnitud del total de enlaces existentes. Como el total de enlaces del problema es de 361 < 103, basta con multiplicar cada coste sobre el anterior en 103. La solución más sencilla, partiendo del valor unidad para la FOP es asignar los siguientes costes en función del tipo de enlace, tal y como se observa en la tabla 2:

Tipo enlace	Coste
FO en propiedad	1
FO de terceros	1.000
Radioenlace	1.000.000

Tabla 2. Costes por tipo de enlace.

El problema del camino más corto está ampliamente estudiado en teoría de grafos y bastaría con aplicar el algoritmo de Dijkstra [4] o el de Bellman-Ford [5]. Inicialmente no se tiene previsto asignar costes negativos por lo que directamente se desecha el algoritmo de Bellman-Ford y se utilizaría el de Dijkstra.

Para calcular el árbol de expansión mínima existen dos algoritmos, el de Prim [6] y el de Kruskal [7]. La complejidad temporal de los algoritmos es diferente pero dadas las dimensiones del problema y la potencia de los ordenadores actuales este aspecto no va a resultar decisivo a la hora de elegir uno u otro. Dadas las peculiaridades del problema, al final se opta por utilizar el algoritmo de Prim, pero con modificaciones o mejoras.

Hasta ahora se han planteado dos posibles soluciones para solucionar el problema inicial: el cálculo del camino más corto con el algoritmo de Dijkstra, o el árbol de expansión mínimo con el algoritmo de Prim. Como no es necesario ir almacenando distancias desde el nodo sumidero (necesario en el algoritmo de Dijkstra), y al existir una preferencia estricta de unos enlaces se opta por el algoritmo de Prim de más fácil implementación.

A grandes rasgos, la mejora introducida en el algoritmo de Prim mejorado es de rapidez, particularmente interesante en el problema a resolver donde existe una gran cantidad de enlaces con costes iguales y donde la diversidad de los mismos es mínima, lo que hace que las necesidades de máquina en la implementación del algoritmo sean mínimas. También se ha considerado un procedimiento de interrupción en caso de que el grafo no sea conexo. Este caso puede presentarse si en el ciclo se utilizan otro tipo de enlaces distintos a los considerados, como puede ser el caso de enlaces satélite.

En una iteración, en el caso de poder enlazar un vértice o nodo por dos lados con la misma distancia, aunque no se han considerado latencias,

se cogerá como antecesor el vértice que presente menos lados o saltos para llegar al nodo origen o sumidero. En este punto el algoritmo para y presenta los datos de los nodos que no es posible enlazar con este nodo sumidero para su estudio posterior.

2.3.2 Cálculo de las capacidades de los enlaces

Hasta ahora sólo se sabe qué enlaces son necesarios para conseguir enlazar todos los nodos, pero no se han detallado las capacidades de los mismos.

La solución del cálculo de capacidades es simple. Basta con ir recorriendo los *caminos* desde los extremos más alejados del sumidero u hojas del árbol e ir añadiendo las capacidades que demanda cada nodo existente en ese recorrido.

Ahora bien, existen nodos que son solamente de tránsito y no demandan capacidad. Puesto que los algoritmos empleados conectan todos los nodos del grafo, en este apartado habrá que fijarse si hay enlaces que, tras el cálculo anterior, su capacidad resultante sea nula. Estos enlaces con capacidad nula tendrán que ser eliminados de la solución pues realmente no son necesarios.

Otra forma de realizar lo anterior es comprobando que los extremos del árbol u hojas no son nodos de tránsito. Estas hojas y los enlaces que las sustentan se podrían ir podando u eliminando en dirección a la raíz o sumidero hasta encontrar un nodo que no sea de tránsito. Para llevar a cabo este procedimiento no sería necesario calcular las capacidades y se podría realizar al finalizar el cálculo del procedimiento anterior. Sería suficiente con ir etiquetando los nodos que son extremos del árbol o camino.

2.3.3 Redundancia de enlaces

Realmente con la solución inicial existirán muchos nodos con al menos dos enlaces. Bastará con que el nodo no sea un extremo para que al menos esté enlazado con su nodo antecesor y con los nodos de los que él es antecesor.

Sin embargo, resulta necesario disponer de redundancia en los enlaces para permitir la recuperación de la red. Lo primero que se nos podría ocurrir es unir nodos extremos entre sí para asegurar la existencia de ciclos en el grafo. Esta solución no es factible por dos motivos. El primero es que no existe infraestructura. El segundo es que, aunque exista la conexión entre esos extremos, al enlazarlos se crea un ciclo que es válido ante la caída de un enlace, pues seguirá existiendo un camino entre el resto de nodos del ciclo. Pero el problema es que sólo nos servirá si el ciclo formado contiene

al nodo sumidero, porque en caso contrario, siempre existirá un enlace que, de fallar, incomunicaría el ciclo formado con el nodo sumidero, y se dejaría de dar servicio, tal y como se ilustra en la figura 3.

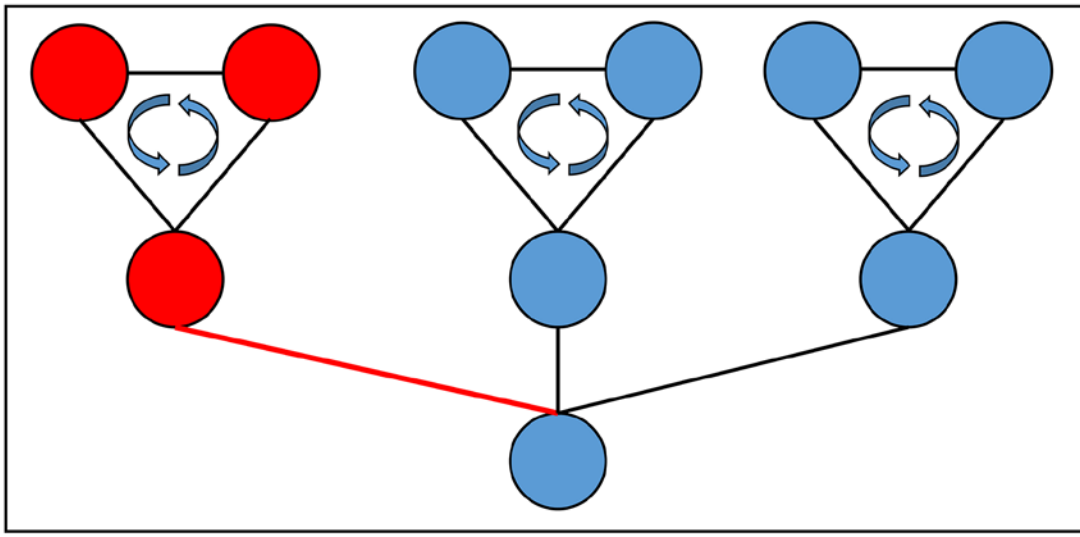


Figura 3. Ciclo sin enlace ante la caída de un enlace (en rojo)

Además, la solución ideal sería crear un anillo con todos los nodos extremos. De esta manera se aseguraría el enlace con el nodo sumidero, a pesar de que pudieran caer varios enlaces. Esta opción es inviable por la no existencia de infraestructura, pero también considerando el despliegue en todo el territorio nacional, ello supondría crear un anillo que prácticamente rodearía la península.

Realmente, con el requisito de que el número de enlaces por nodo del núcleo protegido tiene que ser de dos, lo que se pretende es asegurar que se continúa dando servicio, aunque se caiga un enlace, por lo que una reformulación del requisito en ese sentido se hace necesario, evitando de esta manera los problemas mostrados en la figura 3, que, aunque cumple con el requisito de que el número de enlaces de cada nodo sea de dos, no da servicio a los nodos marcados en rojo.

Por otra parte, al eliminar una arista, el resultado es la obtención de dos grafos conexos, por lo que parece lógico pensar que bastaría con utilizar cualquier arista existente para unir esos dos grafos y generar un único grafo conexo. Sin embargo, esta solución no valdría pues afectaría a los caminos y las capacidades necesarias, tal y como se ve en la figura 4.

La solución al problema será ir eliminando los enlaces de la solución original uno a uno, quitar la etiqueta de los nodos afectados o no enlazados por la eliminación de ese enlace y aplicar de nuevo los pasos anteriores.

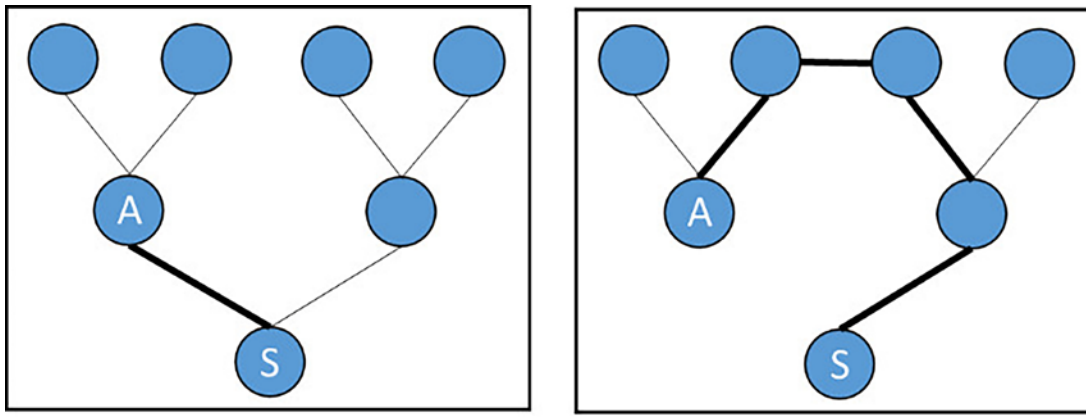


Figura 4. Diferencia de caminos entre S y A al quitar en enlace SA

Para el cálculo de las capacidades se compararán las inicialmente obtenidas con las nuevas quedando como resultado final la mayor de las dos. De esta forma, se asegura que siempre habrá enlace de todos los nodos con el nodo central, aunque caiga un enlace.

3. Resultados

Todas las soluciones se han implementado usando una solución sencilla realizando los algoritmos en VBA.

Cuando se ejecuta por primera vez el algoritmo de Prim se consigue detectar aquellos nodos que no es posible enlazar. Esto indica que no existe ningún camino o enlace terrestre que llegue desde esos nodos al sumidero. La interpretación que se le daría a estos resultados, partiendo del supuesto de que actualmente todos los nodos tienen conexión hacia los CPD, que se encuentran en el sumidero, es que en el presente trabajo solo se han considerado los enlaces terrestres. Sin embargo, además de los enlaces terrestres también se utilizan enlaces por satélite, por lo que es de sospechar que estos grupos de nodos dispongan al menos de un enlace satélite que los conecte con el resto de la red.

Tras la realización del diseño inicial de la red sin redundancia de enlaces, se trata de simular aquellos nodos que se quedarían sin conexión ante la caída de los enlaces utilizados en el diseño inicial de la red. En ningún caso se consideran ya los nodos *no conectados* tratados en el apartado anterior. Los resultados que se ofrecen en este apartado son útiles para identificar cuellos de botella en la red, identificando nodos o grupos de nodos que en el camino hacia el nodo sumidero solo dispongan de una alternativa de enlace para unirse al resto de la red.

La solución a este problema se puede afrontar secuencialmente de la siguiente forma. Una vez identificados los nodos, comprobar que no

existe algún enlace satélite que los comuniquen con el resto de la red. En caso negativo, si se pretendiera intentar automatizar y que se ofrecieran propuestas de nuevos enlaces, se podría realizar introduciendo los datos de las coordenadas de los emplazamientos y buscando los emplazamientos más cercanos. La limitación del número de emplazamientos propuesto se puede realizar por número de emplazamientos o por distancia. Finalmente se debería valorar la viabilidad de las propuestas realizadas, la posibilidad de doblar el enlace que se ha caído con otra tecnología distinta (por ejemplo, si el enlace caído es de FO, montar un radioenlace) o asumir el riesgo de que ese emplazamiento sólo disponga de un enlace.

Una vez analizados los nodos no conectados y aquellos sin conexión ante una caída, se va a ver los enlaces junto con las capacidades necesarias para enlazar los nodos, tanto en la primera ejecución del algoritmo (sin redundancia de enlaces), como la capacidad final necesaria de estos tras la simulación de la caída de enlaces, que se correspondería a la solución final para cumplir los requisitos establecidos (a excepción de los casos considerados en los puntos anteriores).

Lo más significativo es que de los enlaces considerados, más de la mitad en la solución final tienen una capacidad igual a cero, o lo que es lo mismo, enlaces que no proporcionan servicio a ningún nodo de los que demandan capacidad, y por tanto no son necesarios, siendo la mayoría radioenlaces. Todos estos enlaces se podrían desmontar con el consiguiente ahorro económico en mantenimiento o alquiler.

El motivo de esta cantidad de enlaces innecesario puede ser debido a que muchos de los nodos existentes en la actualidad no van a formar parte del núcleo protegido de la I3D y las comunicaciones de estos nodos van a ser suministrados por la red SARA, correspondiéndose a establecimientos que no disponen de sistemas que afecten a la defensa o manejen información clasificada.

