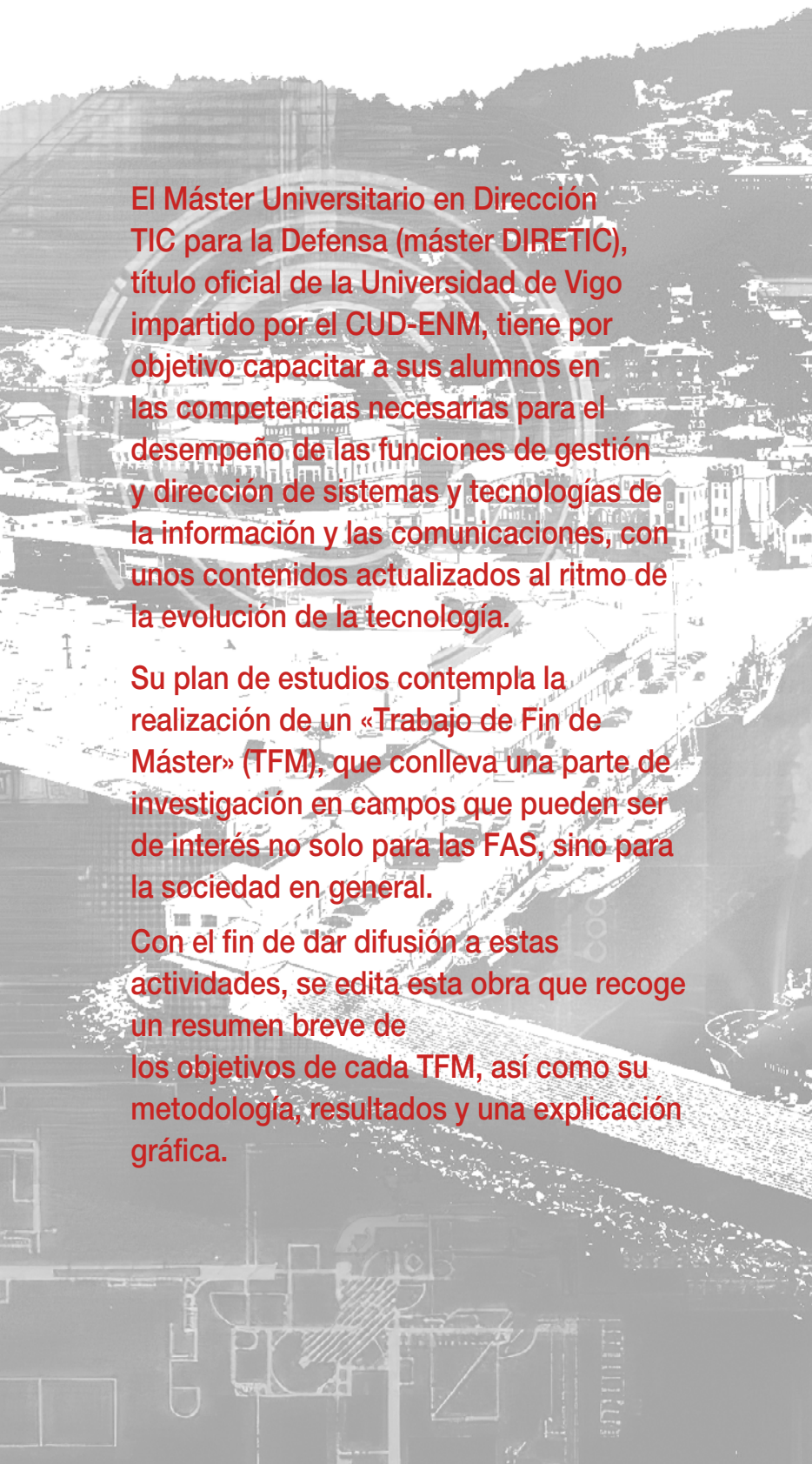
Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2021-2022

Centro Universitario de la Defensa en la Escuela Naval Militar

MINISTERIO DE DEFENSA



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

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

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

Actividades investigadoras enmarcadas en los Trabajos Fin de Máster del curso 2021-2022

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

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 083-22-313-5 (impresión bajo demanda)
ISBN 978-84-9091-723-7 (impresión bajo demanda)

NIPO 083-22-314-0 (edición en línea)

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

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 2021-2022, 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/123456789/518

Índice de contenidos

Índice por autores

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de Información

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de Información

Diseño de una infraestructura segura para proporcionar un servicio de teletrabajo

Autora: Abad Gutiérrez, Laura (gatilo101@gmail.com)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – Este trabajo trata de presentar una arquitectura para dotar de teletrabajo a cualquier organización con altos requisitos de seguridad. Para ello se propone el diseño de un sistema en el que de principio a fin se pone el foco en la seguridad, dotando a cada elemento de los mecanismos necesarios para garantizarla y dedicando un especial esfuerzo en realizar las pruebas adecuadas sobre el sistema implantado, que permitan evidenciar que tal seguridad existe.

Además, se basará en soluciones de virtualización de escritorios que por una parte permitirán el acceso a los servicios corporativos desde ubicaciones remotas, y por otro mantendrán una infraestructura *on-premise* que se podrá beneficiar tanto de la seguridad física como lógica que la organización ya viene manteniendo sobre sus instalaciones, sistemas e información.

La implementación de este sistema se realizará de manera integrada con los servicios que la organización presta de manera presencial. Los escritorios virtuales ofrecerán un modo de trabajo en el que la experiencia de usuario no se verá afectada, ni en la calidad del servicio ni en el modo en que se realizan las tareas habituales.

Todos los elementos, tanto hardware como software, que conforman la infraestructura se instalan siguiendo las guías de seguridad que sean de aplicación, y una serie de buenas prácticas, tratando siempre de emplear dispositivos acreditados. Sin olvidar por supuesto, cumplir con las diferentes normas y legislación aplicable tanto por la parte del teletrabajo como por la del propio centro de proceso de datos.

Palabras clave – VDI, teletrabajo, escritorio virtual, citrix, vmware

1. Introducción

Hace casi ya dos años, desde marzo de 2020, que el teletrabajo irrumpió de manera imprevista en la vida de muchas personas. La pandemia mundial ha supuesto el desencadenante de un cambio en la manera de trabajar de muchas organizaciones, y en pleno siglo XXI, este fenómeno repentino ha pillado a muchísimas empresas con el pie cambiado.

En el caso concreto de España, gozamos de una buena posición con respecto a la inmersión en tecnologías de la información. El informe del DESI 2020 [1] (Índice de la Economía y la Sociedad Digitales) nos coloca por encima de la media europea en el índice de digitalización de la economía y la sociedad, especialmente en el ámbito de la conectividad de muy alta capacidad, gracias al despliegue de infraestructura como la fibra, 4G y 5G. Lo cual nos indica que nuestro país se encuentra en una situación aventajada en cuanto al potencial de implantación de teletrabajo que no podremos dejar de aprovechar.

El planteamiento de los auténticos retos que supone el teletrabajo, es lo que me ha motivado a elegir este trabajo, para dar respuesta a una necesidad creciente de las organizaciones, poniendo especial énfasis en garantizar la seguridad de los datos y los sistemas.

2. Desarrollo

2.1. Tecnologías de aplicación

La primera cuestión que se nos plantea es referente al principal mecanismo para acceder a aplicaciones y datos corporativos, es decir: ¿cuál es realmente la mejor manera de proporcionar teletrabajo?

La respuesta a esta pregunta plantea una primera elección: ¿Una red privada virtual, *¿Virtual Private Network (VPN), o una infraestructura de escritorios virtuales, Virtual Desktop Infraestructure (VDI)*?

El primer caso supone acercar el puesto de trabajo de cada trabajador a su propia casa con unos cambios mínimos, permitiendo la conexión a la red local a través de un túnel VPN, del mismo modo que si estuviese en la oficina. En el segundo, el planteamiento implica un cambio importante en la infraestructura, no tanto en la parte del trabajador, que gracias a la tecnología de escritorios virtuales contará con una experiencia de usuario similar, sino en la parte de las TIC, que deberán desplegar esta nueva infraestructura e integrarla en su centro de proceso de datos.

Si evaluamos comparativamente las diferentes características que ofrece cada alternativa desde varios puntos de vista, tenemos lo siguiente:

Hardware

VPN depende en gran medida del hardware del usuario, ya que todo el procesamiento se realiza en los dispositivos del cliente. El hardware antiguo

y los sistemas operativos obsoletos pueden afectar al rendimiento y a la productividad. A esto debemos añadir la dificultad que supone mantener y administrar estos equipos remotamente.

Por otro lado, VDI tiene requisitos mínimos de hardware, y los dispositivos de los usuarios finales no suponen restricciones importantes para garantizar la experiencia de usuario. El procesamiento se realiza en el lado del servidor, utilizando recursos dedicados asignados a la máquina virtual que ejecuta el escritorio.

Almacenamiento de datos y seguridad

Hay una gran diferencia en la forma en que VPN y VDI manejan los datos. En el caso de VPN se protegen los datos mientras están en tránsito, enviándolos a través de un túnel cifrado. Mientras que los datos en el túnel llegan de forma segura al usuario, no tienen límites de seguridad una vez que están en el dispositivo del cliente. Pueden moverse y copiarse externamente sin restricciones. Tener archivos de la organización copiados localmente supone un peligro para la seguridad.

Cuando se utiliza VDI, las aplicaciones y los datos permanecen en la máquina virtual que ejecuta la estación de trabajo. Por lo tanto, los archivos están protegidos en los servidores de la organización. Los administradores pueden configurar los escritorios virtuales para restringir el movimiento de datos fuera de la red corporativa.

Rendimiento

Sin duda, VPN pierde la carrera en cuanto a rendimiento para las cargas de trabajo más grandes. Dado que las redes privadas virtuales dependen de los dispositivos de los usuarios finales, están limitadas a los recursos del usuario final y a la velocidad de conexión. Por lo tanto, diferentes usuarios tienen diferentes resultados de rendimiento dependiendo de su hardware y calidad de conexión. Además, el cifrado y descifrado de grandes cantidades de datos también puede afectar a la velocidad y al trabajo remoto.

VDI proporciona un entorno más rápido y una mejor experiencia de usuario porque cada usuario tiene asignados recursos para su estación de trabajo virtual. En lugar de tener que depender de los dispositivos del usuario, VDI utiliza recursos de servidor dedicados para mejorar las capacidades de personalización y rendimiento.

Gestión y mantenimiento

En lo que respecta a la gestión de la VPN, el servidor o infraestructura que la gestiona, es más fácil y menos costoso de mantener. Sin embargo, el mantenimiento de los dispositivos cliente es más complejo, ya que utilizan recursos externos. Esto requiere conectarse al dispositivo para solucionar problemas o realizar actualizaciones.

A diferencia de lo que ocurre con VPN, los administradores pueden actualizar y solucionar fácilmente los problemas de una infraestructura de escritorios virtuales porque disponen de una gestión centralizada del sistema. Los administradores pueden actuar sobre toda la infraestructura y tener un estrecho control sobre todo el entorno. Debido a la complejidad del sistema, esta solución requiere administradores cualificados que puedan garantizar que todo está bien configurado.

Coste

El coste puede jugar un papel importante a la hora de decidir entre VPN y VDI, ya que difiere drásticamente. Si se está buscando únicamente una solución rentable, VPN puede resultar la mejor opción. Debido a sus mínimos requisitos de hardware y a un mantenimiento menos costoso, pero normalmente se deben considerar otros factores que pueden justificar una mayor inversión.

Al contrario, VDI es una solución más cara, ya que incluye añadir toda una de una capa adicional de software y una nueva infraestructura para alojar el sistema VDI, hardware de servidor y recursos dedicados para cada estación de trabajo, lo que requiere una alta inversión inicial, pero que se ve compensada a largo plazo por los ahorros en costes de administración y mantenimiento.

En definitiva, como podemos observar en los aspectos tratados, los mecanismos de control, acceso, seguridad y administración que ofrece VDI lo convierte en la opción más adecuada para utilizar en el diseño de un sistema en el que estas características son imprescindibles, sin olvidar que además el empleo de escritorios virtuales nos va a permitir mantener la experiencia del usuario al máximo nivel.

2.2. Proveedores

Si echamos un vistazo al mercado, la cantidad de opciones disponibles para proporcionar una infraestructura de escritorio virtual, es elevada y parece que cada vez los arquitectos de sistemas van a disponer de más opciones, ya que las alternativas no dejan de crecer.

- Las características que debemos evaluar a la hora de elegir un determinado proveedor van a ser las siguientes:
- Una presencia consolidada en el mercado, con soluciones probadas, contrastadas y que ofrezca continuidad y estabilidad.
- Que disponga de un servicio de soporte de calidad y eficaz.
- Que disponga de técnicos cualificados, y sean capaces de prestar apoyo en las intervenciones que deban realizarse en la infraestructura.
- Que ofrezcan productos fáciles de implementar, integrar, y tengan capacidad de ofrecer soluciones adaptadas para cada cliente.

- Que dispongan de herramientas fáciles de gestionar y proporcionen una administración simplificada.
- Que cuenten con una oferta adecuada de formación completa y de calidad.
- Que proporcionen I+D+I suficiente para evolucionar sus productos y soluciones, renovando las tecnologías, adaptándose a las nuevas necesidades y ofreciendo continuamente tecnología actualizada e innovadora.

Si evaluamos los principales proveedores de soluciones virtuales que garanticen estas premisas, centramos el abanico de opciones en Vmware, Citrix y Microsoft. Todos ellos ofrecen productos estables de largo recorrido, y ampliamente conocidos. La mejor opción es combinar las fortalezas de cada proveedor y diseñar una solución combinando productos de cada uno de ellos.

De Citrix implementaremos la parte de virtualización de escritorio que ofrece gracias a su completa infraestructura de Citrix Virtual Apps and Desktops, una experiencia de usuario con el escritorio virtual cercana al PC tradicional. Vmware proporcionará su amplio conocimiento de hipervisores y será la tecnología empleada tanto para implementar los servidores que serán virtuales, como la infraestructura de clientes con vCenter y vSphere. Microsoft aportará toda la parte de distribución de software, aplicaciones, parches, y sistemas operativos dando soporte a los sistemas tanto en servidores como en clientes.

2.3. Implementación del teletrabajo

La virtualización de escritorio se trata de un modelo de virtualización basado en máquinas virtuales de sistemas operativos cliente. Este modelo de virtualización ofrece a los usuarios acceso remoto a escritorios completos de Windows (fundamentalmente) sin necesidad de disponer de hardware potente en el origen, ya que los escritorios se ejecutan en el centro de datos, en un conjunto o clúster de servidores.

Se debe diseñar e implantar una infraestructura que abarque desde el puesto de cada teletrabajador, los sistemas de comunicaciones, controles de acceso, etc., hasta los servidores y sistemas de almacenamiento que darán soporte al sistema, logrando mantener en todo momento las condiciones de seguridad exigidas.

Dado que las ubicaciones en las que se podrá teletrabajar no pertenecen a la propia organización, esta no tendrá ningún mecanismo de control sobre las medidas de seguridad física. Por ello se ha determinado definir un sistema en el que el puesto físico que utilice el trabajador no pueda albergar ningún tipo de información, más allá de la configuración para la conexión. Estos puestos serán ordenadores portátiles configurados para que no pueda realizarse ningún trabajo en local.

Como hemos avanzado en el punto anterior, el sistema estará basado en la tecnología de escritorios virtuales de Citrix (VDI), de manera que toda la información se mantendrá almacenada en el CPD de la organización.

El escritorio virtual que se mostrará a cada usuario será una simulación de su puesto de trabajo físico que tendría en modalidad presencial. Contará, salvo alguna excepción justificada, con los mismos accesos, servicios y aplicaciones de los que disponía habitualmente.

El sistema se compone de cuatro partes principales:

1) Puesto de trabajo de usuario asegurado.

Aunque se podría tratar de cualquier dispositivo, por homogeneizar, se va a concretar en un equipo portátil (puede ser del mismo tipo y modelo de los usados de manera habitual en la organización), con sistema operativo Windows 10 y fuera de dominio. Este equipo estará asegurado utilizando los siguientes mecanismos de aseguramiento y gestión:

- Cifrado del disco duro mediante CRYHOD
- Bastionado con las guías CCN-STIC-599B19
- Gestionado mediante el cliente de SCCM de Microsoft
- Con cliente Citrix EPA
- Agente Antivirus McAfee
- McAfee DLP Endpoint
- McAfee Endpoint Security

De esta forma se trata de garantizar la integridad del mismo y que se evite que el usuario pueda filtrar información en formato digital del equipo. Este equipo no podrá realizar ningún trabajo en local y solo podrá trabajar una vez se conecte con la infraestructura de la organización.

2) Sistema de comunicaciones cifradas seguro.

Junto al puesto de usuario se encuentran los dispositivos que facilitarán las comunicaciones con los sistemas corporativos de manera segura. Para el acceso a la red (Internet) se ha optado por utilizar un dispositivo 4G ya que se trata de la manera de conexión más independiente.

Además, las comunicaciones seguras serán posibles a través de un sistema basado en el uso de cifradores personales EPICOM EP960, proporcionados con los equipos de teletrabajo, que están configurados para conectarse a unos cifradores EP430DIC en las instalaciones centrales de la organización.

Este sistema de cifra se trata de una versión comercial, que está certificado por el CCN-CERT [2] para versiones con cifra nacional. Además, el sistema cuenta con cortafuegos para proteger los cifradores. Este sistema de comunicaciones se apoya en el acceso externo con que ya cuenta la organización y las infraestructuras existentes, como son los

balanceadores F5, que proporcionan alta disponibilidad y diversidad de accesos a Internet.

3) DMZ.

Esta zona proporciona un nivel extra de seguridad al servir de puerta acceso a los equipos de teletrabajo antes de acceder a los sistemas e información corporativos de la organización.

Esta capa de acceso cuenta con:

- Balanceadores NetScaler que validarán el acceso de los miembros de la organización en teletrabajo a través de validación con usuario y contraseña del dominio.
- Servidor de actualizaciones de seguridad de los portátiles (WSUS) y distribución de software.
- Servidor gestor del software seguridad del portátil (antivirus, control de puertos, etc.) EPO.
- Servidores que prestarán los servicios de seguridad del CCN-CERT (CARMEN).
- Servidor de licencias Microsoft KMS para licenciar los equipos portátiles.

4) Infraestructura de virtualización de escritorios.

Podemos ver la arquitectura en la figura 1. Muy brevemente, vemos como consta de cuatro capas diferenciadas:

- Capa de usuario: Compuesta por la parte de equipos clientes que disponen de Citrix Receiver bajo el que se accede a los recursos disponibles para un usuario dado.
- Capa de acceso: Las implementaciones típicas para usuarios externos requieren que estos realicen conexiones cifradas seguras que admitan el protocolo HDX, como Citrix Gateway. En el acceso se establece un canal desde el dispositivo cliente, a través de un protocolo llamado ICA que es el que permite establecer ese diálogo virtual, presentando la máquina virtual al cliente como si fuera un vídeo interactivo, y proporcionando así esa seguridad de que los datos no viajarán fuera de la organización.
- Capa de control: La capa de control se utiliza para agrupar y presentar los principales componentes de la implementación de Citrix Virtual Apps and Desktops, que son los recursos. Aquí se encuentra el servidor Delivery Controller que es el intermediario que maneja las solicitudes de sesiones de usuario, tanto a aplicaciones como a escritorios virtuales. También gestiona el equilibrio de carga y la disponibilidad y las conexiones a los recursos que se ofrecen. En esta capa también se encuentran la base de datos

SQL y el servidor de licencias Citrix, encargado de mantener y suministrar licencias para las conexiones de los usuarios.

- Capa de recursos: La capa de recursos es una presentación de todos los recursos a los que los usuarios autorizados pueden acceder. También es la parte de la arquitectura donde los administradores establecen la mejor manera de administrar y controlar los recursos que se ofrecen, mediante la creación de políticas para otorgar o restringir funciones a los usuarios.
- Capa de hardware: La capa de hardware proporciona la infraestructura virtual que necesitan el resto de capas: de acceso, control y recursos. Supone el *canal de suministro hardware* para todo el entorno.

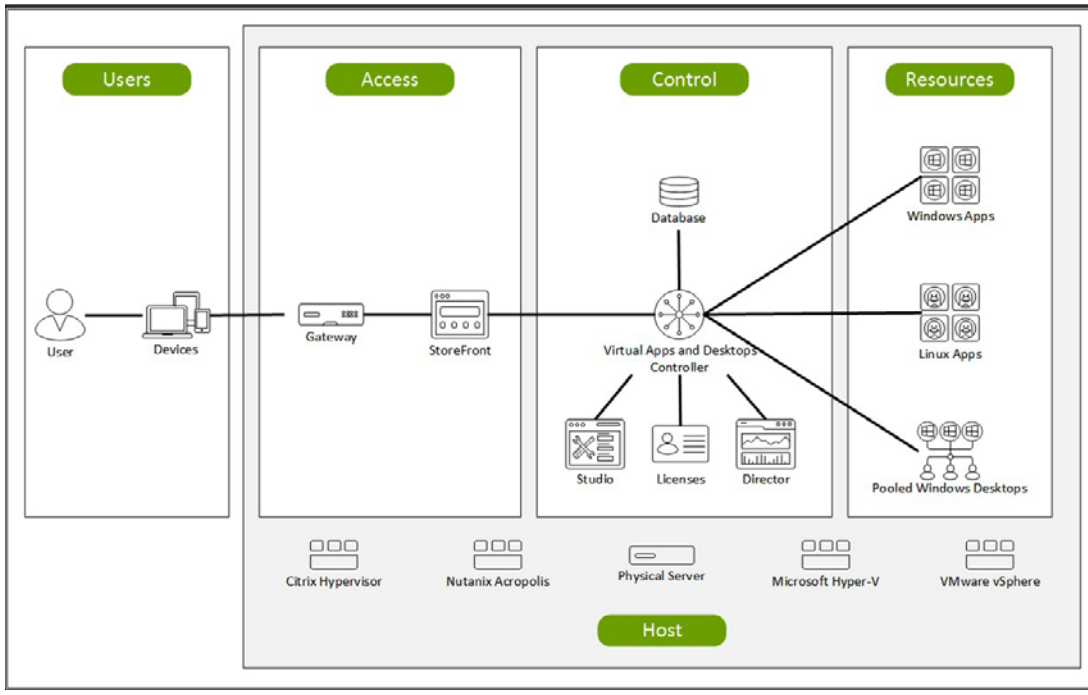


Figura 1. Arquitectura VDI

3. Resultados

El principal objetivo de este trabajo se basa en dos grandes pilares: Servicio de teletrabajo y seguridad. Hemos visto en el apartado anterior de manera esquemática como se implementaba una infraestructura como solución de teletrabajo. Para poder dar por alcanzados los objetivos debemos además garantizar la seguridad.

Para ello, se plantea implementar mecanismos que permitan proteger los sistemas y conocer la respuesta de dichos sistemas ante acciones o situaciones no previstas que puedan poner en riesgo la seguridad. Debemos medir cuánto de seguro es, ya que sin esas medidas no será

posible conocer las capacidades que se realmente ofrecen, ni llevar a cabo acciones correctivas.

Además del aseguramiento del puesto del usuario y los servicios prestados en la DMZ, se implementarán una serie tanto de medidas compensatorias, como aplicación de buenas prácticas, que permitirán garantizar la seguridad y realizar un seguimiento de los eventos de seguridad, dotando a los responsables de seguridad TIC de la capacidad de detección y respuesta antes incidentes de seguridad. Destacamos las siguientes acciones:

- Cifrar los ficheros de configuración y datos de las máquinas virtuales, así como sus instantáneas, para asegurar la seguridad de los datos críticos.
- Todos los sistemas alojados en una misma infraestructura virtual deben estar separados a través de firewalls, que filtren el tráfico de red y permitan solamente las comunicaciones definidas en cada uno de los sistemas, de modo que los aísle adecuadamente e impida la ejecución de código dañino e intentos de ataques o explotación de vulnerabilidades.
- Se debe contar con una correcta auditoria de los sistemas, que permita disponer de un registro que permita tanto realizar un análisis forense de un incidente como investigar un determinado comportamiento.
- Se debe mantener para todos los usuarios el principio de menor privilegio, dotando a cada grupo de usuarios los roles adecuados para su función y segregando correctamente dichos roles.
- Debe contarse con un adecuado plan de contingencia que permita la recuperación de los servicios en caso de desastre. En la política de copias de seguridad debe estar definido el plan de actuación que incluirá una copia remota de los datos a suficiente distancia que deberá mantenerse periódicamente.
- Se debe configurar el mayor nivel de auditoría asumible en cada dispositivo (cifradores, servidores, equipos, etc.).
- Se deben aplicar las guías STIC en cada sistema instalado que disponga de ella.
- Se debe configurar DLP en los equipos y deshabilitar cualquier tipo de conexión inalámbrica, así como protocolos que no deban utilizarse, como SSH, RDP, etc.
- Incorporación de sistemas de seguridad de aprendizaje autónomo que facilitan un continuo análisis de comportamientos y detectan las anomalías.

4. Conclusiones

Mi propósito al elegir y desarrollar este TFM no es otro que el de proporcionar un marco de referencia que pueda servir como base para diseñar un modelo, de las múltiples opciones posibles hoy en día, para implantar un sistema de teletrabajo con la mayor garantía de seguridad posible.

Hemos sido testigos a lo largo de estos dos últimos años de la necesidad de disponer en las organizaciones de mecanismos y sistemas que posibiliten esta nueva forma de trabajar. En este punto, debo resaltar varios datos que he observado durante mi investigación para este trabajo. Uno de ellos es el bajo nivel de penetración del teletrabajo que hay en nuestro país y en muchos otros aún hoy en día.

Dado que existen muchas vías de proporcionarlo, he de reconocer que me sorprende que sea así, por un lado, porque en lo que a tecnologías respecta, hemos podido comprobar que el mercado actual cuenta con multitud de proveedores con soluciones aplicables a todos los niveles. Por otro lado, porque garantizar la seguridad resulta sencillo, puesto que este modelo permite aprovechar los mecanismos de seguridad con los que ya se contaba en las organizaciones, ya que básicamente la información y los sistemas permanecen en el centro de datos.

Partiendo de este como diseño posible, y acompañado del auge de las comunicaciones, es previsible y deseable que este modo de trabajo se extienda y se normalice como un estándar en las empresas que puedan adoptarlo. Espero que con el tiempo lo habitual sea esta modalidad y, como incluyo en una de las líneas futuras, no exista diferencia entre teletrabajo y presencialidad, aprovechando la flexibilidad que ofrecen estas tecnologías.

Referencias

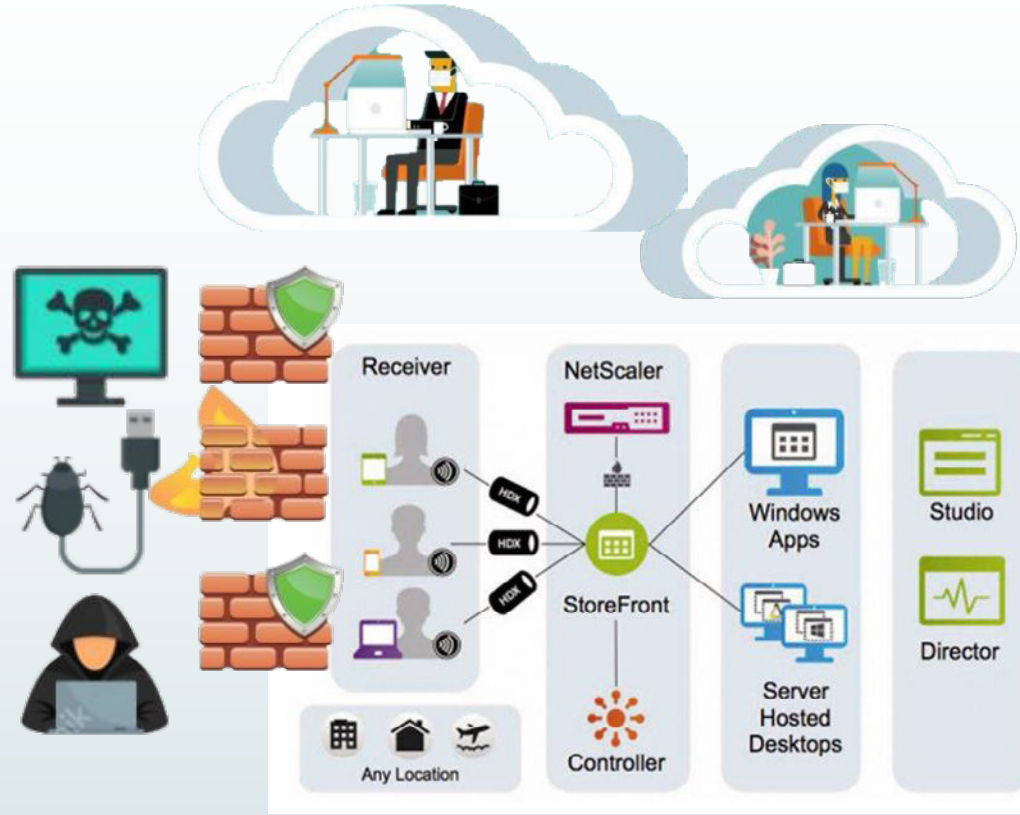
[1] Comisión Europea: Índice de la Economía y la Sociedad Digitales (DESI), 2020.

[2] CCN-CERT. CCN-STIC-105. Catálogo de Productos y Servicios de Seguridad de las TIC. Diciembre 2021.

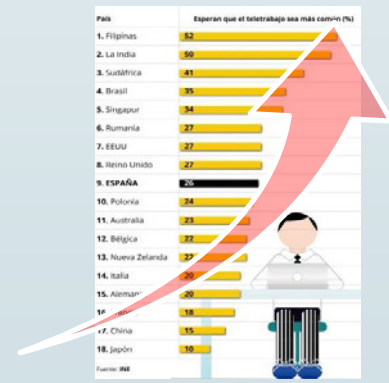
Diseño de una infraestructura segura para proporcionar un servicio de teletrabajo

Autor: Laura Abad Gutiérrez
Director: Miguel Rodelgo Lacruz

Universidad de Vigo



- ✓ Seguridad
- ✓ Escalabilidad
- ✓ Ubicuidad
- ✓ Eficiencia



cn-cert centro criptológico nacional

Mecanismos para la geolocalización de usuarios en Twitter

Autor: Andrés Pintos, Benjamín (ben73and@hotmail.es)
Directora: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – En este documento se tratan los dos métodos principales descritos en la literatura académica sobre la geolocalización en Twitter: el basado en el análisis de texto y el de análisis de las redes de usuarios. Se profundiza en las técnicas que emplea cada uno de ellos, especialmente aquellas relacionadas con el procesamiento del lenguaje natural, algoritmos de Machine-Learning y las relacionadas con el análisis de grafos.

Posteriormente, se implementan en código Python los mecanismos necesarios para llevar a cabo todo el proceso de geolocalización siguiendo algunos de los métodos descritos. Para lo cual, se obtienen diversos conjuntos de tweets utilizando la API de Twitter y se almacenan en una base de datos MongoDB. Seguidamente se lee la información relevante y se inicializan las estructuras de datos que, tras su etapa de preprocesado, se utilizarán en los algoritmos de Machine-Learning o análisis de grafos que permitirán la clasificación de los mismos como pertenecientes a una localización u otra.

Aunque el código presentado no pretende competir en eficacia y exactitud con los métodos descritos en la literatura académica, sí que nos permite obtener una visión completa de su funcionamiento, permitiendo descender a los detalles de implementación, como las librerías que se precisan, las estructuras de datos, los parámetros que determinan el comportamiento de los algoritmos de clasificación, las herramientas de visualización y presentación de resultados, etc. Obtendremos gracias a ello conclusiones de índole práctica relacionadas con los distintos mecanismos de geolocalización y que permitan seleccionar el más adecuado en función de la utilidad final para la que se emplee tal localización.

Palabras clave – Twitter, geolocalización, Machine-Learning, procesamiento de lenguaje natural, análisis de grafos.

1. Introducción y objetivos

Twitter es una de las redes sociales más populares con 396 millones de usuarios activos en abril de 2021. Además, a efectos de obtención de información, Twitter es especialmente interesante puesto que es una plataforma abierta sencilla de monitorizar y que proporciona un enorme volumen de datos. Actualmente se generan más de 500 millones de tweets diarios.

Uno de los elementos de información que resultan de especial utilidad es la ubicación de los individuos que utilizan la red social. Un análisis de la opinión que tienen los clientes de un producto, obtenido a partir de los tweets, nos dará información de qué está pasando, pero para saber cómo actuar, a menudo necesitamos conocer la ubicación de esos usuarios. Este es el objeto de lo que se denomina geomarketing, una de las muchas aplicaciones que tiene la geolocalización de Twitter. Pero no es la única, algunos estudios utilizan la geolocalización para, por ejemplo, analizar las evacuaciones durante catástrofes [1] o para predecir la situación del tráfico [2].

Sin embargo, los usuarios son cada vez más conscientes de la importancia de esta información y son más reticentes a exponer su privacidad. Así pues, aunque Twitter permite que los usuarios geolocalicen sus tweets, el porcentaje de los que lo hacen es muy bajo. Hasta tal punto es así que la propia red social eliminó en junio de 2019 la posibilidad de geolocalizar con precisión la ubicación de los tweets, debido a que los usuarios no la utilizaban [7]. Sin embargo, el interés en conocer ese dato de los usuarios sigue existiendo. Este documento trata precisamente esa cuestión ¿qué mecanismos existen para obtener la localización de un usuario en Twitter?

Además de presentar los distintos métodos existentes en la actualidad descritos en la literatura académica, el objeto de este trabajo es el de implementar en código algunos de esos métodos con el fin de obtener una visión detallada de los mismos y profundizar en su funcionamiento. Mediante esta metodología conseguiremos obtener conclusiones prácticas que sirvan para la realización de posteriores trabajos y describiremos los diferentes mecanismos que se utilizan para el proceso de geolocalización, desde la recogida y almacenamiento de datos hasta la presentación de resultados, todo ello utilizando técnicas de Machine-Learning o análisis de grafos. Hay que resaltar, sin embargo, que no es el objeto de este trabajo obtener un algoritmo con un alto grado de exactitud, comparable con los de la literatura académica. Se trata más bien de completar el hueco que hay entre la descripción teórica de los distintos métodos y su implementación práctica.

2. Desarrollo

2.1. Estado del arte

La geolocalización es el proceso por el cual asignamos una ubicación geográfica concreta a un tweet. En [3] podemos encontrar diferencias de

matiz entre conceptos como *geocoding*, *geoparsing* o *geotagging*. En este documento utilizaremos el término geolocalización de forma indistinta. Este proceso se puede llevar a cabo con distinta granularidad, en función de la aplicación a desarrollar. Puede ser suficiente identificar el país o la ciudad, o requerirse un detalle mayor e identificar barrios, distritos o calles. En [4] se definen los tipos de localización según estos criterios.

Un esquema general del proceso de geolocalización se puede encontrar en [5]. El proceso se puede dividir en cinco fases:

- Adquisición de datos. Para llevar a cabo esta fase se pueden utilizar diversas técnicas mencionadas en [6].
- Preprocesamiento de los datos. En esta fase se filtran los datos y se adaptan al formato requerido por los algoritmos de localización.
- Determinación del modo de localización. Consiste en seleccionar el formato de la respuesta de los algoritmos de localización: sí ofrecerán unas coordenadas numéricas, una etiqueta que identifique una ubicación o una etiqueta que identifique una cuadrícula geográfica definida arbitrariamente.
- Aplicación del algoritmo de localización. Para lo cual existen tres técnicas fundamentales:
  - Métodos basados en análisis de textos, que se subdivide a su vez en dos:
    - Utilización de diccionarios toponímicos (*gazeteers*), que nos permitirán realizar la transformación de una cadena de texto a una ubicación geográfica, tal y como podemos encontrar en [8, 9].
    - Algoritmos de Machine-Learning, que requerirán datos de aprendizaje para, posteriormente inferir las localizaciones de otros datos, en base a lo aprendido, tal y como se describe en [10, 11]
  - Métodos basados en el análisis de redes de usuarios: exploran las relaciones de los usuarios en la red social para la construcción de grafos sobre los que se aplicarán diversas técnicas para inferir la ubicación, a partir de la información existente para algunos de los nodos de dicho grafo, como podemos encontrar en [12, 13].
  - Métodos híbridos que combinan los anteriores para mejorar la exactitud soslayando los inconvenientes que tiene cada uno aplicado de forma aislada.
- Resultado y evaluación. Donde se valoran los resultados obtenidos y, si se precisa, se realizan los ajustes necesarios en las fases anteriores, conformando un proceso iterativo.

2.2. Metodología y herramientas.

Para la implementación de algunos de los más representativos métodos de geolocalización descritos anteriormente, se han utilizado diversas herramientas software, como la base de datos MongoDB, el lenguaje de programación Python, u otros programas de presentación y análisis de grafos como Gephi. Todo ello en un entorno local, utilizando un ordenador portátil con unas características poco significativas.

2.3. Obtención de los datos.

Para la obtención de los datos se ha utilizado la librería Tweepy de Python que, facilita el acceso a la API de Twitter que es la que facilita el acceso público a los tweets. Para utilizar la API de Twitter es necesario registrarse y seleccionar un modo de acceso. Algunos de ellos tienen coste y otros no. Para este trabajo se ha utilizado la versión de la API 1.1 y el modo de acceso sin coste.

El acceso a la API de Twitter tiene unas limitaciones, según el modo que se utilice. De tal modo que, por ejemplo, existe una restricción en el número de tweets que se pueden obtener mediante consultas. Esta situación, obliga a que, si se desean obtener grandes cantidades de datos, sea necesaria una planificación en la obtención y la dedicación de recursos informáticos durante periodos prolongados de tiempo. Cada uno de los tweets nos proporciona, no solo el propio texto, sino una información bastante extensa sobre el usuario, como el número de seguidores o un campo denominado *location*, en el que los usuarios pueden especificar, en texto libre datos sobre su ubicación general. No todos los usuarios lo utilizan, algunos indican el país mientras que otros pueden indicar hasta la dirección postal. En cualquier caso, los metadatos, en formato JSON, que se obtienen de los tweets constituyen los datos que utilizarán los distintos algoritmos de geolocalización. En nuestro caso, hemos obtenido diversos conjuntos de tweets que hemos almacenado en colecciones de una base de datos de MongoDB.

2.4. Algoritmos basados en análisis de textos.

Dentro de este tipo de algoritmos hay dos categorías: los que utilizan diccionarios de topónimos y los que utilizan Machine-Learning para el análisis de los propios tweets.

Los del primer tipo utilizan API, como la que ofrece GeoNames, que permiten diversos tipos de consultas. Así, es posible especificar una cadena de texto y GeoNames tratará de identificar algún lugar relacionado y ofrecerá las coordenadas del mismo. En el código que hemos elaborado, obtenemos de un tweet, el campo *location* del objeto *user* y llamamos a la API de GeoNames para que nos diga cuál es su ubicación. Para el conjunto de datos que denominamos tweets_spain, recogido en un área que incluye

fundamentalmente la península ibérica, hemos obtenido los resultados mostrados en la tabla 1.

Número de tweets analizados	14.990
Tweets con user.location = “”	189
Tweets con localización no resuelta	363
Tweets con localización resuelta dentro del área de obtención	13.909
Tweets con localización fuera de límite	529

Tabla 1. Geolocalización del conjunto tweets_spain mediante GeoNames

Figura 1. Representación de las localizaciones ofrecidas por GeoNames

Podemos ver que GeoNames nos ha ofrecido coordenadas de prácticamente para el 94 % de las cadenas de texto en las que el usuario había especificado algo. Posteriormente, hemos constatado que cerca del 4 % de esas coordenadas estaban fuera del área de búsqueda especificada en la API de Twitter, por lo que obviamente son erróneas. Algunos de estos errores corresponden a cadenas de texto del tipo *Silent Hill* o *vlc* que los usuarios han especificado con un sentido distinto al que GeoNames atribuye.

Con posterioridad, podemos representar, también mediante código, la ubicación de las coordenadas ofrecidas por GeoNames, obteniendo la figura 1.

Por otro lado, pero incluidos dentro de la categoría de métodos basados en el análisis de texto encontramos aquellos que utilizan técnicas de Machine-Learning. Para analizar su uso hemos utilizado diversos conjuntos de datos. Cada tweet del conjunto es un documento, la totalidad de ellos constituye el corpus y el conjunto de palabras utilizado es el vocabulario.

Para aplicar los algoritmos de Machine-Learning, en primer lugar, debemos preprocesar los documentos, para lo cual, convertimos todas las palabras a minúsculas, eliminamos códigos, símbolos, signos de puntuación,

emoticonos, palabras con números, palabras con menos de tres letras, etc. En definitiva, todo aquello que no se pueda identificar como una palabra con significado. Para llevar a cabo esta fase, se utilizan diversas funcionalidades de librerías de Python que nos permiten la *tokenization*, eliminación de *stopwords*, etc.

De todas esas palabras eliminamos aquellas que tienen una frecuencia de aparición inferior a un determinado umbral y seguidamente eliminamos los tweets que se hayan quedado vacíos. El conjunto obtenido tras el procesamiento previo lo subdividiremos en un subconjunto que utilizaremos para entrenamiento de los algoritmos de Machine-Learning y otro para test.

El siguiente paso es construir una matriz con tantas filas como tweets y tantas columnas como palabras y rellenar las celdas con el cómputo de la frecuencia de aparición de las palabras en cada tweet/documento.

Finalmente aplicamos los algoritmos de Regresión Logística, Máquina de Vectores Soporte (SVM) y Bosque Aleatorio a la matriz obtenida. Para cada uno de ellos es necesario realizar un estudio del valor de los hiperparámetros que ofrecen el mejor resultado de exactitud (*accuracy*).

Se ha aplicado el procedimiento descrito sobre dos conjuntos de tweets diferentes: correspondientes a tweets procedentes de Madrid y de Ciudad de México. El resultado obtenido permitió la clasificación con una exactitud de casi el 70 %. En la tabla 2 se observan los valores de exactitud (*Accuracy*), precisión (*Precision*) y exhaustividad (*Recall*) obtenidos por el algoritmo SVC sobre dichos conjuntos.