4. Conclusiones

Se puede concluir que el algoritmo propuesto sí que es válido para ser utilizado y proporcionar una primera aproximación a la topología de red de telecomunicaciones terrestre de la I3D, identificando posibles cuellos de botella en la red y definiendo los enlaces necesarios y las capacidades de los mismos, hasta donde permite la red considerada. Esta primera aproximación se debe complementar con el estudio de los casos en los que no se pueden cumplir los requisitos.

También se podría utilizar como un algoritmo de enrutamiento centralizado estático creando las tablas de enrutamiento basadas en los nodos predecesores, calculados y almacenados al ejecutar el algoritmo. La tabla inicial sería inmediata en la primera iteración o inicial del algoritmo.

En las sucesivas iteraciones realizadas simulando la caída de los enlaces, se podrían también almacenar en una tabla los resultados asociados a ese enlace, de manera que cuando el sistema de supervisión de la red detecte la caída de un enlace, o bien se envíen automáticamente los nuevos enrutamientos almacenados en las tablas, o incluso tenerlas ya almacenadas en los distintos nodos de la red y lo único que se deba transmitir es el identificador del enlace caído, para que cada nodo afectado aplique la nueva tabla de enrutamiento asociada, pasando a ser un enrutamiento distribuido.

Se podría ampliar introduciendo también los enlaces por satélite, con lo que se toda la red de telecomunicaciones de la I3D. Dadas las especiales características de estos, sólo se utilizarían como última posibilidad. Esto se traduciría para el algoritmo en atribuir a estos enlaces un coste superior que esté un orden de magnitud respecto al número total de enlaces por encima de los tipos de enlaces más costosos hasta ese momento. En nuestro caso sería de 109.

Finalmente, si se decide tener una mayor seguridad en la red basada en una mayor redundancia, se podrían hacer nuevas iteraciones simulando la caída de dos o más enlaces simultáneamente y calculando los enlaces y las capacidades necesarias. Aunque la caída de más de dos enlaces debería considerarse como excepcional, y llegado el caso incluso se podría suplir con la utilización, aunque limitada en capacidad, de medios desplegables.

Referencias

[1] Instrucción 58/2016, de 28 de octubre, del secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa, BOD, 2016, pp. 26181-26351.

[2] «Portal de administración electrónica,» [En línea]. https://www.administracionelectronica.gob.es/pae_Home/dam/jcr:898162f1-2682-483e-9e43-50f2d3a08eff/20151002-Plan-transformacion-digital-age-oopp.pdf. [Último acceso: 11 10 2020].

[3] L. R. Ford y D. R. Fulkerson, (1962) «Flows in Networks» Princeton University Press.

[4] E. Dijkstra, «A note on two problems in connection with graphs» Number. Math. 1, pp. 269–271, 12 10 1959.

[5] C. E. L. R. L. R. a. C. S. Thomas H. Cormen, (2001). Introduction to Algorithms, Second Edition, Vols. 1 de 2, Section 24.1: The Bellman-Ford algorithm, MIT Press and McGraw-Hill, pp. 588–592.

[6] R. C. Prim, (1957). «Shortest connection networks and some generalisations» Bell System Technical Journal, n.º 36, pp. 1389–1401.

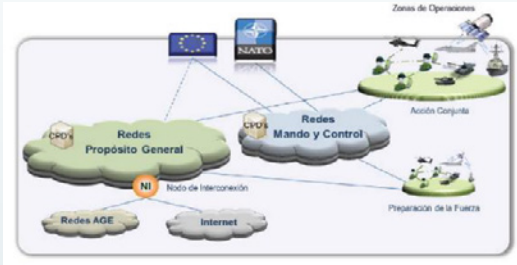
[7] J. B. Kruskal, (1956) «On the shortest spanning subtree of a graph and the traveling salesman problem» Proc. Amer. Math. Soc., n.º 7, pp. 48-50.

Aproximación a la Topología de la Red de Telecomunicaciones Terrestres de la I3D del Ministerio de Defensa

Autor: Félix, Bargueño, Díaz-Villarejo
Directora: Milagros, Fernández, Gavilanes

Introducción

Con este trabajo se pretende realizar una primera aproximación a la Topología de la Red de Telecomunicaciones Terrestres de la Infraestructura Integral de Información para la Defensa (I3D), partiendo de la infraestructura existente en la actualidad.



Desarrollo

Lo que se pretende es definir un algoritmo que pueda utilizarse para ayudar a definir la red y estudiar sus bondades.

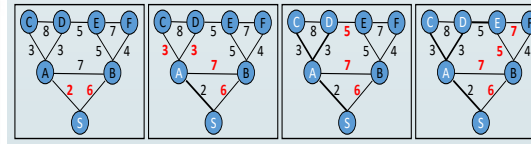
Los requisitos que se le van a pedir a la red, se centran en los siguientes parámetros:

- Capacidad de salida desde cada nodo.
- Redundancia de enlaces.
- Preferencia estricta de unos tipos de enlaces sobre otros.

El problema consiste en definir los enlaces necesarios entre nodos y las capacidades de los mismos que satisfagan los requisitos.

Estudiados diversos enfoques desde la teoría de grafos, dadas las preferencias estrictas de unos enlaces sobre otros, se opta por aplicar el algoritmo de Prim mejorado y adaptado al problema, calculando posteriormente las capacidades necesarias de cada enlace para esa solución.

Para asegurar la supervivencia de los servicios en caso de caída de un enlace, se simula su caída uno a uno, volviendo a aplicar el algoritmo completo para hallar una nueva solución.



Conclusiones

Se ha comprobado que el algoritmo propuesto es válido para ser utilizado con datos reales, identificando posibles cuellos de botella en la red, definiendo los enlaces necesarios y las capacidades de los mismos, para poder cumplir los requisitos

Reingeniería de procesos para la implantación de un sistema de calidad en un laboratorio de informática forense

Autor: González Carvajal, Juan Carlos (jcgc@interior.es)
Directores: Pérez Rivas, Francisco Manuel (frperez@icoiig.es)
y Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – La rápida evolución tecnológica y el modo en el que la digitalización se ha implantado en todos los ámbitos de nuestra vida, hace que las evidencias digitales, sean cada vez más importantes para resolver problemas en el ámbito penal, civil, laboral o mercantil.

Un laboratorio de informática forense es el encargado de generar estas evidencias digitales, pero el mismo debe estar actualizado y debe estar gestionado correctamente si quiere ser eficiente y competitivo en el mercado.

El objetivo de este trabajo de investigación es mejorar un laboratorio de informática forense, el mismo no está siendo productivo y está perdiendo cuota de mercado respecto a sus competidores.

Para poder llevar a cabo esta investigación, se ha realizado un estudio de cada una de las fases fundamentales de la actividad forense, analizando las metodologías y recomendaciones más valoradas.

Para la metodología de informática forense se ha decido utilizar la del especialista Eoghan Casey en sus cuatro fases, preparación, conservación, análisis y reconstrucción. Para la mejora de los procesos se ha llevado a cabo una reingeniería de los mismos con las tareas de revisión, actualización y mejora continua. Una vez realizados estos pasos se llevará a cabo la implantación de un sistema de gestión de la calidad basado en la norma UNE-EN ISO 9001:2015 y que el mismo pueda ser certificable.

Se pretende que la organización madure, que se conozca mejor interna y externamente, que este conocimiento le permita aprovechar mejor las oportunidades y que pueda identificar y evitar que se materialicen las amenazas existentes. Mejorar la imagen de la organización frente a los clientes y las demás partes interesadas. Todo ello con una metodología de mejora continua orientada a la excelencia.

Una vez aplicados los cambios, el laboratorio de informática forense se encuentra preparado para afrontar los nuevos retos tecnológicos y normativos además de ser competitivo en el mercado.

Palabras clave: procesos, calidad, informática, forense, mejora.

1. Introducción

La calidad en una organización son todas aquellas características que le permiten satisfacer sus necesidades implícitas o explícitas. La calidad mejora los productos y servicios, reduce los costes y permite incrementar la rentabilidad financiera. La calidad es el objetivo que orienta todas las actuaciones de la organización, generando integración y motivación de los trabajadores.

La reingeniería de procesos, consiste en llevar a cabo una revisión profunda y el rediseño potente de los procesos de una organización.

La calidad total está relacionada con procesos de mejora gradual, esta calidad se alcanza llevando a cabo cambios parciales o moderados en la organización. Sin embargo, la actividad de reingeniería de procesos implica cambios más profundos y radicales.

Aunque muchos opinan que estos conceptos son opuestos, y aunque efectivamente existen muchas diferencias, hay varias similitudes entre los dos enfoques. Los dos implican cambios, mientras la calidad lleva a cabo los cambios de forma gradual, la reingeniería los hace de forma drástica. Las dos actividades necesitan de unos requerimientos de formación e información, requieren de datos objetivos, ambos tienen como fin la mejora de la organización y el alcance de los objetivos de la misma, todo ello dirigido hacia la excelencia.

La rápida evolución tecnológica y el fuerte incremento de usuarios, hacen que los eventos digitales se multipliquen, esto implica que cada vez se hacen más necesarias las evidencias digitales para dar resolución a numerosos tipos de incidentes, ya sean corporativos, penales, civiles o administrativos. Los peritos informáticos con sus informes o dictámenes deben definir la naturaleza, acciones y autores relacionados con estos incidentes.

Para llevar a cabo esta tarea, es preciso conocer los conceptos fundamentales de su profesión y seguir un procedimiento de investigación estructurado y metodológico.

El objetivo de este trabajo es mejorar un laboratorio de informática forense, realizar los cambios que le permitan mantenerse actualizado y competitivo en el mercado. Para conseguir esto, se realizará una reingeniería de procesos, un análisis de los mismos cambiando aquellos que no sean eficientes o productivos. Una vez que los procesos estén redefinidos, se implantará un sistema de gestión de la calidad enfocado a la mejora continua.

2.Estado del arte de la informática forense

La actividad informática se ha convertido en una práctica cada vez más habitual en nuestra vida diaria a nivel personal y profesional.

Si en los años 60 los sistemas informáticos estaban supeditados a los organismos gubernamentales y la investigación, esa tendencia fue cambiando rápidamente y en los años 70 los *mainframes* ya eran comunes en las grandes empresas. En la década de los 80 aparecieron los minicomputadores o PC, llegando a muchas empresas y centros universitarios, alcanzando a 10 millones de usuarios. Diez años después en los 90, estos ordenadores ya estaban en la pequeña empresa y en los hogares, llegando a 100 millones de usuarios. En el año 2000 los ordenadores portátiles e Internet permitieron alcanzar una cifra aproximada de 1.400 millones de usuarios, representando un 20 % de la población mundial.

Gracias al avance de la ciencia y la tecnología a lo largo del tiempo, el campo de acción de las ciencias forenses se ha hecho más amplio. Con la aparición de los dispositivos de procesamiento automático de información y de la revolución de los sistemas informáticos, nace un nuevo ámbito de acción, la informática forense.

La creciente dependencia de los sistemas informáticos y de los dispositivos digitales ha dado paso a las nuevas oportunidades delictivas. Los ordenadores se usan con más frecuencia como herramienta para el delito, lo que plantea nuevos y constantes retos para los informáticos forenses.

Durante último cuarto del siglo XX se ha generalizado el uso de ordenadores y de Internet. Por todo esto hay que reconocer que la informática forense se encuentra en una etapa de desarrollo frente a la trayectoria histórica de otras ciencias forenses.

La informática forense también presenta debilidades, se diferencia de otras ciencias forenses porque las pruebas que examina son pruebas digitales, para hacer frente a estas debilidades, un laboratorio de informática forense se fortalece implantando un sistema de gestión de calidad, este le permite conocer mejor todos los procesos del mismo y tener una visión rápida de sus fortalezas y debilidades, así como de los riesgos existentes.

3. Metodologías para la mejora

Para llevar a cabo los cambios necesarios, es muy aconsejable apoyarse en normativas, estándares y buenas prácticas ya contrastadas. Debemos poner en práctica las acciones que han demostrado un buen rendimiento en determinados contextos, para que ahora en nuestra situación aporten similares resultados.

3.1. Metodología para la informática forense

En la informática forense se aplican una serie de metodologías orientadas a la investigación forense y pericial, cada una de estas metodologías tiene sus ventajas y sus inconvenientes. Unas metodologías se centran más en la escena del delito, otras en la información y otras en el flujo de la información. Las fases fundamentales de una metodología básica pueden resumirse en cinco, la identificación, la adquisición, la preservación de las evidencias, el análisis y la presentación con el informe. Manteniendo todo el ciclo documentado y verificado.