	Precision	Recall	F1	Support
0 (Madrid)	0.65	0.78	0.75	1254
1 (México)	0.74	0.59	0.66	1290
Accuracy			0.69	2544

Tabla 2. Informe de clasificación Madrid/México del algoritmo SVM

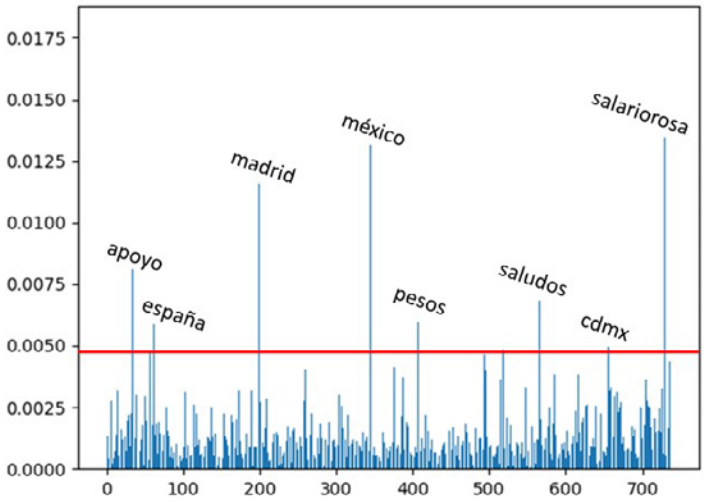
En la tabla 3 se muestran los resultados de la matriz de confusión correspondientes, donde se ofrecen los valores en los que se predijo correcta o erróneamente cada una de las clases.

		Clases predichas	
		0	1
Clases reales	0 (Madrid)	(TN) 981	(FN) 273
	1 (México)	(FP) 525	(TP) 765

Tabla 3. Matriz de confusión de la clasificación Madrid/México con el algoritmo SVM

Para analizar cuáles fueron las palabras que, tras el entrenamiento, obtuvieron unos coeficientes más elevados y que, por tanto, tienen más

peso en la clasificación, obtuvimos la gráfica de la figura 2, en la que hemos indicado de qué palabra se trata y cuántas apariciones tiene dicha palabra en los subconjuntos correspondientes a los tweets de Madrid y Ciudad de México.



Palabra	Madrid	México
"apoyo"	8	93
"españa"	105	11
"madrid"	107	2
"méxico"	4	124
"pesos"	1	36
"saludos"	8	68
"cdmx"	0	44
"salariorosa"	0	101

Figura 2. Coeficientes de las palabras más significativas en la clasificación Madrid-México

2.5. Algoritmos basados en análisis de redes de usuarios.

Este método se fundamenta en que es más probable que dos usuarios compartan la misma ubicación si entre ellos existe una relación en la red social. Esa relación puede ser de diverso tipo: un usuario puede ser un seguidor (*follower*) de otro, o ser seguido (*followee*), o ser citado en un intercambio de tweets, etc.

Para obtener la lista de seguidores de cada uno de los usuarios hemos tenido que realizar una consulta a la API de Twitter. Estas consultas son costosas puesto que están limitadas a un máximo de 15 cada cuarto de hora. Obtener la lista de seguidores de 3.000 usuarios distintos supone unas 50 horas.

Para aplicar este algoritmo a un caso real, hemos obtenido el grafo correspondiente a los usuarios de otro conjunto de datos que hemos denominado tweets_mad_bar obtenido a partir de 2.500 tweets procedentes de la ciudad de Madrid y, otros tantos, procedentes de la ciudad de Barcelona. El grafo obtenido, una vez filtradas las celebridades, se puede observar en la figura 3, donde los nodos de los usuarios de Madrid se muestran en color rojo y los de Barcelona en verde.

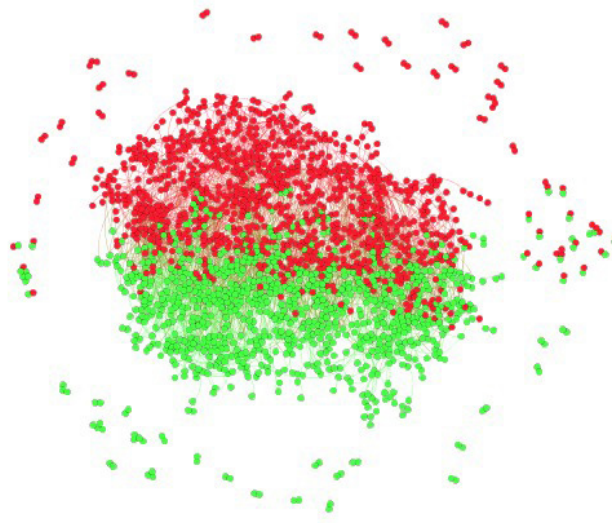


Figura 3. Grafo del conjunto tweets_mad_bar

Puesto que en este conjunto conocemos las ubicaciones reales de los nodos, podemos etiquetar únicamente un porcentaje de ellos, aplicar el algoritmo de propagación de etiquetas y, posteriormente comparar si la etiqueta predicha se corresponde con la real. Este experimento lo hemos repetido etiquetando el 10 %, el 20 % y el 30 % de los nodos de cada ubicación. Puesto que el algoritmo de propagación de etiquetas no es determinista, sino que sus resultados varían en función de variables aleatorias internas, hemos repetido las pruebas cinco veces y obtenido las medias de los resultados.

En la tabla 4 vemos que para el 10 % de los nodos etiquetados, las etiquetas se han propagado hasta el 94 % del total de nodos y se ha obtenido una exactitud en la propagación del 63.8 %, porcentaje que sube hasta el 77.6 % en el caso de etiquetar el 30 % de ellos. También podemos ver en dicha tabla los valores de precisión, exhaustividad y los correspondientes a las matrices de confusión de cada prueba.

Nodos	1553	Madrid	803	51.7%				
		Barcelona	750	48.3%				
Etiquetas Inicio	**Expansión**		**PRE**	**REC**	**F1**	**ACC**	**TRUE**	**FALSE**
10%	94%	Madrid	0.656	0.646	0.648	0.638	490.4	269.6
		Barcelona	0.624	0.648	0.624		444.8	259.2
20%	95%	Madrid	0.772	0.678	0.722	0.728	520.2	247.8
		Barcelona	0.690	0.782	0.732		552.8	155.2
30%	96%	Madrid	0.814	0.744	0.774	0.776	580.0	200.0
		Barcelona	0.746	0.814	0.778		584.8	133.2

Tabla 4. Resultados de propagación de etiquetas en tweets_mad_bar.

3. Resultados y discusión

En los conjuntos de tweets recogidos, se ha constatado que menos del 1 % de los usuarios utiliza la funcionalidad de etiquetado de los tweets con coordenadas. Por lo que tratar de inferir localizaciones con gran precisión, a un nivel por debajo de ciudad, requiere la obtención de varios cientos de miles de tweets, con el fin de conformar un conjunto de referencia significativo.

Con el método de geolocalización que utiliza diccionarios de topónimos, se han podido ubicar el 94 % de los usuarios que han incluido información en el campo *location*. Sin embargo, se ha podido comprobar que, al menos, un 4 % son erróneas, debido a que el usuario ha especificado un texto ambiguo que no se ha podido resolver correctamente. En definitiva, este método ofrece buenos resultados, pero depende de que el usuario especifique su localización y lo haga de forma que sea interpretable geográficamente por las API que implementan los diccionarios de topónimos.

Respecto al método de análisis de textos basado en el vocabulario utilizado por los usuarios en sus tweets, hemos podido diferenciar entre los tweets procedentes de las ciudades de Madrid y Ciudad de México, consiguiendo una exactitud del 69 %.

Por último, en cuanto a los algoritmos que analizan las relaciones entre los usuarios de la red, hay que destacar fundamentalmente el tiempo que requiere la construcción de dichas redes debido a la limitación de acceso que impone la API. Por el contrario, la información obtenida, resulta más insensible al paso del tiempo, puesto que no parece probable que los usuarios cambien sus relaciones de seguimiento o amistad con frecuencia.

Al aplicar el algoritmo de propagación de etiquetas, para distinguir entre usuarios de Madrid y Barcelona, y etiquetando únicamente un 10 % de usuarios en cada clase, podemos clasificar correctamente al 63.8 % del conjunto. Además, se constata que las etiquetas se propagan al 94 % de los usuarios, por lo que la cantidad de nodos aislados que no han sido etiquetados es pequeño.

4. Conclusiones

A lo largo del trabajo hemos presentado los mecanismos, herramientas y técnicas que se utilizan para la implementación de los métodos de geolocalización. Desde la obtención de los tweets, su almacenamiento, el procesado de los datos, la interacción con las API de información toponímica, los algoritmos de Machine-Learning y los algoritmos de análisis de grafos, hasta las herramientas y utilidades de representación gráfica de resultados.

Los métodos descritos tienen sus limitaciones y una aproximación híbrida en la que se utilicen de forma simultánea varios de ellos podrán llegar a ser

más eficaz. Hemos constatado que la utilización aislada de los diccionarios toponímicos solo se puede aplicar al 50 % de los usuarios, que son los que cumplimentan el campo *location* en el perfil de usuario. Por otro lado, los algoritmos basados en las diferencias de vocabulario empleadas en las diferentes localizaciones resultan muy sensibles a la temática (*topics*) que eventualmente se trataba en cada ubicación durante las fechas en las que se recogieron los tweets para llevar a cabo el aprendizaje de los algoritmos de Machine-Learning. Por último, los algoritmos basados en las relaciones entre usuarios tienen el inconveniente de no poder etiquetar aquellos nodos aislados y la gran cantidad de tiempo requerida para la construcción del grafo correspondiente debido a las limitaciones de acceso a la API de Twitter.

En definitiva, este trabajo puede servir como base para otros futuros en los que se profundice sobre alguno de los métodos presentados con el fin de mejorar la exactitud, mejorando las técnicas de preprocesado o utilizando información adicional que permita asignar un factor de ponderación, o peso, a los vértices de los grafos o a las características analizadas por los algoritmos de Machine-Learning.

Referencias

[1] Kumar D., (2018 abril), Ukkusuri S. «Utilizing geo-tagged tweets to understand evacuation dynamics during emergencies: a case of study of hurricane Sandy» Proceedings of the web conference. 1613-20. Disponible en https://doi.org/10.1145/3184558.3191619

[2] Carroll D., (May 05 2021) «From Twitter to traffic predictor» Carnegie Mellon University. News. https://www.cmu.edu/news/stories/archives/2021/may/traffic-prediction.html Disponible a 27/12/2021.

[3] Schosser S., Toninelli D., Cameletti M., (2021), «Comparing methods to collect and geolocate tweets in Great Britain» Journal of Open Innovation: Technology, Market and Complexity. https://doi.org/10.3390/joitmc7010044

[4] Kotzias D., Lappas T., Gunopulos D., (Nov. 2015), «Home is where your friends are: Utilizing the social graph to locate twitter users in a city». Information Systems. 57, 77-87 https://doi.org/10.1016/j.is.2015.10.011

[5] Luo X., Qiao Y., Li C., Ma J., Liu Y., (Ago. 2020), «An overview of microblog user geolocation methods» Information Processing and Management, 57; https://doi.org/10.1016/j.ipm.2020.102375

[6] Lin J., Cromley R.G., (2017), «Inferring the home locations of Twitter users based on the spatiotemporal clustering of Twitter data» Transactions in GIS. 22, 82-97 https://doi.org/10.1111/tgis.12297

[7] «Twitter will remove precise location tagging in tweets, citing lack of use» https://techcrunch.com/2019/06/18/twitter-will-remove-location-tagging-in-tweets-citing-lack-of-use/ [Disponible a 23/12/2021]

[8] Han B., Cook P., Baldwin T., (2012), «Geolocation prediction in social media data by finding location indicative words» Proceedings of COLING 2012: Technical Papers. 1045-62.

[9] Drezde M., Osborne M., (2016), «Geolocation for Twitter: Timing Matters» Proceedings of NAACL-HLT. 1064-69. http://dx.doi.org/10.18653/v1/N16-1122

[10] Chi L., Lim K.H., Alam N., Butler C.J., (2016 Dec.), «Geolocation prediction in twitter using location indicative words and textual features» Proceedings of the 2nd Workshop on Noise user-generated Text. 227-34. https://aclanthology.org/W16-3930.pdf

[11] Lourentzou I., Morales A., Zhai C., (2017 Jan.) «Text-based geolocation prediction of social media users with neural networks»

IEEE International Conference on Big Data, 696-705 https://doi.org/10.1109/BigData.2017.8257985

[12] Rahimi A., Cohn T., Baldwin T., (2015 junio) «Twitter user geolocation using a unified text and network prediction model» Proceedings of the 53rd annual meeting ot the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing. 630-6. http://dx.doi.org/10.3115/v1/P15-2104

[13] Jayasinghe G., Jin B., McHugh J., Robinson B., Wan S., (2016 Dec.) «CSIRO Data 61 at the WNUT geo shared task» Proceedings of the 2nd workshop on noisy user-generated text. 218-26. https://aclanthology.org/W16-3929.pdf

Mecanismos para la geolocalización de usuarios en Twitter.

Autor: Benjamín Andrés Pintos
Directora: Milagros Fernández Gavilanes
Universidade Vigo

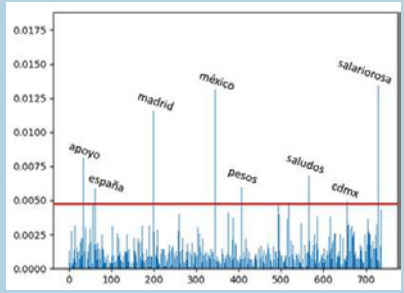
Introducción

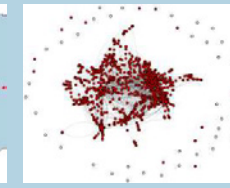
Twitter se ha convertido en una fuente de información valiosa con fines científicos, comerciales o incluso políticos. La posibilidad de averiguar la ubicación geográfica de procedencia de los tweets se aplica en el geomarketing, para ajustar el foco de las campañas publicitarias, pero también en estudios relacionados con la evacuación ante catástrofes o la predicción del tráfico. En este trabajo se revisan los métodos actuales y se implementan mediante código alguno de ellos con el objeto de obtener un mayor grado de comprensión de los mismos. No es el objetivo del trabajo conseguir valores de exactitud que compitan con la bibliografía académica, sino mostrar los mecanismos de implementación que utilizan los diversos métodos de geolocalización.

Metodología y Desarrollo

En la bibliografía académica podemos encontrar métodos de localización de dos grandes tipos: los que se basan en el análisis de textos, tanto de los propios tweets, como del perfil de los usuarios de Twitter; y los que se basan en el análisis de las redes sociales, construyendo grafos en los que se representan las relaciones de seguimiento o amistad.

Tras una descripción profunda de las técnicas que se emplean en dichos métodos, realizamos una implementación en lenguaje *Python* de algunos de ellos. En el trabajo se presenta el código necesario para la adquisición de los tweets a través de la API de Twitter, el almacenamiento en una base de datos de *MongoDB*, diferentes técnicas de preprocesamiento y la aplicación de técnicas de análisis de grafos y algoritmos de Machine-Learning para clasificar los tweets como procedentes de una u otra ubicación.





También se aborda la utilización de API's de diccionarios toponímicos para la obtención de coordenadas, como *GeoNames*, así como el empleo de otras herramientas como *Gephi* para la visualización de los grafos.

Resultados

Utilizando los diccionarios toponímicos se consigue una geolocalización para el 94% de los usuarios que cumplimentan el campo *"location"* del perfil de usuario.

Mediante el análisis del vocabulario empleado en los tweets, se consigue el 69% de exactitud en la clasificación de los usuarios procedentes de Madrid y Ciudad de México.

En el grafo que representa las relaciones de seguimiento entre usuarios procedentes de las ciudades de Barcelona y Madrid, se consigue, etiquetando el 10% de los usuarios de cada ciudad , y mediante el algoritmo de propagación de etiquetas, una exactitud del 64%.

Conclusiones

Todos los métodos de geolocalización expuestos tienen sus ventajas e inconvenientes, por lo que una aproximación híbrida, en la que se emplearan de algún modo todos ellos, resultaría más eficaz. Los métodos que emplean diccionarios toponímicos solo se pueden utilizar con el 50% de los usuarios. Por otro lado, los que emplean el análisis de textos son muy sensibles a la temática tratada durante las fechas de la recogida de datos, dificultando la utilización del modelo tiempo después. Por último, los que se basan en redes de usuarios requieren mucho tiempo para la construcción del grafo de relaciones, debido a las limitaciones de acceso de la API de Twitter.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Diseño de un sistema de ciberseguridad aplicable a un buque de la Armada

Autor: Carrasco Sandino, Miguel (mcarsan@fn.mde.es)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – El presente trabajo tiene como objetivo sentar las bases del diseño de un sistema de ciberdefensa que se pueda instalar en buques de la Armada española. La creciente adopción de soluciones tecnológicas de automatización en dichos buques, hace que se vean más expuestos a ciber ataques con los consecuentes riesgos asociados. Por lo tanto, en el presente texto, se pretende establecer una metodología adecuada para el desarrollo del sistema, identificar los requisitos aplicables a un sistema de ciberdefensa, caracterizar los sistemas a bordo que deben ser supervisados, y realizar un análisis de riesgos de dicha caracterización.

Todos estos pasos se han llevado a cabo sin perder de vista que las instalaciones a bordo de los buques poseen cierto grado de clasificación en función de la información que manejen, y, por lo tanto, es de aplicación cierta normativa que no se puede obviar en el diseño de un sistema que supervise todos los sistemas conectados a bordo.

Por último, se ofrece una configuración tanto de software como de hardware que sea capaz de soportar la instalación y operación del sistema de ciberdefensa, así como el procedimiento de desarrollo del software necesario hasta llegar a una solución de compromiso que cubra la totalidad de los requisitos del sistema, identificados al principio del proceso. Adicionalmente se incluye una planificación tentativa de la duración de los diferentes procesos.

Palabras clave – Ciberdefensa, sistema, buque, requisitos, desarrollo, análisis.

1. Introducción

La adopción de la tecnología de automatización en las plataformas de la Armada es un hecho patente. La desaparición del servicio militar obligatorio a principios del siglo XXI, forzó la adopción de dotaciones más reducidas en los buques, desarrollando nuevas tecnologías que permitían el pilotaje de la maquinaria a distancia, y de manera desatendida. Todas estas tecnologías, sumadas a las cada vez más complejas propias de un buque de guerra moderno, como son los sensores, sistema de combate y comunicaciones, actualmente están basadas en redes informáticas. Los buques de guerra poseen kilómetros de redes en su interior, que conectan los diferentes elementos.

Por lo tanto, el riesgo de ciberataques lleva presente desde el mismo momento en que se adoptaron dichas tecnologías. Esta realidad ha forzado a las FAS a desarrollar soluciones de ciberdefensa para que sean instaladas a sus unidades más críticas (Jefe del Estado Mayor de la Defensa (JEMAD), 2011).

En el caso de la Armada, este hecho se materializó en el año 2018, como una orden ejecutiva del Estado Mayor de la Armada (EMA), de dotar de un sistema de ciberdefensa a los buques en desarrollo y construcción.

El presente trabajo trata de establecer las pautas a seguir para poder diseñar efectivamente un sistema de ciberseguridad embarcable que permita ofrecer las garantías necesarias para ofrecer una defensa frente a posibles ataques cibernéticos.

2. Consideraciones previas

Lamentablemente, en el ámbito de ciberdefensa en entornos militares, la información de partida disponible es casi nula, por lo que, para el desarrollo de nuestro sistema, es necesario partir casi de cero. Tenemos constancia de que los países de nuestro entorno están trabajando en sistemas similares, pero son muy celosos de compartir información alguna al respecto. Son instalaciones muy sensibles y es normal que no se quiera compartir información.

Afortunadamente, en España existe normativa aplicable en el campo de la ciberdefensa. Está indicada especialmente para infraestructuras críticas, como pueden ser centrales nucleares o centros de control de tráfico aéreo, por ejemplo, que requieren de sistemas preventivos para garantizar un funcionamiento seguro. Dicha normativa establece reglas que se deben cumplir en dichas instalaciones, así como en las que se maneja información clasificada. Además, la acreditación de los sistemas para poder manejar dicha información es realizada por el mismo estamento, el Centro Criptológico Nacional, por lo que es un buen punto para empezar.

En nuestro caso, la información de partida incluye entre otras, la siguiente documentación:

1) Concepto de ciberdefensa militar del JEMAD (2011 y 2018)
2) Normativa STIC del Centro Criptológico Nacional (CCN) (Centro Criptológico Nacional, 2020), (Centro Criptológico Nacional, Julio 2012) y (Centro Criptológico Nacional, Enero 2009)
3) Esquema Nacional de Seguridad, del CCN (Centro Criptológico Nacional, 2022)

En [1] ya se marcaban las características generales que debe cumplir un sistema de ciberdefensa. Adicionalmente con el mandato del EMA referente a la inclusión de sistemas en los buques, se dejaban vislumbrar los esbozos de unos requisitos de alto nivel, que nos ayudarán a definir las capacidades y características que necesitaría un sistema válido.

Además, resulta tremendamente conveniente el definir al comienzo de un programa de desarrollo la metodología a utilizar durante el mismo. En este caso se propone la utilización de la ingeniería de sistemas como metodología de desarrollo, debido a los buenos resultados que se han obtenido en otros programas recientes, y a que en la Dirección General de Armamento y Material (DGAM) es de uso común.

La mecánica de esta metodología estriba en la definición de unos requisitos de sistema de alto nivel, sobre los que se van definiendo los sistemas primero (SDR) y los componentes después (PDR). A cada paso se va estableciendo mayor nivel de detalle. Se definen una serie de hitos para cada uno de los pasos, y no se pasa al siguiente hasta que se presenta el estado del programa en cuestión, y se aprueba por el órgano ejecutivo al cargo de su seguimiento.

Una vez que cerrado el diseño (CDR), empieza la fase de construcción/ montaje y pruebas de componentes, hasta que el sistema completo es capaz de entrar a la fase de pruebas (TRR). En ese momento, todos los requisitos de sistemas deben ser verificados uno a uno por medio de las pruebas correspondientes, hasta llegar a verificar los requisitos de alto nivel, momento en el cual, el diseño está listo para la entrada en servicio. Este tipo de desarrollo también es conocido como desarrollo en V.

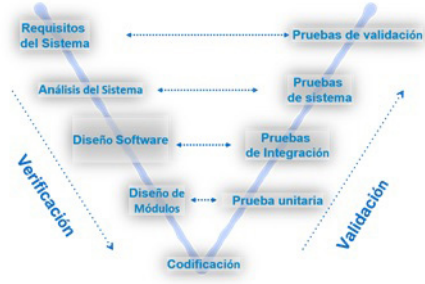


Figura 1. Modelo de desarrollo

3. Requisitos del sistema

El paso siguiente propuesto tras definir la metodología, es la generación de los requisitos de alto nivel, y de los sistemas necesarios para que la configuración de nuestra propuesta sea válida.

Por lo tanto, tomando de base los documentos ejecutivos y la normativa de aplicación al sistema, se crean una serie de requisitos, que nos permiten desarrollar el sistema desde ese punto.

Las características principales que el sistema debe poseer se pueden enumerar en la siguiente lista:

1) Prevenir los incidentes de seguridad informáticos.
2) Obtener la capacidad de análisis forense, para poder identificar el alcance o efectos producidos por cualquier incidente.
3) Obtener la capacidad de resiliencia.

El cumplimiento de estas características se puede traducir a necesidades de nuestro sistema de manera que:

Para el cumplimiento de 1) se propone la instalación de un sistema de colección y correlación de eventos (SIEM), que permita la generación de reglas de correlación de eventos, así como la presentación de dichos eventos al operador. También se deberán instalar sensores de tráfico de red con monitorización que permitan la detección de anomalías de red en sistemas de información con diferente grado de clasificación. Para esto se prevé la instalación de sistemas de prevención y detección de intrusos (IPS/IDS).

Para el cumplimiento de 2) la consola de seguridad tendrá capacidad de identificar el alcance real del incidente y el deterioro producido en los sistemas clasificados. La consola de seguridad tendrá capacidad de recoger pruebas y evidencias válidas que permitan la investigación del origen y sean admisibles en un proceso legal. Por lo tanto, será necesaria adicionalmente la instalación de un sistema de almacenamiento adecuado a tal tarea.

Para el cumplimiento de 3) La consola de seguridad (SIEM) y los sensores asociados tendrán capacidad de operación autónoma alternativa independiente de la alimentación principal, así como sistemas de alimentación ininterrumpida (SAI) que les permitan operar aún con limitaciones eléctricas, durante al menos una hora.

Los servidores dispondrán de medios de respaldo que proporcionen capacidad de recuperación (redundancia). La arquitectura de recuperación de los servidores de respaldo debe garantizar, en caso de caída o pérdida de los servidores principales, la recuperación del sistema en un tiempo inferior a una hora.

4. Caracterización del sistema

Para poder dimensionar un sistema que cumpla con dichos requisitos, previamente hay que realizar una caracterización de los sistemas que posee nuestro *barco de pruebas*, que es un barco ficticio con los sistemas más comunes existentes en los diferentes buques de la Armada.

Debido a la aplicación de la normativa CCN-STIC, es necesario realizar una división basada en el nivel de clasificación de la información que manejan las diferentes redes. En el caso de nuestro buque, se han considerado tres grados distintos de nivel de clasificación:

Difusión limitada, confidencial y reservado.

Parte del trabajo de caracterización implica determinar para cada instalación del buque, a qué grupo pertenece, en la tabla 1 se recogen algunos ejemplos a modo ilustrativo.

Difusión Limitada	Confidencial	Reservado
WANPG, SICP, Red Administrativa, etc.	Red de sensores, Sistema de combate.	Sistemas de comunicaciones, mando y control.

Tabla 1. Descripción de redes en función de su grado de clasificación.

Tras realizar esta primera distribución, realizamos una mayor segmentación en base a los siguientes parámetros. Para las instalaciones de nuestro buque de pruebas se han identificado 5 dominios, con 15 redes distintas, a las que están conectadas 62 instalaciones, que poseen hasta 455 elementos únicos que poseen algún tipo de software. También se han identificado 7 interconexiones entre dominios. En el trabajo se realiza también una identificación del tipo de elemento por función (Pc, portátil, switches, etc.) así como de los interfaces que poseen (Ethernet, USB, teclado, serie, etc.).

Una vez realizada la composición completa de la instalación y sus dependencias, el siguiente paso es definir el valor de cada activo de buque, utilizando una valoración en base a la triada CID (Confidencialidad, Integridad y Disponibilidad), tomando como referencia las consecuencias resultantes si un elemento dado fallara por culpa de un ataque.

Una vez determinados los activos y su valoración el siguiente paso es realizar un análisis de riesgos.

5. Análisis de riesgos

Para la realización del análisis de riesgos se ha utilizado la metodología MAGERIT, que es la indicada por el CCN en sus guías STIC.

Esta metodología sigue el detalle mostrado en la figura 2, para la cual, una vez determinados los activos, se identifican las amenazas a las que pueden verse expuestos. Se comprueban las salvaguardas actualmente

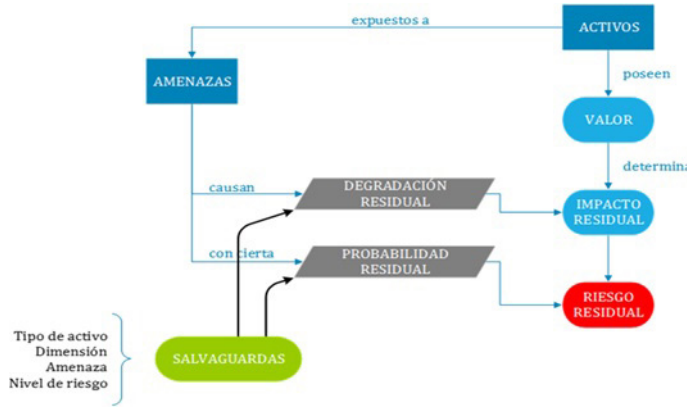


Figura 2. Metodología utilizada para el análisis de riesgos

dispuestas y se determina como son de eficaces frente al riesgo potencial al que se encuentra expuesto el sistema. Se estima el impacto en caso de materialización de la amenaza. Y por último se estima el riesgo definido como el impacto ponderado con la tasa de ocurrencia de la amenaza (probabilidad y degradación).

En caso de resultar inaceptable se consideran nuevas salvaguardas con el objetivo de reducir el riesgo a un valor que hemos fijado como objetivo. La ventaja de la utilización de MAGERIT es que propone la utilización de la herramienta PILAR, la cual incluye un completo catálogo de amenazas y salvaguardas, y además proporciona cierta automatización del análisis.

Durante la realización del análisis se comparan las distintas iteraciones del mismo, hasta comprobar que el nivel de riesgo residual es aceptable tras la incorporación de las diferentes salvaguardas, quedando identificadas en el texto del trabajo.

6. Solución de diseño

Una vez determinadas las salvaguardas a nuestra propuesta queda por determinar la solución hardware y software sobre la que construir nuestro sistema.

La solución hardware se basa en 3 servidores y switches, cada uno dedicado a un dominio según el grado de clasificación. Todo el hardware debe estar alojado en un armario de dimensiones reducidas que permita su embarque. Cada uno de los servidores se encontrará redundado por una segunda unidad, dándonos un total de 6 servidores para cumplir con los requisitos de resiliencia.

Cada dominio se encuentra respaldado por una SAI. La solución software será casi en su totalidad virtualizada, por lo que se incluye un PC de gestión por sistema para su operación y administración. Además, en el armario se incluyen los elementos de alimentación del mismo, así como

un panel de control del sistema de ciberdefensa, una unidad de control interna y por último se incluye un KVM común a todos los servidores para poder operar el sistema desde el propio armario. La disposición del mismo se puede observar en la figura 3.

La solución software se compone de una plataforma virtualizada con VMWare sobre la que corre el siguiente software. La aplicación SIEM, que es la encargada de recoger los registros y Logs de eventos de todo el sistema. La aplicación escogida es Q-Radar de IBM. Para el almacenamiento se ha escogido la solución Jovian DSS. Para la aplicación de detección y protección de intrusiones, así como el firewall se ha escogido Fortinet. Para la detección de amenazas basadas en el comportamiento, se ha escogido la solución de Nozomi Networks.

La adopción de estas soluciones de software por sí solas no es suficiente para un correcto desempeño de las tareas de ciberdefensa para nuestro buque, ya que el sistema debe aprender las características del buque y ser entrenado conforme a los parámetros normales de funcionamiento.

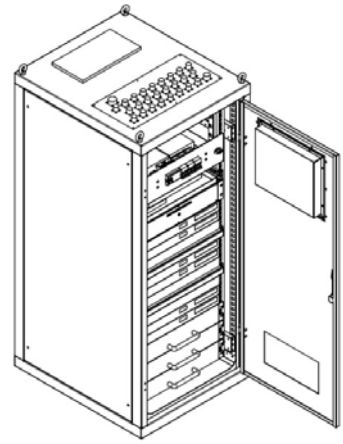


Figura 3. Disposición del armario del sistema

Afortunadamente, todos los buques de última generación adquiridos por la Armada, han sido adquiridos a través de Navantia. El astillero público posee en cada una de sus factorías unas instalaciones llamadas LBTS (*Land Based Test Site*), las cuales son utilizadas para integrar los diferentes sistemas que posee cada buque, y replican la realidad de todos los sistemas conectados a bordo en tierra. La disponibilidad de este tipo de instalaciones es de gran ayuda a la hora de poder entrenar nuestro sistema de ciberdefensa, ya que este es capaz de descubrir en el proceso las interacciones y parámetros normales de funcionamiento de todos los elementos conectados del buque. Esta base de conocimiento, una vez adquirida, formará parte de la base de datos de conocimiento necesaria para un correcto desempeño de la función de ciberdefensa a bordo de

cada buque. En el trabajo se incluye así mismo una planificación del tiempo necesario para llevar a cabo dicho entreno, así como el resto de pasos antes de tener el sistema totalmente operativo.

7. Conclusiones

El presente trabajo presenta una propuesta de desarrollo de un sistema de ciberdefensa aplicable a buques de la Armada. No obstante, el sistema en sí, es una parte de lo necesario para conseguir una protección más amplia. Es igualmente necesaria la concienciación y formación del personal que opera los buques, para interiorizar las políticas implícitas que permitan reducir los riesgos de ciberataques. De igual manera, la configuración, operación, sostenimiento y explotación de estos sistemas, requerirá de personal especializado, medios y financiación adecuada a lo largo del tiempo, por lo que se deberían asegurar estos tres elementos para conseguir la más amplia protección posible en los buques de la Armada de manera continuada en el tiempo.

Referencias

[1] Jefe del Estado Mayor de la Defensa (JEMAD) (2011). Concepto de Ciberdefensa Militar.

[2] Centro Criptológico Nacional (2020), CCN-STIC-301 Medidas de Seguridad de las TIC a implementar en sistemas clasificados.

[3] Centro Criptológico Nacional (julio 2012), CCN-STIC-302 Interconexión de CIS.

[4] Centro Criptológico Nacional (enero 2009), CCN-STIC-303 Inspección STIC.

[5] Centro Criptológico Nacional (enero 2022), «Esquema Nacional de Seguridad». [En línea]. Disponible: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1003.

Diseño de un sistema de ciberseguridad aplicable a un buque de la Armada

Autor: Miguel Carrasco Sandino
Director/es: Miguel Rodelgo Lacruz

Universidad de Vigo

Introducción

La creciente automatización de los sistemas a bordo de los buques así como la adopción de soluciones tecnológicas de última generación suponen un riesgo frente a ciber ataques, que actualmente no tiene mitigación. Es por esto que los últimos buques han de poseer cierto grado de defensa en este aspecto y se hace mandatorio la instalación de sistemas de ciber defensa a bordo. El presente trabajo describe una solución de diseño para poder integrar un sistema de ciber defensa en los sistemas de un buque tipo, así como el procedimiento para poder dimensionar de una manera los componentes del mismo.

Metodología

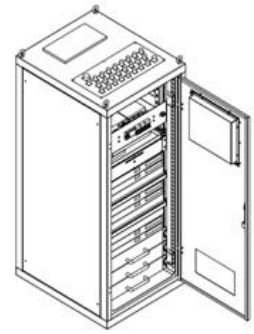
La metodología propuesta para este trabajo se lista a continuación:

- Gestión y desarrollo del programa: Ingeniería de sistemas.
- Caracterización del sistema a defender.
- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT.
- Herramienta de análisis de riesgos: PILAR.
- Normativa de aplicación: Guías CCN-STIC, Esquema Nacional de Seguridad (ENS).

La aplicación de estas diferentes metodologías, junto con la generación de unos requisitos consistentes basados en las necesidades que el sistema debe cumplir, son la base de partida del trabajo.

Todos estos pasos se han llevado a cabo sin perder de vista que las instalaciones a bordo de los buques poseen cierto grado de clasificación en función de la información que manejen, y por lo tanto, es de aplicación cierta normativa que no se puede obviar en el diseño de un sistema que supervise todos los sistemas conectados a bordo

Resultados



Como resultado del trabajo, se ofrece una configuración tanto hardware como software válida para la instalación a bordo de un buque, así como el procedimiento necesario para entrenar el sistema de ciberdefensa para cada tipo de buque. Se incluye también una planificación estimada con la duración de cada proceso.

Conclusiones

El presente trabajo presenta una propuesta de desarrollo de un sistema de ciberdefensa aplicable a buques de la Armada.

No obstante, el sistema en sí, es una parte de lo necesario para conseguir una protección más amplia. Es igualmente necesaria la concienciación y formación del personal que opera los buques, para interiorizar las políticas implícitas que permitan reducir los riesgos de ciberataques.

De igual manera, la configuración, operación, sostenimiento y explotación de estos sistemas, requerirá de personal especializado, medios y financiación adecuada a lo largo del tiempo, por lo que se deberían asegurar estos tres elementos para conseguir la más amplia protección posible en los buques de la Armada de manera continuada en el tiempo.

Agradecimientos

Agradezco a mi familia, compañeros, mandos y mi tutor por haberme permitido llevar este trabajo a buen puerto.

Técnicas criptográficas ligeras para dispositivos IOT

Autor: Gordillo Vega, Emilio José (egorveg@ea.mde.es; ejgorveg@gmail.com)
Directores: Vales Alonso, Javier (Javier.vales@upct.es)
y Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – El IOT abre un nuevo paradigma en la sociedad del futuro en el que todo tenderá a estar interconectado, se estima que se superen los 50.000 millones de elementos conectados a final de esta década.

Con el avance técnico, la interacción de las personas y los sistemas de información, las redes, sensores, sistemas de comunicación y computadoras han disminuido de tamaño, aumentado su capacidad de cálculo y se han abaratado, de forma que podemos encontrar estos dispositivos en cualquier lugar, electrodoméstico o, en general, *cosa*, ya que es posible encontrarlo en la ropa o, incluso, en el propio cuerpo humano.

No obstante, la información que contienen debe protegerse y una forma de hacerlo es con algoritmos criptográficos. Estos algoritmos se utilizan diariamente para proteger transacciones de Internet, y ofrecen una manera de verificar el origen de los datos y de evitar que se intercepte la información que contienen, con un alto nivel de confianza.

Sin embargo, el uso de técnicas criptográficas con dispositivos IOT, al tener una baja potencia de cómputo, no pueden realizarse con métodos complejos y se deben utilizar algoritmos de criptografía ligera, que permitan un nivel de seguridad aceptable para este tipo de dispositivos.

Este trabajo expondrá algoritmos ligeros de cifrado para dispositivos IOT probando que son seguros y que deben ser introducidos en estos dispositivos para que la información que contienen no esté expuesta. Estas técnicas dependerán del software embebido en cada dispositivo y se deberá aplicar un tipo de criptografía adaptada a cada clase.

1. Introducción

1.1. El Internet de las Cosas

El Internet de las Cosas o IoT (proviene de *Internet of the Things*) consiste en la interconexión de objetos de uso cotidiano con otros de su alrededor.

El IoT tiene enormes ventajas, pero es esencial proteger esos dispositivos de los ataques de aquellas personas que quieren acceder a ellos. El uso de la criptografía ayuda a proteger estos dispositivos y su autenticación, y proporciona una seguridad sencilla y sólida con la que podemos mantener la confidencialidad e integridad de los datos que contienen en su interior.

No obstante, el uso de técnicas criptográficas plantea diversos retos. Uno de ellos es que los algoritmos criptográficos que se emplean para cifrar o descifrar las transmisiones requieren muchos recursos informáticos, lo que supone una carga adicional para este tipo de sistemas, que son, por la propia naturaleza del IoT, extremadamente limitados.

A menudo existe un compromiso entre el método de criptografía utilizado y la seguridad general del dispositivo. Para los dispositivos IoT que no tienen limitaciones de Hardware y Software, es posible aplicar la llamada *criptografía convencional*, pero en la mayoría de los casos por la propia naturaleza del dispositivo esto no es posible, y hay que recurrir a la *criptografía ligera*.

1.2. Criptografía

La criptografía la podemos dividir en criptografía clásica, moderna y ligera.

La criptografía clásica la componen son los sistemas de cifrado anteriores a la II Guerra Mundial y se corresponden a una época anterior al nacimiento de las computadoras.

La criptografía moderna supuso una evolución con la aparición de las primeras computadoras ya que se contaba con tres factores que no se tenían hasta el momento, velocidad de cálculo, avance de las matemáticas y nuevas necesidades de seguridad.

Nacieron nuevos y complejos sistemas criptográficos, que según el tratamiento del mensaje:

- Cifrado en bloque: El cifrado se realiza en grupos de bits de longitud fija, llamados bloques. (DES, AES, IDEA y TWOFISH)
- Cifrado en flujo: El cifrado se realiza convirtiendo el texto claro en texto cifrado bit a bit. (RC4, SEAL y A5)

Además, según el tipo de clave utilizada para el cifrado, se clasifican en:

- Criptografía simétrica. Los que los procesos de cifrado y descifrado son llevados a cabo por una única clave.
- Criptografía asimétrica. Los procesos de cifrado y descifrado son llevados a cabo por dos claves distintas y complementarias. (RSA y Diffie-Hellman)
- Funciones Hash: Tipo especial de criptosistemas que no utilizan el concepto de clave (MD5 y la familia SHA).

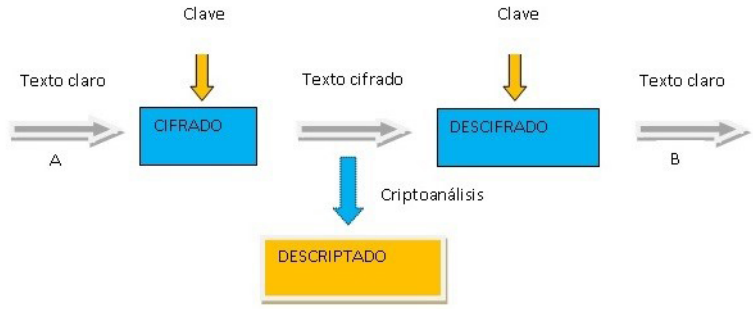


Figura 1. Proceso de cifra de un mensaje

La Criptografía ligera proporciona una arquitectura más escalable y canalizada. Requieren las puertas equivalentes mínimas normalmente por debajo de 2000 GE implementables en circuitos más pequeños y con requisitos de potencia mínimos.