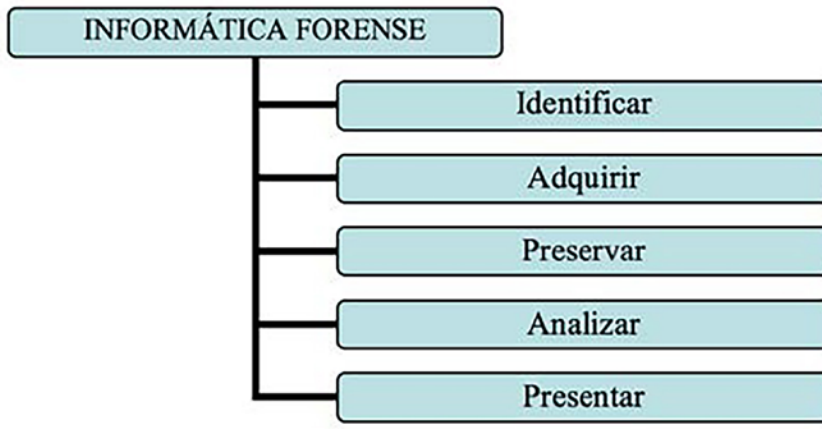


Figura 3-1. Fases básicas de la metodología forense

Para nuestro laboratorio se va a desarrollar la metodología de Eoghan CASEY en su versión del 2011, se ha seleccionado esta metodología porque es la más completa y la que mejor encaja en la tipología de los casos actuales. Esta metodología se estructura en 4 fases y 10 tareas, quedando las fases de esta manera:

[1] Preparación, estudio y documentación

[2] Conservación o recogida

[3] Examen y análisis

[4] Reconstrucción e informes

3.2. Reingeniería de procesos

La reingeniería de procesos es un desarrollo estructurado de revisión, actualización y mejora continua de los procesos internos de las organizaciones, ya sean estratégicos u operativos, que persigue mejorar su rendimiento a partir de pequeños cambios tanto en los sistemas productivos como en los organizacionales.

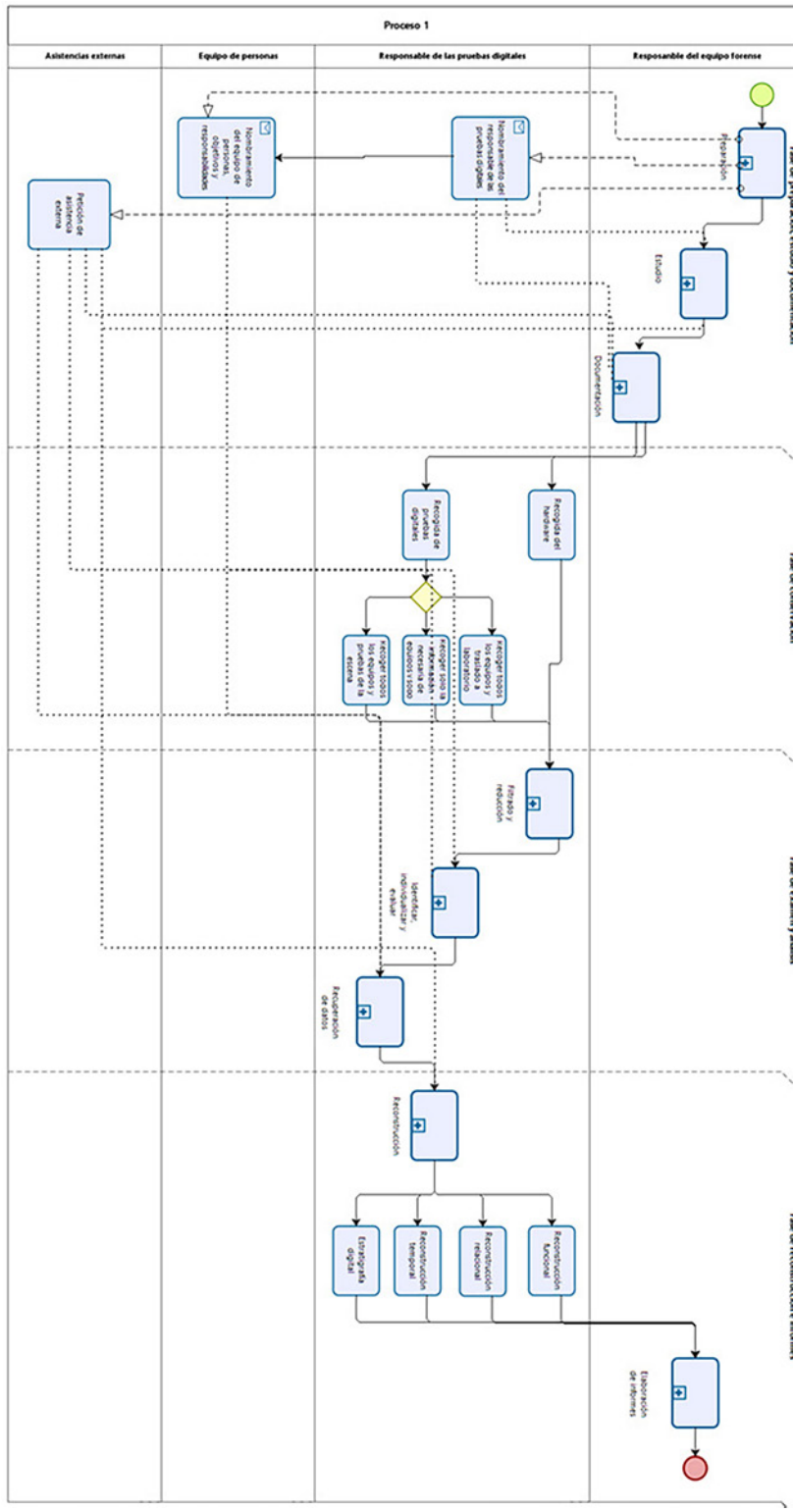


Figura 3-2. Flujograma metodología Eoghan Casey 2011. (Elaboración propia)

Se busca obtener mejoras significativas en materia de costes, calidad, servicio y rapidez, alcanzando con ello los objetivos de la organización, buscando siempre la mejora continua.

La reingeniería de procesos es necesaria cuando:

- La productividad está por debajo de los objetivos
- Se busca ser líderes en el sector
- Es necesario redefinir el producto por los cambios en el mercado
- Se produce una competencia agresiva en precios y hay que responder
- Se pretende mejorar para mantener el liderazgo

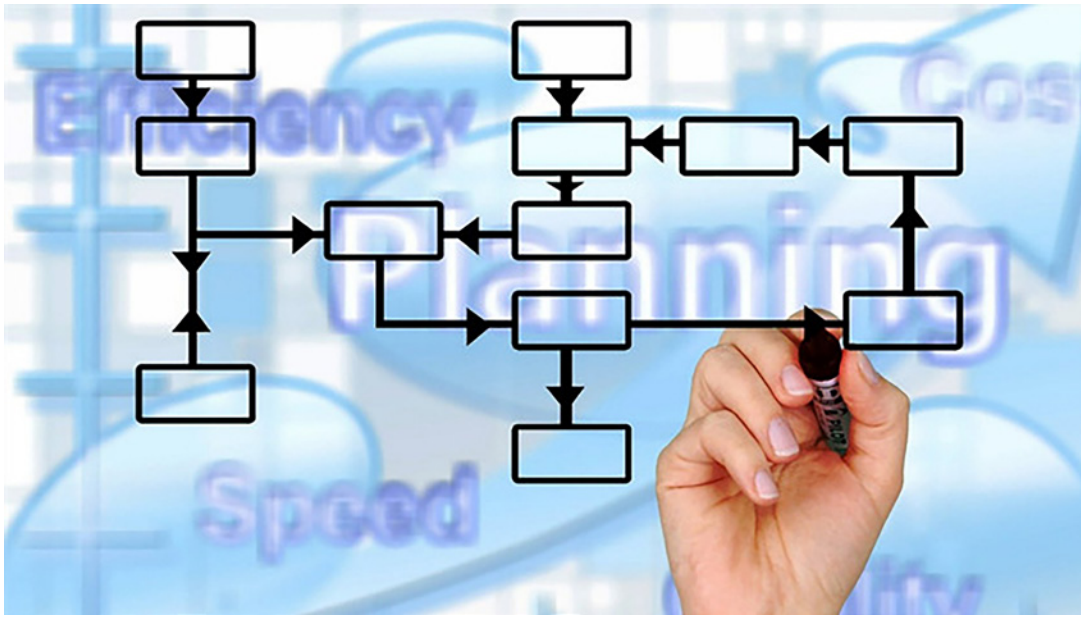


Figura 3-3. Flujograma de procesos (www.transformapartnering.com/reingeniería-procesos) [2]

3.1. Sistema de gestión de la calidad

Cuando nos referimos a la calidad, nos referimos a un término que puede adoptar diferentes interpretaciones, podríamos definirlo como el «grado en el que un conjunto de características inherentes cumple con unos requisitos preestablecidos», podríamos verlo como una característica de un producto, o algo que le aporte un rasgo diferenciador, también puede interpretarse como un requisito, que sería la «necesidad o expectativa establecida», generalmente implícita u obligatoria. Con cualquiera de las interpretaciones que le asignemos, una cosa esta clara, la calidad aporta valor.

Los sistemas de gestión de la calidad, han demostrado que las organizaciones que los implementan obtienen beneficios y ventaja competitiva respecto a las organizaciones que no lo han hecho.

Para implementar esa calidad en nuestra organización es preciso contar con un sistema de gestión, que es el conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

Estos sistemas de gestión están basados en normas, la más utilizada es la ISO 9001, ya que tiene el reconocimiento internacional, es una norma genérica y de aplicación a todos los sectores de actividad.

Esta norma establece los requisitos que hay que llevar a cabo cuando una organización necesita demostrar su capacidad para proporcionar regularmente productos o servicios que satisfagan los requisitos del cliente, los legales y reglamentariamente aplicables.

La mejora continua en la ISO 9001 es un requisito indispensable y fundamental que debe estar presente en todas las áreas de la organización. Gracias a la mejora continua se logra verificar la eficacia del sistema y su sostenibilidad en el tiempo. «El proceso de mejora continua debe ser planificado, sistemático y organizado, buscando la mejora de forma progresiva y recurrente».

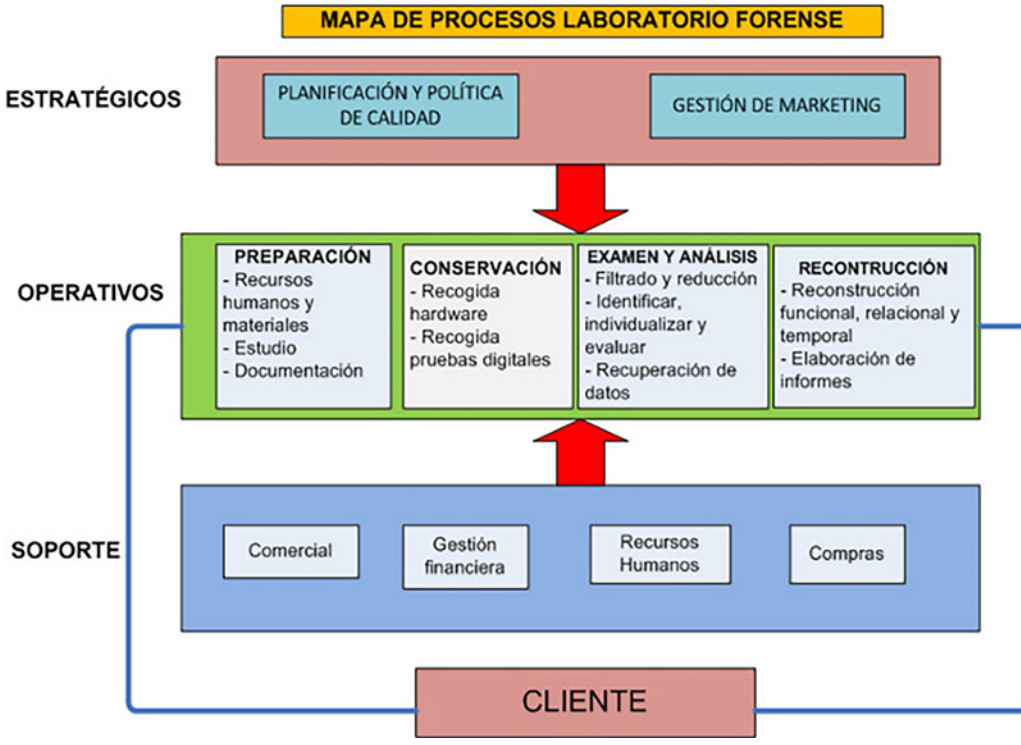
Figura 3 4. Representación PDCA en la norma ISO 9001:2015 (www.equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/)[3]

4. Implantación de un sistema de gestión de la calidad

Se van a desarrollar los pasos orientados a implantar un sistema de gestión de calidad en el laboratorio de informática forense, una vez tomada la decisión estratégica por la dirección y seleccionado personal para la puesta en marcha del sistema, se van a definir los pasos necesarios para implantarlo con éxito. Esta implantación se llevará a cabo en cuatro bloques o fases:

Fase 1. Preparación

En esta fase se diseña el sistema de gestión estableciendo el mapa de procesos de la organización a tres niveles, se definen las políticas y los objetivos de calidad, se establecen los roles y las responsabilidades (Matriz RACI) y se provisionan los recursos.



Matriz de asignación de responsabilidad (RACI)

	DIRECTOR	R. Operación	R. Soporte	Márketing	Trabajador Op.	Trabajador So.	Planificación
Operación / Preparación		A		C	R		I
Operación/ Conservación		A		C	R		I
Operación / Análisis		A		C	R		I
Operación / Reconstrucción		A		C	R		I
Soporte / Contabilidad			A	C	R	R	I
Soporte / RRHH			A	C		R	I
Márketing				R			

Figura 4-1. Mapa de procesos y matriz RACI

FASE 2. Implantación

La fase de implantación lleva una tarea previa de difusión, concienciación y capacitación de los trabajadores de la empresa.

Fase 3. Evaluación y análisis

Una vez puesto en marcha el sistema de calidad y contando ya con datos de los diferentes procesos, es preciso realizar auditorías internas para conocer y analizar los valores de los procesos de seguimiento y medición. Los datos obtenidos facilitarán la toma de decisiones.

Fase 4. Certificación

Una vez que el sistema se encuentra implantado en gran parte, es conveniente iniciar las acciones orientadas a la certificación, en este proceso de auditoría externa se conocerán las recomendaciones y las no conformidades respecto de la norma y, por otro lado, los puntos fuertes de la organización y las oportunidades de mejora.

4.1. Factores críticos de éxito

Para que el proceso de implantación llegue a buen fin, es preciso que se den ciertas condiciones que actúan como factores críticos del éxito del sistema, son los siguientes:

Implicación: La implicación de la dirección debe ser clara y decidida.

Cultura de calidad: Todos los miembros de la organización deben asumirla como propia e integrarla en cada uno de los procedimientos y productos.

Registros y documentación: Debe recogerse por escrito todas las acciones, asignar roles y definir responsabilidades para eliminar dudas.

Control: Se requiere un buen cuadro de indicadores para conocer la eficacia de nuestros planes.

Capacitación: Se requiere de un equipo de personas con conocimientos sobre la organización y amplia experiencia en sistemas de gestión.

5. Conclusiones

- El rápido avance tecnológico y la importancia de las evidencias digitales en numerosos ámbitos, hacen que los laboratorios de informática forense precisen una revisión y evaluación constante si pretenden ser competitivos.
- La organización debe adaptarse a la exigencia de los mercados, el constante cambio técnico y normativo precisa estar preparado para realizar cambios constantes que le permitan mantenerse entre las organizaciones de referencia.

- Cualquier organización es capaz de detectar mejoras en su gestión, pero no consiguen ponerla en marcha por la falta de sistematización y de planificación.
- Se ha constatado que, si una organización no es productiva ni eficiente, debe llevar a cabo una revisión profunda y un rediseño potente de sus procesos.
- A parte del rediseño de los procesos, es aconsejable implementar un sistema de gestión de la calidad, este se hace necesario para poder tener un control efectivo de la organización y trabajar con eficacia en un mercado cada vez más complejo.
- La calidad sería el modo en el que la organización entiende que debe realizar sus productos y servicios y aplicarlo a todas sus actividades.
- Hace ya varios años que los sistemas de gestión de la calidad llegaron para quedarse, han ido mejorando con el tiempo, pero siempre buscando elementos que permitan el crecimiento en las organizaciones y mayor satisfacción del cliente.
- Las Normas ISO son un referente de calidad a nivel mundial, permiten a las organizaciones la estandarización y mejora de sus procesos, su funcionamiento y reconocimiento, lo cual es de vital importancia para la supervivencia de las empresas en un mundo globalizado.
- Una vez implementado el sistema de gestión de la calidad, el laboratorio de informática forense tiene un control efectivo de actividades y procesos y cuenta con un nivel de información que le permite alinear los productos y servicios con las expectativas del cliente.
- El sistema de gestión tiene una función integradora, ya que hace partícipe del mismo a todo el personal de la organización y a las demás partes interesadas.
- Se ha incrementado la motivación de los trabajadores, ahora conocen lo que se espera de ellos y son conscientes de que su calidad en el trabajo es medida y conocida por la alta dirección de la empresa.
- Al mantener la filosofía de la mejora continua, este sistema de gestión será más eficaz y reportará más beneficios cuanto más maduro esté.
- Se puede afirmar que la gestión por procesos y el sistema de gestión han sido claves en mejorar la eficiencia, la productividad y alta competencia del laboratorio forense objeto de este trabajo de investigación.

Agradecimientos

A mis compañeros del máster, a mis directores del TFM Francisco Manuel y Norberto, al Centro Universitario de la Defensa, a la Universidad de Vigo y al conjunto de profesores y colaboradores por su gran trabajo.

Referencias

[1] Casey, E. (2004). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Baltimore, EE. UU.: Eoghan Casey (noviembre 2020)

[2] Las claves de la Reingeniería de Procesos: beneficios, metodología y factores críticos de éxito. www.transformapartnering.com/reingenieria-procesos (septiembre 2020)

[3] La norma ISO 9001:2015 (www.equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/) (noviembre 2020)

Reingeniería de procesos para la implantación de un sistema de calidad en un laboratorio de informática forense

Autor: Juan Carlos González Carvajal

Director/es: Francisco Manuel Pérez Rivas y Norberto Fernández García

Universidad de Vigo

Introducción

Con objeto de mejorar la productividad de un laboratorio de informática forense, se llevará a cabo una reingeniería de procesos en base a una metodología y buenas prácticas analizadas.

Esta reingeniería será el primer paso para llevar a cabo la implantación de un Sistema de Gestión de la Calidad basado en la norma ISO 9001.

Una vez el Sistema de Calidad esté en producción, se iniciará el proceso de certificación en la norma ISO 9001:2015.

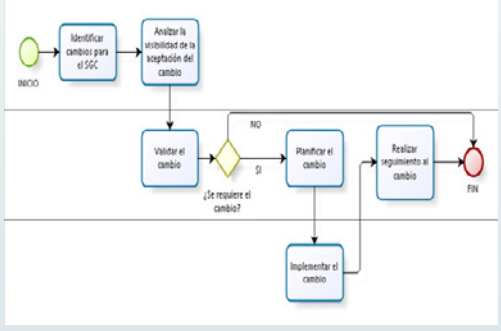
Resultados

- Procesos más eficientes y eficaces
- Mejora en la productividad del laboratorio
- Mejora en la imagen corporativa
- Motivación de los empleados
- Consecución de los objetivos de la organización
- Certificación ISO 9001 de nuestro sistema

https://online-tesis.com/normas-iso/

Metodología

Gestión por Procesos



Sistema de Calidad Total

https://safetya.co/phva-procedimiento-logico-y-por-etapas/

Conclusiones

- La gestión por procesos es el éxito de la transformación empresarial
- Es aconsejable guiarse por las normas, estándares y buenas prácticas, ya que estas tienen acreditada su efectividad
- Los sistemas de gestión de la calidad involucran a todo el personal de la organización contribuyendo al incremento de la motivación y productividad de los mismos
- Estos sistemas aportan información lo que permite la evaluación y mejora
- Los sistemas de calidad total aportan una mejora continua que lleva a la excelencia

Agradecimientos

A mis compañeros del Máster, a mis Directores FranciscoManuel y Norberto, al Centro Universitario de la Defensa, a la Universidad de Vigo y al conjunto de Profesores y Colaboradores del Máster por su gran trabajo.

Internet como canal de comunicaciones para redes clasificadas, posible solución versátil y segura para despliegues militares

Autor: González Sierra, Bernardo (bgsierra@fn.mde.es)
Director: Zamorano Pinal, Carlos (externo.czamorano@cud.uvigo.es)

Resumen – La necesidad de despliegue de unidades militares a lo largo de toda la geografía mundial requiere de canales de comunicación versátiles, seguros y relativamente económicos. El uso de Internet, prácticamente accesible en cualquier parte del mundo, permitiría que se pudiera extender el mando a aquellas unidades situadas en lugares remotos a través de los sistemas de mando y control (C2). La gran capilaridad de Internet y su coste reducido podrían sustituir los canales de comunicación militares, tales como los satélites militares, las líneas dedicadas en propiedad y los radioenlaces.

Con este trabajo se pretende encontrar una solución comercial, versátil y segura que permita a los jefes de los ejércitos extender su mando y control, sin importar donde se encuentren sus fuerzas, utilizando la red de redes, siempre cumplimentando la normativa nacional sobre información clasificada.

Palabras clave: Internet, redes clasificadas, sistemas militares, canal de comunicaciones, mando y control, seguridad, DMZ.

1. Introducción

1.1. ¿Por qué sería necesario utilizar Internet como canal de comunicación?

En la era de las nuevas tecnologías, los ejércitos necesitan sistemas de mando y control para poder extender el mando a todas sus unidades, estén cerca o lejos de los puestos de mando.

Las operaciones militares hoy en día no solo se circunscriben al campo de batalla. El auge de la guerra híbrida, unido a conflictos de pequeña intensidad, pero con gran repercusión social y humanitaria han hecho que se tengan que desplegar muchas unidades militares a lo largo de la geografía mundial para poder completar sus objetivos.

Esta cantidad de misiones implican una gran cantidad de puntos de presencia de los sistemas de mando y control militar que prestan sus servicios sobre sistemas de información clasificada. Desplegar los puntos de presencia de los sistemas clasificados conlleva la extensión de redes seguras que se suele realizar mediante soluciones militares tradicionales utilizando satélites gubernamentales o líneas dedicadas, con un coste elevadísimo y poca disponibilidad /capilaridad.

1.2. Necesidad

La necesidad de despliegue de redes clasificadas en zonas de operaciones demanda el acceso a un canal de comunicaciones versátil,

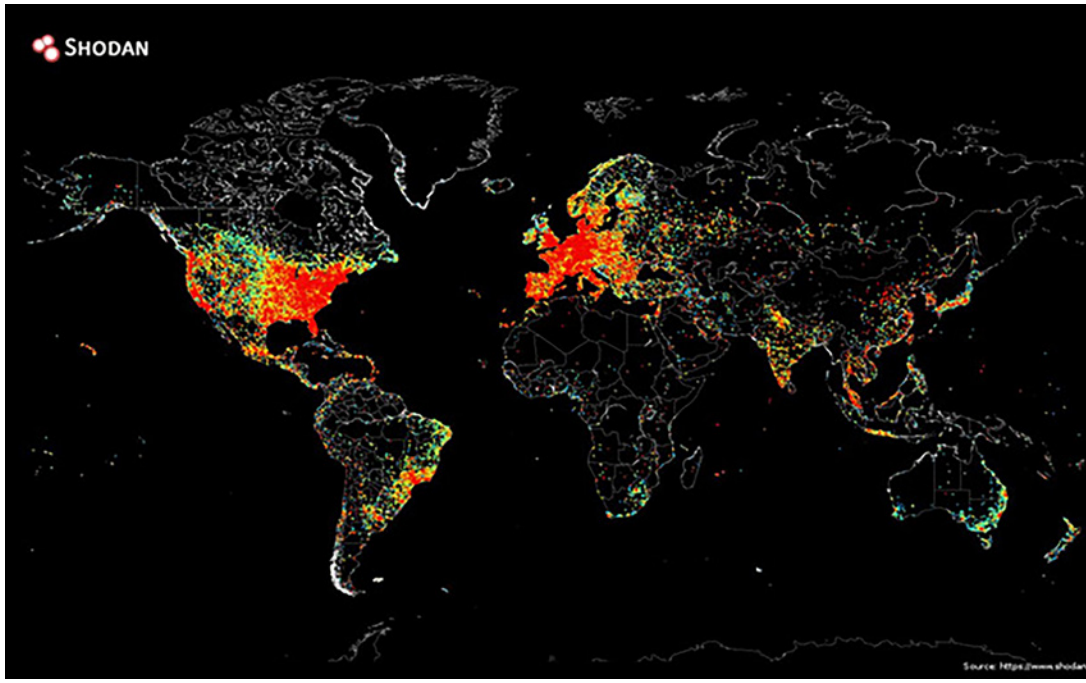


Figura 1. Mapa de calor de dispositivos conectados a Internet en el año 2014 (imagen obtenida de [1])

accesible y económico, que pueda sustituir a las conexiones a través de satélites militares o líneas dedicadas, sin disminuir el nivel de seguridad exigido.

La conexión a Internet es cada día más accesible y su cobertura es más extensa. Localizar un punto de conexión en las zonas de operaciones donde se despliegan los contingentes militares suele ser relativamente fácil, incluso en países del tercer mundo. Esta accesibilidad podría ser una solución para aquellos puntos de presencia de las redes clasificadas de mando y control de los ejércitos en zona de operaciones.

1.3. Objetivos

Los objetivos de este trabajo son:

1. Demostrar que el uso de Internet como canal de comunicación para los sistemas C2 militares es una solución versátil y económica que puede cumplimentar los estándares de seguridad exigidos.

2. Proponer una solución técnica (DMZ) con tecnología actual que facilite el despliegue de unidades en zonas de operaciones usando Internet como canal de comunicaciones.

2. Desarrollo

2.1. Requerimientos de seguridad de los sistemas clasificados

Desde el comienzo de las civilizaciones la información ha sido clave, y siempre se han buscado maneras de protegerla. Desde el empleo del bastón Skytale griego para cifrar mensajes, empleado en el siglo V a.C., hasta la máquina Enigma, empleada por los alemanes en la Segunda Guerra Mundial, los Estados han intentado proteger aquella información sensible que podía poner en peligro su poder. La necesidad de proteger aquella información sensible implica un desarrollo de normas y leyes que fijen cómo se debe emplear la información clasificada y cómo se debe proteger para evitar que llegue a manos que puedan poner en peligro la estabilidad de la nación.