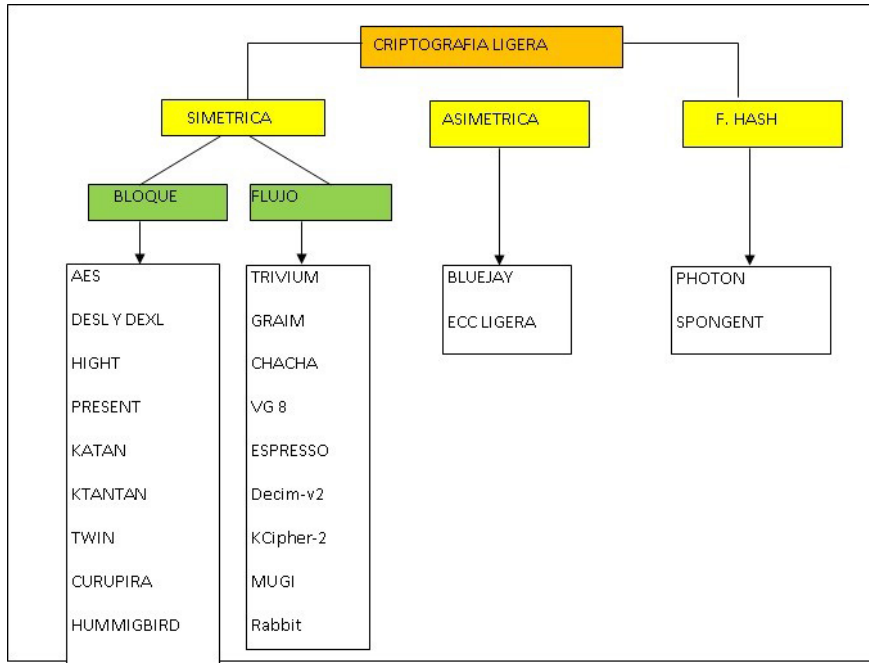


Figura 2. Algoritmos criptografía ligera

1.3. Ataques criptográficos

Los ataques buscan encontrar la clave utilizada en el proceso de cifrado y descifrado. Cada ataque tiene un método para descubrirla, los principales son:

- Ataque de búsqueda exhaustiva o de fuerza bruta
- Criptoanálisis diferencial/lineal
- Criptoanálisis integral
- Ataque algebraico/Ataque cubo
- Ataque Meet-in-the-middle/Biclique
- Ataque de clave relacionada
- Ataque de canal lateral/Ataque de fallos diferenciales
- Ataque de correlación
- Ataque distintivo
- Ataque Chosen-IV
- Ataque de deslizamiento
- Ataque de compensación de tiempo y memoria
- Ataque de suposición
- Ataques de rebote y super-sbox

2. Desarrollo

Se tratan tres casos en los que se intentará demostrar que la criptografía ligera es útil para garantizar la información transmitida por los dispositivos IoT.

2.1. RFID

RFID utiliza las ondas de radio para comunicarse con un microchip, que puede estar montado sobre gran cantidad de soportes (RFID puede incorporarse a un producto, animal o persona).

Figura 3. Protocolo RFID

Las etiquetas RFID han abierto la puerta a múltiples posibilidades y cada día surgen nuevas aplicaciones que las contemplan. En general, podemos emplear esta tecnología sobre cualquier aplicación de identificación en el sector logístico, cadena de suministro, producción, etc.

Es imprescindible que las etiquetas solamente revelen su identidad a los lectores de RFID autorizados.

El protocolo de autenticación SASI demuestra que la criptografía ligera o ultraligera es útil para garantizar la información transmitida por los dispositivos IoT

2.2. WSN

Está formada de pequeños dispositivos autónomos o nodos, con recursos limitados como baja potencia computacional, transmisión de datos limitada y restricciones de potencia, y que utilizan sensores para monitorear condiciones físicas o ambientales, procesan estos datos y los envían por señales de radio.

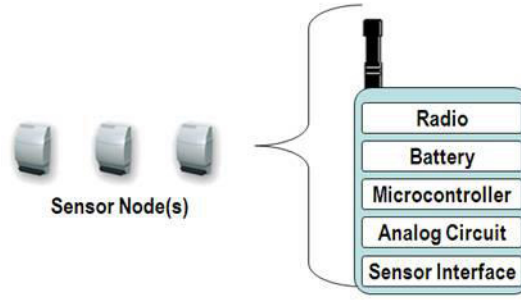


Figura 4. Componentes de un sensor

Las aplicaciones más comunes de las WSN son aplicaciones militares, monitorización ambiental en lugares cerrados y al aire libre, agricultura y monitorización de la salud, pero para las comunicaciones se utilizan protocolos de comunicación inalámbrica como Wifi, Zigbee o Bluetooth. Las redes de sensores están expuestas a múltiples ataques, pero debemos proteger la autentificación y el envío de datos, que debe ser confidencial.

No se han encontrado algoritmos de criptografía ligera para WSN, no obstante, algunos autores han demostrado que usar criptografía de clave pública en WSN se puede considerar una realidad y no un concepto teórico, debido a que la ECC aporta mejor rendimiento en cómputo y almacenamiento de claves que otros criptosistemas como el RSA.

2.3. Smart Cards

Una Smart Card incorpora un chip electrónico y puede contener datos secretos, certificados digitales o claves privadas asociadas a ellos y lleva a cabo por sí misma sus propias operaciones criptográficas no necesitando una batería.

Las tarjetas inteligentes se comunican con los lectores mediante contacto físico directo o mediante RFID u otro estándar de conectividad inalámbrica de corto alcance.

Figura 5. Smart Card

Iniciar sesión con una Smart Card ofrece una forma fuerte de autenticación porque usa identificación basada en criptografía y prueba de posesión (PIN), no obstante, y aunque son ampliamente utilizadas, existen varias formas en que las Smart Cards pueden ser atacadas, uno de estos ataques es el DPA, pero existen otros como el ataque interno, Man-in-the-middle, ataque de repetición, ataque de suplantación de identidad, de denegación de servicio y el ataque de robo de verificación

ECC se considera el mejor para la autenticación de tarjetas inteligentes, ya que el modelado de ECC dificulta al extraer la información. Los cifrados simétricos ligeros como AES, TRIPLE DES y PRESENT se aplican para el cifrado de datos de las tarjetas inteligentes y son eficientes, pero también se pueden utilizar cifrados de flujo para evitar el rellenado de ceros de los bloques.

3. Resultados y discusión

Ejemplo práctico 1. Caso de estudio de un algoritmo criptográfico a utilizar en una sonoboya.

Las sonoboyas son del tipo AN/SSO-47 y realizando una aproximación razonable, el tiempo mínimo entre pulsos podemos considerarlo de 10,00 kHz. Aplicando el Teorema de muestreo de Nyquist-Shannon tendremos que tomar una tasa de muestreo de 20,00kHz y a 16 bits por muestra tendremos 320.000 bits, es decir 313,42kB. Asumiendo una compresión razonable de 1:4, el *throughput* o tasa de transferencia es de 78,35 kB/s.

No podemos aplicar ninguno con tasa inferior a los 78,35 kB/s con lo podremos implementar los cifrados AES, HIGHT, PRESENT, PRINCE Y TWINE.

La sonoboya tiene un consumo activo significativo, pero se quiere resguardar su batería el máximo tiempo. Dado que el número de puertas equivalentes es proporcional al consumo y queremos minimizarlo, escogeremos el algoritmo que menos puertas lógicas presente, que en este caso es PRESENT que tiene 1570 GE para una clave de 80 bits o 1884 GE para una clave de 128 bits y consumo de 2,35µw.

Figura 6. Sonoboya AN/SSO-47 (tomada de internet)

Ejemplo práctico 2. Marcapasos SJM

En 2017 se puso en riesgo a casi medio millón de personas que portaban un marcapasos *St Jude Medical*, debido a que la información que transmitía no poseía ningún tipo de cifrado. La vulnerabilidad permitía que un usuario no autorizado, pudiera hackearlos de forma remota.

Figura 7. Marcapasos St Jude Medical (tomada de internet)

La propuesta para este caso de estudio es que necesitamos un sistema de cifrado asimétrico para establecer la clave de sesión con un método de criptográfico ligero. De estos trabajos se presentaron dos, BLUEJAY y ECC LIGERA.

BLUEJAY es adecuado para plataformas ultraligeras (un total de 2000-3000 GE), además romperlo es difícil y está pensado para la autenticación en RFID por lo cual se considera más adecuado que la ECC LIGERA, que, aunque es más eficiente, requiere más de 10.000 GE y esto incrementaría el consumo del marcapasos que, como se ha comentado, es un requerimiento esencial en este dispositivo.

Ejemplo práctico 3. Hidrófono

Los hidrófonos son dispositivos que captan el sonido bajo el agua y lo convierten en señales de audio para posteriormente convertir estas señales en señales eléctricas.

Tiene una frecuencia de hasta 180kHz lo que lleva a una tasa de muestreo de 360kHz muestras. Si consideramos 16 bits por muestra, supondría 5.760 kB. Con una compresión eficaz de un 25 %, se tendría una tasa de datos significativa, en el entorno de los 1.440 kB = 1,4 MB.

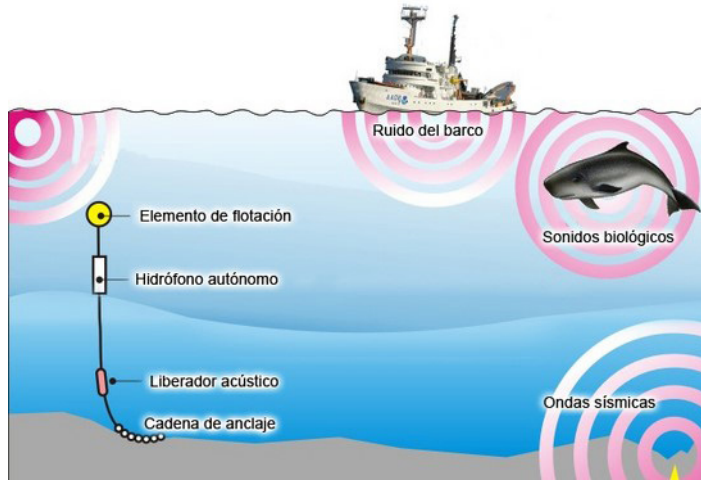


Figura 8. Esquema de un hidrófono

Utilizando la tabla que mostraba el rendimiento de los distintos cifrados, tenemos que aplicar el cifrado PRINCE que es indicado para tasas superiores a 533,3 kB/s.

El consumo es algo mayor con 3.491 GE pero cuenta con un buen nivel de seguridad.

4. Conclusiones

Los dispositivos IoT están a la orden del día y seguirán en continuo crecimiento, vivimos en un mundo conectado a Internet y es evidente que se seguirán introduciendo dispositivos de este tipo en el futuro.

Estos dispositivos envían y reciben datos de Internet, y la seguridad de estos datos debe garantizarse con objeto de que no caigan en manos de ciberdelincuentes.

La criptografía es un método realista y de bajo coste, que puede ayudar a garantizar esta seguridad que necesitamos, pero al ser dispositivos con recursos limitados, ya que no poseen ni memoria, ni CPU ni energía, es la llamada *criptografía ligera* la que puede dar respuesta a las necesidades

crecientes de seguridad en dispositivos restringidos, porque no es posible aplicar los algoritmos más robustos de la criptografía convencional al consumir demasiados recursos.

Estos algoritmos ligeros están avanzando mucho, hay interés por estandarizarlos y frecuentemente surgen nuevas publicaciones. De hecho, la *criptografía ligera* está sustituyendo a los algoritmos de criptografía simétrica que son los que más se utilizan en criptografía.

Los algoritmos ligeros no son resistentes a todos los ataques criptográficos, pero ya que es imposible implementar una criptografía convencional, constituyen muchas veces la única forma de que estos dispositivos dispongan de seguridad.

El término *ligero* abarca demasiados dispositivos y debería de existir una división que podíamos denominar criptografía ultraligera y criptografía ligera para categorizarlos mejor.

En particular, y aparte del consumo de energía, esta división es necesaria debido a los diferentes niveles de seguridad que exigen estos algoritmos. Hay que elegir bien estos algoritmos para adecuar el algoritmo utilizado al dispositivo.

Referencias

[1] Thakor, V.A (et al.) (2019) «Cryptography Algorithms for Resource-Constrained IoT Devices», Digital Object Identifier.

[2] Saddkhan, S.B. y Salman, A.O. (2018) «A Survey of Light-weight-Cryptography. Status and Future Challenges», International Conference on Advances in Sustainable Engineering and Aplications (ICASEA).

[3] Philip, M.A., (2017), «A Survey On Lightweight Ciphers For IoT Devices», IEEE International Conference on Technological Advance-ments in Power and Energy (TAP Energy).

[4] Mobahat, H., 2010, «Authentication and Lightweight Cryptog-raphy in Low Cost RFID», 2.ª International Conference on Software Technology and Engineering (ICSTE).

[5] Gunathilake N. A. (et al.) (2019). «Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications» IEEE 5th World Forum on Internet of Things (WF-IoT).

[6] Rodríguez Flores L. A., (2014). «Arquitectura hardware compacta para criptografía ligera de llave pública» Grado Maestría en Ciencias en la especialidad de Ciencias Computacionales.

[7] Lucena López M. J. «Criptografía y seguridad en computadores» 4.ª Edición, Version 0.6.2

[8] García Flores L. A., (2014). «Tesis en Maestría en ciencias en la especialidad de ciencias computacionales» Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE).

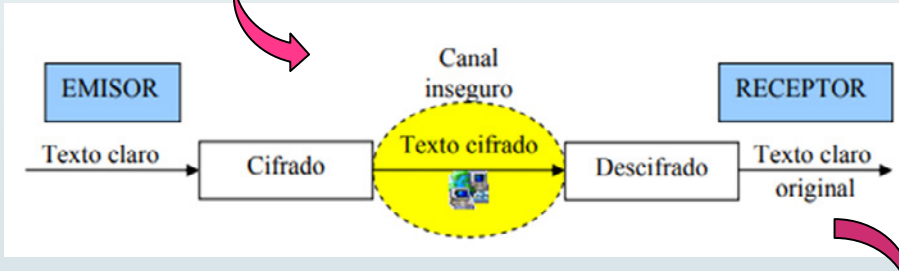
Técnicas criptográficas ligeras para dispositivos IOT

Autor: Emilio José Gordillo Vega
Universidad de Vigo
Directores: Javier Vales Alonso y Milagros Fernández Gavilanes

Introducción

El IOT (Internet Of Things) abre un nuevo paradigma en la sociedad del futuro en el que todo tenderá a estar interconectado,

La información que contienen estos dispositivos debe protegerse y una forma de hacerlo es con **algoritmos criptográficos.**



Muchos dispositivos IOT apenas poseen memoria, ni CPU, ni energía, pero necesitan un mínimo de seguridad en la transmisión de los datos, la **criptografía ligera** puede ofrecer soluciones de seguridad para estos dispositivos.

Análisis de seguridad en las Smart Cities

Autor: Gutiérrez Hernández, Andrés Antonio
(andres.antonio.gutierrez@alumnos.uvigo.es)
Directores: Vales Alonso, Javier (Javier.vales@upct.es)
y Rodríguez Martínez, Francisco Javier (franjrm@uvigo.es)

Resumen – Las ciudades son una de las características más identificables de la especie humana, las hay en todas las culturas y representan un poderoso indicador de crecimiento económico y social. Hoy en día la mayor parte de la población se desplaza a áreas urbanas para la mejora de su calidad de vida.

El propósito de este trabajo es el de ofrecer mediante un ejercicio teórico de análisis de riesgos una visión de la seguridad en la ciudad inteligente.

Una ciudad inteligente es aquella que se encuentra en un proceso de mejora continua, especialmente TIC, para mejorar su sostenibilidad, calidad de vida, eficiencia de servicios y competitividad.

En ese sentido llama la atención la incorporación de nuevas tecnologías como Big Data, Data Mining, el uso de la nube y aquellas relacionadas con el Internet de las Cosas.

Durante el análisis se identifican los servicios que describen con más exactitud a la mayor parte de las ciudades inteligentes de hoy en día en España, como la gestión de residuos o control avanzado de tráfico. Se identifican los activos más importantes de estos servicios. Posteriormente se analizan las ciberamenazas más comunes. Finalmente se correlaciona amenaza y activos para obtener un mapa de calor de riesgos.

Como resultado se observa que aumentan algo nuevos entornos de riesgos como contadores inteligentes y dispositivos IoT. Sin embargo, lo más llamativo es cómo aumenta la dependencia con la infraestructura TIC tradicional, el aumento de puntos de acceso a internet y las relaciones con terceros, especialmente por la nube.

Palabras clave – Ciudad, Inteligente, Seguridad, Riesgos, Análisis

1. Introducción

Las ciudades son una de las características más identificables de la especie humana, las hay en todas las culturas y representan un poderoso indicador de crecimiento económico y social. No obstante, el funcionamiento de las ciudades dista de ser perfecto, las agrupaciones de población exigen una demanda muy alta de recursos, energía, agua y de servicios como educación, seguridad o sanidad entre otros. Las ciudades son un agente importante en el calentamiento global por sus emisiones y consumo. Además, el crecimiento se prevé que seguirá incrementándose en el tiempo y para 2050 se estima que el 70 % de la población vivirá en grandes ciudades. [1] La unión de estas dos situaciones ha creado el concepto conocido como ciudades inteligentes o Smart Cities. Este comprende la necesidad de propiciar un desarrollo sostenible y eficiente de las ciudades junto a la necesidad de transformar digitalmente el funcionamiento de estas. Lo que nos indica que el concepto de ciudad inteligente va más allá de digitalizar una ciudad, sino que involucra también una reestructuración del funcionamiento de la misma, incluido una orientación sostenible y de conciencia con el medio ambiente. La ciudad inteligente es un objetivo complejo, que implica líneas estratégicas, tácticas y operativas sostenidas en el tiempo. El propósito de este trabajo es el de ofrecer mediante un ejercicio teórico de análisis de riesgos una visión de la seguridad en la ciudad inteligente. Al realizarlo de esta forma se ofrece una forma práctica y con perspectiva de lo que un responsable de seguridad debe tener en cuenta cuando se trate con dichas ciudades.

2. Desarrollo

2.1. Recreación de ciudad inteligente e identificación de activos

En el trabajo se ha intentado recrear una ciudad que se aproxima a la actualidad española en este aspecto. A título informativo se han definido algunos datos generales de la ciudad que podrían ser útiles en la valoración del riesgo.

Algunos datos de ciudad modelo:

- País: España
- Número de habitantes: 300.000
- Localización y medio ambiente: Se encuentra situada en la costa, en la desembocadura de un río de poco caudal. El cambio de estaciones suele ser suave pero los últimos años se ha incrementado las temperaturas en verano y el frío en invierno. Los últimos años ha habido nevadas.
- Cultura, historia y aspectos relevantes: Ciudad de origen medieval. Se dispone de mucho patrimonio histórico en forma de fortalezas y templos religiosos.

- Otros: La ciudad tiene un centro de protección de datos en el edificio del ayuntamiento. Hay otro pequeño centro de datos en la comisaría de policía local. Se tienen medidas estándar de gestión y de seguridad TIC en ambos sitios.

Si se unen los servicios de ciudad inteligente más comunes de las ciudades españolas en la actualidad y los extraídos de procesos de innovación que se esperan se implanten en un corto plazo, se puede tener un caso de uso realista para realizar el análisis de riesgos. Hemos añadido por interés académico el seguimiento de brigadas, para que haya servicios de todos los ámbitos definidos por él. Estándar UNE.

La ciudad a analizar tendrá por tanto estos servicios, que serán los considerados para hacer el análisis de riesgo. Puede que la ciudad disponga de otros servicios, pero en la metodología del análisis se escoge aquellos que se consideran apropiados. Por ejemplo, puede que hubiera un servicio de bicicletas inteligente pero no se considera relevante por su madurez y alcance dentro de la ciudad.

N.º	Servicios	Dominio
1	Página web corporativa	Gobernanza
2	Portal de transparencia	Gobernanza
3	Sede electrónica	Gobernanza
4	Redes sociales	Gobernanza
5	Aplicaciones móviles de información y atención al ciudadano	Gobernanza
6	Consumo y calidad del agua	Entorno
7	Monitorización del consumo energético en edificios privados y hogares	Entorno
8	Recogida de residuos	Entorno
9	Control de tráfico	Movilidad
10	Gestión de puntos de recarga de vehículos eléctricos	Movilidad
11	Medición medioambiental: calidad del aire	Entorno
12	Seguimiento y actividad de efectivos y brigadas	Bienestar

Tabla 1. Servicios seleccionados para su análisis en la ciudad inteligente.

2.2. Identificación de amenazas

Tras el anterior análisis se han seleccionado diez vulnerabilidades en base al estado actual del ciberespacio en relación a amenazas. El criterio para su selección ha sido su variedad respecto a tipos de MAGERIT [2], la probabilidad de acuerdo a los informes de ciberamenazas y su relación con las tecnologías de la ciudad inteligente. También se ha seleccionado la amenaza de nevadas, dado que como se dice en las condiciones de contorno son habituales los últimos años.

Se les ha asignado una probabilidad en este caso en función de la accesibilidad que pueda tener un actor en el ataque, en cuanto al impacto

se considera el daño que puede tener un activo medio en el caso de materializarse dicha amenaza.

N.º	Amenaza	Aproximación MAGERIT	Probabilidad	Impacto
1	Ransomware	[A.29] Extorsión	MEDIA	ALTO
2	Cryptojacking	[A.7] Uso no previsto	MEDIA	MEDIO
3	Spearfishing	[A.30] Ingeniería social	MEDIA	MEDIO
4	Robo de información	[A.19] Divulgación de la información	BAJO	MEDIO
5	DDoS	[A.24] Denegación de servicio	MEDIA	ALTA
6	Nevadas	[I.7] Condiciones inadecuadas de temperatura y húmedad	BAJA	MEDIO
7	Campaña de noticias falsas	[E.15] Alteración accidental de la información	BAJA	BAJA
8	Error de configuración	[E.4] Errores de configuración	ALTA	BAJO
9	Covid-19	[E.28] Indisponibilidad del personal	BAJA	MEDIO
10	Inundación	[N.2] Daños por agua	BAJA	ALTO

Tabla 2. Selección de amenazas y ponderación de impacto y probabilidad.

3. Resultados y discusión

3.1. Resultados de análisis de riesgos

Como resultado de la ponderación de la criticidad de los servicios escogidos en contraposición a la probabilidad de que una amenaza se materialice y el impacto que puede causar sobre ese servicio se obtiene un mapa de calor con un valor para cada riesgo encontrado:

Servicios y amenazas analizados.	Fake news	Robo de información	Nevadas	Covid-19	Error de configuración	Inundación	Cryptojacking	Spearfishing	Ransomware	DDoS
Aplicaciones móviles de información y atención al ciudadano	1	2	2	2	3	3	4	4	6	6
Consumo y calidad del agua	2	4	4	4	6	6	8	8	12	12
Control de tráfico	2	4	4	4	6	6	8	8	12	12
Gestión de puntos de recarga de vehículos eléctricos	1	2	2	2	3	3	4	4	6	6
Medición medioambiental: Calidad del aire	1	2	2	2	3	3	4	4	6	6
Monitorización del consumo energético en edificios privados y hogares	1	2	2	2	3	3	4	4	6	6
Página web corporativa	2	4	4	4	6	6	8	8	12	12
Portal de transparencia	1	2	2	2	3	3	4	4	6	6
Recogida de residuos	2	4	4	4	6	6	8	8	12	12
Redes sociales	2	4	4	4	6	6	8	8	12	12
Sede electrónica	3	6	6	6	6	9	12	12	18	18
Seguimiento y actividad de efectivos y brigadas	3	6	6	6	6	9	12	12	18	18

Tabla 3. Mapa de riesgos a nivel de servicios Smart por amenaza analizados.

3. Conclusiones de análisis de riesgos

Para el caso particular de la ciudad ficticia analizada se puede extraer las siguientes conclusiones:

De la propagación del valor de criticidad de los activos que componen los servicios:

- Los activos más importantes transmiten su criticidad a los sistemas sobre los que se soportan. Esto se ve reflejado en cómo el valor de riesgo de los dos sitios, el CPD del ayuntamiento y de la comisaría, junto a elementos transversales como la electrónica de red aumentan considerablemente.
- La ciudad inteligente fomenta la participación de diferentes organizaciones y es importante gestionarlas correctamente.
- También en ese sentido se observa un aumento exponencial de conexiones a proveedores de internet para satisfacer las comunicaciones de todos los sensores IoT. En el caso solo suponemos que se contratan servicios de conexión (LTE, LPWAN, etc.).
- Finalmente, sorprende que para el empleo de otros sistemas aparezcan servicios SaaS como por ejemplo las tiendas de aplicaciones móviles.
- Las aplicaciones suelen dividirse en tres partes, un *back-end* en el que se procesa la información, un *front-end* desde el que accede el usuario y una parte novedosa es que ahora se tiene una zona de captación de la información. De entre esas tres, no obstante, la criticidad se sigue acumulando en la zona del *back-end*.
- Las aplicaciones de *big data* en ese sentido no cambian mucho a nivel de composición con respecto a sus contrapartidas tradicionales. Aunque sean bases de datos noSQL siguen siendo una fuente de información (crítica o no según su aplicación) y el proceso de tratamiento no reporta muchas diferencias en términos de seguridad.

De los riesgos encontrados:

- Pese a la aparición de las redes de dispositivos IoT para la captación de la información, el mayor riesgo se sigue acumulando en aplicaciones de negocio críticas.
- Se observa que las infraestructuras que afectan a tráfico, canalización de agua y aprovisionamiento de energía tienen una importancia alta para una ciudad y por tanto es recomendable plantear medidas de seguridad.
- Otras aplicaciones, aunque aportan valor añadido no comportan tanto riesgo. En esta categoría podríamos incluir sobre todo las de tipo informativo para el ciudadano: portales de transparencia, información meteorología o de otro tipo sobre la ciudad.

4. Conclusiones

Tras la realización de la investigación del concepto de ciudad inteligente, la evolución normativa, las tecnologías empleadas y analizar la seguridad siguiendo el proceso de un análisis de riesgos se puede extraer lo siguiente:

- Actualmente todavía no se ha llegado a una implantación suficiente, en España, como para decirse que la mayor parte de las ciudades se consideran inteligentes. Esto parece así con los municipios de mayor tamaño, pero no es una línea general.
- Aunque no se hayan implantado muchos servicios de ciudad inteligente, no es necesariamente contraproducente. Del análisis se puede ver que los riesgos TIC de las organizaciones aumentan al acumularse el número de aplicaciones y servicios que se utilizan. Luego es mejor retrasar la implantación para que se pueda llevar a cabo con la seguridad suficiente.
- Pese a que el concepto de ciudad inteligente está muy extendido y hay varios estándares. En lo referente a seguridad de la información e implantación de una arquitectura todavía hay margen de trabajo. Especialmente para establecer un marco para implantar sistemas en el que diferentes entidades puedan participar, es decir, que entidades privadas y públicas puedan coordinar sus aplicaciones TIC dentro de una arquitectura capaz de balancear la seguridad y la funcionalidad.
- Que la irrupción de nuevos servicios que se construyen con nuevas tecnologías ofrece mayor valor, pero conllevan nuevos riesgos. No obstante, en general estos riesgos son similares a los ofrecidos por servicios TIC tradicionales y el valor añadido que se obtiene es superior.

4.1. Medidas que se pueden aplicar a una ciudad inteligente.

Tras la realización del análisis de riesgos se pueden aventurar una serie de medidas que reducirían los riesgos y mejorarían la seguridad.

Desde el punto de vista estratégico:

- Tal y como exige el ENS [3] y recoge el estándar ISO 27001 es necesario la elaboración de una política de seguridad que sea apoyada por la Dirección. Esto ofrece una visión de trabajo que engloba a la seguridad y marca un compromiso de la organización con ella.
- El empleo de un punto de vista de seguridad holístico se hace más necesario. Esto significa incluir el punto de vista de seguridad a todos los niveles del ciclo de vida de los sistemas TIC. Es especialmente importante en el diseño de la arquitectura y en la compra o desarrollo de nuevos sistemas.

Desde el punto de vista táctico:

- Se deben incluir criterios de calidad y seguridad en la compra y puesta en funcionamiento de dispositivos IoT. Tal y como se recoge en los informes del CCN, los ataques a la cadena de suministro están en aumento. Evitar comprar elementos inseguros reducirá incidentes de seguridad en el futuro.
- Establecer principios de seguridad en las relaciones con terceros. Asegurar que los SLAs y acuerdos contractuales con servicios en la nube o con proveedores de servicios públicos incluyen apartados relacionados con la seguridad de la información que satisfagan los requisitos de seguridad de la ciudad.
- Elaborar campañas de concienciación y servicios de soporte a incidentes. Pese a la formación actual, que ya incluye seguridad de la información, los incidentes debido a ingeniería social y correos siguen en aumento. Es necesario seguir concienciando en las organizaciones de la ciudad inteligente y a los ciudadanos que hagan uso de ellas.

Desde el punto de vista técnico y operativo:

- Establecer sistemas de recuperación de la información que contemplen en diferentes ubicaciones los datos y los sistemas. Además, asegurar que parte de estos se almacenan de forma aislada para evitar que se contaminen en caso de que se encuentren con amenazas del tipo ransomware o malware.
- Debido a que muchas de las tecnologías que se emplean se aprovechan de protocolos web y API de servicios es recomendable el uso de WAF y revisión de medidas de seguridad web, como las que se definen en OWASP para garantizar la seguridad de los puntos de entrada. Esto es también válido muchas veces para servicios en la nube.
- Procurar reducir la superficie de exposición de los sistemas de la ciudad unificando sitios sobre los que se gestionan los sistemas TIC. Por el contrario, dentro de cada sitio segmentar los sistemas en función de sus necesidades para equilibrar las necesidades de seguridad.
- Usar arquitecturas de IoT que permitan que los dispositivos se conecten con un conmutador puede facilitar su protección, reduciendo la ventana de ataque de sujetos que operan mediante internet. La probabilidad de que los ciudadanos o habitantes comprometan los dispositivos es menor que la de que sean fuerzas ajenas a la ciudad como entidades con objetivos políticos, delincuentes y demás.
- El uso de sistemas IoT que sean capaces de actuar sobre infraestructura crítica de la ciudad puede considerarse un riesgo. En caso

de fallo estos sistemas deben estar pensados para poder seguir funcionando, aunque se produzca una degradación del servicio. Un ejemplo es la prioridad de la señalética en caso de corte de luz de un semáforo.

- Se deben disponer de sistemas para la actualización de los dispositivos IoT de forma automática. Aunque individualmente no suponen un riesgo alto para la ciudad, las vulnerabilidades de estos dispositivos pueden suponer un riesgo en su conjunto sobre todo si con el paso del tiempo no son actualizados.
- En algunas ocasiones puede ser útil utilizar la tecnología *blockchain* aplicada a los dispositivos sensores / actuadores. Dado que pueden necesitar de bases de datos que ayuden para un pequeño análisis que se pueda realizar en los capilares es posible que usar una base de datos distribuida sea una solución. Esto permitiría seguir operando en conjunto en caso de denegación de conexión y caída de la base de datos central.
- Intentar en la medida de lo posible mantener los dispositivos fuera del alcance de los viandantes o que sean de fácil acceso para personal no autorizado. Se pueden utilizar protecciones, vallas, recintos o colocarlos en altura.
- Una ciudad que dependa mucho de los sistemas TIC debe disponer de un sitio de respaldo. Valorar el uso de un sistema híbrido de nube y propietario puede ser útil.

Agradecimientos

Agradezco este proyecto a todas las personas que me han prestado apoyo, mi tutor Javier Vales Alonso y a mi familia que ha aguantado estoicamente este último año.

Referencias

[1] AENOR (2016). UNE 178201 Ciudades inteligentes. Definición atributos y requisitos.

[2] Ministerio de Hacienda y Administraciones Públicas (2012). MAGERIT versión 3.

[3] Gobierno de España (2010). Real Decreto 3/2010 Esquema Nacional de Seguridad.

Análisis de seguridad en las Smart Cities

Autor: Andrés Antonio Gutiérrez Hernández
Director/es: Javier Vales Alonso y Francisco Javier Rodríguez Martínez

Universidad de Vigo

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Gestión de proyectos de innovación tecnológica para la seguridad en el Ministerio del Interior

Autora: Machín Prieto, Rosalía (rmp@interior.es)
Director: Álvarez Sabucedo, Luis (lsabucedo@det.uvigo.es)

Resumen – El acceso a Fondos de financiación europeos por parte del Ministerio del Interior para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y demás organismos dependientes de la Secretaría de Estado de Seguridad (SES), supone apostar y participar en el desarrollo de nuevas tecnologías y sus aplicaciones con la finalidad de mejorar la función pública y mantener la seguridad de la ciudadanía española.

Dichas iniciativas europeas facilitan el acceso a importantes inversiones en investigación y nuevas tecnologías de información y comunicación claves, como son el 5G, el internet de las cosas (IoT), la inteligencia artificial (IA), la computación cuántica, el *blockchain* y la ciberseguridad, y en general toda la digitalización de datos, que, a corto y medio plazo, crecerá de forma exponencial.

Si bien las tecnologías y las nuevas identidades digitales generan oportunidades y beneficios para todos, a la inversa, plantean nuevas amenazas y riesgos. La mayoría de los delitos tienen un elemento digital, y para garantizar investigaciones exitosas y una prevención efectiva del delito, las unidades de investigación competentes tienen que mantenerse actualizadas.

El presente trabajo expone cómo los proyectos de financiación europeos permiten desarrollar nuevas tecnologías para adquirir métodos y capacidades cada vez más innovadores en la lucha contra los diferentes tipos de delincuencia y cómo, además, han surgido líneas de trabajo estratégicas en materia de seguridad tecnológica para España a través de los diferentes grupos de expertos, los consorcios de proyectos o las redes especializadas europeas.

Se pretende demostrar que la cooperación público-privada entre FCSE, industria y academia, es vital para garantizar el acceso al talento, al conocimiento, y a nuevos mercados nacionales e internacionales,

y de este modo abordar eficazmente los desafíos tecnológicos en seguridad (ciberdelito, el crimen organizado y el terrorismo).

La Comisión Europea respalda la importancia de reforzar dicha cooperación tecnológica a través de diferentes programas de financiación I+D+i, entre los que destacan Horizonte2020 (H2020), Horizonte Europa (HE) y el nuevo Programa Europa Digital (DEP).

Palabras clave – innovación tecnológica, sinergia, clúster, seguridad, amenaza, digital.

1. Introducción

La tecnología, la innovación y la digitalización son la base del nuevo orden global. No se puede negar que el cambio tecnológico ha llegado a todos los ámbitos de la sociedad, la economía y la política, generando una nueva dimensión en las relaciones internacionales y en el campo de la seguridad.

El conocimiento científico, el acceso a la tecnología, su desarrollo y regulación, se han convertido en elementos imprescindibles para los Estados y para sus sociedades. Las relaciones de poder ya no solo se basan en la excelencia tecnológica, la defensa y la seguridad, sino también en la necesidad de alcanzar la hegemonía en el ciberespacio o en construir nuevos espacios de datos.

Las nuevas revoluciones tecnológicas vinculadas con los sistemas de información y de comunicación (TIC), han generado nuevas áreas de colaboración y competición. La digitalización y la creación de redes globales para el intercambio de información fueron lideradas en un primer momento por Estados Unidos. La segunda fase, y en la que actualmente nos encontramos, basada en las redes 5G, el Internet de las Cosas (IoT), la tecnología cuántica y la inteligencia artificial (IA), se está desarrollando entre una aguerrida competición entre China y Estados Unidos.

El poder acceder a las primeras generaciones de nuevas tecnologías, integrar algunas de las tradicionales o diseñar y mantener las nuevas infraestructuras de las redes de datos, son aspectos críticos en los que se basa la *seguridad nacional* de las nuevas sociedades.

Es por ello que la Unión Europea está realizando grandes inversiones a través de programas de financiación europeos, entre los que se destacan en el presente trabajo *Horizonte Europa HE* (I+D+i) y *Programa Europa Digital DEP*. Se considera, que un mayor número de proyectos paneuropeos, en los que se ponen en común los recursos de todos los Estados miembros, ayudará a alcanzar economías suficientes para ser más competitivos en los mercados globales, y competir con los grandes gigantes tecnológicos. Esta es la apuesta que hace Europa para el 2030.

El análisis de *Big Data* y las técnicas de inferencia a través de procesos de *inteligencia artificial*, abren el campo para nuevos servicios, mucho más personalizados y también mucho más útiles en el ámbito de la Defensa y Seguridad. Se plantean importantes preocupaciones en cuanto a la privacidad del individuo y su autonomía individual. Muchos Estados buscan el equilibrio entre vigilancia y libertad, debido a la creciente tendencia de actividades delictivas relacionadas con el cibercrimen y el robo de identidades.

A tener en cuenta igualmente, que la *computación cuántica*, está destinada posiblemente, a convertirse en un importante elemento de cambio. Aquel Estado que desarrolle una computadora cuántica alcanzará

un estatus privilegiado, ya que conseguirá tener acceso a todas las redes, así como eludir sus sistemas de encriptación.

El equipamiento y los materiales adecuados a desarrollar por industrias estratégicas, son también elementos críticos en el ámbito de innovación tecnológica. La *fabricación aditiva* (impresión 3D), es posible que rediseñe las cadenas de suministro y a futuro, sustituya la fabricación convencional en importantes áreas. Los investigadores ya están trabajando en *impresión 4D*, procesos de nueva generación para productos que se modifiquen a sí mismos, respondiendo a cambios ambientales como el calor y la humedad.

En paralelo, las sociedades se enfrentan a problemáticas generadas en el campo de la seguridad por las nuevas tecnologías en su uso diario. La posibilidad de interaccionar con otras personas de todo el mundo y acceder a todo tipo de información, no solo ofrece ventajas para los ciudadanos. La sobreabundancia de información y las falsas propagandas con fines ilícitos (*fake news*) en el ciberespacio, pueden llegar a desacreditar personas o instituciones, incluso a desestabilizar a la población (*desinformación*).

El liderazgo tecnológico del sigo XXI ha sido asumido por el sector privado, ofreciendo nuevos servicios y bienes de consumo. La Industria de Defensa y Seguridad no ha sido financiada hasta el momento, en muchos casos, por los Estados en la medida que se debería, a través de programas militares o de seguridad interior. Pero sí, en el caso de Europa y concretamente de España, a través de los citados programas de financiación europeo I+D+i.

Se van a presentar algunos de los proyectos de innovación tecnológica y digital de los últimos años, cofinanciados por la UE (*STARLIGHT, CLOSEYE, BiObserver,* etc.), que ayudan a que los agentes españoles y europeos que velan por la seguridad de los ciudadanos (Fuerzas y Cuerpos de Seguridad, Guardias de Fronteras, Servicios de Control y Protección de Aduanas, etc.), se beneficien de nuevas herramientas para su trabajo operativo diario.

El principal objetivo del presente trabajo es ayudar al lector a entender cómo a través de programas de financiación europeos y nacionales de la Unión Europea (Horizonte Europa, Horizonte2020, Programa Europa Digital), y de la cooperación internacional, se facilita a las Fuerzas y Cuerpos de Seguridad del Estado (Ministerio del Interior) acceso a herramientas provenientes de la *investigación y la innovación que le ayuden a desempeñar su función esencial: El mantenimiento de la seguridad de los ciudadanos.*

2. Desarrollo

El presente trabajo pretende describir cómo la *investigación* y la *innovación tecnológica* en materia de seguridad contribuyen de forma estratégica a *definir políticas internacionales en materia TIC* de la UE y entre ellas la de España de la mano del Ministerio del Interior (Estrategia I+D+i Ministerio del Interior, Contribución al Espacio Seguro de datos europeo, etc.).

Igualmente se ha puesto énfasis en la definición de los principios orientadores europeos en materia TIC para la seguridad de sus Estados miembros, los que, junto con las tecnologías emergentes validadas en proyectos de corte europeo y tratadas en los diferentes grupos de expertos, han surgido líneas de trabajo en materia de tecnológica para España, como son:

- El apoyo por parte de España y el Ministerio del Interior para que Europa alcance su *autonomía estratégica* en el ámbito TIC.
- El impulso de la *cooperación internacional* a través de grupos de expertos, grupos de trabajo, alianzas tecnológicas, consorcios de proyectos europeos, etc., para definir la gobernanza de la tecnología en el campo de la seguridad.
- Entender cómo se facilita a través de programas de financiación europeos y nacionales (Horizonte Europa, Horizonte2020, Programa Europa Digital) *herramientas* provenientes de la *investigación* y la *innovación a los Cuerpos de Seguridad.*

Los últimos avances en materia de políticas de seguridad reflejan la situación cambiante de la UE, donde los Estados miembros se enfrentan a las grandes crisis que amenazan a las personas y a la sociedad. Las tecnologías innovadoras se utilizan cada vez más *para desempeñar actividades delictivas*, como la ciberdelincuencia, el extremismo violento y la radicalización que conducen a actividades de terrorismo, crimen organizado o abuso sexual infantil. Para participar en tales actividades, los delincuentes hacen uso de las últimas tecnologías aplicadas al uso de entornos como la Dark Web y al uso de nuevas herramientas de cifrado.

Los desarrollos para hacer frente a desafíos, como la crisis de refugiados de 2015 o la consolidación de *Espacio Schengen* (un espacio sin controles fronterizos en las fronteras interiores) (eu-LISA European Agency, 2021), todavía están en pruebas y se validan a través de los correspondientes programas I+D+i. En los últimos años, los Estados miembros de la UE, han restablecido temporalmente los controles en las fronteras interiores tras importantes ataques terroristas en ciudades europeas y tras la pandemia de COVID-19.

La investigación y la innovación apoyan los objetivos específicos establecidos en la Estrategia de Seguridad de UE. Estos incluyen la investigación en nuevas técnicas de análisis forense digital, detección de explosivos, técnicas para almacenar evidencias digitales en investigaciones de policía judicial, por ejemplo, para la detección de pornografía infantil online.

La Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) representa ante la Comisión Europea al Ministerio del Interior en los proyectos de I+D+i en los que este participe, principalmente dentro de programas como el 8.º Programa Marco,

Horizonte 2020 y el actual 9.º Programa Marco, *Horizonte Europa*, o aquellos proyectos de carácter innovador de fondos europeos ejecutivos como son una rama de los FSI (Fondos para la Seguridad Interior), o el nuevo Programa Europa Digital DEP.

A través de su área de I+D+i, la SGSICS y por tanto el Ministerio del Interior gestiona, coordina y fomenta la participación de proyectos de I+D+i en nuevas tecnologías a modo de *inversión eficiente*, haciendo de enlace con la *industria* y la *Academia* nacional y europea.

El área I+D+i intenta aumentar la tasa de participación proporcionando apoyo a las unidades de las Fuerzas y Cuerpos de Seguridad del Estado (CNP y GC) y demás organismos dependientes, coordinando iniciativas a nivel Administración General del Estado (AGE) como la Comunidad de Usuarios Nacional (CoU España).

El área I+D+i SGSICS, fomenta además la *cooperación internacional* en materia tecnológica a través de los grupos de expertos, grupos de trabajo, foros y redes tecnológicas en los que participa como Punto Nacional de Contacto del Ministerio del Interior (*HLEGI-A* Comisión Europea, *WG-AI* Eu-lisa, Grupo de Expertos IA de EUROPOL, *CERIS-CoU* europea, *ENLETS, IFAFRI*, etc.)