La principal norma que regula los secretos oficiales en España es la Ley 9/1968, de 5 de abril (BOE n.º 84, de 6 de abril de 1968), sobre Secretos Oficiales (LSO), que fue modificada por la Ley 48/1978, de 7 de octubre (BOE n.º 243), y por el Decreto 242/1969, de 20 de febrero. El Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), es el organismo responsable de coordinar y garantizar la seguridad de las tecnologías de la información, así como de la promulgación de las guías CCN-STIC que indican las normas, instrucciones, y recomendaciones para mejorar el grado de ciberseguridad de los organismos públicos.

2.2. Soluciones militares tradicionales

Las redes de acceso a las telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D) tienen como objeto transportar todo tipo de servicios de datos, voz y vídeo de los sistemas de información del Ministerio de Defensa. Dichas redes se apoyan en diferentes medios de transmisión propios como son fibras ópticas oscuras e iluminadas mediante equipos de multiplexación óptica DWDM y radioenlaces distribuidos por todo el territorio nacional. Por otro lado, también utiliza otros medios contratados como son circuitos dedicados en tecnología TDM y Ethernet para el segmento terreno y alquiler de ancho de banda en los satélites Spainsat y Xtar-EUR en el segmento espacial.

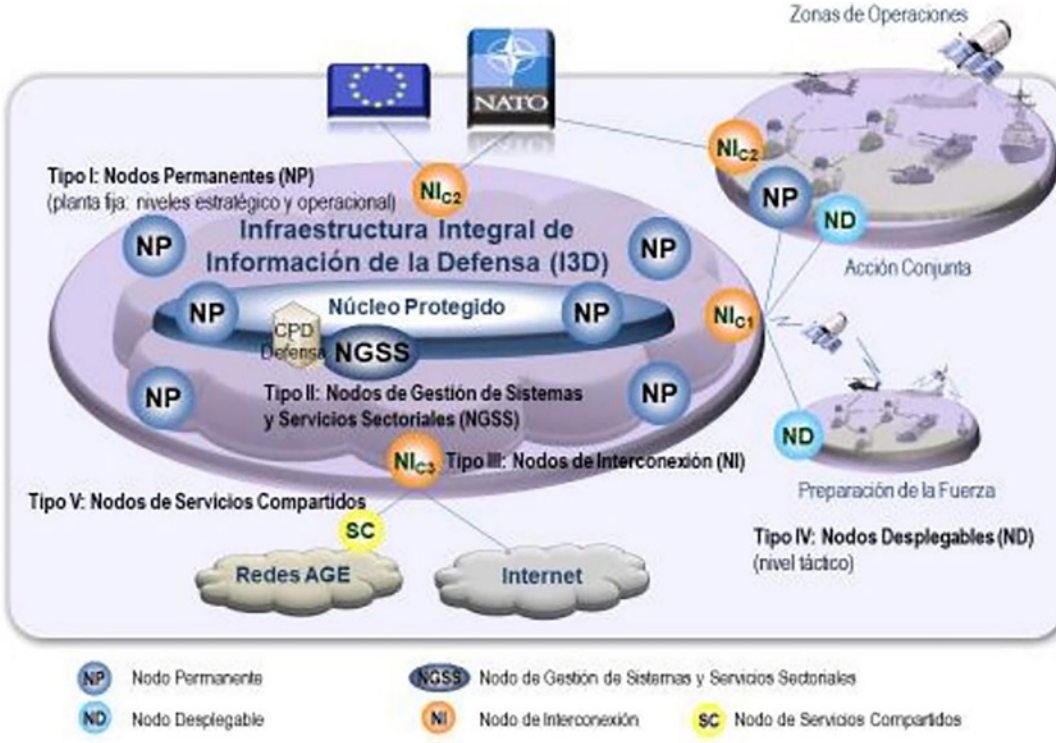


Figura 2. Esquema de las redes de acceso a la I3D (imagen obtenida de [2])

En la figura 2 se muestran todas las redes, las no clasificadas (Red de propósito general o WANPG) y las clasificadas (núcleo protegido). En el caso de las redes clasificadas que competen a la realización de este trabajo, se emplean medios de transmisión propietarios, bien sea mediante fibra óptica, radioenlaces o empleando la parte gubernamental de los satélites Spainsat y Xtar-EUR. El principal sistema de transmisión en los despliegues de unidades en las zonas de operaciones es el uso de sistemas satelitales dada la complejidad y carestía que supone desplegar medios de transmisión propietarios fuera del territorio nacional. Siguiendo la normativa nacional vigente, todas las transmisiones de las redes clasificadas deberán estar

cifradas, usando cifradores hardware publicados en la guía CCN-STIC-105 *Catálogo de productos de seguridad de las tecnologías de la información y la comunicación.*

2.3. Elementos de interconexión. Los sistemas de protección de perímetro (SPP)

Un sistema de protección de perímetro (SPP) consiste en una combinación de recursos hardware y/o software denominados Dispositivos de protección perimetral (DPP), cuya finalidad es intervenir el tráfico de entrada y salida en los puntos de interconexión de los sistemas, en especial en aquellos que se encuentran en la frontera de la red.

Un DPP según el CCN es «el hardware y/o software, cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los sistemas» y según el NIST «un dispositivo (p. Ej., gateway, enrutador, firewall o túnel cifrado) que facilita la adjudicación de diferentes políticas de seguridad del sistema para los sistemas conectados o proporciona protección de límites. El límite puede ser el límite de autorización de un sistema, el límite de la red organizativa o un límite lógico definido por la organización» [3].

2.4. Sistemas de cifrado

La criptografía es la ciencia que mediante métodos y herramientas matemáticas puede cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando para ello dos o más claves, logrando en algunos casos la confidencialidad, en otros la autenticidad o bien ambas simultáneamente. Consiste en la conversión de datos en un mensaje codificado para que sea ilegible. Se transforma un mensaje en algo inteligible que solo puede ser leído si se dispone de la clave secreta [8].

Todos los sistemas de cifrado deben cumplir la función Dk (Ck(m)) =m, es decir, que, si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m.

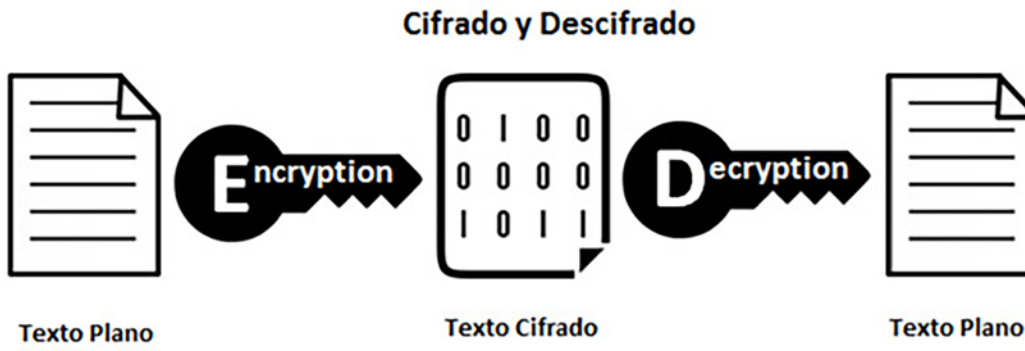


Figura 3. Esquema de un sistema de cifrado (imagen obtenida de [4])

2.5. Zona desmilitarizada o DMZ

La DMZ o zona desmilitarizada es una red perimetral que protege la LAN interna de una organización del tráfico no confiable. Es una subred que se encuentra entre la Internet pública y las redes privadas. Expone los servicios externos a redes que no son de confianza y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en las redes internas utilizando firewalls para filtrar el tráfico.

El objetivo final de una DMZ es permitir que una organización acceda a redes que no son de confianza, como Internet, al tiempo que garantiza que su LAN permanezca segura. Las organizaciones suelen ubicar los servidores para el sistema de nombres de dominio (DNS), protocolo de transferencia de archivos (FTP), correo, proxy, protocolo de voz sobre Internet (VoIP) y servidores web en la DMZ.

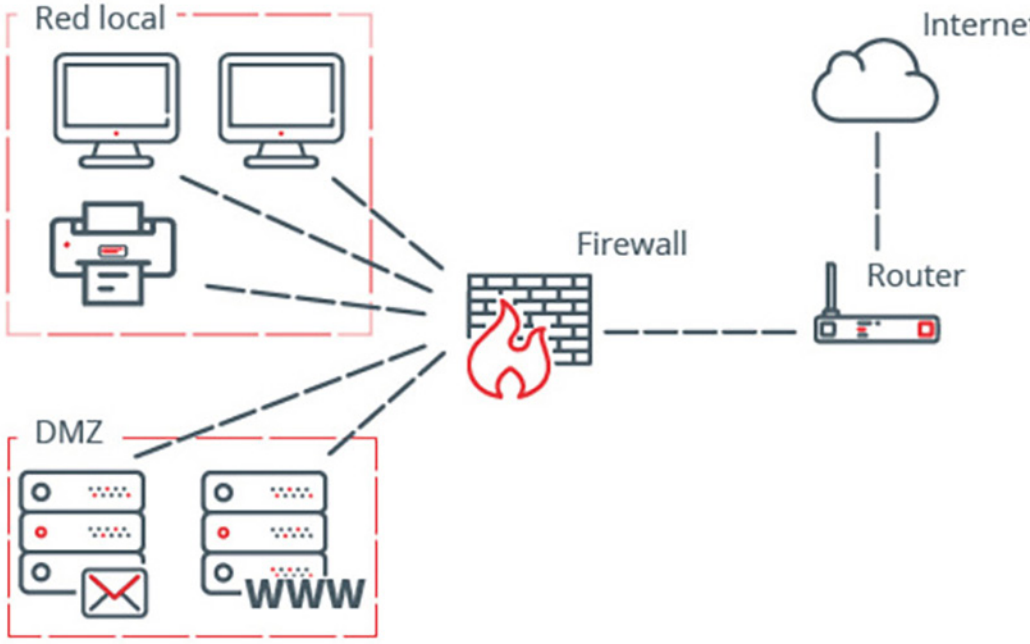


Figura 4. Esquema de una DMZ (imagen obtenida de [5])

2.6. Solución técnica propuesta

Para los sistemas C2 clasificados empleados en zona de operaciones que se quieran unir a la red usando canales de comunicaciones inseguros, se necesita una alta protección tal y como indica la normativa nacional, no siendo necesario romper la continuidad de los protocolos. Usando distintos dispositivos de defensa perimetral. En este caso se propone el uso de una DMZ en ambos emplazamientos para garantizar la triada CIA del sistema.

En la figura 5 se materializa el concepto general de la solución y para evitar los riesgos inherentes al uso de una red insegura como es Internet, se incrementa la protección de las DMZ con cifradores dado la sensibilidad de la información que se transitará por estas redes.

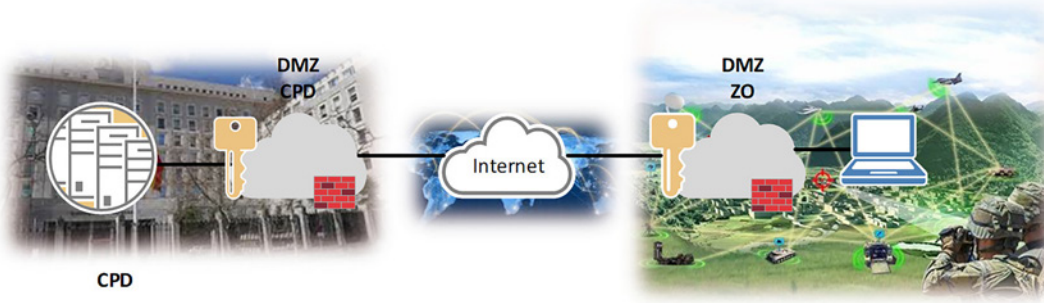


Figura 5. Diagrama conceptual de la solución técnica propuesta

La solución que se propone es la instalación de dos DMZ. Una en la zona de operaciones donde el router con acceso a Internet tendría una VPN con túnel IPSec con el router conectado con Internet en el CPD. La función de ese túnel es enmascarar el tráfico cifrado que se intercambiaría entre los cifradores, teniendo que ser cifradores hardware por requerimiento de seguridad establecido en distintas guías CCN-STIC. Ambas DMZ estarían provistas de un firewall exterior que protege a los cifradores hardware. Después de los cifradores se instalaría otro firewall interior que protege los activos que se despliegan en zona de operaciones o en la DMZ del CPD, estos firewalls deberán ser de un fabricante diferente a los exteriores para permitir la defensa en capas y evitar un único punto de fallo.