Por otro lado, y teniendo en cuenta que Europa seguirá mejorando los mecanismos para desarrollar los servicios TIC que ofrece a sus ciudadanos, es esencial poner en valor la *vigilancia tecnológica*. La revisión de las tecnologías que se consideran disruptivas en el entorno europeo e internacional de seguridad es uno de los principales ejes en el epígrafe IV del presente trabajo.

Igualmente se van a describir algunas de las medidas que el Ministerio del Interior español va a tomar para asegurar la *transferencia* de los resultados de los proyectos de investigación. En último término con la finalidad de diseñar mejor la estrategia de participación en dichos programas, y subvencionar aquello que realmente es necesario en el ámbito operativo.

El uso de las redes 5G y 6G, la investigación en *computación avanzada*, la inclusión de nuevos procesos de IA en los sistemas, el diseño de los nuevos espacios seguros de datos y la aplicación de *blockchain* a las transacciones, supone un gran desafío.

El Ministerio del Interior está realizando fuertes inversiones para acelerar el despliegue del 5G, tanto en zonas urbanas como rurales para mejorar la conectividad y alcanzar un sistema móvil de banda ancha interoperable paneuropeo para radiocomunicaciones. Reflejo de ello es la participación coordinada por la SGSICS, de Policía Nacional y de Guardia Civil en el proyecto H2020 BROADWAY.

España también impulsará la investigación asociada al 6G, como ya lo está haciendo con las principales empresas españolas que están participando de lleno en el proyecto comunitario HEXA-X.

La I+D+i europea considera a la *Computación Avanzada (HPC)* también una tecnología disruptiva, prueba de ello es la inversión que ha realizado en los últimos programas de trabajo en este ámbito. El Proyecto H2020 *Exscalate4Cov* (E4C[1]) es el consorcio público-privado que representa al centro de competencia más avanzado en Europa. Destinado a combatir el coronavirus, combinando recursos de supercomputación e inteligencia artificial, además de instalaciones experimentales donde se realizan las consiguientes validaciones técnicas.

Europa, desde 2018, dio un paso adelante en el desarrollo (I+D+i) de tecnologías cuánticas promoviendo la inversión en una infraestructura de comunicaciones ultra segura en toda Europa y una red de centros de operaciones de seguridad con inteligencia artificial. Dicha iniciativa, financiada con fondos EU, se conoce como *Quantum Flagship*. Quedan reflejados en el trabajo proyectos aprobados como el H2020 *2D-SIPC* y H2020 *Quantum Internet Alliance-QIA*.

La inteligencia artificial IA, puede ser una herramienta útil para afrontar las nuevas amenazas digitales. Su uso podrá ser extendido para acelerar la identificación y respuesta ante las vulnerabilidades y ataques dirigidos. El uso de la *nube* y el *Big Data*, suponen nuevos desafíos relacionados, ya que la navegación de los datos libres en el ciberespacio, aumenta la posibilidad de su robo o de su uso indebido.

Haciendo uso de las correspondientes tecnologías, los cuerpos policiales, podrán aprovechar las fuentes de datos digitales a su máximo potencial ahorrando tiempo en la revisión de evidencias. Con Big Data y *algoritmos* cada vez más sofisticados será posible hacer predicciones cada vez más precisas. Se prevé tomar decisiones más consistentes. Prueba de ello son las validaciones técnicas que se están realizando por parte de las fuerzas y cuerpos de seguridad europeas, entre ellas Policía Nacional y Guardia Civil (SGSICS), en proyectos como H2020-AI-*STARLIGHT*, H2020-AI-*RED ALERT H2020* o el proyecto nacional CIEN-*AIMARS*.

Otra parte importante de la seguridad será la protección de los datos cuando estos se intercambian. Vinculado a la IA, el *Blockchain* proporciona seguridad y descentraliza el entorno en el que se llevan a cabo muchas transacciones digitales. Esta nueva tecnología descentralizada ofrece a los usuarios (personas y empresas) la posibilidad de gestionar y controlar los flujos de datos y su utilización. Permitirá la portabilidad de los mismos en tiempo real, utilizando algoritmos para cifrar información, descentralizar los datos y aumentar de forma segura la privacidad entre los usuarios. Las aplicaciones del Blockchain son muy amplias, más allá de las criptomendas. Prueba de ello es el proyecto *H2020 LOCARD*, cuyo objetivo es desarrollar una plataforma de gestión integral que permita el almacenamiento de datos de evidencias digitales y pueda garantizar la cadena de custodia en investigaciones de policía judicial.

Es importante destacar que España apoya la reutilización de datos tanto privados como públicos, en particular los datos industriales en los que se basa las nuevas líneas estratégicas de I+D+i. Igualmente, el Ministerio del Interior también apoyará el desarrollo de un marco de la UE sobre el uso de inteligencia artificial. Este marco debe garantizar que la tecnología de inteligencia artificial pueda desarrollarse e implementarse en Europa y en España al tiempo que garantiza que la tecnología no se utilice de manera inapropiada. Es por ello que el Ministerio del Interior representado por la SGSICS trabaja con la Comisión Europea en grupos de expertos de IA, como en *el HLEG-AI*, y en *CAHAI*, entre otros.

Los *espacios seguros de datos* van a cobrar especial importancia durante el periodo *2021- 2027*, y habrá que atender tanto a su infraestructura de carácter tecnológico como a la gobernanza de los mismos. El valor de los datos reside en su uso y reutilización.

En la actualidad, no hay suficientes datos disponibles para que sean reutilizados en I+D+i, por ejemplo, para el desarrollo de procesos de inteligencia artificial y entrenamiento de sus algoritmos. Las problemáticas empiezan por la titularidad de los datos, siguen por la identificación de los usuarios de los datos, y pueden llegar hasta la naturaleza que tienen los mismos.

La *interoperabilidad* y la *calidad* de los datos son aspectos clave para el despliegue de procesos basados en IA. Se han identificado problemas importantes de interoperabilidad que dificultan la combinación de datos que provienen de diferentes sectores. Estas problemáticas se agravan todavía más cuando se hace referencia a Estados o Naciones diferentes.

Para que los espacios seguros de datos sean operativos, se necesitan organismos públicos y privados que fomenten la innovación acorde a los marcos jurídicos existentes.

Aunque un espacio europeo seguro de datos para la Innovación no estaría únicamente dirigido al desarrollo de la IA en el ámbito científico, sí que supondría una mejora en los resultados de investigación de la UE, estableciendo vínculos entre los dos programas de financiación I+D+i más relevantes: HE y DEP.

El éxito de estas iniciativas llegaría a suponer una mejora no solo en la soberanía tecnológica de los Estados miembros, sino también en la lucha contra el crimen organizado y el terrorismo en el ámbito digital, y, por ende, una mayor protección de la Seguridad Nacional. Los Estados miembros podrán validar sus propias herramientas digitales, y ofrecer servicios centralizados, basándose en esquemas comunes. Al *reducir la dependencia de proveedores* de terceros países, se podrían ver disminuidas amenazas de tipo malicioso, además de establecer estándares de calidad en el entorno UE.

Las agencias europeas, *Eu-Lisa y EUROPOL*, con el *feedback* de los Estados miembros, están evaluando en la actualidad las distintas arquitecturas posibles para implementar este espacio común de datos seguros, valorando cuatro posibilidades: individual, centralizada, federada e híbrida, explicadas en el trabajo.

El conocimiento del mapa de las diferentes convocatorias y ayudas públicas orientadas a la seguridad, los mecanismos de participación, la experiencia en preparación de ofertas y la experiencia en la gestión integral (técnica, administrativa y financiera) de proyectos europeos y nacionales I+D+i del Ministerio del Interior, a través de la SGSICS se ponen en valor en el presente trabajo. Para obtener financiación I+D+i europea y nacional que resulte impulsora de necesidades específicas de las Fuerzas y Cuerpos de Seguridad del Estado, el Ministerio del Interior, SGSICS va a utilizar los siguientes mecanismos:

El área I+D+i SGSICS, que articula su función en varios ejes prioritarios: gestión integral de proyectos I+D+i (H2020, HE, DEP, etc.), realización de prospectiva tecnológica (grupos de trabajo, *networking*), gestión tecnológica, que abarca la trasferencia tecnológica y explotación (PCP, CPI, AI, etc.), Función Tractora (creación e impulso de consorcios nacionales y europeos, con industria y con universidad) y Difusión del Conocimiento (jornadas informativas, *workshops*, etc.).

La Comunidad de usuarios finales española (CoU – CERIS), coordinada por la SGSICS, supone un fuerte impulso para cooperación público-privada nacional en seguridad. El alto número de proyectos de I+D+i, la desconexión entre la investigación y la obtención de resultados tangibles en muchos casos, la dificultad de comercialización de soluciones provenientes de I+D+i, y la falta de mecanismos de engranaje entre los diferentes programas de financiación dificultan la comunicación y el intercambio de conocimientos entre los usuarios finales nacionales y todavía más con los europeos.

Es muy necesario asegurar la transferencia de los resultados de los proyectos de investigación para los usuarios finales del ámbito de la seguridad. Lo que requiere un intercambio adecuado de información sobre actualizaciones de políticas o resultados de proyectos (de investigación). La principal función de la COU-España es *identificar oportunidades de financiación y sinergias* entre los diferentes programas I+D+i y proponer medidas para facilitar la interacción. Otra función importante será la de intentar evitar duplicidades en la participación por parte de los usuarios finales (FCSE, Policías Forales, Protección Civil, Defensa, Puertos del Estado, Instituciones Penitenciarias, etc.) en los diferentes programas de financiación, por ejemplo, entre Policía Nacional y Guardia Civil. Si la necesidad es conjunta, es preferible participar conjuntamente, que desviar el doble de recursos del Ministerio del Interior para la misma tarea.

El Centro Tecnológico para la Seguridad, CETSE realiza funciones de observatorio tecnológico del Ministerio del Interior. Continuando con su misión de proporcionar el conjunto de herramientas tecnológicas que permitan conseguir sus objetivos de la manera más eficaz y eficiente a las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil) así como al propio Ministerio del Interior, la SGSICS sigue impulsado el desarrollo de nuevas iniciativas TIC para dar soporte a las unidades operativas.

Claro ejemplo son los proyectos internos impulsados por el CETSE, por ejemplo, de reconocimiento facial avanzado, que incluyen procesos de IA, y que desarrollan conjuntamente con CNP, GC y CNI: BiObserver y BioRetriever. También reseñar el Proyecto H2020 I-LEAD, a través del cual se comparten tecnologías y metodologías que utilizan las FCSE europeas en la actualidad para trabajar en investigaciones digitales.

La mayoría de los Estados miembros dependían y dependen completamente de Horizonte 2020 y actualmente de HE, para cubrir sus necesidades de soluciones de seguridad innovadoras. Dichos programas representan el 50 % de la financiación pública global para la investigación de seguridad en la UE. Las convocatorias de H2020 *Sociedades Seguras: protección de la libertad y la seguridad de Europa y sus ciudadanos*, están en consonancia con la investigación e innovación responsables, involucrando a la sociedad en temas sensibles de seguridad.

El objetivo tratado en el epígrafe V del trabajo, es explicar el alcance de la I+D+i en Seguridad en UE a través de los programas *Horizonte Europa HE* (9.º Programa Marco) y *Horizonte2020* (8.º Programa Marco).

No solo como se trabaja en el desarrollo de nuevos productos tecnológicos para satisfacer las necesidades de aquellos cuerpos que se encargan del mantenimiento de la seguridad, sino que también comprender fenómenos muy tenidos en cuenta por la Comisión Europea, como la radicalización violenta, la seguridad de las entradas fronterizas, la protección de las infraestructuras críticas contra cualquier tipo de amenaza, incluso los ciberataques, o el desarrollo de intervenciones más efectivas para el mantenimiento de la seguridad ciudadana en general.

Además, se ha intentado reflejar las medidas (tópics) que se están implementando a través de los diferentes Programas Marco de Investigación e Innovación de la UE, en concreto los de HE (2021-2027), Clúster 3, Destino: *Seguridad Civil para la Sociedad*, para desarrollar e implementar por parte de los Estados miembros y de España, herramientas de última generación, de utilidad para la función policial. (Lucha contra el crimen organizado y el terrorismo FCT, la gestión de fronteras BM, la resiliencia de infraestructuras INFRA, la resiliencia de las sociedades DRS y la Ciberseguridad CS).

En el epígrafe VI se han dado unas pinceladas del *Programa Europa Digital DEP* (2021-2027). Se ha explicado la fórmula para financiar las capacidades digitales estratégicas de los Estados miembros de la UE, con un presupuesto global previsto de 7.500 millones de euros. DEP complementa a otros programas como HE, el Mecanismo Conectar Europa para la infraestructura digital y, finalmente, el Fondo de Seguridad Interior (ISF).

El Programa Europa Digital reforzará las capacidades digitales críticas de la UE centrándose en las áreas clave de inteligencia artificial (IA), ciberseguridad, informática avanzada, infraestructura de datos, gobernanza y procesamiento, el despliegue de estas tecnologías y su mejor uso en todos los ámbitos de las sociedades europeas.

3. Conclusiones

Ha quedado patente que, cumpliendo con el objetivo inicial de *visibilizar el enfoque proactivo en la búsqueda de programas y soluciones tecnológicas por parte del Ministerio del Interior* español, se facilita el acceso a los productos y soluciones tecnológicas de seguridad que puedan ser posteriormente aplicables con éxito por las unidades operativas de las FCSE. Además, la participación en dichos programas y proyectos, crea *canales de comunicación* con los Estados miembros de la UE y las Agencias europeas correspondientes, para que, de forma colaborativa, se pueda acceder a las ayudas financieras europeas.

Queda reflejado también a lo largo del trabajo, no solo la importancia de la cooperación internacional en materia de seguridad e I+D+i, si no la necesidad, para tener éxito en los proyectos, de la colaboración entre Administración Pública, industria y universidad nacional y europea. La *cooperación público-privada* concluye como un factor esencial en la gestión de proyectos europeos I+D+i, y en general, en el impulso de las nuevas tecnologías para la seguridad.

El apoyo del Ministerio del Interior y del resto de Estados miembros, junto con las inversiones en I+D+i, no solo económicas, sino también de *capital humano*, van a contribuir al posicionamiento de la UE como un actor tecnológico, industrial y normativo líder en tecnologías digitales, Big Data, IA, computación cuántica, 5G, blockchain y espacios seguros de datos. Los usuarios finales validando junto con la industria nacional y europea, todas aquellas tecnologías que cubren sus necesidades en el ámbito de la seguridad, van a fomentar que España se convierta en *una nación emprendedora*.

Con la participación en los proyectos europeos anteriormente explicados y en los diferentes mecanismos de colaboración europea (grupos de expertos, foros tecnológicos, grupo de trabajo, etc.) se da *mayor visibilidad* a la profesional labor que realizan las Fuerzas y Cuerpos de Seguridad

en nuestro país, gracias en cierta medida, a los nuevos desarrollos tecnológicos con los que cuentan para realizar su trabajo. Fortaleciendo de esta manera, aún más, la imagen y la *Marca de España* en la gobernanza de la tecnología, aplicada también al ámbito de la seguridad.

Se cumple con el objetivo del presente trabajo, ya que queda evidente cómo a través de Programas de Financiación Europeos y Nacionales (HE, H2020, DEP) se facilita a las FCSE acceso a *herramientas provenientes de la I+D+i que le ayudan a desempeñar sus funciones esenciales:* El mantenimiento de la *seguridad* de los ciudadanos, la lucha contra el crimen organizado y el terrorismo, y la protección de las fronteras y de las infraestructuras críticas. La finalidad última es *completar ciclos de innovación*, desde que se investiga un producto hasta que llega a mercado. Y España, con la ayuda de los mecanismos del Ministerio del Interior, aunque no en todos los casos, lo consigue.

Figura 1. Estrategia UE en seguridad, Fuente: ec. europa.eu

Agradecimientos

A mis padres, *Santos Machín Vázquez* y *Carmen Prieto Fuertes,* por la educación y valores que me han dado y me siguen dando. Por inculcarme la ilusión por aprender y superarme.

A mis padrinos, *Manuel Formigo Vilas* y *María José González Briones*, por el apoyo incondicional y el cariño ofrecido lejos de casa.

A mi director de TFM Luis Álvarez Sabucedo, por su buena predisposición, su buen hacer y su paciencia infinita.

GESTIÓN DE PROYECTOS DE INNOVACIÓN TECNOLÓGICA PARA LA SEGURIDAD EN EL MINISTERIO DEL INTERIOR.
NUEVAS TECNOLOGÍAS, HORIZONTE EUROPA (2021-2027)

Autora: Rosalía Machín Prieto
Director: Luis Álvarez Sabucedo
Universidad de Vigo

Introducción

Los Fondos de Financiación Europeos promueven el desarrollo de nuevas tecnologías con la finalidad de mejorar la función pública y mantener la seguridad de la ciudadanía española.

Sus Programas Marco facilitan el acceso a importantes inversiones en I+D+i y TIC claves para Seguridad

5G /6G
Internet de las Cosas (IoT)
Inteligencia Artificial (IA) y Espacios Seguros Datos
Computación Cuántica
Blockchain
Ciberseguridad

Metodología

Las nuevas TIC plantean nuevas Amenazas y Riesgos para el Ministerio del Interior SGSICS (FCSE)
La mayoría de los delitos tienen un componente DIGITAL

Programas de Financiación europeo I+D+i y TIC

Redes y Foros de expertos UE

Estrategias y Gobernanza MIR I+D+I, IA para Seguridad

Comunidades de usuarios finales nacionales y europeas

Cooperación MIR SGSGIC-CETSE-FCSE Observatorio - TECH

Mecanismos Adquisición CE /CDTI

PROYECTOS VALIDACIÓN DE NUEVAS TECNOLOGÍAS y ACCESO A NUEVAS HERRAMIENTAS de apoyo a:

FCT Lucha contra el Crimen Organizado y Terrorismo
BM Protección de Fronteras Exteriores
INFRA Protección de Infraestructuras Críticas
DRS Seguridad y Resiliencia de las sociedades
CS Ciberseguridad y Seguridad Digital

Conclusiones

Completar ciclos de Innovación
Transformación digital en seguridad
Herramientas para las unidades operativas
Visibilidad marca España y labor FCSE
Cooperación público-privada
Cooperación internacional + Europol y Eu-Lisa
Apoyo a las políticas tecnológicas EU
Innovation Hubs - Innovation Labs
España = nación emprendedora

Estudio de configuración de terminales tipo *thin client* o *zero client* entornos de alta clasificación a través de redes públicas

Autor: Marqués Collado, César (cmarcol80@gmail.com)
Directores: González Coma, José P. (jose.gcoma@cud.uvigo.es)
y Troncoso Pastoriza, Francisco (ftroncoso@cud.uvigo.es)

Resumen – Este trabajo fin de máster consiste en el estudio de la normativa aplicable y requisitos para la conexión de terminales a redes de alta clasificación (según el Esquema Nacional de Seguridad o Sistemas Clasificados) publicados por el Centro Criptológico Nacional así como la realización de una propuesta de prototipo que implemente todas las necesidades, tanto de software como de implementación de protocolos sobre un equipo sin almacenamiento permanente y haciendo uso del mínimo hardware imprescindible para posibilitar el uso del sistema.

Para la realización del estudio de requisitos, se realizará el compendio y análisis de la documentación aplicable a conexión de sistemas, securización de equipos, equipos multidominio y configuraciones seguras de software de las series 300, 400, 500 y 600 del Centro Criptológico Nacional.

También se tienen en cuenta las recomendaciones y requisitos que hacen referencia al Esquema Nacional de Seguridad (serie 800) y son de aplicación en el alcance de este trabajo fin de máster.

En caso de que el software o los protocolos que se decidan usar o recomendar en un prototipo, no esté contemplado en las guías de securización del Centro Criptológico Nacional, se proponen guías alternativas de otras entidades y organismos, y como última posibilidad, se tiene en cuenta las buenas prácticas de configuración y securización o configuraciones de software y protocolos similares.

Palabras clave – Esquema Nacional de Seguridad, seguridad, redes clasificadas, VPN

1. Introducción

Debido a las necesidades digitales de nuestra sociedad, ha sido necesario establecer un marco en el cual los entes de auditoría puedan establecer un nivel en la seguridad de los datos que se manejan no solo de forma técnica sino de forma reglada en la que se establecen procedimientos, configuraciones y estructuras de gestión que lo soporte.

Teniendo en cuenta estas necesidades el Centro Criptológico Nacional (CCN) según la normativa que se establece en la Ley 11/2001 de referencia[1], es el encargado de velar por el cumplimiento de la seguridad de la información en las instituciones nacionales y el responsable último del equipo de respuesta a incidentes (CERT) nacional, para llevar a cabo esta misión y ser capaz de regir tanto las relaciones con la administración como los sistemas de información que manejen información tanto pública como privada, se ha establecido en la referencia [2] las medidas requeridas por este centro, teniendo el nombre de Esquema Nacional de Seguridad (ENS).

En esta necesidad de regulación de los sistemas de información, el CCN en su relación con entes públicos y privados no solo establece los requisitos y necesidades de los sistemas de información que han de mantener de los requisitos de seguridad tanto física como lógica de la información, sino que establece guías tanto de estructuras de seguridad en entidades, de procedimientos en el flujo de información, de requisitos en equipos físicos y virtuales así como la adecuación y validación de estos componentes al ENS. En el sitio web del CCN, referencia [3], se encuentran todas las guías del ENS actualizadas permanentemente.

2. Desarrollo

En este proyecto se indican los requisitos y procedimientos para establecer una comunicación entre dispositivos con un sistema operativo mínimo instalado en un disco duro o incluso sin disco duro, de nivel alto o superior desde una red pública a una red *segura* y para ello se establece, como mínimo las restricciones del nivel alto del ENS equivalentes al nivel de Difusión Limitada en Sistemas de Información Clasificados.

Como elementos de acceso a la red privada, se realiza la conexión con un sistema que haga las veces de router o cifrador, y considerar que la red que sirve al usuario es una red de área local (LAN) segura.

El objetivo de este trabajo es estudiar si un equipo, sin sistema operativo ni almacenamiento como es un ZeroClient o con un almacenamiento mínimo, pero que no sea capaz de ejecutar un sistema operativo completo como puede ser un ThinClient, es capaz de acceder a una red clasificada a nivel alto del ENS o superior.

Una vez que esta máquina disponga de conectividad con el entorno, se importa una máquina virtual predefinida de un servidor de máquinas virtuales y ejecutarla con las restricciones necesarias.

Para esta máquina se requiere que en caso de ser comprometida bien por elevación de privilegios o bien porque sea intervenido el terminal, ser capaz de desconectarla del entorno al que está conectado.

En la figura siguiente, se establece un entorno clasificado (abajo a la derecha) con los servicios disponibles y una conexión hacia el exterior mediante una red privada no clasificada que finaliza en un terminal ThinClient/ZeroClient.

Esta red privada, podrá atravesar otro tipo de redes de las que se desconoce su confianza como pueden ser redes públicas como internet o privativas.

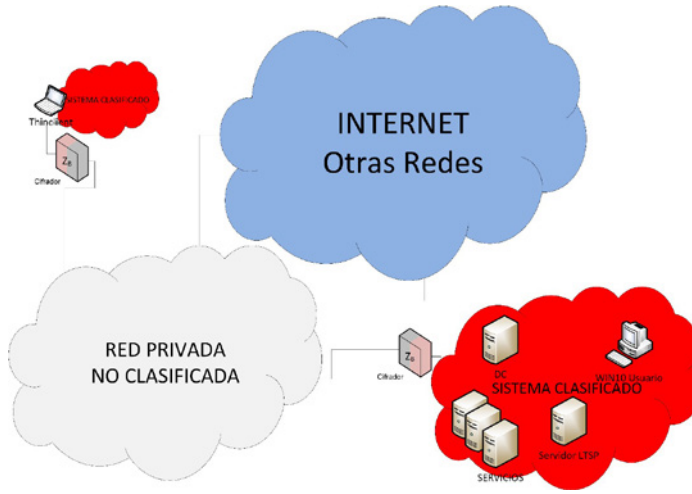


Figura 1. Interconexión del sistema

Se puede establecer la siguiente tabla en cuanto a seguridad de la información, en la que las filas inferiores tienen menos requisitos de seguridad que las filas superiores.

ENS	Sistemas Clasificados
	Secreto
	Reservado
	Confidencial
ENS Nivel Alto	Difusión Limitada
ENS Nivel Medio	
ENS Nivel Bajo	

Tabla 1. Equivalencias ENS – Sistemas clasificados

Los sistemas de la columna izquierda se rigen por el ENS según la referencia [2] mientras que los sistemas de la columna derecha se rigen por la normativa de Sistemas clasificados del CCN según la referencia 1 [4]. No

obstante, se puede apreciar que el nivel ENS nivel alto y el nivel difusión limitada de los sistemas clasificados coinciden en nivel de clasificación, exigencias y certificación.

2.1. Particularidades de conexión a redes

En la actualidad, la conexión a un sistema de ENS a través de una red pública supone la conexión por medio de una VPN a los servidores de interconexión nodo II del sistema al que haya que conectarse y una vez establecida la conexión y tunelizada, establecer el enlace con el mismo dispositivo al servidor.

Para este trabajo se utiliza lo establecido en la guía CCN-STIC-302 Interconexión de sistemas (CCN), la cual especifica que en sistemas clasificados la interconexión se debe hacer según la siguiente figura.

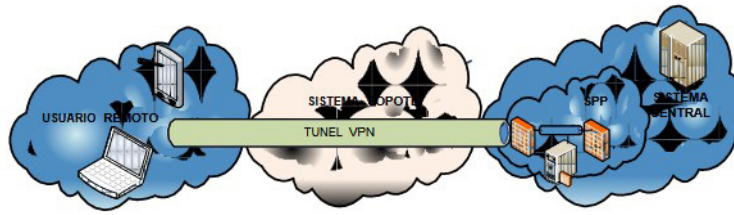


Figura 2. Conexión de sistemas mediante redes públicas. Extraído de [4]

Se plantea una arquitectura en la que un dispositivo configurado como un router sea el encargado de establecer un túnel con la dirección pública del servidor, y una vez establecido esta conexión, a modo de túnel, se establezca una sesión de conexión a una máquina que sí este en el dominio seguro, pero situada en una zona desmilitarizada (DMZ) del sistema.

En cuanto al equipamiento a utilizar, en el entorno tanto del Esquema Nacional de Seguridad como de sistemas clasificados, existe un catálogo de equipamiento probado y aceptado por el Centro Criptológico Nacional. Este catálogo se publica en la guía STIC del CCN 105, referencia [6].

En sistemas clasificados además del uso de los elementos del catálogo se debe acreditar la firma radioeléctrica de los equipos según la guía STIC del CCN de referencia [7].

En los sistemas clasificados con ENS superior a *alto*, no es posible la conexión desde redes externas, por lo que para que este trabajo pueda ser de aplicación a sistemas regidos por el ENS y a sistemas clasificados, se definen dos alternativas en cuanto al modo de acceso de los clientes:

- Sistemas clasificados: Conexión mediante una red pública en la que se despliegan equipos que simulan los elementos de cifra

entre los dos segmentos de red a través de una red privada, esta configuración sería la que habría que desplegar en sistemas clasificados con el nivel de *reservado* o superior.

- Sistemas ENS: Conexión mediante una red pública y tecnología de VPN, que sí está permitida en los tres niveles del ENS y en los sistemas con clasificación de *confidencial* o *difusión limitada*.

Para llevar a cabo la segmentación de la red, se han definido las siguientes redes para cada uno de los cometidos que se llevarán a cabo, todas ellas aisladas salvo por las reglas definidas en un cortafuego/router:

- Red de Gestión: Red utilizada para la configuración de los distintos elementos del sistema (servidores y electrónica de red) red. Se despliegan los servidores, electrónica de red y los equipos de administradores. No permite interconexión con otras redes.

- Red de Servicios: Red utilizada para desplegar los servidores que ofrecen servicios a ser consumidos en la red.

- Red de Usuarios: Red para los equipos de los usuarios.

- Red DMZ: Red para los equipos no confiables incluyendo el servidor de máquinas virtuales para los ThinClient/ZeroClient. Se restringe el acceso a los puertos necesarios para los servicios que se desplieguen en esta red.

- Red OpenVPN: Red para simular los despliegues del ENS, se despliega una máquina cliente con Sistema Operativo Windows 10 y un cliente OpenVPN que se valida contra el cortafuego. Por medio de esta red se deberá tener acceso a la de usuarios para iniciar una conexión de escritorio remoto en una máquina real de la red de usuarios.

- Red Z local: Red para simular los despliegues de sistemas de clasificación *reservado* o superior, se establece que la conexión se realice mediante dispositivos criptográficos hardware aprobado por la guía *CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación*, referencia [6], como pueden ser los EP430, estos elementos se comportan como enrutadores con cifrado robusto punto a punto.

- Red Z remoto: Red en la que se despliega el ThinClient o ZeroClient.

- Red WAN: Red solo disponible en ENS con acceso a internet.

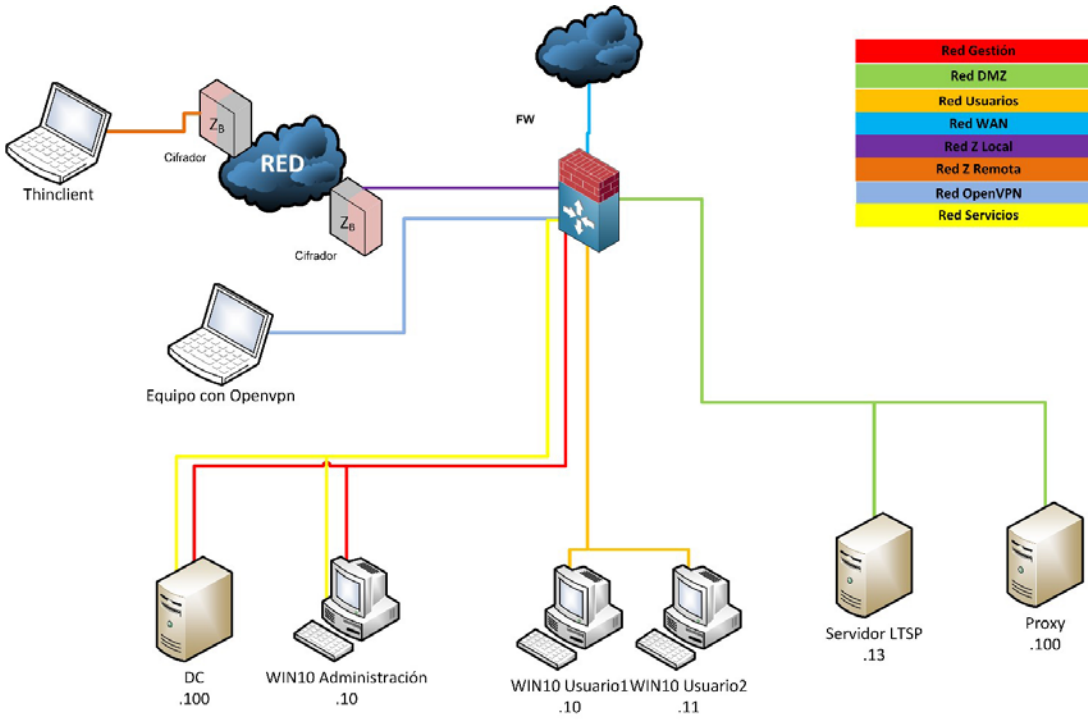


Figura 3. Despliegue

2.2. Despliegue Software.

Para llevar a cabo este trabajo, se ha debido desplegar y configurar el siguiente software:

El despliegue de software y su configuración que se va a realizar en cada uno de los elementos es el sistema será el siguiente:

- Cortafuego
  - Imagen de pfsense de la versión 2.5.2.
- Thinclient
  - No tiene disco duro ni ningún software instalado.
  - Imagen ISO con arranque mínimo por red.
- Equipo Openvpn
  - Windows 10 LTSC no integrado en dominio
  - OpenVPN 2.5.2 x86-64_w64_mingw32
  - FireFox 94.0.2
- Controlador de Dominio
  - Windows Server 2016 con las guías del CCN relativas a este entorno y a los clientes Windows 10 que formarán parte del dominio.

- Win10 Administrador
  - Windows 10 LTSC con las guías del CCN aplicadas para la versión del sistema operativo instalado.
- Win10 Usuario
  - Windows 10 LTSC con las guías del CCN aplicadas para la versión del sistema operativo instalado.
- Servidor LTSP
  - Ubuntu Server LTS versión 20.04.03 básico.
  - Paquetes extras en la instalación del proyecto LTSP
  - Ltsp
  - ltsp-binaries
  - dnsmasq
  - nfs-kernel-server
  - openssh-server
  - squashfs-tools
  - ethtool
  - net-tools
  - epoptes
- Proxy
  - Linux Centos 7
  - Squid
- Emulado de red Z (WANem)
  - Imagen de WANem versión 2.3

2.3. Emulador de redes

Los cifradores son dispositivos físicos que realizan una separación física entre dos redes, una considerada segura, llamada zona roja y otra considerada insegura, llamada zona negra. Los cifradores establecen un túnel cifrado entre los equipos, utilizando una red pública o privada no segura a la que están conectados sus interfaces *negros*, de modo que los segmentos rojos se comunican como si estuvieran a un salto de distancia de una red IP segura.

Al realizar un túnel atravesando la red WAN, el paso de la red LAN roja identificada como red Z local a la red LAN roja red Z remota, se verá afectada por todos los problemas referentes a la transmisión IP de la red WAN. Para la emulación de este hecho, se ha usado un emulador de red llamado WANem el cual es un emulador de redes desarrollado por TATA Consultancy Services de código abierto licenciado bajo la Licencia Pública General de GNU GPL v2.

En este trabajo se ha realizado la abstracción de los cifradores mediante la configuración indicada en la figura siguiente:

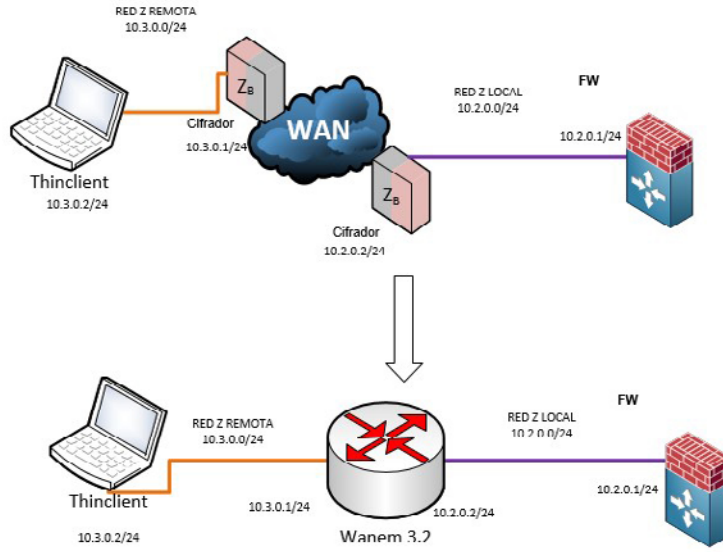


Figura 4. Emulación de cifradores

2.4. Bastionado del sistema

Para obtener un sistema con clasificación *reservado* o superior, se han utilizado las guías del CCN referentes a cada uno de los componentes software descargadas de la parte privada del portal web del CCN. Específicamente se ha realizado el bastionado del controlador de dominio, de los equipos de administración y de usuarios.

Tras el bastionado del sistema, se han tenido que definir políticas específicas para que se pueda hacer sesión de escritorio remoto sobre los equipos de usuarios, puesto que una de las acciones que se llevan a cabo en la securización es la desactivación y eliminación de los componentes que permiten la ejecución del servidor de escritorio remoto.

2.5. Imágenes de arranque

Para poder ejecutar máquinas virtuales, es necesario tener una máquina capaz de montar una iso generada por el administrador del sistema con la información de conexión, como es la dirección IP local, la dirección IP del servidor, la ruta donde estén las imágenes de las máquinas a ejecutar.

Se ha optado por el uso del protocolo iPXE en lugar del protocolo PXE presente por defecto en casi todas las BIOS, debido principalmente a dos aspectos:

- La recomendación del CCN de desactivación del protocolo DHCP
- El tener que atravesar dos cifradores, lo que conlleva el atravesar dos redes distintas hace imposible la propagación de DHCP desde la red que pertenece al router hasta la red del extremo remoto de los cifradores.

Con estos requisitos se ha elegido el uso del protocolo iPXE el cual permite una máquina con un dispositivo externo, es capaz de arrancar y solicitar la información de arranque según lo especificado en este medio de almacenamiento sin necesidad de un servidor DHCP, a diferencia del protocolo PXE.

Esta imagen de arranque realiza la petición al servidor de máquinas virtuales, el cual se ha basado en el proyecto Linux Terminal Server Proyect, el cual sirve una imagen del sistema operativo Ubuntu con la herramienta de acceso a escritorio remoto Remmina.

3. Resultados y discusión

A la finalización del proyecto se ha desplegado un ThinClient y un ZeroClient con una imagen iso generada para tal efecto y se ha comprobado la carga correcta de la máquina virtual con el sistema operativo Ubuntu. Desde esta máquina se ha comprobado el acceso mediante Remmina al escritorio de los equipos de usuarios y su uso sin deficiencias.

Por medio del emulador de redes se han realizado configuraciones típicas de redes militares como puede ser el límite del ancho de banda a 10 megabytes por segundo y la inclusión de retardos de 200 milisegundos.

Además de las pruebas funcionales, se han realizado pruebas de seguridad realizando distintos tipos de escaneos de redes y se ha observado que se cumple el principio de mínima exposición de servicios y puertos abiertos.

4. Conclusiones

Se ha comprobado el uso de ZeroClients en sistemas clasificados en ubicaciones que supongan un cambio de red y, por ende, no se acceda mediante DHCP.

Estos sistemas se deben conectar según las indicaciones del CCN mediante cifradores hardware, por lo que el equipamiento a desplegar sería un cifrador, el propio ThinClient y un enrutador.

Con la configuración adecuada, se ha comprobado que un atacante desde la red en la que se encuentra el ThinClient deberá suplantar la IP de dicho equipo para intentar atacar los servicios desplegados.

Referencias

[1] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

[2] CCN, CCN-STIC 801 (2019), Esquema Nacional de Seguridad, Responsabilidades y Funciones. [Internet] https://www.ccn-cert.cni.es/.

[3] CCN, CCN-STIC 800 Guías del Esquema Nacional de Seguridad. [Internet] https://www.ccn-cert.cni.es/.

[4] CCN, CCN-STIC 301 (2020), Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados. [Internet portal privado] https://www.ccn-cert.cni.es/.

[5] CCN, CCN-STIC 302 Interconexion de Sistemas. [Internet portal privado] https://www.ccn-cert.cni.es/.

[16 CCN, CCN-STIC 105 (2021), Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación. [Internet] https://www.ccn-cert.cni.es/.

[7] CCN, CCN-STIC 104 Catálogo de productos con Clasificación ZONING, [Internet] https://www.ccn-cert.cni.es/.

Estudio de configuración de terminales tipo “thin client” o “zero client” a entornos de alta clasificación a través de redes públicas.

Autor: César Marqués Collado

Director/es: González Coma, José P. y Troncoso Pastoriza, Francisco

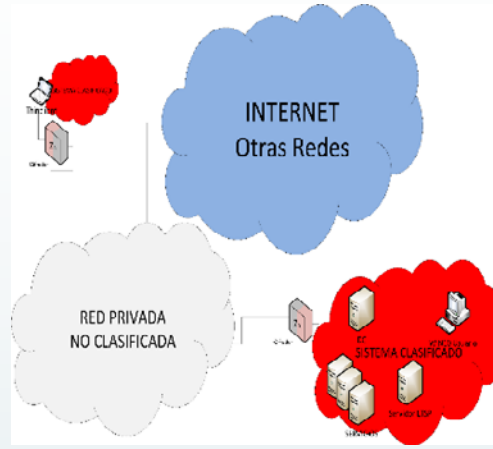
Universidad de Vigo

Introducción

En un entorno en el que las TIC están presentes en todos los procesos de obtención de información, se hace necesario disponer de sistemas desplegables que accedan a las redes de los organismos de forma fiable, y no supongan una amenaza en el plano de la seguridad de dicho sistema.

Por ello se propone el uso de equipos sin sistema operativo conjugado con las necesidades que se determinen.

Resultados

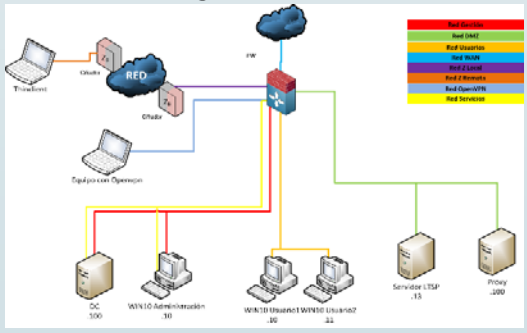


Conexiones seguras viables desde equipos remotos atravesando redes públicas

Conclusiones

Es posible la conexión segura mediante ThinClient o ZeroClient usando redes públicas o privadas no seguras, desplegando imágenes securizadas de sistemas operativos mínimos.

Las tecnologías no comerciales o que no están en catálogos seguros son usables en sistemas seguros si se configuran siguiendo buenas prácticas y realizando auditorías de seguridad exhaustivas.



Recursos

En materia de Seguridad de la Información, el **CNI** mediante las guías publicadas por el **CCN** pone a disposición de los administradores de sistemas recomendaciones y guías de implantación seguras.

Los proyectos de código abierto como son LTSP e iPXE proponen ampliaciones de funcionalidad a otro tipo de herramientas como puede ser el WDS (Windows Depoy System) o el PXE (Preboot eXecution Environment).

Sistema de información corporativode seguridad, integrado en entornos desplazados de consejerías y agregadurías de interior

Autor: Martín Ramírez, Pablo Óscar (pmr@interior.es)
Director: Álvarez Sabúcedo, Luis (lsabucedo@det.uvigo.es)

Resumen – El presente trabajo aborda la definición de un sistema de información para la utilización y explotación por parte de las distintas consejerías y agregadurías del Ministerio del Interior, desplazadas por el mundo.

El citado sistema deberá de mantener en la mejor disposición posible las capacidades de transmisión, almacenamiento y en su caso análisis o explotación de la información integrada, ya sea de carácter crítico o cualquier otra, en ámbitos de terrorismo u otras amenazas relevantes competencia de las FCSE.

El sistema de información permitirá guardar, gestionar y enviar documentos en distintos formatos, siempre teniendo en cuenta las limitaciones de conexión en algunos de los países en los que está desplegado este personal.

En relación a lo anterior, todas las comunicaciones darán prioridad a la seguridad y comunicación de los incidentes o datos, sobre cualquier otra consideración, debido a la importancia e inmediatez requerida para este tipo de informaciones.

Se valorarán las distintas arquitecturas software para la elección de la que más se adecue a las necesidades planteadas y al ecosistema de implantación.

Posteriormente esta información podrá ser cedida en el caso que así se disponga, para su integración y explotación, en los sistemas de inteligencia que se considere oportuno, tanto del Ministerio del Interior como en el Ministerio de Defensa en su caso.

Palabras clave – extranjero, información, disponibilidad, sistemas de información, Plataforma Web

1. Introducción

Dentro de la organización del Ministerio del Interior y según el R.D. [1] de estructura orgánica que lo regula se establecen una serie órganos directivos, a los que se atribuyen una serie de competencias y responsabilidades.

La Dirección General de Relaciones Internacionales (DGRIE) tiene entre otras competencias la responsabilidad en materia de Cooperación Policial Internacional [2], para el cumplimiento de esta misión existen un total de 84 funcionarios, consejeros y agregados de Interior desplegados por el mundo, todos ellos son miembros de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Estos funcionarios desplegados poseen las competencias del MIR en sus países de influencia, ejecutando labores en todos los ámbitos de las FCSE: información, terrorismo, inteligencia, seguridad, delincuencia transnacional, protocolo, etc.

De todas las actuaciones llevadas a cabo por los funcionarios se elabora la correspondiente documentación, estos documentos son puestos en conocimiento de los Órganos superiores, mediante su transmisión a través de las cuentas de correo del MIR.

Parece oportuno suponer que este medio de transmisión no es el más seguro y adecuado para esta función, además el actual sistema requiere de una labor de gestión, organización y atención continua por personal funcionario de la DGRIE para hacer posible que los documentos lleguen en tiempo y forma a las personas indicadas.

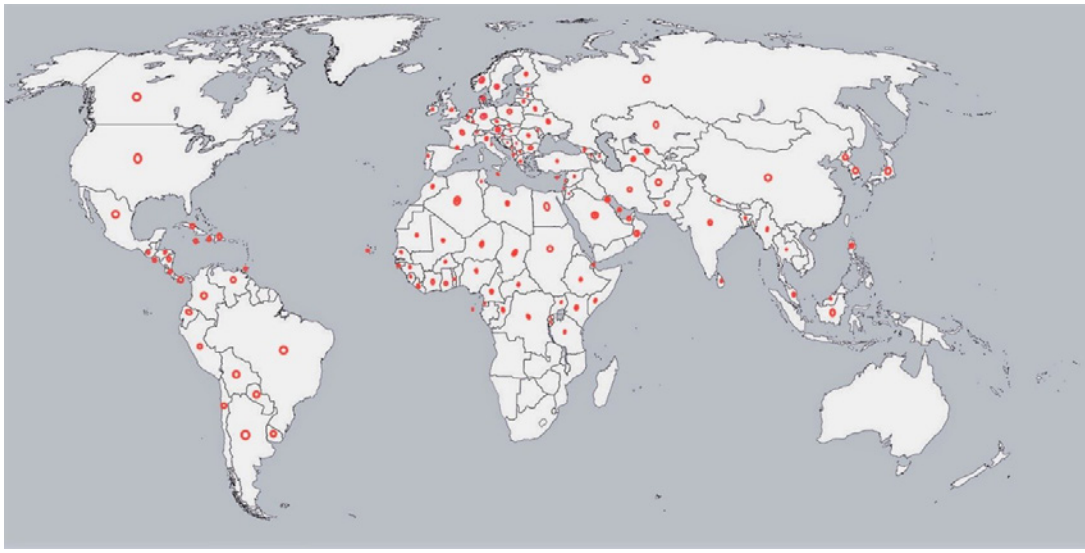


Figura 1. Mapa del despliegue de las consejerías y agregadurías de Interior

Por este motivo desde la DGRIE se propone a la unidad TIC competente del MIR, Subdirección General de Sistemas e Información y Comunicaciones para la Seguridad (SGSICS) [1], la definición de una solución tecnología que permita mejorar las capacidades de transmisión de la información, y que además solvente las deficiencias en seguridad y otros aspectos que tiene el actual sistema.

2. Desarrollo

Para abordar las necesidades indicadas por la DGRIE se plantea como principal objetivo la sustitución del correo electrónico del MIR por un sistema de información, que permita facilitar el trabajo del personal desplegado en las embajadas (consejeros y agregados de Interior), así como, optimizar la gestión, aseguramiento y control de la información por los Servicios Centrales del Mir.

La memoria del trabajo abordará los siguientes aspectos para proponer la solución más indicada.

1) Tecnologías posibles: en el que se describirán los principales tipos de arquitecturas de los sistemas de información sus ventajas e inconvenientes.
2) Especificaciones del sistema: se pretende establecer una especificación técnica, que sirva de base para la construcción e implementación del futuro sistema.
3) Análisis del sistema: en el que se hará una definición del alcance y capacidades del sistema con el objetivo de proponer una solución segura, y que aporte valor añadido a toda la información transmitida y almacenada.
4) Requisitos del sistema: en el que se describirán todos aquellos requisitos funcionales y no funcionales que deberá de cumplir el sistema.

2.1. Tecnologías posibles

En la memoria aparecen figuras de las diferentes tipologías de arquitectura, además se incluye una descripción y un cuadro comparativo de algunas de las ventajas e inconvenientes de cada una de ellas, en relación a las otras, esta comparativa la hace el autor teniendo en cuenta el futuro ecosistema de implantación.

Como se pone de manifiesto en la memoria tras el análisis de las ventajas y desventajas de las distintas arquitecturas, llegamos a la conclusión: de que todas ellas poseen ventajas e inconvenientes por lo que deberemos de implementar aquella que mejor se adapte a nuestras necesidades y entorno de despliegue.

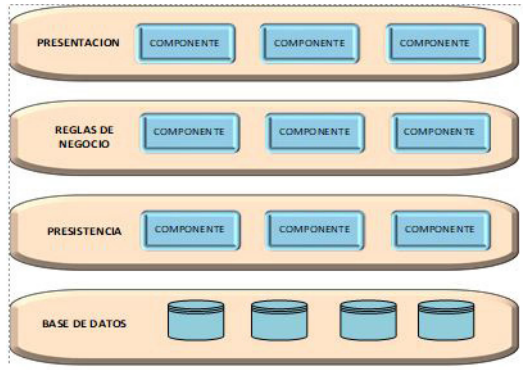


Figura 2. Arquitectura monolítica distribuida en capas

2.2. Especificaciones del sistema

Evaluando algunos requisitos como: número de usuarios del futuro sistema (aproximadamente 100 usuarios), el equipamiento de acceso (un equipo PC portátil), y los estándares de desarrollo que tiene la SGSICS actualmente.

Además de lo anterior aprovechando la experiencia en otros proyectos intentaremos que este nuevo sistema se integre con los demás, buscando una administración conjunta, un despliegue y mantenimiento lo más sencillo posible, y todo ello mejorando las actuales capacidades del correo electrónico en los aspectos principales de seguridad y funcionalidad.

La solución más idónea para este caso, dadas las circunstancias actuales de la SGSICS, que posee varios proyectos de espectro similar, sería la implementación de una aplicación Web con una arquitectura monolítica distribuida en capas que permita el acceso desde un navegador.

Acceso al sistema

En la actualidad, la SGSICS provee a cada uno de los consejeros y agregados de Interior desplegados por el mundo, de un equipo PC portátil.

La configuración del mismo permite el acceso al portal del Ministerio y en concreto al correo electrónico del dominio **@interior.es** usado en el MIR, el en la siguiente figura podemos observar la forma de acceso al portal del MIR.

El certificado electrónico de *funcionario público*, expedido por la Fábrica Nacional de Moneda y Timbre, se comprueba y valida, este método de autenticación nos habilita el acceso al portal del Ministerio.

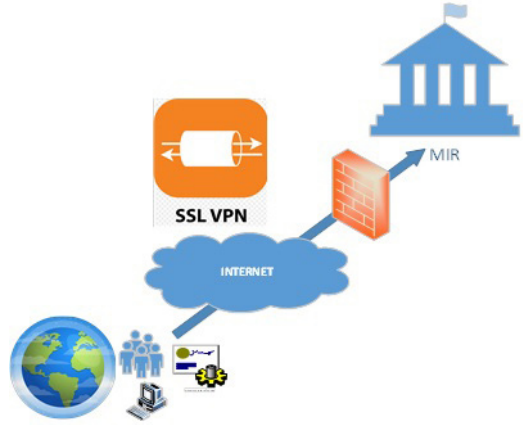


Figura 3. Acceso al Sistema de información

Arquitectura del sistema

Arquitectura lógica

En este apartado se describirá el modelo de capas que constituye la arquitectura lógica del sistema (presentación, lógica de negocio, datos). El modelo de capas se presentará mediante un diagrama esquemático. Cada una de estas capas estará formada por diferentes módulos o componentes.

El código de toda la aplicación estará hecho en el lenguaje definido según las especificaciones de la SGSICS.

Se realizará el diseño, implementación y despliegue de una aplicación basada en patrones MVC (Modelo Vista Controlador). Se trata de un patrón frecuentemente adoptado en aplicaciones web, donde:

- La vista es la página HTML y el código que provee de datos dinámicos a la página.
- El modelo es el Sistema de gestión de base de datos y la lógica de negocio.
- El controlador es el responsable de recibir las peticiones de entrada desde la vista.

La elección de Java como estándar de desarrollo de esta aplicación, se debe principalmente al conocimiento de esta plataforma de software por los futuros responsables del equipo de desarrollo y manteniendo de la SGSICS, esta elección posibilitará fácil evolución y adaptación del sistema a las futuras necesidades de los usuarios.

Además, el desarrollo con Java facilita la integración con todo el ecosistema de aplicaciones de la SGSICS y con el SGBD de Oracle.

Arquitectura física

Se presenta el particionado físico del sistema de información, representado como nodos y comunicaciones entre nodos.

Se identifican como nodos los elementos de infraestructura más significativos de la arquitectura en la que se va a implementar el sistema de información.

- Gestores de datos: Oracle
- Tipos de puesto cliente
  - APP Cliente Operador
  - APP Cliente Administrador
- Servidores:
  - Servidores de aplicaciones web
  - Servidor de correo electrónico
  - Servidores de BBDD
- Comunicaciones:
  - Clientes Web se comunicarán bidireccionalmente por https.
  - Las comunicaciones se realizarán bidireccionalmente por https.

Los criterios para diseñar la arquitectura se obtienen a partir de directrices tecnológicas o de integración, propias de la instalación, y del catálogo de requisitos del sistema de información.

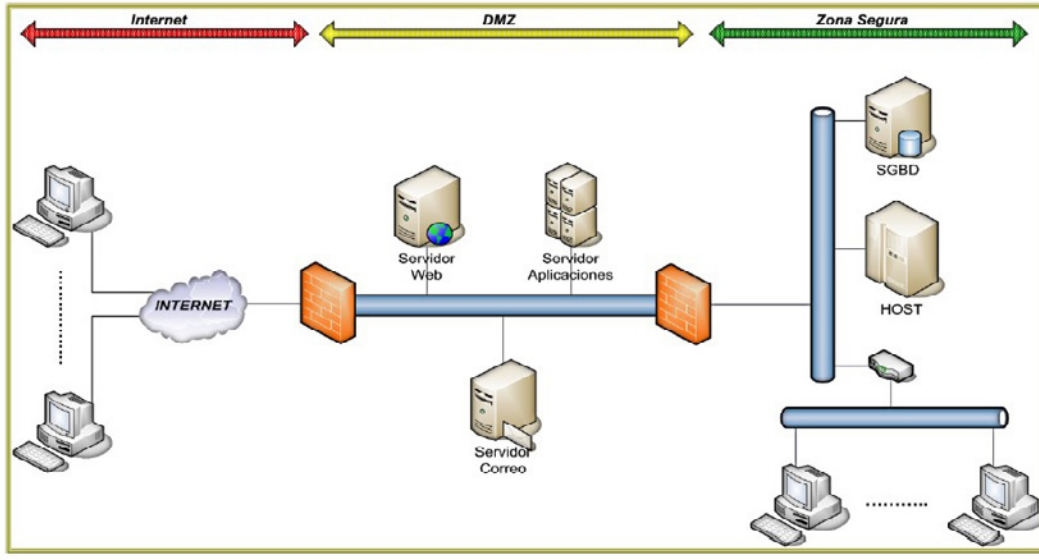


Figura 4. Diseño de arquitectura física, integración en la SGSICS

2.3. Análisis del sistema

El objetivo de esta sección es definir el alcance y análisis del Sistema de Información, que consiste en el intercambio seguro de información (ficheros) entre organismos dados de alta en el sistema, evitando así el uso de correo electrónico.

Descripción general del sistema

En el sistema aquí descrito la información estará estructurada principalmente en entidades, una entidad principal a la cual llamaremos *entidad principal* se corresponderá con las consejerías/agregadurías y organismos principales. Los usuarios accederán al contenido de los documentos desde el menú de la *entidad principal*. Se mostrará el listado de las actividades, que generalmente serán novedades sobre las que se quiere hacer algún tipo de seguimiento.

Cada *entidad principal* puede contener actividades de tipos diferentes, según su categorización, a su vez estas actividades incluirán documentos en distintos formatos, que serán clasificados y ordenados, pudiendo versionarse los documentos que se introduzcan en el sistema.

Se habilitará también un sistema de mensajería para avisar a los usuarios de que deben atender algún asunto a la mayor brevedad posible.

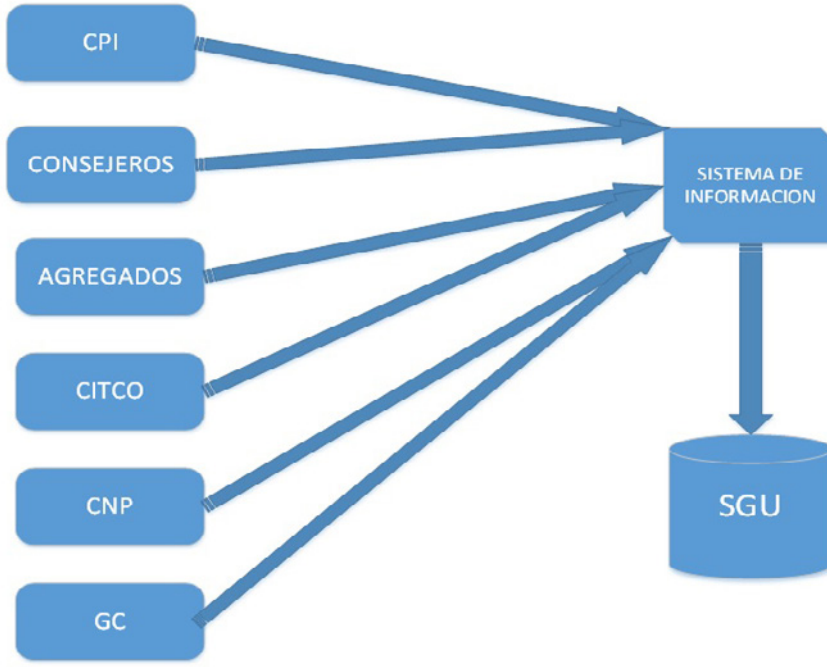


Figura 5. Interacción de los elementos y sistemas involucrados

2.4. Requisitos del sistema

En esta parte de la memoria quedan definidos los principales requisitos del sistema, tanto los funcionales que de forma específica se deberán de aplicar al futuro sistema, como los no funcionales que de forma más genérica se aplican a la mayoría de los proyectos que forman parte del Catálogo de la SGSICS [3].

3. Resultados

Como se explica a lo largo de este documento y teniendo en cuenta las circunstancias que afectan a la definición del sistema:

- Número de posibles usuarios del sistema y forma de acceso.
- Dispersión y localización de los usuarios.
- Volumen aproximado y tipo de la información que se deberá de tratar.
- Restricciones de seguridad en el almacenamiento y transmisión de la información.
- Necesidades y otros requisitos que nos transmiten los usuarios finales.
- Capacidades de la SGSICS, para la evolución y mantenimiento del sistema.

Se ha definido en el documento un sistema de información que teniendo en cuenta la relación anterior de requisitos es capaz de cubrir todas las necesidades planteadas.

4. Conclusiones

El presente trabajo ha resuelto el objetivo inicialmente identificado de ofrecer un modelo completo para una solución tecnológica alternativa a la utilización del correo electrónico del MIR, como método de intercambio de información.

Evaluadas las necesidades trasmitidas por la DGRIE, por parte de la unidad tecnológica del Ministerio con competencia en la materia SGSCIS, se ha definido en este documento una solución que cubre todos los requisitos planteados y que además añade notables mejoras en seguridad y funcionalidad respecto al anterior método.

Agradecimientos

Agradecer a todos los profesores del máster su gran implicación y profesionalidad, su predisposición para hacer de este máster lo más ameno y didáctico posible, en especial al director de este trabajo por su cercanía y guía.

No quiero olvidarme de nuestra directora del máster, que ha atendido todas nuestras dudas y peticiones con la mayor compresión y empatía, haciendo que el esfuerzo de compaginar nuestras responsabilidades diarias y el estudio haya hecho posible llevar a buen término este curso.

Muchas gracias a todos.

Referencias

[1] «BOE» Real Decreto de Estructura Orgánica del Ministerio del Interior https://www.boe.es/eli/es/rd/2020/08/04/734.

[2] «BOE» Ley 2/2014, de la Acción y del Servicio exterior del Estado https://www.boe.es/eli/es/l/2014/03/25/2/con.

[3] SGSICS, Metodología de Implantación de Proyectos y Control de Calidad, MIR.

Sistema de información corporativo de seguridad, integrado en entornos desplazados de Consejerías y Agregadurías de Interior.

Autor: Pablo Óscar Martín Ramírez
Director: Luis Álvarez Sabúcedo

Universidad de Vigo

Introducción

La intención de este trabajo es la definición de una solución tecnológica que permita la sustitución del correo electrónico del MIR como medio de transmisión de información, entre las Consejerías, Agregadurías y los Órganos Centrales del MIR.

Esta necesidad ha sido transmitida a la unidad TIC del MIR, competente en esta materia, por la Dirección General de Relaciones Internacionales y Extranjería(DGRIE),responsable de la coordinación de los funcionarios desplazados.

Mapa de despliegue de los funcionarios.

Metodología

Para la definición de un sistema que se adapte a las necesidades planteadas, se han tenido en cuenta distintos aspectosen el trabajo:

- Tecnologías posibles.
- Especificaciones del sistema.
- Análisis del sistema.
- Requisitos del sistema.

Una vez motivados y definidos los puntos referenciados anteriormente en la memoria, se concreta una solución tecnológica que cubra las necesidades planteadas y que aporte mejoras en otros aspectos como:

- Seguridad en las comunicaciones.
- Facilidad en la gestión.
- Elaboración de informes.
- Control de accesos.
- Aseguramiento de la información.

Conclusiones

El presente trabajo ha resuelto el objetivo inicialmente identificado de ofrecer un modelo completo para una solución tecnológica mas segura, y alternativa, a la utilización del correo electrónico del MIR como método de intercambio de información.

También se abordan en el trabajo las líneas estratégicas para dotar a la solución de nuevas capacidades y funcionalidades que se necesiten a futuro.

Como ejemplo de posibles mejoras se plantea la compartición e integración de los datos para su explotación en otros Sistemas de Inteligencia, del MIR o de otros Ministerios.

Agradecimientos

Agradecer a todos los profesores del Master la implicación y profesionalidad, su predisposición para hacer de este Master que se ha realizado en unas circunstancias tan difíciles, lo más ameno y didáctico posible, en especial al Director de este trabajo por su cercanía y guía.

Blockchain y otras tecnologías para la seguridad. Aplicación sobre el registro documental de información clasificada

Autor: Méndez García, Ángel (pitrinos@fn.mde.es)
Directores: Rodríguez Martínez, Francisco Javier (franjrm@uvigo.es)
Álvarez Sabucedo, Luis (lsabucedo@det.uvigo.es)

Resumen – En el Estado español, distintos organismos manejan a diario gran cantidad de información tanto de origen nacional como de otros Estados y organizaciones, que puede comprometer o afectar al propio Estado, a la seguridad nacional o a la de otros Estados, organismos u organizaciones internacionales. Por ello debe ser protegida. Esa información se conoce como información clasificada y se rige por una normativa específica.

Las tecnologías de la información y las comunicaciones (TIC) permiten en la actualidad la gestión eficaz y segura de cualquier información en soporte digital, utilizando distintas técnicas y procedimientos y, como no, personas. La normativa nacional para la protección de la información clasificada, recogida en las Normas de la Autoridad Nacional para la protección de la información clasificada, exige un tratamiento específico para ese tipo de información, conforme a una serie de procedimientos y requisitos, depurados y establecidos tras muchos años de experiencia y mejora continua.

Dado que la información clasificada exige un especial cuidado en lo relativo a su seguridad, a que cada vez más la información se maneja en soporte digital, y a que, como se ha mencionado, las TIC ofrecen garantías suficientes de seguridad a la información clasificada, los órganos responsables de su manejo y custodia deberían disponer de herramientas basadas en las TIC que garanticen la gestión segura y la protección de este tipo de información. Pero la realidad es muy distinta. Los servicios de protección de información clasificada no disponen de herramientas TIC apropiadas.

La normativa exige que esas herramientas informáticas estén aprobadas por la Oficina Nacional de Seguridad (responsable principal en la estructura nacional de protección de la información clasificada) para el manejo de este tipo de información.

Este trabajo plantea una posible solución, analizando distintas TIC disruptivas, emergentes o maduras como puedan ser *blockchain*, la criptografía visual, o el *Data Loss Prevention* entre otras.

Palabras clave – Información clasificada, blockchain, criptografía visual, Smart Contracts, gestión documental.

1. Introducción

1.1. Antecedentes

Todas las naciones del mundo han manejado históricamente y con mayor o menor acierto, información que por su valor debía estar al alcance de muy pocos y que por ello se protegía de una u otra forma. Era información clasificada (en adelante, se utilizará indistintamente la denominación o la abreviatura IC).

Los organismos y estructuras del Estado español, incluidas las Fuerzas Armadas (en adelante FAS) manejan a diario gran cantidad de esa IC: contiene datos que pueden comprometer la seguridad nacional o la de organizaciones internacionales. Por ello debe ser protegida.

La normativa nacional para la protección de la IC exige que este tipo de información se gestione y trate de una manera específica, conforme a unos procedimientos y requisitos, depurados y mejorados tras muchos años de experiencia y mejora continua.

En España existe una estructura nacional, consistente en una serie de oficinas, responsables de custodiar y proteger ese tipo de información. Estas Oficinas se conocen como servicios de protección de información clasificada (SPIC).

1.2. Objetivo

La motivación de este trabajo arranca de la percepción de un potencial problema por falta de soluciones TIC en lo relativo a la trazabilidad, registro y manejo de la IC en los SPIC. Esta potencial debilidad fue identificada en el curso de la relación laboral normal del autor con estas oficinas.

Este trabajo pretende estudiar el problema en profundidad y proponer posibles soluciones a las necesidades que tiene la estructura nacional de protección de la IC de manejar, registrar y controlar la citada información, aprovechando los avances en distintos campos de las TIC y otras tecnologías que podrían ser disruptivas en este campo.

2. Desarrollo

2.1. Definiciones previas

Información clasificada es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad entendiéndose como información todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

La información puede estar clasificada en distintos grados en función del perjuicio que puede ocasionar su difusión no autorizada. En España los grados reconocidos son *secreto, reservado, confidencial y difusión limitada*.

A su vez, se debe distinguir entre información clasificada española o extranjera (propiedad de otros países u organizaciones internacionales, como OTAN o Unión Europea).

Documentación clasificada es cualquier soporte que contenga información clasificada registrada, en cualquier formato físico (escrito, impreso, cinta, fotografía, mapa, dibujo, esquema, nota, soporte informático, óptico o vídeo, etc.). La más tradicional es en formato papel, aunque cada día se hace un uso más extensivo de los soportes informáticos.

Es decir, que la IC no se considera documentación clasificada hasta que no sufre el proceso de registro. Es un acto que le infiere una serie de características que obligan a su debido tratamiento. Esto significa que hay que garantizar la confidencialidad, integridad y disponibilidad de la citada información. A su vez, la trazabilidad y el no repudio son relevantes.

2.2. Normativa y estándares

La normativa relativa a las TIC es numerosa y profusa. Partiendo de la normativa ISO (ISO/IEC 27000:2018), pasando por el estándar Common Criteria para productos software, el estándar TIA 942 para la instalación de centros de datos o Data Center.

A su vez, para la información clasificada existe también numerosa normativa a nivel nacional e internacional. Comenzando por la Ley de Secretos Oficiales, siguiendo con las Normas de la Autoridad Nacional para la protección de la información clasificada, las guías CCN-STIC, y llegando a las normas internas del Ministerio de Defensa como las Normas de seguridad de la información para elaboración, clasificación, cesión, distribución y destrucción de información en el Ministerio de Defensa.

Toda esta normativa en su conjunto impone una serie de requisitos y restricciones al manejo y registro de la información clasificada. Cualquier red, sistema informático o dispositivo de almacenamiento de información clasificada en soporte digital que maneje ese tipo de información debe cumplir unos estrictos protocolos de seguridad tanto a nivel de seguridad física, de emanaciones electromagnéticas, seguridad del personal que los utiliza y seguridad documental, lo que acaba perfilando el estudio realizado en este trabajo sobre las tecnologías TIC que podrán o no implementarse para mejorar la situación actual de los SPIC.

2.3. Tecnologías disruptivas y emergentes aplicables a la protección de la información clasificada.

En este trabajo se analizan las siguientes tecnologías:

- Blockchain
- Criptografía Visual
- Software y hardware de cifrado offline
- Tecnología de impresión con tinta ultravioleta
- Borrado seguro de datos
- Prevención de pérdida de datos (Data Loss Prevention)
- Cifradores hardware

2.4. Trabajos relacionados. Iniciativas relevantes existentes

Existen numerosos artículos y trabajos relacionados con la gestión documental, las arquitecturas de seguridad en redes de comunicaciones, y tecnologías como blockchain, Data Loss Prevention, o criptografía visual.

El estado del arte en estas tecnologías y arquitecturas es muy diverso y se encuentra en continua evolución. Se ha procedido en este trabajo a una revisión de distintos artículos académicos e informativos en fuentes como IEEE.org, ResearchGate.net, y fuentes abiertas de Internet.

No obstante, *no se han encontrado trabajos relacionados con el manejo de la información clasificada*, quizás por su carácter sensible y por ello los trabajos que puedan existir al respecto no sean de acceso público.

En lo referente a iniciativas relevantes existentes, se exponen en el trabajo varios proyectos interesantes, como el Proyecto Cert Chain de la Armada para la implementación de una red blockchain que permita supervisar y controlar documentación de mantenimiento que implique desmontaje de los elementos de los nuevos submarinos S-80, para posteriormente comprobar que los elementos mantienen la certificación previa.

Otro proyecto de alto interés es la herramienta Libro de Registro, proyecto liderado por la Oficina Nacional de Seguridad (ONS) del CNI, que pretende subsanar el problema existente en los SPIC nacionales respecto de la gestión y registro de documentación clasificada. Si bien el proyecto es interesante, la herramienta se ha diseñado para su uso en terminales aislados, y no en una red de Oficinas, lo que inicialmente le resta atractivo.

Otras herramientas o soluciones tecnológicas relevantes basadas en iniciativas del Centro Criptológico Nacional son, por ejemplo, la herramienta CARLA, que supone un avance en la protección del dato, permitiendo una mejora notable de la trazabilidad de documentos. Entre sus actuales limitaciones está que solo se autoriza su uso para redes que manejen

información clasificada nacional y de grado difusión limitada. Un desarrollo de la herramienta para su uso en redes que manejen información clasificada hasta secreto supone un interesante desafío y mejorará la seguridad en una futura red informática entre los distintos SPIC.

3. Resultados y discusión

Resultado de un análisis de las diversas tecnologías, sus posibilidades y su aplicabilidad, se presenta a continuación una tabla con los resultados, para cada tecnología y tipo de implementación resultante del trabajo.

Se quiere destacar en este punto que, si bien se trata de una interpretación del autor basada en su conocimiento y el estado actual de desarrollo de muchas de esas tecnologías, la tabla no se debe considerar estática, ya que en el futuro muchas de las soluciones que se descartan aquí podrían perfectamente ser de aplicación.

Como posible discusión, se considera que los fabricantes de varios de los productos y herramientas expuestas en este trabajo, deberían llevar a cabo el I+D+I necesario para aportar mejoras a sus soluciones de forma que permitan su uso en redes de información clasificada de grado hasta secreto y ámbitos nacional, OTAN y UE.

ANÁLISIS DE APLICABILIDAD DE LAS DISTINTAS TECNOLOGÍAS ANALIZADAS

Herramienta	Tecnología	Aplicable	Observaciones
Blockchain	Trazabilidad permanente	SI	Red federada. Uso de oráculos y Smart Contracts viable. En continuo desarrollo de nuevas funcionalidades y amplio soporte.
Criptografía visual	Autenticación/ Confidencialidad	SI	Uso para autenticación y no repudio.
CARLA (Sealpath)	Protección del dato	NO	Limitado a IC difusión limitada nacional. Solo S.O. Windows y limitado soporte de protección a ficheros. Requiere mayor desarrollo.
McAfee DLP	Data Loss Prevention	SI	Garantiza la seguridad de los datos dentro de la red e impide la exfiltración no autorizada de información clasificada. Tecnología madura y con soporte.
Aplicación Libro de Registro (ONS)	Libro de registro documental	NO	Instalación on premise. No permite su uso en red. No compatible con otras tecnologías como blockchain. Requiere mayor desarrollo (uso en red, compatibilidad con BC, DLP, etc.)
BLANCCO File eraser/Drive eraser	Software de borrado seguro	SI	Software aprobado por CCN. Deberá ser acreditado para uso con IC SECRETO o equivalente.
Solpheo Suite	Herramienta de gestión documental	NO	Desarrollo enfocado al ámbito empresarial, centrado en posibilitar teletrabajo.

ANÁLISIS DE APLICABILIDAD DE LAS DISTINTAS TECNOLOGÍAS ANALIZADAS

Herramienta	Tecnología	Aplicable	Observaciones
Herramienta Shaadow	Herramienta de no repudio	SI	Se desconoce la tecnología subyacente. Solo aplicable a ficheros pdf. Contratado actualmente por el EMAD.
Software EP-880	Cifra offline de ficheros	SI	Garantiza la confidencialidad, autenticidad y el no repudio de la IC. Actualmente solo se autoriza su uso para cifrar IC nacional de grado difusión limitada.
Cifradores HARDWARE	Cifra online de datos	SI	Exigido por normativa para redes que manejan IC. Pendiente de disponer de cifradores para todos los ámbitos
GPG4Win/ GnuPG	Criptografía de clave pública (cifra offline)	SI	Alternativa a EP880. Garantiza la confidencialidad, autenticidad y el no repudio de la IC. Pendiente de certificación por parte del CCN para su uso con IC secreto o equivalente.
PKI	Criptografía de clave pública (cifra offline)	SI	Requiere de infraestructura de AC, y certificados validados (FNMT)
Dispositivo USB cifrador EP852	Cifra offline de ficheros	SI	Exigido por normativa para transferencia o almacenamiento cifrado de ficheros.
Tinta UV	Autenticación/ no repudio	SI	Utilización en tarjetas de credenciales ocultas para acceso a las sesiones de los terminales, o para el marcado invisible de documentos clasificados.

Tabla 1. Comparativa de tecnologías aplicables.

4. Conclusiones

La investigación inicial demuestra la necesidad que tiene la ONS y los OOC del ámbito de las FAS de disponer de una red segura para el intercambio de IC.

Existen diversas tecnologías, algunas de ellas disruptivas y otras innovadoras, que pueden aumentar la seguridad de la citada red, garantizando en gran medida la disponibilidad, integridad y confidencialidad de esa IC. Es innegable que ciertas soluciones empleadas en el momento actual son susceptibles de mejora en ciertos aspectos que pueden considerarse críticos.

A su vez, otras tecnologías garantizan la trazabilidad como blockchain. No obstante, para la implementación de todas las tecnologías aplicables contempladas en este trabajo y que mejoraran aspectos claves, será preciso un proyecto que permita integrarlas en el ecosistema actual del Ministerio de Defensa para garantizar la sostenibilidad e interoperabilidad con otras herramientas en uso actualmente.

Dados los requisitos de seguridad que debe cumplir una aplicación software para poder manejar IC y servir de herramienta de registro documental, es muy recomendable diseñar y crear una aplicación desde cero. Del mismo modo, parece razonable sugerir una arquitectura de red basada en la seguridad, liderada por el CNI o la ONS por su parte, y el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, por parte del Ministerio de Defensa. Como complemento, otras autoridades de la AGE pueden participar del proyecto. El punto de partida es el software Libro de Registro de la ONS.

Blockchain se ha mostrado como la tecnología más disruptiva y que más valor aporta en lo tocante a trazabilidad, inalterabilidad y seguridad. Se ha demostrado que existen iniciativas en el ámbito militar de gran interés basadas en ella y que mejorarán en un futuro cercano las operaciones militares, la gestión logística, y la seguridad de las redes militares ya sean para propósito general (sin clasificar) como de mando y control (clasificadas). La evolución y maduración que ha experimentado en otros ámbitos como la logística empresarial o la DeFI (decentralized finance) puede aprovecharse en este ámbito.

Este trabajo demuestra que blockchain tiene aplicación práctica en la gestión y manejo de IC. No se han encontrado estudios previos específicamente sobre este ámbito. Por eso este TFM abre una nueva línea de investigación en el ámbito militar que no se había abordado previamente.

Por último, hay que tener en cuenta que la normativa, al igual que las tecnologías, está sujeta a cambios. Durante el desarrollo de este trabajo se ha producido un cambio sustancial en la normativa de aplicación a nivel nacional. En 2022 se va a modificar la NS/05 contenida en las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, y se sustituirán varias guías CCN-STIC por unas nuevas Instrucciones Generales y otras guías denominadas ahora Recomendaciones, adaptando todo el conjunto al Esquema Nacional de Seguridad (ENS).

Independientemente de lo anterior, la metodología del análisis realizado hace que este trabajo mantenga su valor. Surgen nuevos estándares, pero se mantiene.

Blockchain y otras tecnologías para la seguridad. Aplicación sobre el registro documental de información clasificada.

Autor: Ángel Méndez García

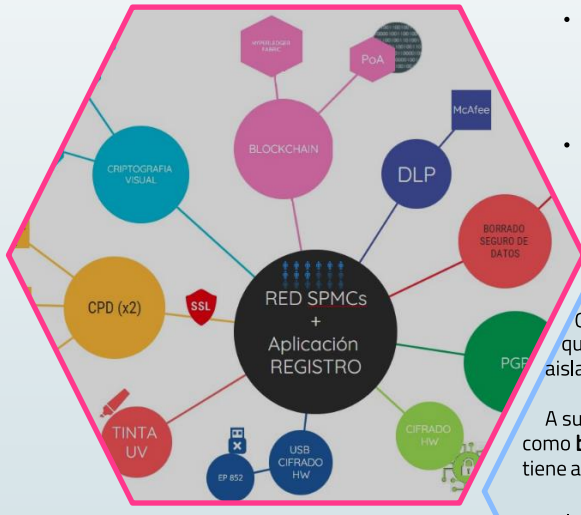
Universidad de Vigo

Directores: Francisco Javier Rodriguez Martínez, Luis Álvarez Sabucedo

Introducción

Esta trabajo trata de resolver el problema de gestión y almacenamiento de información clasificada de los órganos de control y servicios de protección de materias clasificadas en las Fuerzas Armadas. Se propone un modelo de software para gestión de documentación clasificada conforme a la Normativa en vigor, tratando de que la herramienta incorpore las tecnologías más seguras y actualizadas posibles aplicables en los Sistemas de Información y las Telecomunicaciones, con el fin de dar una solución a un problema que todavía no había sido planteado ni resuelto.

Palabras clave: información clasificada, gestión documental, protección, Blockchain, criptografía visual extendida.



Resultados

Se establecen como tecnologías candidatas para el desarrollo de una red aislada segura y una aplicación software de gestión documental las siguientes:

Blockchain Criptografía Visual Tinta Ultravioleta
Data Loss Prevention PKI Dispositivo USB EP852
Software de borrado seguro de datos
Herramienta Shaadow® de no repudio (atribución)
Software de cifra offline EP880 y GPG4Win/GnuPG
Cifradores hardware certificados por el CCN

Metodología

- Encuesta previa a órganos de control. Nivel nacional.
- Revisión sistemática no formal.
- Investigación para determinar la necesidad de la herramienta informática.
- Investigación de la posibilidad de implementar tecnologías como blockchain, Data Loss Prevention, y Criptografía Visual para aumentar la seguridad en la protección de la información clasificada, y la gestión documental de ese tipo de información.
- Propuesta de solución.

Conclusiones

Existen diversas tecnologías disruptivas, y Otras emergentes, innovadoras o maduras que pueden aumentar la seguridad de una red aislada segura de gestión de información clasificada.

A su vez, otras tecnologías garantizan la trazabilidad, como **blockchain**. Este trabajo demuestra que *blockchain* tiene aplicación práctica en la gestión y manejo de IC.

Para la implementación de todas las tecnologías aplicables contempladas en este trabajo, será preciso un proyecto que permita integrarlas en el ecosistema actual del Ministerio de Defensa que garantice la sostenibilidad e interoperabilidad con otras herramientas en uso actualmente.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Estudio y propuesta de uso del lenguaje ArchiMate® para generación de arquitecturas NAFv4 en el Ministerio de Defensa

Autor: de Pedro Cibanal, Manuel Ángel
(mdepcib@ea.mde.es; mdepcib@gmail.com)
Directores: Rodríguez Martínez, Francisco Javier (franjrm@uvigo.es)
y Villalba Madrid, Antonio (avilmad@fn.mde.es)

Resumen – Si bien en un principio las arquitecturas vienen ligadas al modelado de software y tecnología su alcance es mucho mayor. La disciplina arquitectura empresarial define una arquitectura como «una descripción formal de un sistema, la estructura de sus componentes, sus interrelaciones, y los principios y guías que gobiernan su diseño y evolución a lo largo del tiempo». Sin que el sistema tenga que ser necesariamente software o hardware, podemos extender su significado por ejemplo a una organización o a un proyecto, lo que ofrece una aproximación holística para describir de una manera diferente multitud de conceptos.

Una arquitectura, a través de puntos de vista estandarizados en un esquema, sirve de lengua franca para proporcionar una manera inequívoca de describir esos conceptos complejos del mundo real.

El Ministerio de Defensa consciente de esta aproximación establece en su Plan Estratégico CIS/TIC (PECIS) que se debe de seguir un marco de referencia para el desarrollo e implantación de arquitecturas en el departamento. Este marco de referencia se basa fundamentalmente en el marco de arquitecturas de la OTAN (NATO Architecture Framework, NAF).

Las arquitecturas sobre NAF pueden ser creadas con el lenguaje ArchiMate®. Este es un lenguaje estándar, independiente y abierto, que puede ser usado de manera polivalente como metamodelo para la realización arquitecturas. Patrocinado por The Open Group®, es compatible con diferente software comercial y es usado como estándar por la OTAN para el desarrollo de sus arquitecturas.

Tras un análisis del estado del arte del uso de arquitecturas, del marco de arquitecturas OTAN (NAFv4) y del lenguaje ArchiMate® se propondrá el uso de dicho lenguaje de manera práctica en diferentes

casos de uso que contemplan desde la migración de arquitecturas de NAFv3 a NAFv4 o la creación de nuevas arquitecturas sobre NAFv4, hasta propuestas de uso como apoyo a actuaciones del Plan de Acción para la transformación digital del Ministerio de Defensa. Para todos los casos de uso se han creado ficheros XML que contienen artefactos arquitectónicos reutilizables para todo tipo de futuras arquitecturas de negocio, información, software, tecnológicas o de proyectos.

Hasta ahora el Ministerio de Defensa solo ha generado únicamente arquitecturas tecnológicas y en formato documental apoyado por herramientas ofimáticas. Con la propuesta de uso de ArchiMate® se proporciona un metamodelo que relaciona todas las entidades generando un fichero con un formato intercambiable y reutilizable al 100 %, lo que estandariza y genera una única fuente de verdad de conceptos. Esta única fuente de verdad facilita no tener que redactar un concepto cada vez que se usa, lo que agiliza la creación de puntos de vista de las partes interesadas y permite a la organización ser ágil, eficiente y eficaz.

Palabras clave – Arquitectura, arquitectura empresarial, ArchiMate®, NATO Architecture Framework Versión 4, NAFv4, TOGAF

1. Introducción

1.1. Capacidad, planeamiento basado en capacidades y marcos de arquitecturas civiles

Las Fuerzas Armadas (FF.AA. o FAS) son un tipo de *negocio* muy peculiar ya que un ejército debe entrenarse y prepararse de manera permanente para hacer cosas que quizá nunca tenga que hacer. Las FAS en tiempo de paz deben desarrollar la capacidad de alcanzar algún objetivo específico aún no declarado y prepararse para el tiempo de guerra.

A esta premisa se le une que debe de obtener recursos de varias organizaciones en tiempo de paz, y en tiempo de guerra, para lograr algún(os) objetivo(s) específico(s).

Esto puede explicar por qué las *capacidades* y el *planeamiento basado en capacidades* ocupan un lugar tan destacado en la defensa.

Por otra parte, las FF.AA. son como otras empresas en muchos aspectos ya que todos los ejércitos realizan algunas actividades empresariales de manera regular. Necesitan reclutamiento, nóminas y otras funciones de back office/administración/apoyo, organizar y lleva a cabo programas regulares de formación, etc.

De un tiempo a esta parte en el mundo civil la disciplina arquitectura empresarial ha proporcionado unos esquemas para organizar las actividades de negocio de organizaciones y sus relaciones con las TIC que apoyan a sus procesos principales de negocio. A través de diferentes representaciones agrupadas (también llamadas vistas de las partes interesadas) se crea lo que se denomina una arquitectura que ayuda a organizar conceptos a las empresas. Dichas arquitecturas pueden seguir diferentes tipos de esquemas dependiendo del tipo de negocio, estos esquemas son los denominados marcos de arquitecturas.