Para incrementar la seguridad, también se desplegará un IDS/IPS en ambas DMZ que reportarán sus logs a un sistema SIEM centralizado en el CPD. Puesto que los despliegues en zona de operaciones son más

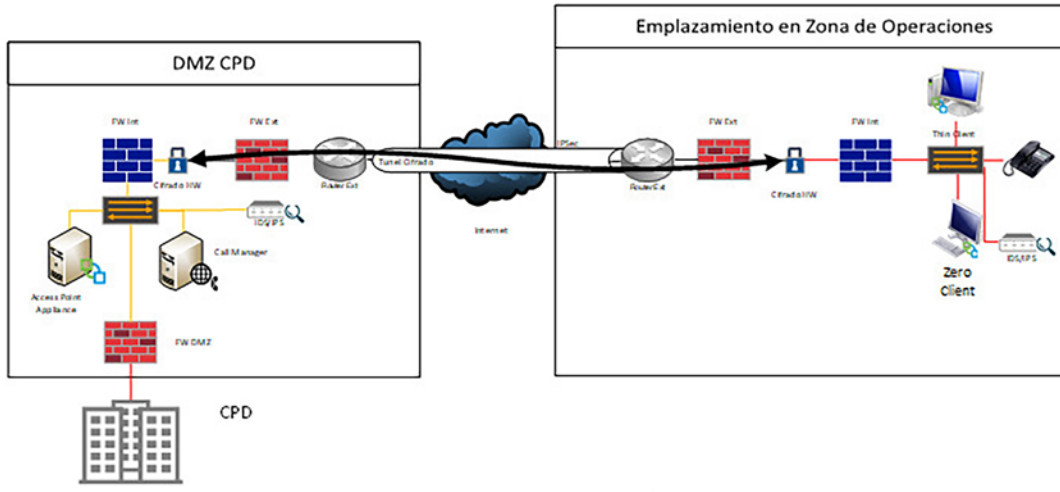


Figura 6. Diagrama de alto nivel de la solución técnica propuesta

vulnerables y susceptibles de sabotajes, ataques, etc., se implementarán *thin/zero clients* desprovistos de medios de almacenamiento interno que puedan ser sustraídos, minimizando los riesgos de pérdida de información sensible. En la DMZ del CPD se ubicará un Unified Access Gateway y un *call manager* que harán de *proxy* entre los escritorios VDI y los teléfonos desplegados y los servicios prestados por el CPD en territorio nacional. Un último firewall en la DMZ del CPD protegerá todos los servicios del CPD.

3. DMZ vs. soluciones militares tradicionales

En este punto se comprobará la bondad de la solución técnica propuesta en este trabajo con las soluciones militares tradicionales empleadas actualmente para dar servicio a todos los nodos de las redes clasificadas desplegadas fuera de territorio nacional.

3.1. Seguridad

La seguridad es un elemento imprescindible en cualquier sistema clasificado. Los principios necesarios para cumplir con los objetivos de seguridad en los sistemas clasificados son: análisis y gestión del riesgo, mínima funcionalidad, mínimo privilegio, nodo autoprotegido, defensa en profundidad, control de configuración, verificación de la seguridad, vigilancia y respuesta a incidentes, monitorización y resiliencia [6]. La normativa vigente establece unos criterios estrictos y claros a la hora de determinar los procedimientos y sistemas para proteger la información clasificada, recogidos en las guías CCN-STIC. La solución técnica propuesta cumple con los requisitos establecidos, estando en línea con lo requerido en las guías CCN-STIC en vigor, destacando el empleo de cifradores IP hardware certificados, que a su vez están protegidos mediante una DMZ. Aun cumpliendo con todos los requisitos de seguridad la solución propuesta en este trabajo, las soluciones militares tradicionales, que emplean redes no expuestas, son más seguras al reducir los riesgos inherentes que conlleva el empleo de redes públicas.

3.2. Disponibilidad

La disponibilidad es la cualidad o condición de la información que permite, a las personas o procesos autorizados, acceder a ella cuando se demande de acuerdo a los requisitos establecidos [6]. En el caso de la solución técnica propuesta la disponibilidad depende íntegramente de los proveedores de Internet contratados en zona de operaciones para suministrar la red de transporte. Esta dependencia de los ISP puede poner en peligro la disponibilidad de la red clasificada, mientras que, en las soluciones tradicionales, principalmente a través de satélites militares, dependería de la accesibilidad a la constelación de satélites militares por parte del receptor en zona de operaciones, normalmente solo condicionada por la situación meteorológica.

3.3. Capilaridad

La capilaridad o capacidad de poder desplegarse en distintas ubicaciones es una cualidad a tener en cuenta a la hora de destacar unidades a lo largo y ancho de la orografía mundial. La solución técnica propuesta es más ventajosa que las soluciones tradicionales ya que el despliegue de un nodo dependería de poder acceder a Internet, siendo esto relativamente sencillo. El 57 % de la población global tiene acceso a Internet [7] y en todos los países donde hay unidades desplegadas actualmente hay proveedores de Internet disponibles.

En el caso de las soluciones tradicionales la capilaridad dependería principalmente de la cobertura de los satélites gubernamentales, no siendo esta global, y que además disponen de un ancho de banda bastante limitado que debe ser compartido con todos los terminales desplegados, tanto en zona de operaciones como en territorio nacional.

3.4. Coste

El coste, aunque en menor medida, también tiene cierta importancia a la hora de desplegar sistemas clasificados dependientes del Ministerio de Defensa. Los recursos económicos son limitados y últimamente esta carencia es cada vez más significativa. En la tabla 1 se puede apreciar una comparativa del gasto necesario para implementar una solución tradicional y la solución técnica propuesta. Esta tabla es un resumen de los datos recopilados y en ella se puede apreciar que la inversión en la solución técnica propuesta es sustancialmente más económica.

CAPEX	**Solución tradicional**	**Solución técnica propuesta**
CPD	113.774,36 €	148.235,57 €
Nodo desplegado	471.926,13 €	22.487,04 €
TOTAL	**585.700,49 €**	**170.722,61 €**

Tabla 1. Comparativa CAPEX de la solución tradicional y la solución técnica propuesta

En lo referente al acceso a la red de transporte. En el caso de la solución propuesta el precio de acceso a Internet es relativamente asequible en los lugares donde hay desplegadas unidades de las Fuerzas Armadas, con un promedio de aproximadamente 18,00 €/Mbps. Es difícil hacer una comparación económica entre la solución técnica propuesta y las soluciones tradicionales, ya que fuera de territorio nacional el despliegue de las redes clasificadas se realiza casi exclusivamente mediante el empleo de satélites militares, cuyos gastos se sufragan de una manera conjunta, pero con importes significativamente mayores. No obstante, y de una manera general se puede afirmar que las conexiones a Internet a través de proveedores locales tendrían un coste más reducido que la conexión a un satélite gubernamental.

3.5. Ancho de banda (BW) y tiempo de despliegue

Los despliegues de satélites militares se mueven entre los 2 y 4 Mbps de ancho de banda, pudiendo llegar a los 8 Mbps para los terminales con mayor capacidad, mientras que las ofertas de los ISP en las zonas de despliegue de las unidades españolas oscilan entre 0,5 y 500 Mbps, con un promedio de aproximadamente 48 Mbps a precios relativamente asequibles, como se constató en el punto anterior.

En cuanto al tiempo de despliegue, la solución tradicional es más ventajosa ya que tanto el terminal como el personal que lo opera se despliegan con las tropas en la zona de operaciones, pudiendo establecerse la conexión en pocas horas una vez establecida su base. La contratación de una conexión de Internet a través de proveedores locales puede demorarse, si tenemos en cuenta que el tiempo de aprovisionamiento de una conexión a Internet en España oscila entre 3 y 15 días, las barreras idiomáticas y la forma de pago (necesidad de una cuenta bancaría local, cambio de moneda, etc.).

4. Conclusiones

Teniendo en cuenta lo presentado en este trabajo, se puede afirmar que el uso de Internet como canal de comunicaciones para redes clasificadas podría ser una solución versátil y segura para los despliegues militares fuera de territorio nacional. La solución técnica propuesta cumple con los estándares de seguridad exigidos por la normativa vigente para sistemas clasificados y cuenta con la enorme ventaja que tiene el despliegue mundial de Internet con su gran capilaridad, permitiendo un acceso a la red de transporte en cualquier parte del mundo con un ancho de banda aceptable a un coste razonable.

El coste del equipamiento necesario en la solución técnica propuesta es casi cuatro veces más económico que las soluciones tradicionales y el precio por Mbps también es más ventajoso.

El gran hándicap de esta solución es la disponibilidad debido a la total dependencia de los proveedores de los servicios de Internet y al tiempo de aprovisionamiento, sumado a que en las zonas de operaciones suele haber conflictos que pueden degradar o inutilizar el acceso a Internet. Los servicios de las redes clasificadas se pueden ver interrumpidos o degradados sin previo aviso y la prioridad de su restablecimiento está fuera de las capacidades de las fuerzas desplegadas.

Ante estos hechos, se considera que la solución técnica propuesta es apropiada para el despliegue de unidades en zona de operaciones, pero debería tener como respaldo una solución tradicional, es decir, acceso a satélites gubernamentales o con varios proveedores de Internet diferentes que hicieran de *backup*.

Agradecimientos

A Susana, Pablo y Álvaro, por permitirme robarles tiempo en familia para dedicarme a la realización de este máster y a todos aquellos que nunca han querido dejar de aprender. El conocimiento no es el fin, es el comienzo.

Referencias

[1] P. Engel, «Bussiness Insider,» 14 septiembre 2014. [En línea]. Disponible: https://www.businessinsider.com/this-world-map-shows-every-device-connected-to-the-internet-2014-9. [Último acceso: 27 agosto 2020].

[2] J. M. N. García, (9 septiembre 2020). «En marcha la nueva red de telecomunicaciones de Defensa por 33,4 millones de euros,». [En línea]. Disponible: https://www.defensa.com/espana/marcha-nueva-red-telecomunicaciones-defensa-33-4-millones-euros. [Último acceso: 12 diciembre 2020].

[3] Joint Task Force. (2020), «NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations Rev. 5», U.S. Department of Commerce, Gaithersburg, MD.

[4] A. d. l. Cruz, (14 febrero 2019) «Criptografía, métodos de cifrado y hashing: cómo las empresas PCI almacenamos datos de forma segura». [En línea]. Disponible: https://paynopain.com/actualidad-fintech/post-experto-fintech/criptografia-metodos-de-cifrado-y-hashing-como-las-empresas-pci-almacenamos-datos-de-forma-segura/. [Último acceso: 4 enero 2021].

[5] «Qué es una DMZ y cómo te puede ayudar a proteger tu empresa» INCIBE, 19 septiembre 2019. [En línea]. Disponible: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa. [Último acceso: 12 octubre 2020].

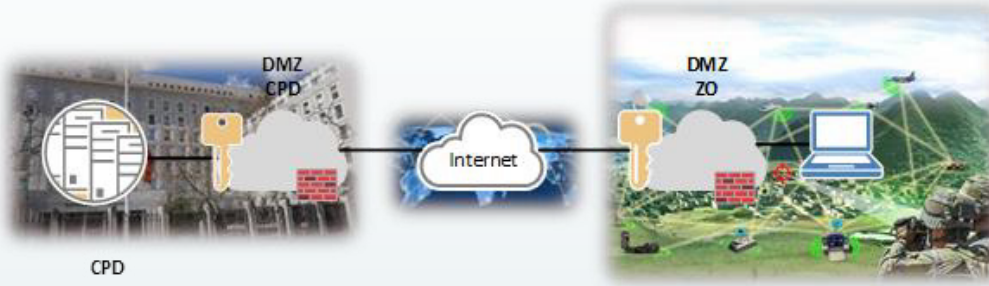
[6] CCN, (2016). «CCN-STIC-001 “Política de Seguridad de las TIC”», Gobierno de España. Ministerio de la Presidencia, Madrid.

[7] «Key Internet Statistics to Know in 2020 (Including Mobile)», [En línea]. Disponible: https://www.broadbandsearch.net/blog/internet-statistics. [Último acceso: 7 enero 2020].

Internet como canal de comunicaciones para redes clasificadas, posible solución versátil y segura para despliegues militares

Autor: Bernardo, González, Sierra
Director: Carlos, Zamorano, Pinal

Universidad de Vigo



La necesidad de despliegue de unidades militares a lo largo de toda la geografía mundial requiere de canales de comunicación versátiles, seguros y relativamente económicos. El uso de Internet, prácticamente accesible en cualquier parte de orbe mundial, permitiría que se pudiera extender el mando a aquellas unidades situadas en lugares remotos a través de los sistemas C2. La gran capilaridad de Internet y su coste reducido podrían sustituir los canales de comunicación militares, tales como los satélites militares, las líneas dedicadas en propiedad y los radioenlaces.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2020/2021

Futuro de la ciberdefensa en las FAS y perfil de carrera para su personal

Autor: Santos Sande, Carlos Alberto (csansan@fn.mde.es)
Director: Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – Las operaciones en el ciberespacio son parte del ámbito operativo más moderno dentro de nuestras Fuerzas Armadas. Así, a raíz de esta necesidad se creó el Mando Conjunto de Ciberdefensa el 19 de febrero de 2013. Después de casi siete años de andadura se considera necesario estudiar cual puede ser su futuro al que inexorablemente va unido el perfil de carrera de su personal. En este contexto, el presente TFM plantea la necesidad de aunar bajo un mismo mando operativo, en este caso el JEMAD, todo lo relacionado con el mundo CIS y el de ciberdefensa. Se propone la creación de un mando único, el Mando Conjunto del Ciberespacio, que se encargue de proveer los servicios CIS, así como un responsable de su ciberdefensa, con la finalidad de solventar las disfunciones operativas existentes en la actualidad.