Por tanto, la mayor parte de los marcos de arquitectura relacionados con Defensa no son propios de las FAS, sino que son en general similares a los sistemas que apoyan las actividades de cualquier otra empresa civil. Tiene un lugar destacado el marco civil de arquitecturas de The Open Group (TOGAF) cuyo uso está muy extendido pero que no proporciona todos los puntos de vista de interés para las organizaciones relacionadas con Defensa.

Es por ello que las organizaciones de Defensa han creado diferentes marcos de arquitecturas, que complementan a dicho marco de arquitectura civil, para apoyar principalmente la generación de *capacidades* y el concepto de *planeamiento basado en capacidades*.

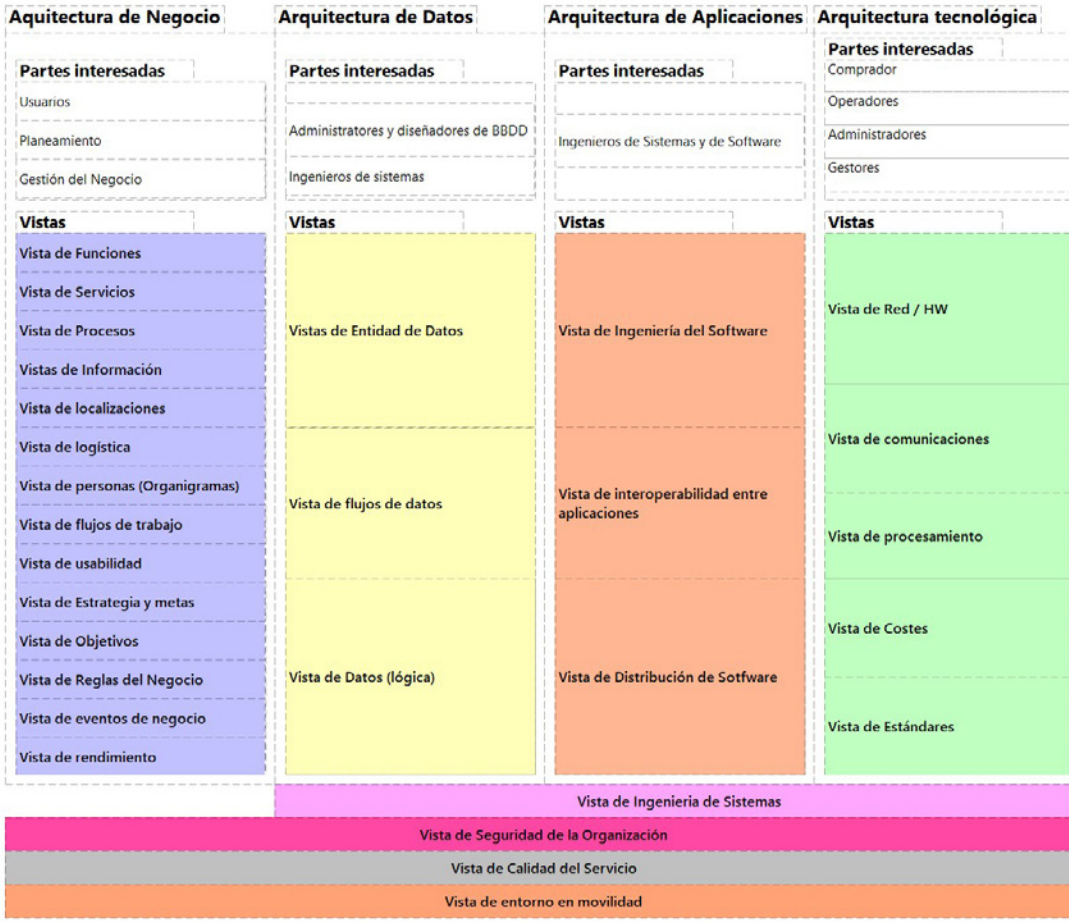


Figura 1. Marco de arquitecturas Open Group (The Open Group Architecture Framework -TOGAF)

2. Desarrollo

2.1. Marco de arquitecturas OTAN – NATO Architecture Framework – NAF

La OTAN siguiendo los estándares y buenas prácticas de TOGAF usa un marco de arquitecturas para la Defensa llamado NATO Architecture Framework (NAF). Este marco de arquitecturas, actualmente en su versión 4, ha ido evolucionando con el tiempo. Sus orígenes se remontan al marco de arquitecturas C4ISR, el marco de arquitecturas del Departamento de Defensa de EE.UU. (DoDAF), el marco de arquitecturas del Ministerio de Defensa de Reino Unido (MoDAF) y el marco de arquitecturas de las Fuerzas Armadas canadienses DNDAF. NAF en su actual versión 4 proporciona las siguientes nuevas características:

- Una metodología para creación/modificación de arquitecturas.
- Una tabla (o grid) para organizar puntos de vista.
- La adopción de metamodelos comerciales entre los que se incluye ArchiMate®.

En la nueva tabla o grid las filas representan los temas de interés y las columnas los aspectos a tener en cuenta. Esta tabla ayuda a los arquitectos a ubicar puntos de vida de las diferentes partes interesadas según el esquema que se muestra en la figura 2.

Figura 2: Marco de arquitecturas OTAN versión 4 (NATO Architecture Framework -NAFv4)

Los puntos de vista puede ser realizados con cualquier tipo de herramienta ya sea gráfica (imágenes, tablas), ofimática (documentos en MS Word, MS PowerPoint o Adobe PDF), lenguaje de bases de datos (UML), etc. Sin embargo, NAF recomienda la utilización de metamodelos, estos son un conjunto organizado y relacionado de conceptos reutilizables. Los metamodelos recomendados por NAF son el Unified Architecture Framework Domain Meta Model-(UAF-DMM®) y ArchiMate®. Este trabajo se centra en el estudio y propuesta de ArchiMate®.

2.2. Lenguaje de arquitectura empresarial Archimate ®

ArchiMate® es un estándar de The Open Group que se usa como lenguaje de modelado de código abierto e independiente para su uso en la disciplina de arquitectura empresarial. Su principal característica es que permite describir, analizar y visualizar las relaciones entre los dominios de negocio de una manera inequívoca y reutilizable.

Existen otros estándares de modelado ampliamente utilizados entre los que destacan:

- UML proporciona un gran nivel de detalle, y una técnica de modelado adicional para:
  - Soporte detallado de modelado de datos.
  - Modelado arquitectónico detallado de software.
- BPMN proporciona un soporte completo de modelado de procesos de negocio.

Complementado estos, ArchiMate® se dedica en la arquitectura empresarial a un nivel grueso (alto) de granularidad (menos detalle, pero abarcando más conceptos) y por lo tanto es más flexible.

Muchos de los conceptos de ArchiMate® provienen de BPMN (aplicados al modelado de procesos) y UML (aplicados al modelado de aplicaciones e infraestructura). Es más, es fácil conectar diagramas ArchiMate® con descripciones más detalladas de UML o de BPMN, pero también con estándares como modelos de negocio (Business model – BMC), modelos de motivación (BMM), cuadros de mando integral (Balanced Scorecard – BS), Canvas de modelo de negocio, modelos de datos (ERD), lenguaje de modelado de sistemas (Systems Modeling Language – SysML), etc.

El núcleo del lenguaje ArchiMate® define una estructura de elementos genéricos y sus relaciones, que pueden además especializarse en diferentes capas. Como puede verse en la figura 3, dentro del lenguaje de ArchiMate® se definen tres capas principales (negocio, aplicación y tecnología) junto con las capas de estrategia, implementación/migración y motivación que complementan a las principales.

De manera alineada con el paradigma *As a Service*, la relación más importante entre las capas principales está formada por las relaciones de *servicio*, que muestran cómo los elementos de una capa son servidos por los servicios de otras capas. Se debe destacar que los servicios no solo tienen que servir a elementos de otra capa, sino que también pueden servir a elementos de la misma capa.

Un segundo tipo de vínculo importante lo forman las relaciones: los elementos de las capas inferiores pueden realizar/acceder/condicionar elementos comparables en las capas superiores; por ejemplo, un *objeto de datos* (capa de aplicación) puede formar parte de un *producto de información* (capa de negocio), o estar formado a partir de un *artefacto* (capa de tecnología) o ser el resultado de un *proceso de una aplicación* (capa de aplicación).

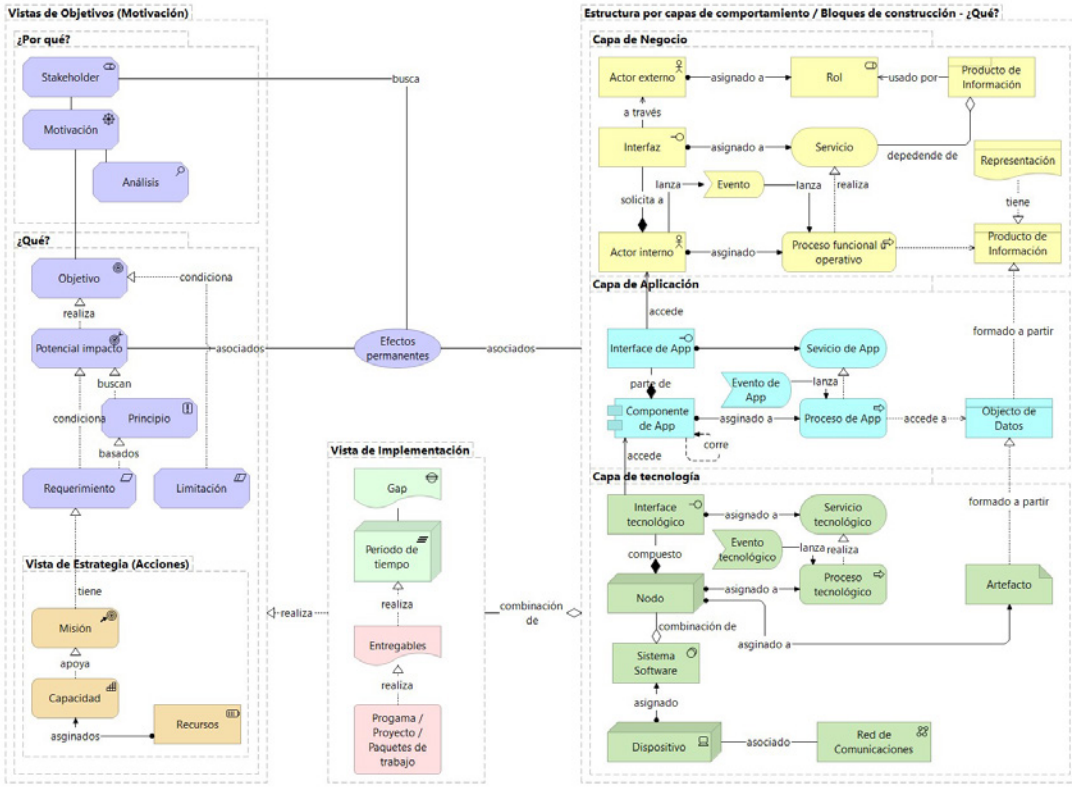


Figura 3. Metamodelo y capas del lenguaje ArchiMate®

2.3. Propuesta de uso del lenguaje Archimate® para la generación de arquitecturas NAFv4

La OTAN en su normativa (NATO Enterprise Architecture Policy), viendo las posibilidades de los marcos de arquitectura y apoyándose en concreto el de NAF, define diferentes niveles de arquitecturas dentro de su organización: nivel empresarial, nivel de capacidad y nivel de proyecto. Todas ellas pueden tener en mayor o menor medida elementos de negocio, información, aplicaciones o tecnología y puntos de vista basados en otros marcos de arquitecturas como por ejemplo el de TOGAF.

Lo interesante de todos estos esquemas, marcos de arquitecturas y vistas de las partes interesadas es que se pueden estandarizar y reutilizar de diferentes maneras ahorrando tiempo y esfuerzo. De manera adicional, siguiendo los esquemas y marcos de arquitecturas nos aseguramos de no dejar algún aspecto sin tratar que pueda provocar problemas a largo plazo, por no haber tenido en cuenta dicho aspecto desde el principio.

Las arquitecturas tienen muchos usos que las otorgan un gran valor como herramientas y pueden ser usadas a diferentes niveles, destacan los siguientes:

- A nivel empresarial: para la toma de decisiones que mejore:
  - El uso de los RR.HH.
  - El despliegue de activos de la organización.
  - Las inversiones.
  - La identificación de responsabilidades y asignación de funciones.
  - La estructuración de actividades en proyectos.
- A nivel de proyecto: para identificar los requerimientos y recursos operacionales para alcanzar los objetivos.
- A nivel de capacidad: para gestión de programas de adquisición y desarrollo de sistemas con garantía de interoperabilidad con futuro entorno de uso.
- A nivel de simulación y modelado del planeamiento operacional: en el contexto militar a través de la implementación de hilos de misión y posibles escenarios de actuación operativa (Mission Threads o Hilos de Misión).
- A nivel de gestión de portfolios: identificando los objetivos y metas a alcanzar o satisfacer con los activos de que se disponen y cómo gestionarlos.

Teniendo en cuenta los anteriores usos, si bien la arquitectura global CIS/TIC del Ministerio de Defensa establece que el uso de arquitecturas basadas en NAF será el medio para la gestión de servicios CIS/TIC del departamento, aún no se ha definido el uso de ningún lenguaje de arquitecturas que facilite el uso del marco de arquitecturas OTAN ni un repositorio de artefactos XML reutilizables.

Se propone con este TFM empezar a usar el lenguaje ArchiMate® no solo para arquitecturas que tengan que ver con medios CIS/TIC, sino para su uso en todas las posibilidades que ofrece la disciplina de arquitectura empresarial y en concreto sobre el marco NAFv4.

Para ello durante el desarrollo del TFM se han realizado de manera practica el modelado de diferentes vistas y casos de uso que van desde la migración de una arquitectura en formato NAFv3 (en documento sin información reutilizable directamente), la creación de nuevas arquitecturas NAFv4 hasta el uso de vistas para apoyar actuaciones del Plan de Acción del Ministerio de Defensa para la transformación digital. Para todos los casos de uso se han creado ficheros XML que contienen artefactos arquitectónicos reutilizables para todo tipo de futuras vistas y arquitecturas de negocio, información, software, tecnológicas, proyectos, hilos de misión, etc.

3. Resultados y discusión

El objetivo principal del presente TFM ha sido analizar, organizar y comunicar las ventajas del uso del lenguaje ArchiMate® en el Ministerio de Defensa.

Siguiendo la estela del camino que ha iniciado la OTAN con la disciplina arquitectura empresarial, basada en estándares de la industria como TOGAF, se propone que de ahora en adelante todos los recursos arquitectónicos que se generen en el Ministerio de Defensa avancen de manera alineada con esta disciplina creando artefactos reutilizables e interconectados en formato XML bajo el marco de arquitecturas OTAN NAFv4 para generación de arquitecturas tecnológicas, de software, de información, de hilos de misión, de negocio y de proyectos y de todos aquellos usos que facilita la disciplina arquitectura empresarial en OTAN.

4. Conclusiones

Todas las organizaciones son entidades complejas y el Ministerio de Defensa no es una excepción.

Representar el conocimiento de una organización resulta ser una tarea difícil, ya que requiere que múltiples conceptos alineados, de forma coherente e integrada, y no como un conjunto de elementos independientes y sin relación entre sí.

El hecho de no ofrecer una representación integrada de este tipo contribuye a la materialización heterogénea y desalineada de los recursos, lo que dificulta la detección de problemas y mejoras, así como la capacidad de evaluar la organización en su conjunto.

Podemos señalar que el uso del lenguaje de arquitectura empresarial ArchiMate® y el marco de arquitectura OTAN (NATO Architecture Framework) posibilitan presentar y reutilizar información de una manera innovadora que supera las limitaciones de la documentación, la comunicación tradicional y la representación de datos, información y conocimiento basadas hasta ahora en ficheros con formato MS Word o Adobe PDF.

La conclusión más relevante de este estudio es que la propuesta de uso de ArchiMate® y su esquema de recursos interconectados aseguran una coherencia y una presentación de información inequívoca. Esto evita el uso de largas redacciones que, en numerosas ocasiones cuando se repiten conceptos, omiten información, son ambiguas o tienen equívocos al no tener como origen una única fuente de verdad.

La identificación y adopción de la disciplina de arquitectura empresarial puede considerarse, por tanto, como un paso fundamental para cualquier organización que quiera estar preparada para actuar en lugar de reaccionar y poder comprender si sus elementos están alineados de una manera

holística. Su adopción permite no solo comunicar información a las partes interesadas, sino gestionar la tecnología para ponerla al servicio del negocio facilitando la transición hacia una organización *data driven*, en la que el acceso a la información está gobernado de una manera coherente actuando como un facilitador en la toma de decisiones.

Para finalizar este punto y mostrar el poder de comunicación de ArchiMate® se muestra en la figura 4 un punto de vista que comunica a las diferentes partes interesadas operativas de las FAS como los Servicios CIS/TIC de la Infraestructura Integral de la Información (I3D) del Ministerio de Defensa apoyan al jefe de Estado Mayor de la Defensa (JEMAD) y a los diferentes comandantes de su estructura operativa (Mando Operativo Terrestre —MOT—, Mando Operativo Marítimo —MOM—, Mando Operativo Aeroespacial —MOA— y Mando Operativo Ciberespacial —MOC—) en el planeamiento estratégico y operativo de una misión.

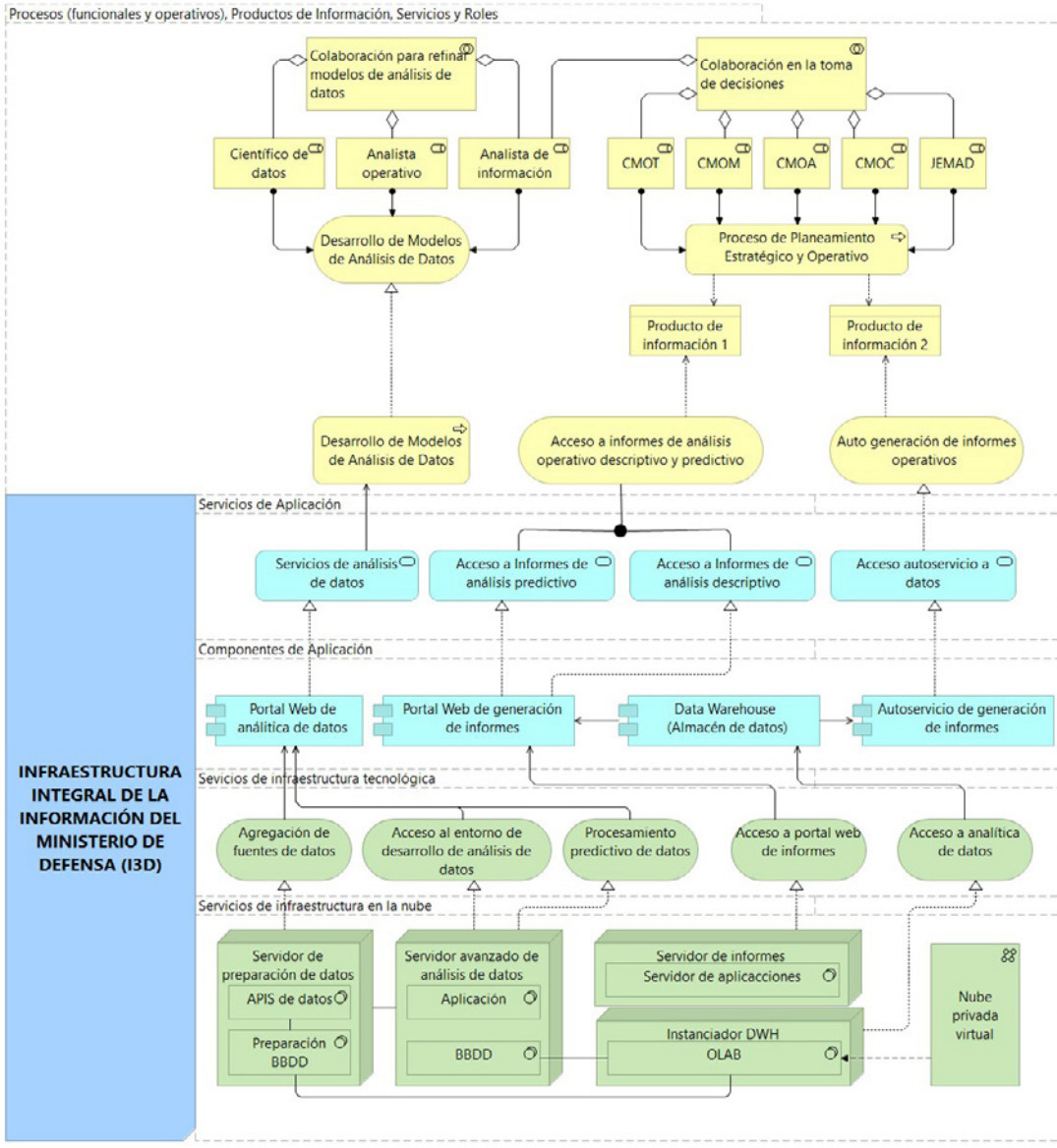


Figura 4. Metamodelo y capas del lenguaje ArchiMate®

Referencias

[1] Ministerio de Defensa, (2017), «Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa». [En línea]. Available: https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/o/politica_de_los_sistemas_y_tecnologias_informacion.pdf.

[2] Ministerio de Defensa, (2018), «Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (PECIS)». [En línea]. Available: https://publicaciones.defensa.gob.es/media/downloadable/files/links/p/l/plan_estrat_gico_de_los_sistemas_pecis_.pdf.

[3] NATO Consultation Command and Control Board – Architecture Capability Team, (9 2020), «NATO Architecture Framework, Version 4». [En línea]. Available: https://www.nato.int/cps/en/natohq/topics_157575.htm.

[4] The Open Group, «The Open Group» [En línea]. Available: https://www.opengroup.org/.

[5] Ministerio de Defensa, (2015), «Plan de Acción del Ministerio de Defensa para la Transformación Digital». [En línea]. Available: https://publicaciones.defensa.gob.es/plan-de-accion-del-ministerio-de-defensa-para-la-transformacion-digital-libro-pdf.html.

[6] NATO Consultation Command and Control Board – C3B, (2014), «ALLIANCE CONSULTATION, COMMAND AND CONTROL (C3) STRATEGY». [En línea]. Available: https://tide.act.nato.int/mediawiki/tidepedia/images/b/bc/C-M%282014%290016_Alliance_C3_Strategy.pdf.

[7] Administración General del Estado, (2015), «https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Estrategia-TIC/Estrategia-TIC-AGE.html». [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:898162f1-2682-483e-9e43-50f2d3a08eff/20151002-Plan-transformacion-digital-age-oopp.pdf.

[8] NATO Consultation Command and Control Board – C3B, (2021), «Enterprise Architecture Policy». [En línea]. Available: https://tide.act.nato.int/mediawiki/tidepedia/images/b/ba/AC322-D%282015%290030-REV1.pdf.

[9] Ministerio de Defensa, (2017), «Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC)». [En línea]. Available: https://publicaciones.

defensa.gob.es/media/downloadable/files/links/a/r/arquitectura_global_sistemas_y_tecnologias_informacion.pdf.

[10] U.S. Department of Defense, (2010), «Chief Information Officer, DoDAF». [En línea]. Available: https://dodcio.defense.gov/library/dod-architecture-framework/.

[11] M. H. y. E. Fellow, (2016), «Technology Update on the Unified Architecture Framework (UAF)». [En línea]. Available: https://www.researchgate.net/figure/A-Simplified-History-of-DoDAF-MODAF-and-NAF-Framework-Family-History-Figure-1-shows-how_fig1_308081427.

[12] NATO Consultation Command and Control Board – Architecture Capability Team, «NATO & Architecting The NATO Architecture Framework» [En línea]. Available: https://www.omg.org/cgi-bin/doc?omg/2019-06-11.

[13] O. Rey, (2019) «Military frameworks, systems engineering and enterprise architecture». [En línea]. Available: https://www.researchgate.net/publication/337293779_Military_frameworks_systems_engineering_and_enterprise_architecture.

[14] OMG System Modeling Language, (2017), «SYSML V2: THE NEXT-GENERATION SYSTEMS MODELING LANGUAGE». [En línea]. Available: https://www.omgsysml.org/SysML-2.htm.

[15] The Open Group, (2018), «TOGAF® Version 9.2, The Open Group Standard (C182), April 2018, published by The Open Group; refer to: www.opengroup.org/library/c182». [En línea]. Available: https://pubs.opengroup.org/architecture/togaf9-doc/arch/.

[16] MEGA INTERNACIONAL, «Update on NATO» 20 03 2019. [En línea]. Available: http://www.paceroom.net/modeler/document/omg-19-03-28.pdf.

[17] OMG Standards Development Organization, (April 2015), «Business Motivation Model (BMM)». [En línea]. Available: https://www.omg.org/spec/BMM/1.3/About-BMM/.

[18] OMG Standards Development Organization, (2010), «Business Process Model And Notation (BPMN)». [En línea]. Available: https://www.omg.org/spec/BPMN/2.0/About-BPMN/.

[19] OMG Standards Development Organization, (2017), «Unified Modeling Language (UML)». [En línea]. Available: https://www.omg.org/spec/UML/2.5.1/About-UML/.

[20] NATO, (2015), «NATO Mission Thread Capstone». [En línea]. Available: https://tide.act.nato.int/mediawiki/tidepedia/images/6/68/TT-151004_NATO_Mission_Thread_Capstone_Bi-SC_2015_NU1147_%28002%29.pdf.

[21] NATO, «AAP-47, Allied Joint Doctrine Development, Edition B, Version 1, dated June 2016» [En línea].

[22] NATO, (04 October 2013) «MC133/4, ACO Comprehensive Operations Planning Directive v2. O». [En línea].

[23] NATO, (6 October 2014) «MC 0458/3, Education, Training, Exercise and Evaluation (ETEE) Policy». [En línea].

[24] NATO, «ACO Forces Standards Volumes I – XI.» [En línea].

[25] NATO, (15 April 2016), «Bi-SC 085-001, Capability Package Directive (Edition 4)». [En línea].

[26] NATO, (April 2009) «PO (2009)0042, Outline Model for a NATO Defence Planning Process». [En línea].

[27] NATO, (June 2013), «APP-15, NATO Information Exchange Requirement Specification Process, Edition A, Version 1». [En línea].

[28] NATO, (23 February 2015), «MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations». [En línea].

[29] NATO, «AAP-16, NATO Manpower Procedures» [En línea].

[30] NATO, (11 July 2013) «SHCMRB/6100/026/13, CRO Urgent Requirements Training Concept». [En línea].

[31] NATO Consultation Command and Control Board – Architecture Capability Team, marzo 2019), «NAFv4 Modeling Guidelines for use of the UAF DMM». [En línea].

[32] NATO, (2017), «NATO MISSION THREAD DEVELOPMENT GUIDE». [En línea]. Available: https://tide.act.nato.int/mediawiki/tidepedia/images/1/11/2017-03-10_NU_0181-NATO-MissionThreads-DevelopmentGuide%28TT170067%29.pdf.

[33] Bizzdesign, (16-9-2016), «Combining ArchiMate® 3.0 with Other Standards – BMM /BS / BMC». [En línea]. Available: https://bizzdesign.com/blog/combining-archimate-3-0-with-other-standards-bmm-bs-bmc/.

[34] Bizzdesign, (8-9-2016), «Combining ArchiMate® 3.0 with Other Standards – UML / SysML / ERD». [En línea]. Available: https://bizzde-

sign.com/blog/combining-archimate-3-0-with-other-standards-uml-sysml-erd/.

[35] Association Française de Normalisation, (2013), «Architecture Frameworks – A Standard to Unify Terms, Concepts, Life-Cycles and Principles». [En línea]. Available: https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.sto.nato.int%2Fpublications%2FSTO%2520Meeting%2520Proceedings%2FSTO-MP-IST-115%2FMP-IST-115-02.pdf&psig=AOvVaw0Lg7g360UHYy39vaRShJzH&ust=1642416490903000&source=images&cd=vfe&ved=2ahUKEwiCq7CtjLb1AhURO.

[36] M.-E. -. H. J. -. Q. D. -. F. A. - Iacob, Modeling Strategy with ArchiMate®, Aldea, 2015.

[37] The Open Group, (2017), «How to Model Enterprise Risk Management and Security with the ArchiMate® Language». [En línea]. Available: https://publications.opengroup.org/w172.

[38] C. F. &. E. Grandry, (2013), «Conceptual Integration of Enterprise Architecture Management and Security Risk Management».

[39] NATO Consultation Command and Control Board – Architecture Capability Team, «C3 Taxonomy Perspective» [En línea]. Available: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/10/pdf/210830-C3-taxonomy-baseline.pdf.

[40] Gobierno de España, «Portal de administración Electrónica,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Racionaliza_y_Comparte/catalogo-servicios-admon-digital.html.

[41] Imagecolorpicker.com, «https://imagecolorpicker.com/,» [En línea]. Available: https://imagecolorpicker.com/.

[42] Ministerio de Defensa, (8-12-2017) «Estrategia de la Información del Ministerio de Defensa». [En línea]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-14417.

[43] Government of Canada, «Department of National Defence / Canadian Armed Forces Architecture Framework (DNDAF)» [En línea]. Available: http://www.forces.gc.ca/en/about-policies-standards/dndaf.page.

[44] J. A. Zachman, (2008), «Zachman International Enterprise Architecture». [En línea]. Available: https://www.zachman.com/about-the-zachman-framework.

[45] OMG Standards Development Organization, (abril 2020), «Unified Architecture Framework». [En línea]. Available: https://www.omg.org/spec/UAF/1.1/About-UAF/.

[46] UK Ministry of Defence, (2012), «Ministry of Defence Architecture Framework». [En línea]. Available: https://www.gov.uk/guidance/mod-architecture-framework.

[47] NATO Consultation Command and Control Board – C3B, (2017), «NATO Enterprise Architecture Directive». [En línea]. Available: https://tide.act.nato.int/mediawiki/tidepedia/images/9/96/AC322-N%282017%290074_NATO_EA_Directive.pdf.

Estudio y propuesta de uso del lenguaje "ArchiMate®" para generación de arquitecturas NAFv4 en el Ministerio de Defensa

Autor: Manuel Ángel de Pedro Cibanal
Universidad de Vigo
Directores: Francisco Javier Rodriguez Martinez y Antonio Villalba Madrid

Introducción

La disciplina Arquitectura Empresarial define una arquitectura como "una descripción formal de un sistema, la estructura de sus componentes, sus interrelaciones, y los principios y guías que gobiernan su diseño y evolución a lo largo del tiempo". Sin que el sistema tenga que ser necesariamente software o hardware, podemos extender su significado por ejemplo a una organización, la gestión de RRHH o a un proyecto. Las posibilidades que se abren son abundantes y se ofrece una aproximación holística para describir de una manera diferente multitud de conceptos.

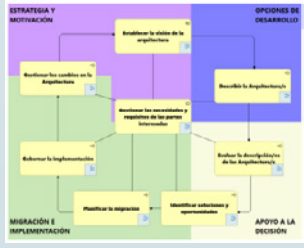
El Marco de Arquitecturas OTAN en su versión 4 (NAFv4) proporciona una metodología para creación/modificación de arquitecturas, una tabla (o grid) para organizar puntos de vista de las principales partes interesadas e instrucciones de como adoptar meta-modelos comerciales entre los que se incluye ArchiMate®.

Metodología

A través del estudio del arte de lo que son las arquitecturas, los marcos de arquitecturas y el lenguaje de Arquitectura Empresarial ArchiMate® se han modelado de manera práctica diferentes puntos de vista para proponer este lenguaje como apoyo a:

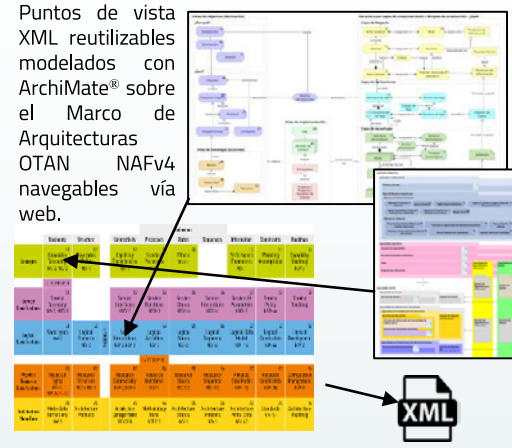
- la creación de nuevas arquitecturas NAFv4,
- la migración de arquitecturas de NAFv3 a NAFv4 y
- el apoyo a Actuaciones del Plan de Acción para la Transformación Digital del Ministerio de Defensa.

Para ello se han seguido los procesos arquitectónicos enunciados en la Directiva OTAN de Arquitectura Empresarial, así como diferente documentación de referencia OTAN y del Ministerio de Defensa.



Resultados

Puntos de vista XML reutilizables modelados con ArchiMate® sobre el Marco de Arquitecturas OTAN NAFv4 navegables vía web.



Conclusiones

El uso del lenguaje de Arquitectura Empresarial ArchiMate® y NAFv4 posibilitan presentar y reutilizar información de una manera innovadora que supera las limitaciones de la documentación, la comunicación tradicional y la representación de datos, información y conocimiento basadas hasta ahora en ficheros ofimáticos con formatos propietarios MS Word, MS PowerPoint o Adobe PDF.

La conclusión más relevante de este estudio es que la propuesta de uso de ArchiMate® y su esquema de recursos interconectados aseguran una coherencia y una presentación de información inequívoca. Esto evita el uso de largas redacciones que, en numerosas ocasiones cuando se repiten conceptos omiten información, son ambiguas o tienen equívocos al no tener como origen una única fuente de verdad.

La identificación y adopción del lenguaje de Arquitectura Empresarial ArchiMate® puede considerarse, por tanto, como un paso fundamental para cualquier organización que quiera estar preparada para actuar, en lugar de reaccionar, generando arquitecturas de sus activos de una manera holística.

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Desarrollo, implementación y evolución de la capacidad *Cyber Situational Awareness (CySA)* en zona de operaciones

Autor: Pérez García, Ángel (aperga1@et.mde.es)
Director: Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – Cada vez son más numerosas las operaciones de mantenimiento de paz en las que España participa a través del Ministerio de Defensa. La gran mayoría de estas operaciones se realizan en el marco de una coalición internacional (OTAN, UE, etc.), lo cual obliga a trabajar con unos medios CIS interoperables, los cuales nos permitan llevar a cabo las labores de mando y control de las operaciones de manera eficaz.

Son una realidad las herramientas que nos permiten tener un conocimiento profundo de la situación en el campo de batalla, pero aún no se dispone de una herramienta que permita integrar el campo de batalla físico con la amenaza cíber.

En este sentido, se está impulsando desde los gobiernos e instituciones la citada integración, considerándose un requisito fundamental, para poder participar en las operaciones de la coalición, disponer de este servicio.

España participa de manera activa en proyectos que persiguen alcanzar este objetivo, pero todos ellos están focalizados en el nivel estratégico, siendo el nivel táctico el primer eslabón de la cadena y la principal fuente de datos de las herramientas de niveles superiores.

Por todo ello, el presente trabajo pretende dar los primeros pasos en el desarrollo de una herramienta que nos permita disponer de información cíber relevante en el nivel táctico y, por lo tanto, tener una Cyber Situational Awareness (CYSA) adecuada a las misiones en las que el Ministerio de Defensa participa.

Palabras clave – CYSA, nivel táctico, operaciones, Awareness, comandante

1. Introducción

La incorporación de España en el siglo XX a distintas alianzas multinacionales, trajo consigo el progreso y la evolución del país en numerosas áreas.

Una de ellas fue sin duda el desarrollo de las Fuerzas Armadas, debido a los estándares que exigía la pertenencia a dichas alianzas.

Estas alianzas, no se llevan a cabo estrictamente en el campo de lo político (estratégico) o lo militar (operacional o táctico), entendiendo *lo militar* como despliegue de fuerzas y reduciéndolo a potencia de fuego y armamento. Hoy en día existe un arma más poderosa que cualquiera de las empleadas en el campo de batalla, es transversal y alcanza a todos los niveles del conflicto, la información. El principal reto y el mayor desafío de una alianza es alcanzar la capacidad de comunicarse, coordinarse y compartir información en el campo de batalla, en tiempo real y con garantías de confidencialidad, integridad y disponibilidad.

Alcanzar la interoperabilidad entre los medios de combate de cada uno de los países que la componen, es uno de los planes más ambiciosos que la OTAN está llevando a cabo en la actualidad, en cuyo desarrollo está invirtiendo miles de millones de euros. Una parte muy importante de este presupuesto, lo está destinando a la interoperabilidad entre sistemas de mando y control.

El programa FMN (Federated Mission Network) [1] es un referente en este campo. En él, países de la OTAN y países amigos no pertenecientes a OTAN, pero con relaciones militares frecuentes, llevan trabajando desde hace más de 10 años para alcanzar la interoperabilidad en los sistemas de mando y control que se han de desplegar en zona de operaciones (ZO).

El programa FMN, por medio de la implementación de espirales sucesivas, quiere alcanzar la interoperabilidad total entre los sistemas de mando y control aliados, y ser capaces de desplegar, en un tiempo muy reducido, los sistemas de cada país participante en la operación y operar como un solo sistema compartiendo los servicios que se determinen para cada operación como se puede observar en la figura 1, la cual refleja el horizonte 2030 de la OTAN.

El concepto de espirales sucesivas consiste en una evolución progresiva tanto de los servicios que ofrece el sistema de mando y control, como de la interoperabilidad entre los miembros de FMN, con esto, conseguimos que la transición sea paulatina y que nadie se quede atrás en el diseño de sus sistemas.

Uno de los servicios objeto de estudio en el programa FMN, el cual ha de ser implementado por cada uno de los países miembros y aliados, es el servicio de Cyber Situational Awareness (CYSA), es decir, el conocimiento de la situación desde el punto de vista del ciberespacio.

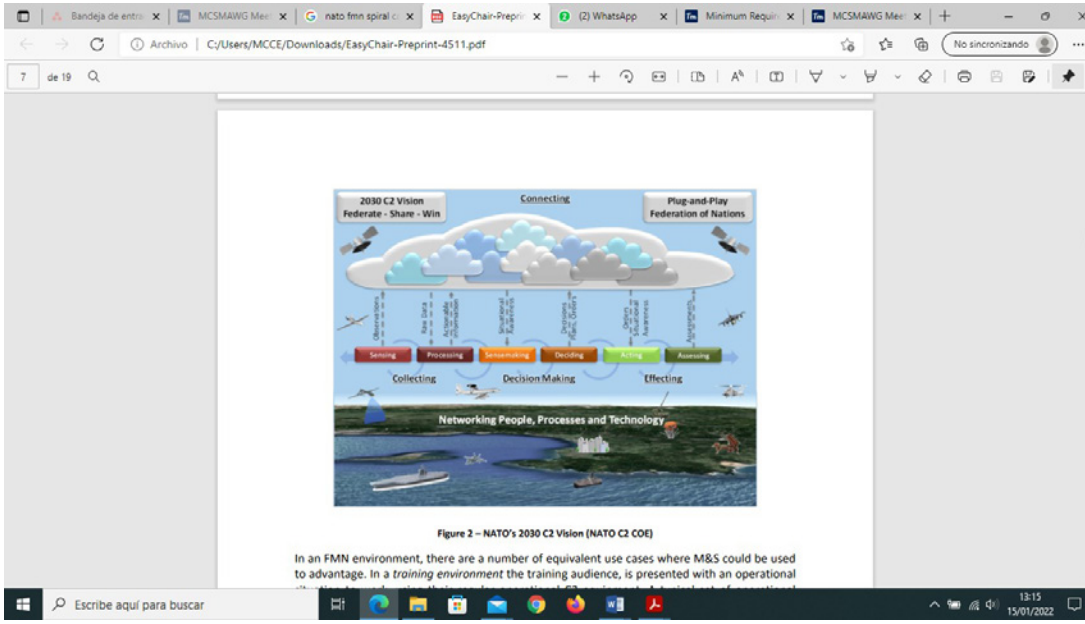


Figura 1. Visión de la OTAN Mando y Control 2030 (Tomada de [2])

Cyber Situational Awareness (CYSA) es, a día de hoy, una idea por desarrollar, existen numerosos estudios y aproximaciones al problema [3] y se están llevando a cabo programas encaminados a desarrollar esta capacidad como los de la European Defence Agency (EDA) [4] y la OTAN en el marco de FMN [1], pero aún no hay ninguno que haya llegado a concretarse y no se espera en el corto plazo.

En este documento se pretende llegar a una aproximación en detalle de cómo recoger en el nivel táctico, los datos necesarios de los distintos sistemas de mando y control que nos permitan, tras ser tratados adecuadamente, presentar al comandante la situación del ciberespacio que afecta o puede afectar a las operaciones en curso o venideras.

2. Desarrollo

La CYSA, de manera general, es el conocimiento de la situación relativa a todo aquello que tiene que ver con el ciberespacio y que puede afectar o influir en nuestras operaciones. Es la evolución natural de la Situational Awareness, tan ampliamente extendida en las operaciones militares y que actualmente no se entiende sin su componente cíber.

La CYSA nos ha de permitir integrar y conocer, en todos los niveles de planeamiento, la amenaza cíber y nuestras capacidades en este ámbito.

Para entender mejor el concepto, no debemos olvidar que la CYSA se nutre de fuentes de información de muy distinta índole, como son las

herramientas de ciberdefensa, de ciberinteligencia, fuentes abiertas (redes sociales, deep web, etc.), acciones ofensivas de reconocimiento, etc.

Las fuentes de información más relevantes para la elaboración de la CYSA las podemos agrupar en cuatro grupos principales: activos, vulnerabilidades, amenazas e incidentes y medidas de ciberdefensa.

2.1. CYSA en el nivel táctico

La CYSA se puede definir como la comprensión de la situación en el ámbito del ciberespacio que el comandante alcanza y en la que fundamenta la toma de decisiones.

No se debe perder de vista que la situación es única y no puede ser subjetiva, por lo que la información que la describe debe ser objetiva.

Cada comandante debe adquirir *su particular* CYSA, para lo cual es necesario que su órgano auxiliar le presente la información con el grado de detalle necesario, atendiendo al ciclo de decisión (ver figura 2), en el cual influye significativamente el tiempo disponible, y a la misión de cada organización operativa.

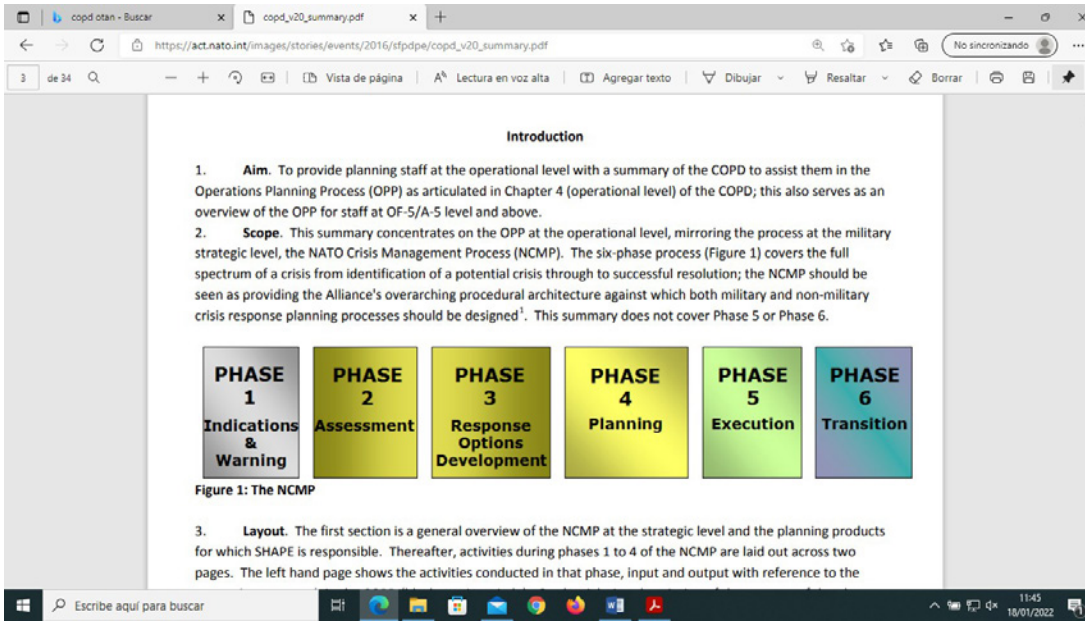


Figura 2. Ciclo de toma de decisión (tomada de [5])

2.2. Componentes de CYSA en el nivel táctico

En el ciberespacio se conducen acciones ofensivas, defensivas y, además, de obtención de información. Para favorecer la comprensión de la realidad, se propone descomponer la situación en el ciberespacio en componentes que ayuden a su estudio y comprensión.

1. Systems Awareness (SA)

   Este aspecto comprende el conocimiento de los sistemas de interés para el comandante, incluyendo las capas lógicas, ligada a la identificación de los elementos de red, el control de la configuración y los comportamientos anómalos, la física, ligada al conocimiento sobre la ubicación física de los componentes tangibles del ciberespacio, y la humana, ligada al conocimiento sobre el personal que tiene acceso a los sistemas.

2. Enemy Awareness (EA)

   Este aspecto estudia el riesgo que supone el enemigo para los sistemas propios o el CKT (terreno clave cíber) de interés para el enemigo, así como las oportunidades de las acciones ofensivas propias contra los sistemas o el CKT en poder del enemigo.

3. Mission Awareness (MA)

   Este aspecto estudia los incidentes de seguridad, las fuerzas de ciberdefensa disponibles, los ataques recibidos, las campañas, genéricas o dirigidas, contra la fuerza desplegada, conjugando la situación de los sistemas y del enemigo para valorar el impacto potencial o real que las acciones en el ciberespacio, propias o enemigas, defensivas u ofensivas puedan tener en la misión.

2.3. Presentación de la CYSA

Debido al dinamismo del ciberespacio, para lograr una adecuada presentación es necesario disponer de información actualizada en tiempo casi real. La obtención de la información debe realizarse mediante procesos automatizados o semiautomatizados que la transfieran a una base de datos única.

Una vez la información ha sido obtenida es necesario su tratamiento y presentación al comandante, ya sea el de la operación o jefe de una unidad CIS o cíber. Como ya se ha mencionado anteriormente, cada escalón de mando tiene un tempo en la operación, por lo que es necesario que la presentación de la CYSA se pueda personalizar. De esta forma se evitará tanto la saturación como la escasez de la información necesaria para la adecuada toma de decisiones.

Los responsables cíber (usualmente la célula cíber de un puesto de mando) de cada escalón de mando son, habitualmente, los encargados de preparar la presentación de la información que debe conocer y entender su comandante. Las células cíber de los escalones superiores aportarán la información obtenida por sus propios medios y que pueda ser relevante para la toma de decisiones del escalón o escalones subordinados.

3. Prototipo

Desde un punto de vista operativo, el prototipo debe poder mostrar el estado de Ciberseguridad de los sistemas y redes, y en especial de aquellos que son críticos para la operación.

Ha de mostrar de manera clara y visual los datos de los indicadores, los cuales han de ser seleccionados por los usuarios finales de la herramienta, es decir, el comandante y el personal que le asesora.

Debe poder, en caso de ciberincidente, definir cuál es el alcance del mismo en la red, y cuál es el impacto en la misión. Es decir, debe poder traducir un ciberincidente (nivel técnico) a un lenguaje operativo, que el comandante y sus asesores puedan comprender de manera visual, intentando dar respuesta a preguntas como:

- ¿Qué impacto tiene ese ciberincidente en la misión?
- ¿Qué riesgo supone una nueva vulnerabilidad en un servicio de un sistema que se emplea en la operación?

Para ello es necesario poder hacer una trazabilidad de las dependencias entre la misión y cada servicio elemental CIS. Es decir, se debe de partir de la misión, e ir desgranando de ella:

- Cuáles son los objetivos de la misión.
- Qué información es necesaria para la misión.
- Cuáles son los sistemas/servicios fundamentales para cada operación.
- Dentro de esos sistemas/servicios, qué subsistemas/subservicios existen y cuáles son esenciales, y así sucesivamente hasta llegar a los servicios más básicos.
- Qué infraestructura (hardware) necesitan dichos servicios/sistemas.
- Que software está desplegado en dichos equipos.

3.1. Modelo de dependencias

En el modelo de dependencias de la figura 3 podemos observar las relaciones entre los distintos elementos. La misión se verá impactada por los elementos de capas inferiores en dos sentidos:

Por un lado, existe una ponderación de las relaciones de dependencia entre la misión y los objetivos, informaciones y servicios/sistemas (% *dependencia* en la imagen), de modo que, por ejemplo, la misión puede verse más impactada por la consecución de un objetivo que de otro, o una información de un servicio/sistema u otro.

Por otro lado, cada elemento del diagrama de dependencias lleva asociado una serie de atributos o características, distintas para cada una

de las capas, cuyo valor impactará en la misión. Por ejemplo, la capa de *Software* lleva asociados los atributos *vulnerabilidad (técnica)* y *ciclo de vida*. El valor que tomen estos atributos provocará mayor o menor impacto en la misión. Si el software es vulnerable, este valor irá ascendiendo en el diagrama de dependencias hasta impactar o repercutir en el valor de la probabilidad de éxito de la misión.

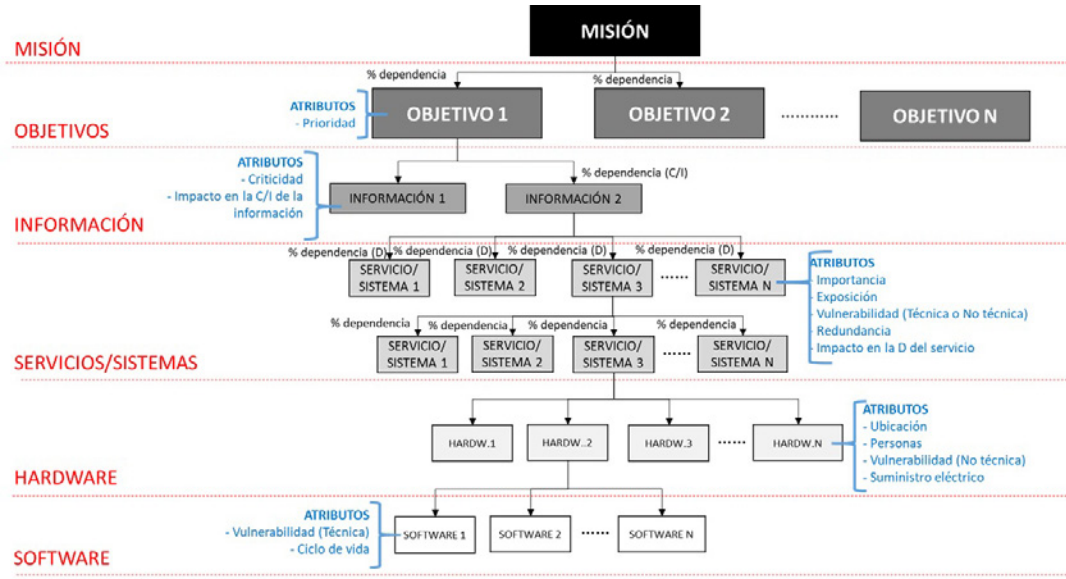


Figura 3. Modelo de dependencias (elaboración propia)

4. Conclusiones

La necesidad de conocer el entorno que le rodea es fundamental para el comandante de una fuerza militar desplegada en un ambiente hostil a la hora de tomar decisiones.

Tradicionalmente los esfuerzos se han orientado a proporcionar información de las tres dimensiones clásicas: tierra, mar y aire, incluyéndose en los últimos tiempos el espacio.

Pero la realidad actual es muy diferente, la entrada de una nueva dimensión, como es el componente cíber, ha cambiado la manera de enfrentarse al enemigo.

Para que la adaptación a este nuevo componente sea rápida y ágil, se ha de considerar como uno más de los 4 tradicionales, y se le ha de incluir en el proceso de toma de decisión.

Los proyectos iniciados por los distintos organismos para integrar la CYSA en los procesos de toma de decisiones o en las representaciones gráficas como la NATO Common Operational Picture (NCOP), no son útiles en el nivel táctico, ya que los datos que estos proyectos ofrecen, son de

alto nivel y no aportan valor al comandante a la hora de tomar decisiones, por lo que es necesario llevar a cabo un desarrollo, más sencillo, que englobe y satisfaga las necesidades del nivel táctico.

En el nivel táctico la integración ha de entrar en detalle en los aspectos más importantes en función de la misión, lo cual obliga a que sea una herramienta sencilla y sobre todo muy flexible para adaptarse a la gran variedad de misiones que han de afrontar las pequeñas unidades.

La automatización de los procesos de obtención de información y una representación gráfica simple e integrable con la maniobra (ver figura 4), serán los pilares del éxito del futuro desarrollo, cuyas ventajas a la hora de la planificación de las operaciones es más que evidente.

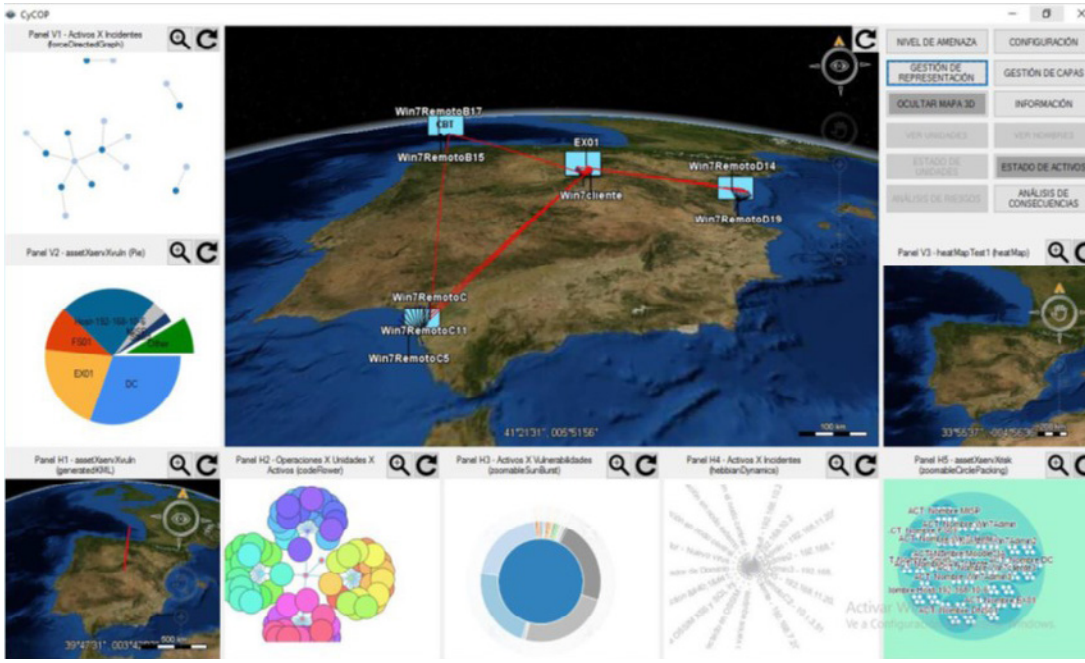


Figura 4. Prototipo Universidad Politécnica de Valencia (tomada de [5]

Referencias

[1] OTAN FMN, (2020), «NATO Cooperation Portal,» [En línea]. Available: https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx. [Último acceso: 13 01 22]. NATO CAX FORUM, «NATO Federated Mission Networking Standards».

[2] S. Jajodia, (2010), Cyber Situational Awarenes ISBN 978-1-4419-0139-2, Primera ed., Springer.

[3] European Defense Agency (EDA), (2017), «Target Architecture & System Requirements for an Enhanced Cyber Situation Awareness (CYSA 2)».

[4] OTAN, (2013), «Comprehensive operations planning directive.».

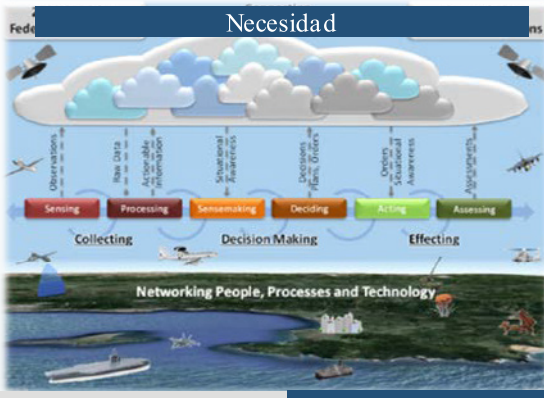
[5] P. M. Estev, (2018), «CYCOP: A cyber hybrid situational awareness and risk analysis visualization tool» Valencia.

Desarrollo, implementación y evolución de la capacidad "Cyber Situational Awareness (CySA)" en zona de operaciones

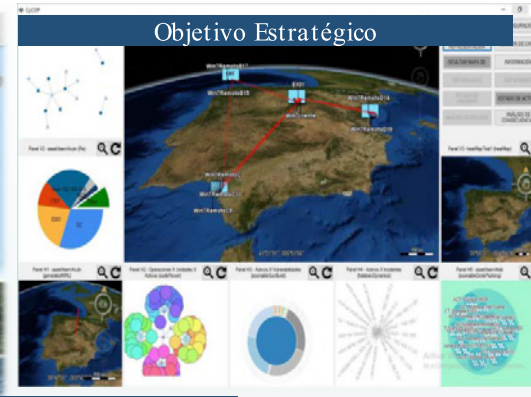
Autor: Ángel Pérez García
Director/es: Norberto Fernández García

Universidad de Vigo

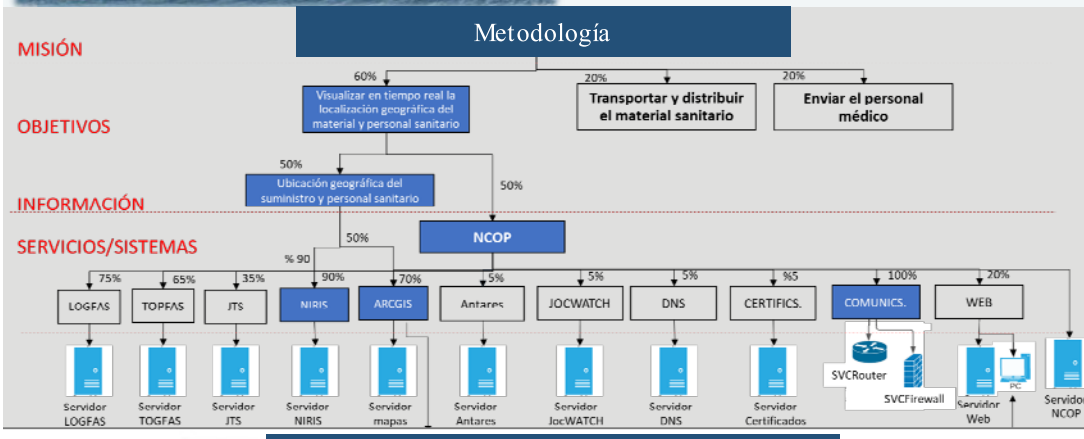
Necesidad



Objetivo Estratégico



Metodología



Resultado final Nivel Táctico

Estudio del estado del arte de las tecnologías de contenedores

Autor: Roca Blázquez, José Luis (jose_luis_roca@outlook.es)
Directores: Suárez Lorenzo, Fernando (fsuarezl@gmail.com)
Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – En este trabajo se ofrece un repaso del estado actual de la tecnología de contenedores. El texto pueda servir como introducción a este campo para personas que, teniendo unos conocimientos técnicos suficientes, no conocen ni han manejado nunca dicha tecnología. Se sigue una secuencia en la que se empieza por explicar los antecedentes históricos de los contenedores; se continúa explicando los fundamentos técnicos de bajo nivel sobre los que se asientan las distintas implementaciones existentes, y esto da pie para conocer las características principales de los contenedores y por qué han supuesto una revolución en el mundo del desarrollo y despliegue de aplicaciones. Se explican asimismo sus posibles usos, y dado que puede surgir la inquietud de comparar los contenedores con la virtualización, se realiza una comparación entre ambas tecnologías, indicando sus similitudes, diferencias y casos de uso.

Ha habido bastantes implementaciones de entornos de contenedores, y algunas de ellas, las más conocidas e importantes, se mencionan en este trabajo. Esto sirve además como argumento para la inclusión de varios intentos de normalización de algunos de sus aspectos en el capítulo dedicado a implementaciones.

En la parte final del trabajo se habla sobre infraestructuras de contenedores y la necesidad de organización mediante lo que se denomina *orquestación*. Se termina con algunos apuntes sobre el futuro de la tecnología de los contenedores, y se añaden las conclusiones y posibles líneas futuras para otros trabajos que puedan complementar a este; los caminos posibles son muchos.

Palabras clave – Contenedores, microservicios, DevOps, orquestación, Docker, Kubernetes.

1. Introducción

Durante las últimas décadas ha habido una evolución en el desarrollo del hardware y del software que ha traído consigo cambios en la manera de implantar sistemas y servicios. Ya en la década de los años 60 del siglo XX se desarrollaban sistemas operativos que permitían homogeneizar el desarrollo de las aplicaciones en distintas plataformas hardware. Con el despliegue de redes de comunicaciones aparece el desarrollo de la provisión de servicios en red y estos se sustentan en plataformas de servidores de distinta manera según evoluciona la tecnología: o bien había una correspondencia unívoca entre servicio ofrecido y servidor físico que lo soportaba, o se usaba un solo servidor para proporcionar varios servicios, o se usaban técnicas de virtualización, ya soportadas mediante nuevas capacidades incorporadas en las modernas CPU, para alojar varias máquinas virtuales en un servidor.

En distintas familias del sistema operativo Unix se llevan implementando desde hace varias décadas formas de ejecución de conjuntos de procesos aislados de otros procesos. Esta forma de trabajo sufrió un desarrollo grande con el añadido de determinadas características a los núcleos de los sistemas operativos, ya no solo de Unix sino también de Linux. Se acuña el término *contenedor* para denominar una unidad de ejecución independiente de otras unidades similares y controladas por un mismo sistema operativo. Esta estructura independiente, si se complementa con herramientas de gestión de usuario, soluciones de despliegue en distintos servidores y entornos de control de clusters, permite proporcionar servicios de una manera muy robusta y fiable.

2. Desarrollo

El núcleo de Linux dispone de una serie de características y capacidades que permiten aislar conjuntos de procesos del sistema operativo que los sustenta, y de otros conjuntos de procesos. Estas características, llamadas cgroups, namespaces y capabilities, son la base para conseguir desarrollar sistemas cada vez más complejos que aportan soluciones de contenedores que anteriormente no eran tan fáciles de obtener.

La posibilidad de disponer de contenedores como conjuntos de procesos con una gran independencia de otros conjuntos concurrentes en la misma máquina brinda enormes ventajas. Inmediatamente se aplica tal posibilidad para soluciones en las que anteriormente se utilizaba la virtualización. En el campo de la virtualización se hace uso de capacidades implementadas ya en las propias CPU y se usan máquinas virtuales que ofrecen a sus sistemas operativos independientes los recursos hardware que el hipervisor determina. El resultado son estructuras relativamente pesadas, pues cada máquina virtual debe contener todos los elementos de un servicio (hardware virtualizado, sistema operativo, aplicaciones,

librerías y datos), aunque muy flexibles, ya que es posible implementar máquinas virtuales con distintos sistemas operativos instalados en un mismo servidor físico. La virtualización permite abstraer los sistemas operativos de las plataformas hardware subyacentes. Los contenedores, por otra parte, son estructuras más ligeras tanto en almacenamiento como en utilización de recursos físicos, si bien tienen algunas limitaciones en relación a las máquinas virtuales; por ejemplo, no se puede tener un sistema operativo completo distinto del sistema operativo base del servidor en el cual se trabaja. Haciendo un paralelismo con la virtualización, pero a otro nivel, puede decirse que los contenedores permiten abstraer las aplicaciones de los sistemas operativos subyacentes. Realmente la virtualización y los contenedores no son tecnologías antagónicas sino complementarias, y cada una de ellas tiene sus propios campos de aplicación. La virtualización permite tener sistemas operativos completos, sean cuales sean, sobre servidores que contienen un hipervisor que les brinda un hardware emulado. En algunos casos es la virtualización la única solución posible, por ejemplo, cuando se desea mantener en funcionamiento una aplicación antigua desarrollada sobre un sistema operativo que ya no se mantiene y no se puede ejecutar en un hardware moderno. Por otra parte, los contenedores conllevan unas enormes ventajas en el desarrollo y despliegue de aplicaciones. Tradicionalmente ha sido habitual codificar aplicaciones como estructuras monolíticas que daban un servicio externo final a base de implementar todas las relaciones entre los distintos elementos internos en un solo bloque. Sin embargo, es relativamente cómodo y bastante eficiente desarrollar aplicaciones de manera que sus funciones internas se dividan en pequeños servicios independientes, y a su vez estos servicios se implementan mediante contenedores. Esta forma de desarrollo con microservicios proporciona flexibilidad y grandes posibilidades de desplegar servicios robustos con tolerancia a fallos y con resiliencia.

A lo anterior se une además la facilidad de despliegue de aplicaciones que se sustentan en contenedores a lo largo de una infraestructura compleja de servidores. Existen herramientas que integran las acciones de desarrollo-compilación y despliegue en clusters. La línea divisoria entre los equipos de desarrollo y producción se hace cada vez más fina, apareciendo el concepto de DevOps para referirse a la fusión entre desarrollo y operaciones, y esto facilita el trabajo de estas áreas y aporta una gran facilidad a la hora de solucionar errores, realizar cambios e implementarlos en una gran infraestructura que soporta distintos servicios. Los sistemas completos CI/CD (siglas por las que se conoce a los entornos de integración y entrega continuas, también desarrollo continuo) son también algunos de los más beneficiados por el desarrollo y perfeccionamiento de las distintas tecnologías de contenedores.

La teoría del aislamiento de conjuntos de procesos debe no obstante ser implementada de alguna manera efectiva y cómoda para que se pueda

usar de manera práctica. En este sentido ha habido distintas soluciones en los últimos años. Las implementaciones implican algún añadido o modificación en algunos casos al sistema operativo base (como, por ejemplo, módulos del kernel específicos para trabajar con contenedores), aunque no siempre es así. Deben incluir desde luego algún sistema de *imágenes*, que son las estructuras de ficheros que se almacenan en repositorios y posteriormente se descargan en los servidores, y a partir de las cuales se construyen de manera dinámica los contenedores según se van creando y ejecutando. Además, las implementaciones también deben tener en cuenta una serie de herramientas para poder operar de manera práctica y real con contenedores, creando imágenes, subiéndolas a un repositorio, descargándolas, ejecutando un contenedor, parándolo, volviéndolo a lanza, eliminándolo, proporcionando listados de imágenes descargadas y de contenedores en ejecución, etc.

Algunas implementaciones no han sobrevivido al paso del tiempo y han dejado de mantenerse, otras lo han hecho, aunque no tienen mucho uso y no están demasiado extendidas. Hay una que ha tenido una gran aceptación y se utiliza ampliamente: docker. Esta solución proporciona todo lo necesario para trabajar con contenedores en entornos reducidos, por ejemplo, en un solo servidor o en un cluster de pocos servidores, permitiendo también crear imágenes y subirlas a repositorios públicos gratuitos (y limitados, evidentemente). Lo interesante es que gracias a docker la tecnología de contenedores se ha dado a conocer ampliamente y se ha extendido muchísimo en relación a la situación anterior a su existencia. Esto se une a las posibilidades ofrecidas por las características de los núcleos de los sistemas operativos de limitar los recursos del servidor (CPU, memoria, comunicaciones...) que se ofrecen a los contenedores albergados en la máquina física en cuestión, así como medir, y por tanto tarificar, el uso real de dichos recursos; en conjunto todo ello ha permitido que crezca enormemente el mercado en lo que se refiere a la posibilidad de contratar plataformas en las que alojar servicios basados en contenedores, al igual que ocurre con los sistemas equivalentes que utilizan la virtualización como servicio.

Los contenedores han facilitado desplegar aplicaciones de manera ágil y cómoda. Por ejemplo puede imaginarse la necesidad de desplegar en alguna organización un servicio de nube que permita a equipos de trabajo y a departamentos de cualquier organización realizar fácilmente trabajo colaborativo, y que ofrezca a los usuarios dados de alta en el sistema un espacio de almacenamiento con estrictos controles de acceso y compartición, sincronización de la información almacenada en dispositivos remotos, capacidades de comunicación mediante mensajes instantáneos y comunicación audiovisual en tiempo real, calendario y almacén de contactos accesibles mediante protocolos estándar, marcadores de navegadores, editores en línea de archivos ofimáticos estándar, acceso tanto desde interfaz web como desde aplicaciones para dispositivos

móviles y más posibilidades gracias a una arquitectura que permite la instalación de añadidos o aplicaciones. Con la tecnología de contenedores es extraordinariamente fácil realizar el despliegue de todos los servicios mencionados en cuestión de segundos. Todo lo anterior se consigue ejecutando una simple orden en una consola de un servidor donde, evidentemente, se haya realizado previamente la instalación de un entorno de gestión y ejecución de contenedores como docker (esta instalación, por otra parte, también es realmente sencilla). Una orden sencilla en docker descarga una imagen y ejecuta un contenedor que ofrece todos los servicios mencionados. Además, y como paso posterior en la demostración de las posibilidades de los contenedores, se puede realizar el mismo despliegue del mismo servicio de nube, pero usando dos contenedores, dividiéndose cada uno de ellos las funciones. Esto es un ejemplo de microservicio. Este despliegue con más de un contenedor se define de manera muy sencilla en un fichero de texto con formato YAML (Yet Another Mark Up Language, formato de fichero ampliamente usado para describir estructuras de datos, configuraciones, formatos de mensajes, etc. y que en este caso se usa para la descripción de un despliegue de contenedores y servicios). El despliegue de estos microservicios según se describe en el mencionado fichero de configuración se realiza también con una simple orden en una consola.

Continuando con el punto de las implementaciones de contenedores y precisamente por el hecho de existir varias de ellas a lo largo del tiempo en el que se han desarrollado los contenedores, se ha hecho necesario proceder a normalizar o estandarizar algunos aspectos de los contenedores. La normalización siempre es un elemento positivo ya que permite desarrollar distintas soluciones que son interoperables y aporta flexibilidad para los administradores de los distintos sistemas a la hora de elegir una u otra solución.

Dado que el objetivo último del desarrollo de aplicaciones suele ser la provisión de servicios en red, es necesario tener en cuenta que lo habitual suele ser el despliegue de los distintos componentes que componen un servicio a lo largo de una infraestructura. Disponer de un servicio soportado por uno o más contenedores en un solo servidor físico no es la solución deseable, entre otras cosas por la posible limitación en el servicio ofrecido por las capacidades físicas del servidor y de los elementos asociados, y principalmente por la existencia de un único punto de fallo que puede suponer la caída total del servicio. Por tanto, es necesario un paso más en el desarrollo e implementación de los contenedores, contemplando el uso de clusters de servidores desplegados incluso en áreas geográficas muy extensas. En este punto es importante la gestión conjunta de toda esa infraestructura, de los elementos que la componen y de los servicios que soporta; es fundamental por tanto el concepto de *orquestación* como conjunto de recursos y herramientas que permiten una gestión integral y fiable. El ecosistema desarrollado por docker contempla el despliegue

de contenedores en distintos nodos mediante una solución denominada *swarm* y además lo hace de una manera sencilla y eficiente. Sin embargo, no se considera que sea una solución lo suficientemente robusta como para soportar servicios grandes en producción. Para ello se han desarrollado otros sistemas de orquestación, y el más conocido y extendido actualmente es kubernetes.

En la actualidad kubernetes es tanto un sistema utilizado *per se* para el despliegue de aplicaciones en infraestructuras complejas como también la base para otros productos, de código abierto y también comerciales, que sirven para gestionar todo lo relacionado con la provisión y comercialización de servicios de alojamiento de contenedores y despliegue de aplicaciones y servicios. Si se realiza una comparación en cuanto a las características y posibilidades entre la solución docker swarm, y kubernetes, se llega a la conclusión de que esta última es mucho más adecuada para infraestructuras especialmente grandes y para servicios que requieren una elevada disponibilidad y una robusta tolerancia a fallos. Naturalmente la potencia y las posibilidades tienen un precio en cuanto a la complejidad de diseño y gestión, que son superiores en el ámbito de kubernetes en comparación con el de docker.

El aspecto del almacenamiento es muy importante en despliegues complejos de servicios. Debe tenerse en cuenta que un contenedor es una estructura efímera que se crea en un servidor de manera dinámica a partir de una imagen, que no es más que un fichero con una determinada composición, en definitiva. Cuando un contenedor se destruye desaparece todo su contenido, y por tanto un contenedor de por sí no almacena nada de manera permanente, salvo que se haya implementado un sistema de asociación o enlace entre algunos directorios de un contenedor y una estructura de almacenamiento en un servidor. Tanto docker como kubernetes ofrecen formas de disponer de almacenamiento permanente que sobreviva al ciclo de vida de los contenedores que despliegen en forma de volúmenes, pero en despliegues reales de kubernetes suele recurrirse a soluciones de terceros que ofrecen una gestión muy mejorada del almacenamiento en clusters de servidores que albergan contenedores.

Las tecnologías de contenedores tienen un futuro bastante prometedor, pues son muchos los campos en los que pueden utilizarse. En muchas organizaciones es difícil dar el paso necesario para adoptar los contenedores como solución de despliegue, pues es necesaria una inversión, formación y tiempo de adaptación. A largo plazo no obstante es de esperar que se haga un uso muy extendido de los contenedores para distintos usos, como por ejemplo la investigación científica donde se requiere disponer de reproducibilidad, los sistemas de gestión de recursos y programación de trabajos o los entornos HPC (High Performance Computing) con aplicaciones de inteligencia artificial, machine learning y análisis de datos.

3. Conclusiones

Partiendo de unas capacidades aparentemente bastante simples en el núcleo de un sistema operativo y tras la implementación y el desarrollo de las herramientas adecuadas se consiguen unas funcionalidades y se posibilitan usos extremadamente potentes y flexibles de los contenedores. El mundo del desarrollo software se ha visto beneficiado en gran medida por el concepto y la materialización de los sistemas de contenedores, y en el ámbito de la gestión del despliegue de aplicaciones y servicios se ha conseguido disponer de herramientas que facilitan enormemente el trabajo y que permiten integrar las áreas de desarrollo y operaciones en las empresas y organismos más complejos. El desarrollo en forma de microservicios se ha visto favorecido por la existencia de la tecnología de contenedores.

Actualmente hay dos implementaciones a distintos niveles que se han popularizado de manera especial: docker y kubernetes. La primera permite construir de manera relativamente sencilla imágenes y gestionarlas en almacenes o repositorios. La segunda puede hacer uso de forma fácil de las imágenes creadas y almacenadas con la primera, y se utiliza ampliamente en los despliegues de servicios en infraestructuras complejas con requisitos especialmente altos en cuanto a robustez y fiabilidad.

Estudio del estado del arte de las tecnologías de contenedores

Autor: José Luis Roca Blázquez

Directores: Fernando Suárez Lorenzo, Milagros Fernández Gavilanes

Universidad de Vigo

Visión general

La tecnología de contenedores se ha desarrollado enormemente en los últimos años y permite disponer de unas capacidades que facilitan enormemente el desarrollo y despliegue de servicios a gran escala. El recorrido desde las características del núcleo del sistema operativo hasta los despliegues masivos es muy interesante…

Esquema del contenido

Fundamentos…

- Características de núcleo (kernel):
  - cgroups
  - namespaces
  - Capabilities

…complementados con …

- Herramientas de gestión
  - CLI
  - gráficas
- Capacidades adicionales…
  - Gestión de almacenes o repositorios
  - Gestión de imágenes
  - Gestión de redes
  - Gestión de almacenamiento

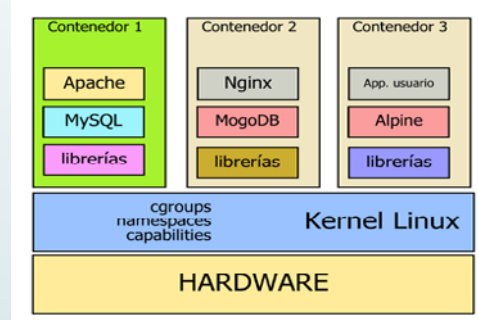
…potenciados mediante …

- Arquitectura interna cliente-servidor
- Normalización de interfaces entre elementos
- Lenguajes sencillos de definición de servicios
- Posibilidad de despliegue en *clusters*
- Arquitectura de gestión modular y ampliable

…permiten …

- Implementación de filosofía DevOps
- Fácil desarrollo mediante microservicios
- Despliegues de servicios robustos y potentes
- Independencia de la infraestructura subyacente

Concepto de contenedor



Definición y despliegue de servicios

```
version: '2'
services:
db:
    image: mariadb
        restart: always
    environment:
        -MYSQL_ROOT_PASSWORD=clavedeadministrador
        -MYSQL_PASSWORD=clavemysql
        -MYSQL_DATABASE=nextcloud
        -MYSQL_USER=nextcloud

app:
    image: nextcloud
        restart: always
    ports:
        -8080:80
    links:
        -db
    environment:
        -MYSQL_PASSWORD= clavemysql
        -MYSQL_DATABASE=nextcloud
        -MYSQL_USER=nextcloud
        -MYSQL_HOST=db
```

docker-compose up -d

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Protección individual en el ciberespacio

Autor: Saiz Blanco, José Manuel (jmsaizb@protonmail.com)
Directora: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)

Resumen – La ciberseguridad y la privacidad online es una de las mayores preocupaciones de la sociedad actual, que va en claro aumento con motivo de la masiva adopción de nuevos dispositivos conectados.

Los usuarios de las distintas tecnologías necesitan aprender ciertos hábitos de uso seguro que les ayudarán, no solo a evitar ser víctimas de algún ataque o engaño, sino también para su futuro profesional, pues poseer cierta cultura en ciberseguridad es un requisito cada vez más demandado.

Este trabajo, utilizando un lenguaje sencillo, dirigido a cualquier persona, sin importar su edad o nivel de conocimientos en informática, pretende enseñar los fundamentos básicos en ciberseguridad que le permitan utilizar, de una forma cómoda y segura, las nuevas tecnologías.

Para ello, el trabajo se dividirá en una serie de apartados que tienen por objetivo cubrir la gran mayoría de casos posibles con los que se puede encontrar cualquier usuario cuando hace uso de los distintos dispositivos que usa a diario. En cada apartado se explicará previamente qué es y para qué sirve la funcionalidad a tratar. Posteriormente se explicará cómo los ciberdelincuentes intentan explotar sus vulnerabilidades o defectos de configuración para, finalmente, acabar cada apartado con unas recomendaciones de seguridad que intentarán evitar o mitigar los efectos indeseados de alguno de esos ataques o engaños.

Para la confección de este trabajo, el autor se ha basado en el conocimiento adquirido como usuario de estas tecnologías, por su experiencia personal como profesor de ciberseguridad y trabajo en distintos departamentos de ciberdefensa en el Ministerio de Defensa de España, así como de la recopilación diaria y más actualizada de los distintos medios de comunicación que se hacen eco de estos mismos asuntos a nivel internacional.

1. Introducción

La ciberseguridad y la privacidad online es una de las mayores preocupaciones de la sociedad actual que va en claro aumento con motivo de la masiva adopción de nuevos dispositivos conectados.

Los usuarios de las distintas tecnologías necesitan aprender ciertos hábitos de uso seguro que les ayudarán, no solo a evitar ser víctimas de algún ataque o engaño, sino también para su futuro profesional, pues poseer cierta cultura en ciberseguridad es un requisito cada vez más demandado.

Este trabajo, utilizando un lenguaje sencillo, dirigido a cualquier persona, sin importar su edad o nivel de conocimientos en informática, pretende enseñar los fundamentos básicos en ciberseguridad que le permitan utilizar, de una forma cómoda y segura, las nuevas tecnologías.

Para ello, el trabajo se ha dividido en una serie de apartados que tienen por objetivo cubrir la gran mayoría de casos posibles con los que se puede encontrar cualquier usuario cuando hace uso de los distintos dispositivos que usa a diario. En cada apartado se explica previamente qué es y para qué sirve la funcionalidad a tratar. Posteriormente se explicará cómo los ciberdelincuentes intentan explotar sus vulnerabilidades o defectos de configuración para, finalmente, acabar cada apartado con unas recomendaciones de seguridad que ayudarán a evitar o mitigar los efectos indeseados de alguno de esos ataques o engaños. Todo ello, sin dejar de lado la constante preocupación por desenvolvernos online de manera segura para proteger también nuestra privacidad.

Para la confección de este trabajo, el autor se ha basado en el conocimiento adquirido durante años como usuario de todas esas tecnologías, en su experiencia personal como profesor de ciberseguridad y trabajo en distintos departamentos de ciberdefensa en el Ministerio de Defensa de España, así como de la recopilación diaria y más actualizada de los distintos medios de comunicación que se hacen eco de estos mismos asuntos a nivel internacional.

2. Desarrollo

El software se ha comido el mundo, como resultado, el mundo es jaqueable.

Nos encontramos inmersos en un mundo completamente digitalizado donde las nuevas tecnologías crecen a un ritmo vertiginoso. Podemos afirmar que estamos asistiendo a una integración cada vez mayor entre el mundo físico y el digital, donde el primero queda representado por el segundo a través de la inmensa cantidad de datos digitales generados por personas, sensores o dispositivos que acaban formando parte de ese 5.º dominio, que los militares, conocemos como *ciberespacio*, por detrás de tierra, mar, aire y espacio.

Estamos viendo como la inmensa mayoría de la población mundial ya posee algún tipo de dispositivo electrónico con conexión a Internet como: teléfonos móviles, relojes inteligentes, tabletas, el router de casa, ordenadores personales y un sinfín de dispositivos inteligentes que los identificamos con la palabra smart delante y que, poco a poco, van adentrándose en todos nuestros hogares: smart TV, smart lock, enchufes inteligentes, asistentes personales de voz, cámaras de seguridad, etc.

Como era de esperar en este difícil mundo en el que vivimos, junto a este prometedor panorama tecnológico, también aparece otra variable en la ecuación que no podemos olvidar y es la que representa los nuevos peligros con los que tenemos que lidiar en el mundo digital o, al menos, nos obliga a estar en estado de alerta para no ser víctimas de un ataque o engaño cibernético. El hecho de que ahora la amenaza no se presente en forma física, no quiere decir que sus efectos no puedan ser devastadores, por lo que debemos estar preparados para defendernos ante estos nuevos riesgos, de tal forma que podamos ser capaces de evitar o minimizar sus posibles daños.

El título de este trabajo lleva por nombre: Protección individual en el ciberespacio, queriendo poner especial énfasis en individual puesto que, a día de hoy, podría dar la impresión que la ciberseguridad es solo cosa de empresas y organizaciones, ya que podemos encontrarnos infinidad de foros, libros y páginas web centradas en tratar la ciberseguridad de la infraestructura tecnológica de la empresa pero, quizás muy pocas publicaciones, centradas en divulgar la seguridad digital del individuo, aunque es cierto que, en nuestro país, existen organizaciones como el Centro Criptológico Nacional (CCN-CERT) y el Instituto Nacional de Ciberseguridad (INCIBE) que sí están realizando un gran trabajo. Sin olvidar al Mando Conjunto del Ciberespacio (MCCE) que realiza una función muy parecida solo que orientada al ámbito militar. Creo que el tema que nos ocupa es de tal calado que bien merecería la pena que se enseñara desde la formación más temprana en los colegios, con asignaturas que aborden, casi en exclusiva, la seguridad informática, ya que es algo con lo que todo ciudadano va a tener que lidiar a diario desde su niñez.

Teniendo en mente que la *seguridad total no existe*, nuestra labor debe centrarse en aprender a gestionar el riesgo, de manera que seamos capaces de proteger nuestros equipos y nos permita reconocer si estamos bajo la influencia de un posible ataque, así como desarrollar la capacidad de reaccionar ante tal probable circunstancia. Mientras utilicemos dispositivos conectados nunca podremos pretender conseguir absoluta *privacidad* o *seguridad*; cómo decía Joshua en la película Juegos de Guerra:

«A strange game. The only winning move is not to play».
(Un juego extraño. El único movimiento ganador es no jugar)

Pero no consiste en *no jugar/no utilizar Internet*, puesto que Internet no deja de ser una maravillosa herramienta que, por encima de todo, nos ofrece muchísimas comodidades y oportunidades.