El nuevo Mando Conjunto del Ciberespacio precisaría de profesionales formados y adiestrados, capacitados para su continua adaptación a la amenaza existente. Este personal operativo precisa de una continuidad en este ámbito, pues el *know-how* y el *expertise* indispensable para combatir a los actores hostiles se alcanzan con un esfuerzo continuo y una dedicación permanente. Actualmente, el perfil de los Ejércitos y Armada no valora este perfil de carrera, imprescindible para combatir en el ciberespacio. Esta es la razón por la que se propone, a corto-medio plazo, la creación de un cuerpo común del ciberespacio, y, a medio-largo plazo, una nueva rama en las FAS, el *ejército del ciberespacio*.

Palabras clave: ciberespacio, independencia, ciberguerrero, Ejército, talento, *Employer Branding*.

1. Introducción

1.1. Motivación

A lo largo de ya más de cuatro años en el MCCD he tenido la oportunidad de apreciar las virtudes y las carencias que posee esta unidad para convertirse en una unidad de combate dentro de las FAS españolas. Esta unidad debería convertirse en el punto de referencia en todos los factores condicionantes relacionados con la ciberdefensa, la ciberseguridad y la ciberinteligencia, tanto para las Administraciones públicas como para el entorno empresarial. Las FAS en muchos ámbitos en los que desarrollan sus capacidades deberían ser, y en muchos casos son, un referente para otras administraciones y para el sector empresarial, como así sucede en otros países de nuestro entorno, pero en especial deberían de serlo en el ámbito del ciberespacio. El MINISDEF debería de potenciar y respaldar al MCCD en diversos campos, tal y como se refleja a lo largo del presente TFM, si se quiere que este mando tenga la capacidad de enfrentarse a los potenciales enemigos que afectan tanto a las FAS como a la Seguridad Nacional en el ciberespacio.

El campo de batalla del ciberespacio es completamente transgresor con respecto a los tradicionales Tierra, Mar y Aire y, en línea con ello, su personal tiene que estar dotado de unas cualidades profesionales y unas características personales diferenciadas de las requeridas y valoradas en la actualidad por los Ejércitos y Armada. En este sentido, estas razones originan que en este trabajo se elaborarán y detallarán propuestas para conseguir que el dominio de las operaciones en el ciberespacio resulte altamente operativo; consiguiendo, a su vez, la captación, retención y motivación del personal operativo en esta joven área de las operaciones militares.

1.2. Objetivos

Los objetivos del presente trabajo claramente son dos: por un lado, y partiendo de la situación actual del MCCD, evaluar hacia donde debe dirigirse este mando tanto orgánica, estructural como operativamente y, por el otro, basándonos en la situación de su personal, analizar cómo debe ser el perfil de carrera hacia el que se debe tender, a diferencia del que existente en la actualidad, para conseguir motivación, se encuentre un elevado grado de captación y, sobre todo, de retención. Se pretenden definir posibles soluciones para disponer de una trayectoria profesional en este ámbito de las operaciones, que permitan conjugar, adecuada y eficientemente, la formación en ciberdefensa, la experiencia que se debe adquirir en el destino y las aspiraciones profesionales de sus miembros.

La finalidad reside en definir una estructura y marcar un futuro para la ciberdefensa dentro de las FAS, de modo que esta sea una plataforma de

desarrollo profesional para sus miembros; consiguiendo, con ello, elevar la operatividad y colocar la labor que realiza este mando en los niveles de excelencia necesarios para situarse como un centro de referencia en este entorno, tanto a nivel militar como civil, y en la esfera nacional e internacional.

2. Desarrollo

Este TFM expone la situación actual de la ciberdefensa dentro de las FAS y cómo es el perfil de carrera de su personal. Partiendo de este punto, se propone una línea de acción que debería seguir la ciberdefensa con la intención de tener un futuro operativo y ser la cabeza de lanza en los futuros campos de batalla en los que intervengan las FAS; los cuales, dado que serán cada vez menos convencionales, obligarán la mayor parte del tiempo a combatir en la conocida como Zona Gris. Por ende, las necesidades específicas de su personal para poder llevar a cabo la misión se diferenciarán de las actualmente demandadas por nuestras FAS.

2.1. Presente y futuro de la ciberdefensa en las FAS

El dominio ciberespacial se define como el dominio global virtual compuesto tanto por las redes interconectadas como por las redes y sistemas aislados o independientes [2]. En base a esta definición el mundo CIS y el de la ciberdefensa deben ir íntimamente unidos. Al comenzar el presente TFM existían tres actores en esta esfera operacional: el CESTIC, la JCISFAS y el MCCD. Los cuales estaban en dos cadenas de mando bien diferenciadas: el CESTIC, como proveedor de servicios CIS, dependiente del SEDEF y la JCISFAS y el MCCD del JEMAD. A finales de 2020, la

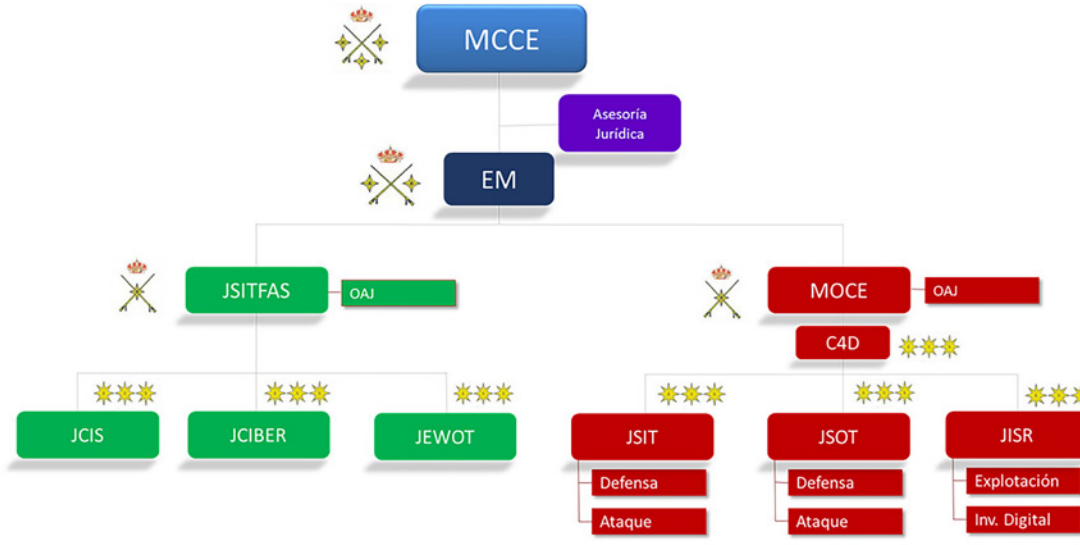


Figura 1. Estructura orgánica del MCCE (elaboración propia)

JCISFAS y el MCCD se integraron en un único mando: el Mando Conjunto del Ciberespacio (MCCE).

En este trabajo se propone que el primer paso para el futuro de la ciberdefensa en las FAS resida en la integración de las tres unidades en una sola, el MCCE, bajo dependencia operativa del JEMAD, responsable de las operaciones; siendo este mando el asesor estratégico en materia de ciberdefensa del JEMAD.

Debajo del MCCE deben colgar dos estructuras diferenciadas: la Jefatura de Sistemas y Tecnologías de las FAS (JSITFAS) y el Mando de Operaciones en el Ciberespacio (MOCE). En este sentido, en relación con los responsables de los sistemas y los encargados de su ciberdefensa, no se considera operativo que estas unidades deban de pertenecer a dos entes separados ni a dos cadenas de mando distintas, como pasa en la actualidad con el MCCE y el CESTIC. EL CMCCE deberá aportar directrices y asignar misiones y responsabilidades a cada una de sus jefaturas subordinadas, pero estando ambas dentro de la misma estructura orgánica, bajo una única dirección y subordinadas a la cadena operativa e integrada en la FC. Por tanto, la JSITFAS será el proveedor de servicios CIS de las FAS y el MOCE dispondrá de las capacidades militares de defensa, explotación y ataque para poder liderar y llevar a cabo las operaciones en el ciberespacio.

2.2. Presente y futuro del perfil de carrera del personal de ciberdefensa

En la actualidad, en las FAS no existe un perfil específico de ciberdefensa, por lo que el personal que desarrolla su labor profesional en este ámbito de las operaciones es valorado acorde a los criterios de evaluación de cada uno de sus ejércitos de procedencia, teniendo en consideración cualidades o perfiles específicos orientados a las necesidades de cada uno de ellos, no teniendo en valor la labor realizada tanto en el MCCD como en las unidades de ciberdefensa propias de los Ejércitos y Armada. En los Ejércitos y Armada se valora la rotación en diversos destinos de su personal y, en el caso de los oficiales, hacer mando en alguna de sus unidades operativas. Las peculiaridades de las necesidades del perfil de carrera del personal del ciberespacio implican penalización a la hora de ser evaluado para el ascenso y no truncar su carrera profesional dentro de su propio ejército.

En el TFM se aportan propuestas con el fin de conseguir que la permanencia en el área de las operaciones en el ciberespacio no penalice al personal que quiera hacer carrera en ella. Se considera que la única forma de conseguir este fin es que el personal se desligue de su ejército de procedencia, para lo cual se indican dos propuestas, una a corto-medio plazo y otra a medio-largo plazo. La primera propuesta es la creación de un cuerpo común del ciberespacio, para conseguir la permanencia de su personal altamente cualificado y adiestrado, pues de lo contrario será imposible conseguir una masa crítica de personal capacitado y especializado en este ámbito. Esta

posibilidad es factible al existir ya la estructura orgánica de los cuerpos comunes, de modo que debería de crearse un nuevo cuerpo para oficiales y suboficiales. La segunda propuesta focaliza la atención en la creación del Ejército del Ciberespacio como una rama independiente como el Ejército de Tierra, la Armada y el Ejército del Aire.

Una vez abordados los aspectos anteriores se plantean diversas formas de reclutar personal para cubrir sus necesidades específicas y que desempeñe su labor en este ámbito de las operaciones:

a) Dentro de las FAS: no se considera que deba existir una academia específica para formar al personal de la fuerza desde el comienzo de su trayectoria profesional. La propuesta que el presente TFM aporta establece que los oficiales y suboficiales deben cumplir servidumbre en sus ejércitos de procedencia en el primer empleo y parte del segundo, con la finalidad de que adquieran las capacidades de liderazgo y gestión del estrés.

Se propone seguir el modelo de la Armada en la especialización complementaria para oficiales. En el segundo año del segundo empleo (respecto a oficiales y suboficiales) se ofertarán plazas de especialización en el ámbito del ciberespacio a personal de los Ejércitos y Armada.

b) Captación de talento fuera de las FAS: se propone crear una comunidad del ciberespacio que posea una estrecha relación con otras instituciones, centros de formación y empresas relacionadas con los sistemas y redes de comunicaciones, la ciberseguridad y la ciberinteligencia, que servirá como fuente para la captación de personal para trabajar en el MCCE basándose en su marca de empleador o *Employer Branding*. Se considera necesario fomentar la imagen del MCCE para atraer a personal civil cualificado en su primera etapa profesional.

Se proponen tres formas de rejuvenecer el MCCE y captar e integrar el talento en este ámbito: captar trabajadores que se integren como personal de complemento, contratar personal civil recién titulado universitario y de centros de formación profesional y la activación de reservistas voluntarios en las escalas de oficiales y suboficiales.

La oferta de plazas para militares de complemento conseguirá cubrir el déficit de oficiales y suboficiales en los primeros empleos militares y permitirá crear una masa crítica de personal técnico en la base de la pirámide organizacional.

Además, se considera necesario focalizar la atención en el reclutamiento a medio plazo, el cual podría abordarse mediante la creación de becas formativas financiadas por el MINISDEF, por medio de las cuales se asumiría la realización de un título universitario o de formación profesional. Una vez finalizada la formación se vincularía el beneficiario a las FAS con un contrato temporal, como es el caso de los militares de complemento.

Una de las principales ventajas derivadas de esta variedad de formas de ingreso reside en la posibilidad de atraer talento sin necesidad de que vistan el uniforme militar, lo cual es un signo diferenciador y una ventaja competitiva con el resto de las FAS.

Mientras no se consiga llevar a cabo la creación de una rama específica del ciberespacio, ya sea Cuerpo Común o Ejército, que asegure un perfil de carrera propio para su personal, se tienen que valorar otras alternativas para incrementar el atractivo de cara a la captación y, especialmente, a la permanencia del personal dentro de este ámbito, en el MCCE o las unidades de ciberdefensa de los Ejércitos y Armada. En este sentido, los aspectos en los que se puede enfocar el mando para mejorar la retención son los siguientes:

a) Valoración del destino: la solución para que el MCCE posea un elevado porcentaje de cobertura de su plantilla, mientras no se cree una rama específica del ciberespacio, es que los Ejércitos y Armada consideren como una unidad de fuerza tanto al MCCE como a las unidades específicas de ciberdefensa de los Ejércitos y Armada.