Lo que sí que toda es que cada cual haga una pequeña valoración de lo que quiere proteger y, para eso, es importante que cada usuario determine su modelo de amenaza, que no es otra cosa que responderse a una serie de preguntas. Veámoslo con un ejemplo sobre cómo proteger nuestro hogar y, después, traslademos las mismas preguntas a nuestro entorno digital:

- ¿qué estás intentando proteger?: joyas, electrodomésticos, documentos financieros, pasaportes o fotos.
- ¿de quién lo quieres proteger?: los adversarios podrían incluir: ladrones, compañeros de habitación o invitados.
- ¿cómo es de probable que tenga la necesidad de protegerlo?: ¿Mi vecindario tiene un historial de robos? ¿Cuánto de confiables son mis compañeros de habitación / invitados? ¿Cuáles son las capacidades de mis adversarios? ¿Cuáles son los riesgos que debo considerar?
- ¿cómo de graves serían las consecuencias si no logras protegerlo?: ¿Tengo algo en mi casa que no pueda reemplazar? ¿Tengo tiempo o dinero para reemplazar esas cosas? ¿Tengo un seguro que cubra los bienes robados de mi casa?
- ¿qué inconvenientes estas dispuesto a afrontar para hacer esto?: ¿Estoy dispuesto a gastarme dinero en comprar una caja fuerte para documentos sensibles? ¿Puedo permitirme comprar un candado de alta calidad? ¿Tengo tiempo para abrir una caja de seguridad en mi banco local y guardar mis objetos de valor allí?

La respuesta a estas preguntas nos hará utilizar unas medidas de seguridad u otras, en algunos casos no será demasiado importante protegerlas y, en otros, resultará de vital importancia protegerlas a toda costa, como nuestras cuentas bancarias, contraseñas, seguridad de nuestros menores y, para ello, siempre habrá que estar dispuesto a sacrificar algo de comodidad y funcionalidad. A nadie le gusta tener que estar ingresando contraseñas continuamente para instalar aplicaciones o tener que meter un pin en el teléfono móvil cada vez que se quiere consultar, pero si no se hace, a la primera de cambio que se pierda o lo roben, ya no habrá forma de que extraigan todos tus datos. Cuando los ciberdelincuentes se hacen con datos sensibles, acto seguido comienzan los chantajes y extorsiones que demandan una cantidad de dinero para no hacerlos públicos o utilizarlos en tu contra. En definitiva, la seguridad siempre lleva un peaje molesto que debemos asumir a cambio de estar más seguros.

Mantener la seguridad cibernética debería ser tan común como mantener la seguridad física. Si hoy en día todos sabemos que debemos cerrar las

puertas de casa o ponernos los cinturones de seguridad al conducir, en no más de diez años, se tendrá el mismo nivel de conciencia para garantizar que también estamos digitalmente seguros.

Una vez alcanzado dicho objetivo y ya partiendo de una base aceptable de conocimiento, las empresas tendrán más fácil conseguir esa implicación de sus trabajadores que les permita alcanzar y mantener ciertos estándares de seguridad, los cuales, incluso podrían llevarse un paso más allá, mediante la ampliación a formación más avanzada que ayude a mantener la empresa bajo unos niveles más que aceptables de seguridad.

Por la cuenta que le trae al negocio y por la seguridad de clientes y proveedores, todas las empresas, sin importar el tamaño, deberían acelerar la concienciación de *todo* su personal en materia de ciberseguridad y no solo al área de sistemas o tecnología. Para ello sería buena idea crear un plan de capacitación en ciberseguridad para sus empleados. Un empleado capacitado no solamente deja de estar encorsetado en el famoso grupo referido como el eslabón más débil, sino que, además, puede detectar e informar al responsable de seguridad de la empresa sobre algún tipo de ataque que esté observando, resultando, así como el primer punto de defensa de la empresa; por el contrario, un empleado que no esté entrenado ni siquiera se va a enterar que fue víctima de un ataque.

Si bien la mayoría de las empresas tienen bastante claro la importancia de la seguridad informática, la seguridad privada, la del individuo normal y corriente, también debería estar totalmente interiorizada por toda la sociedad y, para colaborar con tal fin, este trabajo muestra cientos de consejos que, de una manera u otra, ayudan a la **protección individual en el ciberespacio.**

3. Conclusiones

En las conclusiones me hubiera gustado decir que ojalá el lector nunca tuviera la necesidad de llevar a la práctica las estrategias aquí expuestas, pero me temo que, a menos que viva en una cabaña, alejado de la civilización y no utilice ningún aparato electrónico conectado a Internet, ese deseo queda ya como algo imposible. Además, esa tampoco es la solución, a millones de personas en todo el mundo les encanta la idea de la transformación y utilizar toda esa nueva gama de tecnología que, aunque es cierto que añade peligros, su razón de ser es la de hacernos la vida más fácil y cómoda.

Lo que sí es cierto es que leer este trabajo ya es un buen comienzo. No hay tiempo que perder a la hora de aprender a securizar nuestra vida digital con el noble objetivo de proteger nuestra privacidad y seguridad online. Hay que adoptar una postura proactiva a la hora de protegernos, evitando, en la medida de lo posible, tener que acudir a una defensa reactiva cuando el daño ya está hecho o todavía está en curso.

Una vez se han adquirido los conocimientos necesarios para desenvolverse en el mundo digital actual, cada persona experimentará la tranquilidad de vivir en un ambiente seguro del que se beneficiará también su familia y, cuando un incidente haya sido inevitable, el lector podrá reaccionar ante un problema que ya ha dejado de serle desconocido, lo cual, es un buen comienzo para mitigar su efecto y evitar que cunda el pánico.

Si el lector ha seguido la gran parte de las estrategias de este trabajo, yo, como autor del mismo, puedo garantizar que su vida digital se habrá visto enormemente fortalecida. Desde ahora se habrá convertido en un objetivo extremadamente difícil de hackear o espiar, lo que obliga a la mayoría de ciberdelincuentes a desecharle como objetivo y centrarse en otros objetivos más fáciles que todavía descuidan sus hábitos online.

La mayoría de los consejos expuestos son consejos básicos que todos, expertos y principiantes, no tenemos más remedio que utilizar si queremos tener una vida relativamente segura cuando utilizamos tanto dispositivo conectado a Internet.

La seguridad total no existe, pero en nuestras manos está la solución para acercarnos a la excelencia, y leer este trabajo ya es un gran paso.

Agradecimientos

Por un lado, quisiera dar las gracias a la Universidad de Vigo por permitirme realizar como TFM la temática que solicité y que tanto me apasiona. También me gustaría agradecer a la universidad que me permitiera realizar un trabajo que en un futuro se continuará para que acabe siendo un libro que se publicará en la editorial RA-MA con el nombre Defensa personal en la era digital, con el fin de que el conocimiento llegue a todos los públicos.

Por otro lado, quiero agradecer al Ministerio de Defensa español el haberme becado para realizar este máster del que tanto he podido aprender en relación a la dirección y gestión de las tecnologías de información y comunicaciones.

Por último y no menos importe, mi más sincero agradecimiento a la tutora del trabajo: Milagros Fernández Gavilanes por la inestimable ayuda prestada.

Referencias

[1] I. Faes, (26 06 2021), «Ciberataques: ¿Se puede despedir a los trabajadores que pican en el fraude?» El Economista. [En línea]. Available: https://www.eleconomista.es/legislacion/noticias/11292289/06/21/Ciberataques-Se-puede-despedir-a-los-trabajadores-que-pican-en-el-fraude.html.

[2] S. Shackford, (21 04 2021), «Lawmakers Look To Stop the Feds From Secretly Buying Your Private Data» Reason. [En línea]. Available: https://reason.com/2021/04/21/lawmakers-look-to-stop-the-feds-from-secretly-buying-your-private-data/.

[3] P. Mozur, C. Kang y A. Satariano, 30 05 2021), «A Global Tipping Point for Reining In Tech Has Arrived» The New York Times. [En línea]. Available: https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

[4] Coalición Internacional, (23 06 2021), «Open Letter to EU and US policymakers». [En línea]. Available: https://fil.forbrukerradet.no/wp-content/uploads/2021/06/2021-06-22-letter-to-policymakers-surveillance-based-advertising.pdf.

[5] Norwegian Consumer Council Translated from Norwegian by the Norwegian Consumer Council, «Surveillance-based advertising» 06 2021. [En línea]. Available: https://fil.forbrukerradet.no/wp-content/uploads/2021/06/consumer-attitudes-to-surveillance-based-advertising.pdf.

[6] The Hacker News, (01 03 2021), «Why do companies fail to stop breaches despite soaring IT security investment?». [En línea]. Available: https://thehackernews.com/2021/03/why-do-companies-fail-to-stop-breaches.html.

[7] H. Granoff, (16 04 2021), «How the Biden Administration Can Make Digital Identity a Reality» Dark Reading. [En línea]. Available: https://beta.darkreading.com/operations/how-the-biden-administration-can-make-digital-identity-a-reality.

[8] M. Dodge, (03 2021), «The Edge». [En línea]. Available: https://www.darkreading.com/edge/theedge/how-to-protect-vulnerable-seniors-from-cybercrime/b/d-id/1340322.

[9] Hack Players, (02 2021), «Los sitios de los principales cibercriminales en la Deep Web». [En línea]. Available: https://www.hackplayers.com/2021/02/sitios-cibercriminales-deepweb.html.

[10] BSA, (2018), «Gestión de software: obligación de seguridad, oportunidad de negocios. Encuesta Global de Software» BSA.

[11] Krebs on Security, (17 05 2021), «Try This One Weird Trick Russian Hackers Hate». [En línea]. Available: https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/.

[12] V. Jakkal, (15 09 2021), «The passwordless future is here for your Microsoft account», Microsoft. [Online]. Available: https://www.microsoft.com/security/blog/2021/09/15/the-passwordless-future-is-here-for-your-microsoft-account/.

[13] J. Marquez, (26 02 2021), «LastPass te rastrea más que cualquier otro gestor de contraseñas: tiene siete “trackers” integrados» Hipertextual. [En línea]. Available: https://hipertextual.com/2021/02/lastpass-te-rastrea-mas-que-cualquier-otro-gestor-tiene-siete-trackers-integrados.

[14] D. Miessler, (03 2021), «Daniel Miessler: The Consumer Authentication Strength Maturity Model (CASMM)». [En línea]. Available: https://danielmiessler.com/blog/casmm-consumer-authentication-security-maturity-model-2/.

[15] B. Toulas, (22 11 2021), «Biometric auth bypassed using fingerprint photo, printer, and glue» Bleeping Computer. [En línea]. Available: https://www.bleepingcomputer.com/news/security/biometric-auth-bypassed-using-fingerprint-photo-printer-and-glue/.

[16] P. Breyer, (06 07 2021), «Patrick Breyer: Chatcontrol. EU Parliament approves mass surveillance of private comms». [En línea].

Available: https://www.patrick-breyer.de/en/chatcontrol-european-parliament-approves-mass-surveillance-of-private-communications/.

[17] P. Elkind, J. Gillum y C. Silverman, «How Facebook Undermines Privacy Protections for Its 2 Billion WhatsApp Users,» Propublica.org, 7 09 2021. [En línea]. Available: https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users.

[18] C. Cimpanu, (30 11 2021), «FBI document shows what data can be obtained from encrypted messaging apps» The Record. [En línea]. Available: https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/.

[19] F. Bracero, (05 05 2021), «La Vanguardia». [En línea]. Available: https://www.lavanguardia.com/tecnologia/20210505/7429802/signal-deja-evidencia-facebook.html.

[20] J. Tidy, (09 2019), «BBC: Why phones that secretly listen to us are a myth». [En línea]. Available: https://www.bbc.com/news/technology-49585682. [Último acceso: 04 2021].

[21] E. Dans, (03 2021), «Enrique Dans: Visualizando la cámara de eco». [En línea]. Available: https://www.enriquedans.com/2021/03/visualizando-la-camara-de-eco.html.

[22] Okey, «There's nothing funny about these impersonations» [En línea]. Available: https://okeymonitor.com/. [Último acceso: 03 2021].

[23] I. Analytics, (03 2021), «IoT 2020 in Review: The 10 Most Relevant IoT Developments of the Year». [Online]. Available: https://iot-analytics.com/iot-2020-in-review/.

[24] IST, (2021), «Combating Ransomware» Institute for Security and Technology.

[25] «Web de La Moncloa,» [En línea]. Available: http://www.lamoncloa.gob.es. [Último acceso: 13 enero 2015].

[26] J. Rodríguez y V. Fernández, (2010), «Cómo redactar el estado del arte de un trabajo, Editorial Genios».

[27] P. Martínez y A. García, (2013), «Cómo escribir una buena memoria de TFG», Publicaciones del 2000.

[28] A. Pérez, «Cómo escribir una bibliografía», Nuevas publicaciones.

[29] Norton, (18 01 2021), «Norton». [En línea]. Available: https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html. [Último acceso: 02 2021].

[30] Xakata, (10 02 2021), «Xakata». [En línea]. Available: https://www.xataka.com/privacidad/cookies-suben-nivel-descubren-metodo-para-rastrear-al-usuario-internet-haciendo-uso-favicons. [Último acceso: 02 2021].

[31] NIST, «Privacy Framework» National Institute of Standards and Technology, [En línea]. Available: https://www.nist.gov/privacy-framework. [Último acceso: 03 2021].

[32] L. (03 2021), «It's time to stop using SMS for anything». [En línea]. Available: https://lucky225.medium.com/its-time-to-stop-using-sms-for-anything-203c41361c80.

[33] J. Cox, (05 2017), «Vice: We Were Warned About Flaws in the Mobile Data Backbone for Years. Now 2FA Is Screwed». [En línea]. Available: https://www.vice.com/en/article/xyezmn/we-were-warned-about-flaws-in-the-mobile-data-backbone-for-years-now-2fa-is-screwed. [Último acceso: 03 2021].

[34] C. P. J. Ireton, (2020), Periodismo, "noticias falsas" & desinformación: manual de educación y capacitación en periodismo, París: UNESCO.

[35] Mitre, (07 2021), «MITRE D3FEND Knowledge Graph». [En línea]. Available: https://d3fend.mitre.org/.

Protección Individual en el Ciberespacio

Autor: José Manuel Saiz Blanco
Director/es: Milagros Fernández Gavilanes

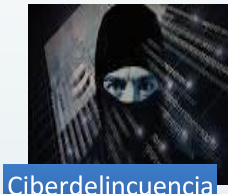
Universidad de Vigo

EN CASA

EN EL TRABAJO

DE VIAJE

Hacktivismo

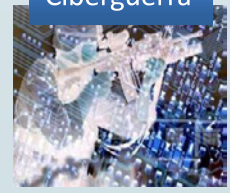


Ciberdelincuencia

Ciberterrorismo

Ciberespionaje

Ciberguerra



Trabajos Fin de Máster

Especialidad en Sistemas y Tecnologías de la Telecomunicación

Redes móviles 5G y su impacto en Internet de las cosas

Autor: Jiménez Cancho, Daniel (myinbox.daniel@gmail.com)
Directores: Merino Gil, Miguel Ángel (externo.mmerino@cud.uvigo.es)
y Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – Los sistemas de telecomunicación permiten el intercambio de información a distancia y, desde sus inicios, han jugado un papel fundamental en la sociedad y han evolucionado según la demanda. Las redes de comunicación móvil son un ejemplo de ello ya que, en apenas unas décadas, han pasado de solo transmitir voz a soportar un abanico innumerable de servicios. La evolución sigue un ritmo vertiginoso y las expectativas para el 5G son elevadas. Se espera una red potente y flexible que cubra los tres escenarios planteados (eMBB, URLLC, mMTC), cada uno con requisitos muy diversos. Para conseguirlo es necesario un cambio radical en la arquitectura de la red, que pasará a estar softwarizada mediante tecnologías como NFV, SDN y MEC.

Uno de los ámbitos más interesados en 5G es Internet de las cosas, ya que la conectividad es crítica en el desarrollo de estas soluciones, pero las tecnologías de comunicación inalámbrica tradicionales no cubren sus necesidades. Como consecuencia surgieron las redes LPWA de bajo consumo y largo alcance, entre las que destacan las soluciones NB-IoT y LTE-M basadas en redes móviles. Su rendimiento cubre los requisitos especificados por la ITU para el escenario mMTC, por lo que han sido incluidas en la especificación 5G. Sin embargo, existen otros tipos de IoT con requerimientos más estrictos para los que se empleará la interfaz radio 5G NR.

Con todo ello, 5G se posiciona como una solución completa y estándar para las comunicaciones en aplicaciones de IoT, lo que facilitará su despegue definitivo.

Palabras clave – 5G, Internet de las cosas, redes LPWA, network slicing.

1. Introducción

Una de las características del ámbito de las tecnologías de la información y comunicación es que está en continua evolución con el objetivo de mejorar las capacidades de los sistemas. Las redes de comunicación móvil son ajenas a ello y, desde su origen, se han desarrollado para satisfacer las necesidades que demandaba el mercado para cubrir distintos escenarios.

Diseñadas inicialmente para dar solo servicio de comunicación de voz, han ido progresando de generación en generación para ampliar el abanico de posibilidades. Este hecho ha ido acompañado de una adopción importante en las sociedades desarrolladas, ya que han permitido el intercambio de cada vez más información, más rápido, desde cualquier lugar y en cualquier momento. Como referencia, a nivel global, a finales del año 2020, el 67 % (5.200 millones) de la población tenía acceso a la red móvil, a la vez que la industria generó un 5.1 % (4.400 billones de dólares) del PIB global [1].

La evolución no se detiene y aparecen casos de uso nuevos que requieren capacidades mayores o distintas en cuanto a conectividad se refiere. Las redes 4G actuales no pueden cubrir estos requisitos, lo que impide el desarrollo de servicios innovadores. Algunos ejemplos destacables son: el internet de las cosas, con una cantidad ingente de dispositivos conectados a la red; la realidad virtual y su demanda de gran ancho de banda; los coches autónomos, en los que la latencia, seguridad y fiabilidad de la red es imprescindible; o las ciudades inteligentes, en las que los requisitos anteriores se entremezclan. En este punto es donde surge el desarrollo de las redes de comunicación móvil 5G, que espera aunar las tecnologías necesarias para conseguir una red potente, flexible, segura y eficiente que cubra las necesidades expuestas anteriormente.

Uno de los escenarios planteados para 5G será el de las comunicaciones masivas, ligadas a IoT, debido a la proliferación de multitud de dispositivos conectados a la red transmitiendo información. De hecho, se espera que en 2025 haya alrededor de 24.000 millones de este tipo de conexiones, duplicando así los valores de 2020, así como que genere ingresos de 900.000 millones de dólares (1). Por tanto, se espera que 5G pueda solucionar los retos para la conectividad que esto entraña y que las soluciones actuales no han conseguido superar, de forma que suponga un impulso clave para el desarrollo de IoT. En este contexto, se propone concretar el estudio del 5G sobre el ámbito IoT para analizar el impacto que supone, previo estudio de la situación actual en cuanto a soluciones de comunicación inalámbrica para IoT.

Por tanto, los objetivos que se establecen para el TFM son los siguientes:

1) Tratar el estado del arte de las redes de comunicación móvil.
2) Estudiar la tecnología 5G desde diversos ángulos.

3) Examinar el concepto de IoT e identificar sus requisitos y retos en cuanto a conectividad.

4) Analizar cómo se posiciona 5G para evaluar su impacto en IoT.

2. Desarrollo

2.1. Redes de comunicación móvil 5G

Las redes de comunicación móvil actuales ofrecen unas capacidades y alcance muy superiores a las de su origen. A pesar de que el 4G sigue mejorando, las nuevas demandas de requisitos suponen un factor clave para el desarrollo de la nueva generación 5G:

— Rápido aumento de la demanda del tráfico de datos, tanto en cantidad como en velocidad.

— Mayor número de dispositivos conectados a la red en todos los ámbitos... y con IoT en el horizonte cercano. Esto supone una densidad elevada de conexiones simultáneas que la red no puede gestionar de forma óptima.

— Mejoras en la eficiencia energética, tanto de la red como de los elementos conectados.

— Los operadores móviles deben mejorar la eficiencia en el mantenimiento y operación de la red.

— Dotar de conectividad a nuevos casos de uso y aplicaciones, de forma que se abran nuevas oportunidades para los operadores móviles de generar beneficios. El coche autónomo, el IoT, las ciudades inteligentes, la industria 4.0... parecen cada vez más cercanos, pero tienen requisitos de conectividad muy específicos que no cubren las redes actuales.

Ante este escenario, la ITU publicó en septiembre de 2015 la recomendación M.2083: *IMT Vision: Framework and overall objectives of the future development of IMT for 2020 and beyond* [2], en la que se define la visión de las redes 5G y un amplio abanico de capacidades ligadas a los casos de uso previstos. Esto implica que también haya una gran variedad de requisitos, por lo que es necesario que la flexibilidad sea uno de los principios de diseño de estas redes. Por ello, se resalta que las capacidades que se definen en IMT-2020 tendrán distinta relevancia y aplicación para cada escenario:

— *Enhanced Mobile Broadband* – eMBB: el requisito principal es un ancho de banda muy alto para transferir una cantidad de datos elevada a gran velocidad. Por tanto, podría decirse que se trata de la evolución natural y a corto plazo de las redes de comunicación móvil actuales en cuanto a mejoras de esos parámetros.

- *Massive Machine Type Communication* – mMTC: el requisito principal es soportar el acceso a la red de una cantidad ingente de dispositivos para transmitir datos de manera concurrente. Este sería el caso de las comunicaciones M2M necesarias para usos como IoT, en los que numerosos dispositivos transmiten datos de bajo volumen, pero de manera continua. Todo ello con el condicionante de hacerlo eficientemente.
- *Ultra-reliable and Low Latency Communications* – URLLC: los requisitos de las comunicaciones son muy estrictos en cuanto a latencia, disponibilidad, fiabilidad y seguridad por la naturaleza crítica de los servicios. Esto habilitaría aplicaciones de tiempo real y el concepto de internet táctil.

El 3GPP comenzó a trabajar en el desarrollo de soluciones para cumplir con los requisitos de IMT-2020 y, como resultado de ello va aprobando y desarrollando sucesivas *releases* para su propuesta a la ITU y posterior estandarización. En este sentido, la *release* 15 ya señaló dos modos de despliegue de las redes de comunicación móvil 5G debido a que deberá acometerse de manera progresiva y convivir con el actual LTE [3]. Durante las primeras etapas se desplegará el 5G en modo *non-stand alone*, que utiliza la nueva RAN para el plano de usuario, pero mantiene el *core* EPC de las redes LTE para el plano de control. Esta fase permitirá mejorar el ancho de banda gracias al uso de nuevas frecuencias, siguiendo así la evolución tradicional de las redes móviles. Finalmente, el 5G en modo *stand alone* estará disponible una vez que se despliegue la infraestructura necesaria, de forma que se elimine la dependencia del EPC de LTE y se use el *core* 5G. Esto permitirá aprovechar las nuevas características y funcionalidades que proporciona la red, tanto a nivel de operación y gestión como de capacidades.

En cuanto a la arquitectura de las nuevas redes 5G, destaca el hecho de que pasa a estar orientada a servicios y virtualizada, lo que favorece su flexibilidad, descentralización y modularidad. Se aplican conceptos como NFV, SDN y computación en el borde, dando como resultado la *softwarización* de la red [4]. Todos estos cambios ocurren tanto en el core como en la RAN, lo que permite aplicar el concepto de *network slicing* para proporcionar múltiples redes lógicas con características distintas y particulares a la aplicación a la que dan conectividad, pero todas sobre una misma infraestructura de red. De esta forma, los operadores móviles podrán ofertar *slices* optimizadas para cada tipo de vertical según los requisitos que demande el caso de uso concreto, de una forma ágil y eficiente.

2.2. Conectividad en IoT

Las soluciones en el ámbito de IoT son variadas y existe una gran heterogeneidad. A pesar de ello, se basan en una arquitectura de alto

nivel formada por tres capas [5]: la capa de percepción u objetos y dispositivos, la capa de sistemas de datos y aplicaciones y la capa de red o comunicaciones que permite el tránsito de datos entre las dos anteriores. Como consecuencia de esta estructura, la conectividad supone uno aspecto crítico en las soluciones IoT. A lo largo de los años se han utilizado tecnologías de diversa índole para permitir la comunicación en IoT dependiendo del escenario y sus requerimientos, por lo que actualmente existe una gran heterogeneidad y fragmentación.

Las comunicaciones en IoT presentan características y requisitos muy diferentes con respecto a las comunicaciones tradicionales, ya que estas últimas están centradas en los humanos:

- El número de dispositivos es muy elevado, dado que la visión final es que cualquier cosa pueda estar conectada, por lo que la red debe ser capaz de gestionar dicha cantidad.
- Los patrones de comunicación son distintos a los de las comunicaciones humanas, ya que predomina el tráfico periódico a ráfagas, y mayor volumen en la subida que en la bajada.
- Los dispositivos son de bajo coste, lo que implica que tienen recursos limitados.
- Los equipos tienen acceso limitado a la energía, por lo que deben tener un consumo energético lo más reducido posible para maximizar su vida útil.
- Como consecuencia de la gran cantidad de elementos conectados, es necesario que la instalación y puesta en marcha sea lo más sencilla y ágil posible.

Dado que las numerosas alternativas de conectividad inalámbrica empleadas tradicionalmente no han conseguido imponerse como soluciones globales para IoT por sus limitaciones, e impulsado por las perspectivas de crecimiento y potencial económico de Internet de las cosas, surgen las denominadas redes LPWA. Sus premisas son proporcionar comunicaciones inalámbricas con un consumo energético reducido y amplia cobertura, adecuadas para las características de IoT. En este escenario aparecen dos enfoques distintos: las basadas en el uso de espectro no licenciado (LoRaWAN® y Sigfox) y las que hacen uso de espectro licenciado por estar basadas en tecnología celular (NB-IoT y LTE-M) [6].

Con respecto a las primeras, el uso de banda libre promete menores costes de despliegue, así como mayor optimización en cuanto a cobertura y consumo energético frente a las redes móviles tradicionales. En cuanto a sus diferencias, destaca que Sigfox se trata de una operadora de red global que se apoya en operadoras locales y funciona mediante suscripciones anuales, mientras que LoRaWAN® es una tecnología que los fabricantes pueden integrar en sus dispositivos y certificarlos para garantizar la interoperabilidad.

En cuanto a las tecnologías *cellular IoT*, presentan como ventajas su escalabilidad, su inmensa huella global y la seguridad y fiabilidad inherentes a las redes de comunicación móvil. Tanto NB-IoT como LTE-M han sido desarrolladas por el 3GPP para satisfacer los requisitos de conectividad de IoT, y justifican la existencia de ambas frente a una única porque presentan características distintas para ampliar el abanico de escenarios que cubren. Mientras que NB-IoT ofrece tasas binarias muy bajas a cambio de consumos y costes muy reducidos y mayor densidad de conexiones, LTE-M ofrece mayor capacidad, menor latencia y soporte a movilidad.

2.3. 5G para IoT

Partiendo de la base de que la ITU indicó para IMT-2020 que los requisitos establecidos no aplican de manera concurrente, sino que son de aplicación según el caso de uso, para IoT masivo hay que tener en cuenta los asociados al escenario mMTC. La recomendación de la ITU M.2410 [7] concreta que el único requerimiento es el de la densidad de conexiones, cuyo valor fija en un millón por kilómetro cuadrado. Además, es interesante destacar que el parámetro de eficiencia energética está asociado al caso de uso eMBB y no hace referencia a mMTC, cuando el consumo energético es uno de los aspectos más relevantes en IoT, como ya se ha indicado.

Teniendo esto en cuenta, con la *release* 15, el 3GPP realizó una autoevaluación de las tecnologías LTE-M y NB-IoT para analizar su rendimiento y comprobar si cumplían lo establecido para IMT-2020 para las comunicaciones de tipo mMTC. Los resultados mostraron que ambas son válidas para cubrir el requerimiento de una densidad de conexiones superior a un millón por kilómetro cuadrado, manteniendo además una latencia inferior a los diez segundos [8]. Como consecuencia de estos resultados, el 3GPP ha propuesto a la ITU estas dos tecnologías como solución para cubrir el caso de uso de mMTC (asociado a IoT masivo) para IMT-2020. De hecho, el 3GPP ha acordado que los escenarios que requieran redes LPWA se seguirán abordando mediante la evolución de NB-IoT y LTE-M, descartando el desarrollo de una nueva interfaz radio [9] y reforzando la idea de que ambas soluciones forman parte de las redes de comunicación móvil 5G. Además, unido a lo anterior, es importante destacar que la interfaz radio de 5G NR se diseñó para permitir varios modelos de despliegue y uso del espectro, por lo que puede coexistir con NB-IoT y LTE-M y cubrir de esta forma los tres escenarios planteados para IMT-2020 mediante una única red 5G.

Por otro lado, si bien es cierto que el escenario habitual y clásico de IoT es aquel que requiere comunicaciones masivas entre máquinas, existen otras aplicaciones que tienen requisitos más exigentes o estrictos como soporte a la movilidad, menor latencia o mayor fiabilidad y disponibilidad. En este sentido, Ericsson define tres tipos de IoT adicionales al masivo (11):

- IoT de banda ancha: parte de los requisitos de mMTC en cuanto a cobertura y eficiencia energética, pero añade capacidades de eMBB para proporcionar comunicaciones con mayor tasa binaria y menor latencia.
- IoT crítico: adopta capacidades de URLLC para permitir latencias muy bajas (hasta 1 ms) con una fiabilidad y disponibilidad muy alta (del orden del 99.9999 %), características necesarias para aplicaciones con requisitos de conectividad muy estrictos por su criticidad.
- IoT para automatización industrial: comunicaciones IoT diseñadas específicamente para aplicaciones avanzadas en el ámbito de la automatización y control industrial. Este escenario ha generado gran interés y, de hecho, el 3GPP creó un grupo de trabajo dedicado a IoT industrial con el objetivo de mejorar la fiabilidad y soportar TSN [12].

Por tanto, teniendo en cuenta los requisitos de estos tres tipos de IoT no masivo, se antoja necesario acometerlos mediante el uso de la nueva interfaz radio 5G NR por dos motivos. El primer es que ni LTE-M ni NB-IoT proporcionan las capacidades para cubrir esas necesidades porque pertenecen al segmento LPWA, orientado a comunicaciones masivas de bajo consumo y largo alcance. El segundo motivo es que, precisamente, la nueva interfaz radio 5G NR está específicamente diseñada para cubrir esos requerimientos de aplicaciones más próximas a URLLC o eMBB.

3. Resultados y discusión

Con el trabajo desarrollado, queda claro que las redes de comunicación móvil permiten (o permitirán) cubrir las diferentes necesidades de conectividad de IoT en cada una de sus vertientes.

Por un lado, NB-IoT y LTE-M están diseñadas para dar conectividad en escenarios de IoT masivo, en los que la densidad de conexiones, la eficiencia energética, la cobertura y el bajo coste son aspectos imprescindibles. Por otro lado, los otros tres tipos de escenarios IoT no masivos que se han definido no pueden cubrirse con NB-IoT o LTE-M, por lo que deberán ser acometidos por la nueva interfaz radio 5G NR. Esta proporciona capacidades que permitirán cumplir con los requisitos de aplicaciones más exigentes en cuanto a ancho de banda, latencia, disponibilidad o fiabilidad de las comunicaciones.

Con todo ello, las tecnologías 5G definidas por el 3GPP facilitarán las comunicaciones para un amplio abanico de escenarios IoT con requisitos distintos bajo una misma red y en la que coexistirán distintas interfaces radio. Este hito es muy relevante y, teniendo en cuenta la trascendencia de la conectividad en IoT, supondrá un impacto importante en el despegue definitivo de IoT.

En primer lugar, el despliegue de 5G permitirá solventar en gran medida las dificultades existentes en la actualidad relativas a la conectividad. Estas tecnologías están estandarizadas, lo que permite la interoperabilidad entre los dispositivos y mejoras en su integración, y están diseñadas para cubrir un gran abanico de escenarios con diversos requisitos. Esto facilitará y agilizará el desarrollo de aplicaciones para IoT, evitando así el uso de varias tecnologías heterogéneas para las comunicaciones. Esto beneficiará tanto a los proveedores de soluciones IoT como a los clientes finales, ya que se reducirá el *time-to-market* de las aplicaciones y supondrá un abaratamiento de costes.

Asimismo, la tecnología 5G permite a los operadores crear redes lógicas con capacidades específicas mediante el *slicing* de la red, por lo que los proveedores de aplicaciones IoT contarán con varias fórmulas para contratar esas *slices*. Esto, unido al amplio rango de frecuencias que soporta 5G y la virtualización de las funciones de la red, posibilita que los proveedores de soluciones IoT contraten una solución de conectividad completamente a medida para cada aplicación o cliente. Además, gracias a la *softwarización* de la red y el uso conjunto de la virtualización y la computación en la nube, los desarrolladores podrán prototipar las aplicaciones y solicitar al proveedor de red el escalado de las capacidades para adecuarse a la demanda de forma ágil y dinámica.

También hay que añadir que el hecho de tratarse de redes móviles lleva una serie de ventajas implícitas, entre las que destaca la cobertura global, ya que presenta una huella tan extensa que, por defecto, habilita la conectividad en prácticamente cualquier lugar para soluciones IoT. Además, se trata de una red con un historial bien contrastado en cuanto a fiabilidad, disponibilidad y seguridad. Estas características son una razón más para que la conectividad no solo no suponga un impedimento para el despegue de IoT, sino que además lo favorezca.

Finalmente, desde el punto de vista de las operadoras, podrán proporcionar una red que cubra los distintos requisitos de las aplicaciones IoT. Teniendo en cuenta el gran volumen de conexiones que contempla el paradigma IoT y la posibilidad de ofertar redes personalizadas *ad-hoc* a los clientes, aparecen nuevas oportunidades de negocio y un mayor potencial de clientes para mejorar los resultados financieros. En este sentido, puede jugar un papel fundamental el sector industrial, el más pujante en cuanto a soluciones IoT por el creciente interés en la industria 4.0. Además, gracias a las características de 5G, podrán hacer todo ello de una forma ágil y eficiente sobre la misma infraestructura de red, reduciendo así los costes asociados a su despliegue, operación, mantenimiento y gestión.

4. Conclusiones

La primera idea clave es que 5G supone un cambio sustancial en cuanto a la evolución de las redes de comunicación móvil, ya que no solo busca

mayores tasas binarias, sino también disponer de una red flexible, potente y eficiente capaz de cubrir distintos casos de uso con requerimientos muy diversos. Como consecuencia, el 5G podrá proporcionar conectividad en los tres escenarios que se han definido: comunicaciones masivas con una gran densidad de conexiones y bajo consumo energético, comunicaciones de banda ancha móvil con tasas binarias muy elevadas y comunicaciones para aplicaciones críticas que requieren latencias muy bajas y fiabilidad y disponibilidad muy altas. El despliegue de esta nueva generación será progresivo según la capacidad de inversión disponible, y habrá varias etapas de transición en las que coexistirá con LTE.

Por otro lado, como consecuencia de estos objetivos tan ambiciosos para 5G, la arquitectura de la red cambia por completo, pasando a estar basada en microservicios virtualizados y separando el plano de control del plano de usuario, lo que permite la descentralización de la red para ganar en flexibilidad y agilidad en su mantenimiento y operación. Por tanto, puede decirse que 5G supone una *softwarización* de la red. Como consecuencia última de todo ello, se habilita el concepto del *slicing* de la red, que consiste en provisionar redes lógicas independientes con distintas capacidades adaptadas al cliente, pero operando sobre la misma infraestructura física de red.

Por otra parte, con respecto a IoT, se trata de un concepto que forma parte del conjunto de tecnologías disruptivas que culminará en la cuarta revolución industrial. Por ello hay numerosos sectores interesados en IoT para el desarrollo de nuevas aplicaciones que les permita mejorar la eficiencia y productividad de sus negocios. No obstante, para el despegue definitivo de IoT hay que considerar uno de los aspectos más críticos para el desarrollo de estas soluciones: la conectividad entre los elementos que la forman. En este sentido, destaca la existencia de una gran heterogeneidad y fragmentación de tecnologías empleadas tradicionalmente. El motivo de esto es que presentan características y limitaciones muy diversas, lo que dificulta la estandarización de soluciones, disminuye la agilidad y aumenta los costes.

Ante este escenario surgen las redes LPWA, caracterizadas por un bajo consumo energético y largo alcance, fundamentales por las características de IoT. Entre las tecnologías disponibles, destacan las basadas en el uso de espectro no licenciado (Sigfox y LoRaWAN®) y las denominadas *mobile* o *cellular* IoT desarrolladas por el 3GPP que emplean espectro licenciado (NB-IoT y LTE-M). A pesar de que todas ellas comparten las premisas LPWA, presentan algunas diferencias tanto técnicas como comerciales que hacen a unas más propicias que otras según el caso de uso.

Concretando sobre las soluciones *mobile* IoT, tanto NB-IoT como LTE-M cumplen con los requisitos estipulados por la ITU en IMT-2020 para las comunicaciones masivas. Por tanto, el 3GPP las ha incluido dentro de la especificación de las redes de comunicación móvil 5G y no contempla

nuevos desarrollos en ese sentido. Sin embargo, existen otros tipos de IoT que no son exclusivamente masivos, como son el de banda ancha, el crítico o el destinado a la automatización industrial. Estos escenarios IoT presentan requisitos más exigentes y estrictos en cuanto a la conectividad que las soluciones LPWA no pueden cubrir. En ese caso será necesario recurrir a la nueva interfaz radio 5G NR, que sí está diseñada para disponer de esas capacidades.

De esta forma, 5G se postula como una solución completa y estándar para las comunicaciones en aplicaciones de IoT, lo que facilitará su despegue definitivo.

Referencias

[1] GSMA. (2021), The Mobile Economy 2021. [Online]. [citado 2021 septiembre. Disponible en: https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/07/GSMA_MobileEconomy2021_3.pdf.

[2] ITU-R. (2015), Recommendation ITU-R M.2083-0. [Online]. [citado 2021 octubre. Disponible en: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!PDF-E.pdf.

[3] Guttman E. (2018), 5G Standardization in 3GPP. [Online]. [citado 2021 septiembre. Disponible en: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/3_Erik_Guttman.pdf.

[4] Observatorio Nacional 5G, (2020), 5G e Industria 4.0: retos y oportunidades de la cuarta revolución industrial. [Online]. [citado 2021 octubre. Disponible en: https://on5g.es/report/5g-e-industria-4-0/.

[5] Moxa. Achieving Interoperability for The Industrial IoT. [Online]. [citado 2021 diciembre. Disponible en: https://pages.moxa.com/Achieving-Interoperability-for-the-Industrial-IoT.html.

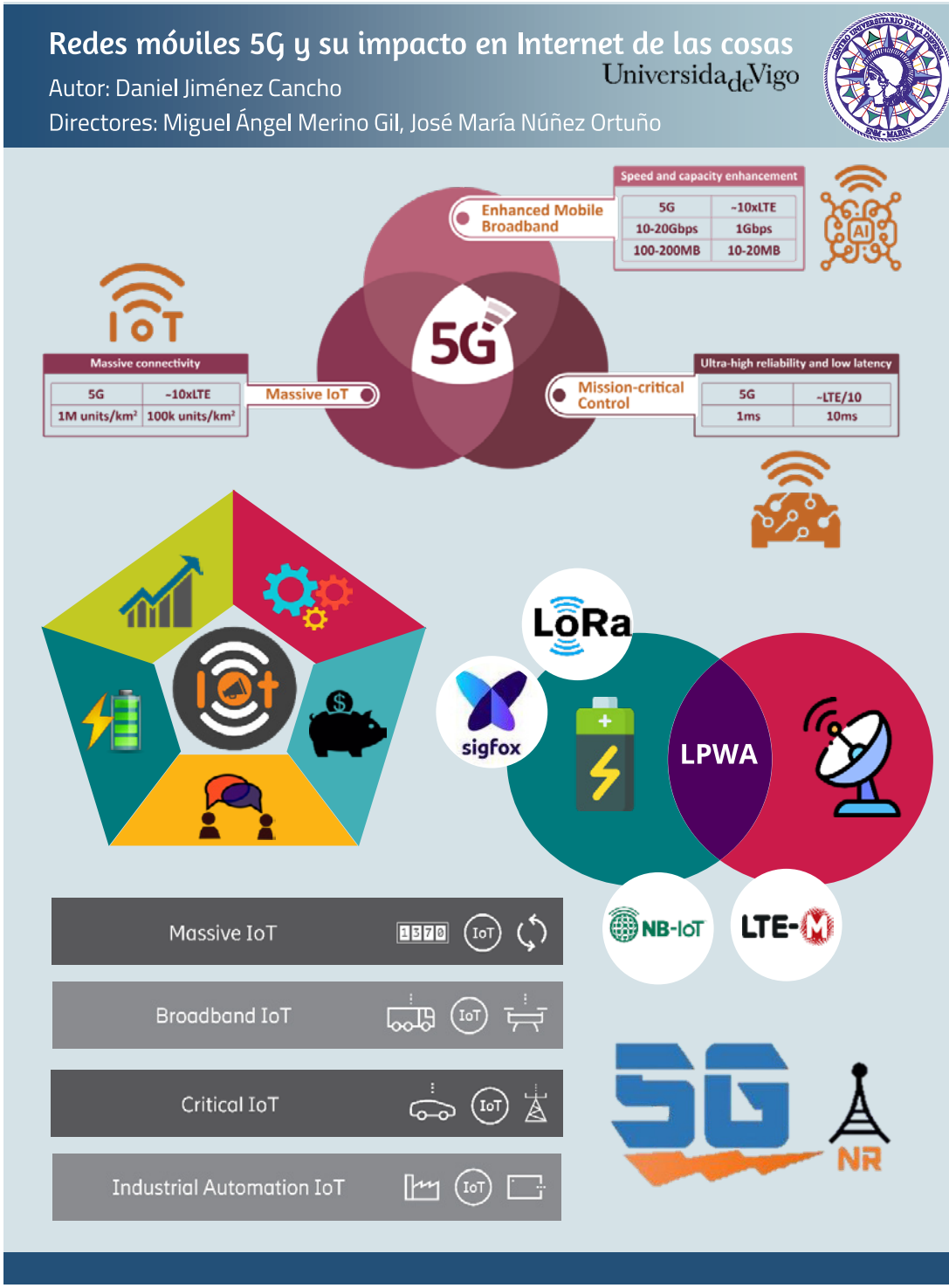
[6] COIT, (2020), Una visión práctica de las redes LPWA en IoT. [Online]. [citado 2021 diciembre. Disponible en: https://www