Los oficiales del MCCE para avanzar en su carrera profesional, en determinados momentos de la misma, han de ejercer Mando de Unidad. Con la finalidad de retener personal adiestrado para combatir en el ciberespacio, actualmente un bien escaso que afecta su desembarco en la operatividad de la unidad, se propone que ciertos destinos dentro de la FOCE o el EM sean considerados como si estuvieran ejerciendo el mando en unidades operativas.

b) Informes personales de calificación (IPEC): los IPEC en el MCCE son superiores a la media, pues su personal está muy especializado, altamente cualificado y realiza su trabajo con un elevado grado de precisión y calidad. No obstante, al depender de los Ejércitos y Armada su ponderación, resulta difícil encontrar un punto de mejora en esta área.

La diferencia de valoración de los IPEC se convierte en un punto más a favor de la creación a corto plazo del C.C. del Ciberespacio, en el cual todos sus profesionales serían valorados por los criterios de una sola institución.

c) Medallas: se propone crear y promover dos tipos de medallas:

— La medalla específica al *Mérito ciberespacial*, que implicaría disponer de una condecoración diferenciadora que premiase la labor realizada en el ciberespacio, y así valorar al mismo nivel los méritos acreditados en cada uno de los ámbitos de las operaciones.

— La *Medalla de Operaciones Permanentes* realizadas en el TN para cada una de las cuatro existentes en la actualidad. La Operación permanente en el ciberespacio tendría su propio pasador con la inscripción CIBERESPACIO. Esta medalla se concedería por una

involucración en la operación por un periodo continuado de dos años, que podrían ser acumulables, y sería valorada al mismo nivel que el resto de condecoraciones por participar en misiones en ZO. Además, esta medalla, que requiere o valora la permanencia del personal en el destino, resultará beneficiosa para el personal del MCCE comparativamente con el personal participante en las otras tres operaciones.

d) Sueldo: realizada la comparativa de los ingresos percibidos por un miembro del MCCE con respecto a otra unidad del Órgano Central (como la UME) o con respecto a expertos en ciberseguridad del entorno empresarial, se concluye que resulta necesario equiparar el sueldo del MCCE al menos al de la UME si se pretende conseguir un grado similar de captación.

Además, dado que resulta prácticamente imposible equiparar los sueldos del personal del MCCE a los percibidos por profesionales con una formación similar y que realizan funciones parecidas en organizaciones civiles, la retención de estos profesionales será complicada si no se consigue que obtengan una proyección profesional dentro de la carrera militar. Esto se puede conseguir, como se ha reiterado a lo largo de este TFM, con la creación a corto-medio plazo del C.C. del Ciberespacio.

e) Proyección internacional: los miembros de las FAS valoran poder salir destinados o en comisión de servicio a vacantes en organismos internacionales. Lo cual se considera gratificante por motivos profesionales, familiares y económicos.

Se propone que el CMCCE prele todas las vacantes y comisiones en el extranjero, tanto relacionadas con CIS como con ciberdefensa. La cobertura de estas vacantes por personal destinado en el MCCE se puede considerar como *win to win* para el militar y para la institución.

Además, se propone que a las vacantes internacionales relacionadas con el ciberespacio y a las plazas relacionadas con el personal CIS de la JSITFAS (en la actualidad JCISFAS) se le pueda exigir que cumplan condiciones de una serie de especialidades o cursos, y lo mismo para el personal de ciberdefensa perteneciente actualmente a la FOCE y en un futuro al MOCE.

f) Formación: en la actualidad, el grado de formación del personal del MCCE se considera elevado, apoyándose en centros de referencia nacionales e internacionales. Por tal motivo, no se plantea ninguna propuesta de mejora, al considerar que la línea formativa que está siguiendo el MCCD en los últimos años es la adecuada para conseguir su fin.

Una vez abordado un diagnóstico relativo a las necesidades del personal para poder desarrollar su labor dentro del ámbito del

ciberespacio y las acciones que se podrían acometer para conseguirlo, tanto en la situación actual en un reciente MCCE como a corto-medio plazo con la creación del Cuerpo Común del Ciberespacio o medio-largo plazo con un ejército independiente, hay que plantearse que no todo el personal podrá llegar a la cima piramidal de la organización. Esta es la razón por la que cobra importancia la reinserción laboral del personal operativo del ciberespacio, cuestión por la cual tiene que preocuparse el MCCE, pues no existe mejor publicidad para una empresa o institución que la que divulguen sus miembros cuando cesan en ella: trato recibido, fomento de su formación y consideración tanto personal como de sus aportaciones y propuestas.

En este contexto, aparece de nuevo el concepto *Employer Branding*, el cual se puede definir, tal y como hemos abordado en el presente TFM, como un conjunto de medidas adoptadas por una organización encaminadas a conseguir que esta resulte atractiva para los profesionales con talento. Por tanto, es un instrumento de gran utilidad para la captación y retención de personal, pero, en este caso, también para la reinserción laboral. Así, si el MCCE se convirtiese en un referente dentro del sector de la ciberseguridad, la ciberdefensa y la ciberinteligencia, y por ende su personal, junto con la cualificación profesional de sus miembros, consideramos que se conseguirá que el perfil de un componente del MCCE sería valorado en gran medida por las empresas del sector.

Figura 2. Reinserción laboral del personal del ciberespacio (tomada [3])

Por tanto, se propone que el concepto *Employer Branding* no se enfoque en exclusividad a la captación de personal, sino también para la reinserción laboral de sus miembros. Si el MCCE consigue posicionarse como un referente en el sector de la ciberseguridad, la ciberdefensa y la ciberinteligencia, la lucha por la captación del talento en este sector tendrá un importante nicho de búsqueda en el Ejército del Ciberespacio.

3. Conclusiones

La finalidad del presente trabajo ha residido en plantear el posible futuro de las fuerzas de ciberdefensa en las FAS y, por consiguiente, definir un perfil de carrera específico para su personal. Para ello, se han reflejado una amplia gama de propuestas con el fin de alcanzar tal objetivo y así situar al ciberespacio como una prioridad dentro de las FAS; creando o potenciando, por tanto, el perfil de carrera de su personal para poder llegar a tal fin. Así, a lo largo del TFM se han expuesto, partiendo de la situación actual de las fuerzas de ciberdefensa en las FAS y del perfil de carrera de su personal, posibles líneas de mejora con la finalidad de consolidar el ciberespacio como un ámbito de las operaciones al mismo nivel que el resto de los dominios.

Por otra parte, se abordan factores justificativos que demuestran la necesidad de crear un perfil específico ciber dentro de los Ejércitos y Armada, con la finalidad de conseguir que el personal que así lo desee pueda tener una trayectoria profesional sin penalización. Esto será un primer paso mientras no se consiga el objetivo prioritario que es la creación de un nuevo Ejército del Ciberespacio dentro de las FAS, que incluya tanto al personal CIS como de ciberdefensa.

A modo de conclusión, se aportan, de forma razonada, una serie de argumentos que inducen la necesidad de conseguir un Ejército del Ciberespacio independiente de los Ejércitos y Armada, pues es la única manera de conseguir la especialización en este ámbito y que las operaciones en el ciberespacio sean lideradas por personal experto y con un nuevo estilo de dirección. La creación de este ejército permitiría entre otros aspectos:

- la consecución de un perfil de carrera apropiado para su personal y la permanencia del mismo,
- obtener una unidad con imagen de marca de empleador o *Employer Branding*, que originaría en el personal militar y civil un interés creciente por trabajar o colaborar en dicha unidad y, por último,
- conseguir que el perfil del profesional que haya formado parte de Ejército del Ciberespacio sea reconocido por el nivel de excelencia que posee en este ámbito (tanto por parte de las empresas civiles en los sectores de la ciberseguridad, la ciberdefensa y la ciberinteligencia, como en el contexto académico), con la finalidad de conseguir su reinserción laboral, en caso de que valorase finalizar su relación profesional con las FAS.

Referencias

[1] PDC-01 (A) Doctrina para el empleo de las FAS.

[2] NATO Cyber Defence Taxonomy and Definitions, 2014.

[3] Página web My Chesco:

https://www.mychesco.com/a/news/national/va-launches-solid-start-to-ensure-veterans-are-contacted-during-initial-transition/

Futuro de la Ciberdefensa en las FAS y perfil de carrera para su personal

Autor: Carlos A. Santos Sande
Director: Francisco Javier Rodríguez Rodríguez
Universidad de Vigo

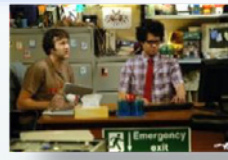
Vocación

Militar

Formación
Valores
Esfuerzo

Academia

Captación



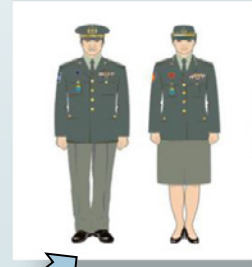
Liderazgo

Profesionalidad

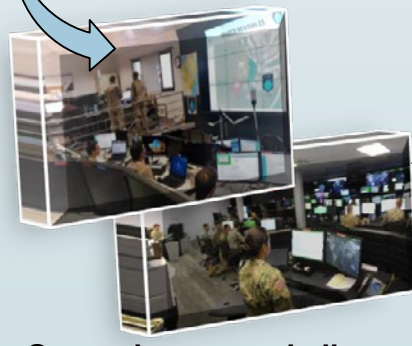
Especialización

Captación

Cuerpo Común / Ejército del Ciberespacio



Employer Branding
Ciberespacio

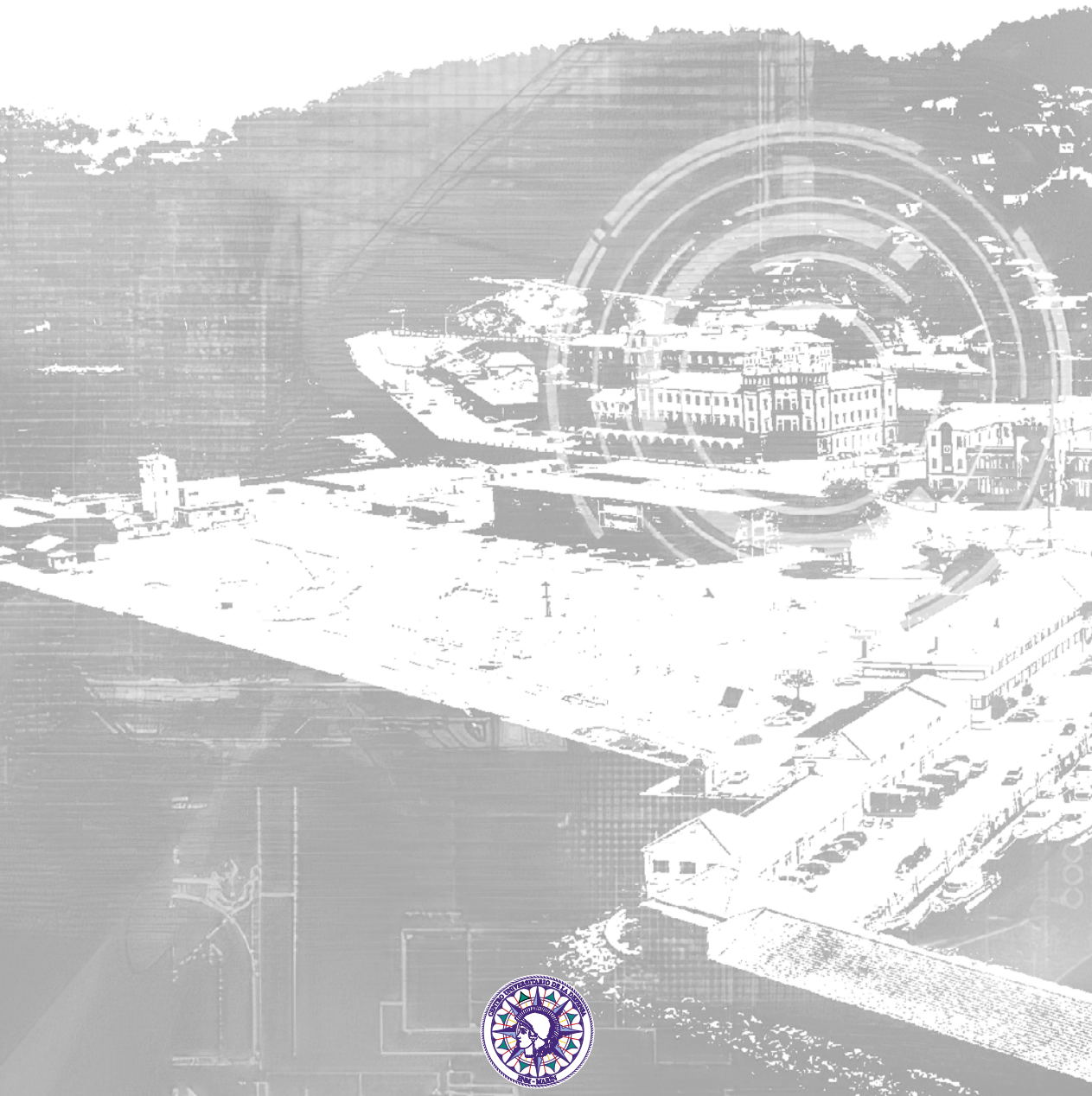


Reinserción laboral
Employer Branding

Futuro

Operaciones en el ciberespacio

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2020/2021



PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL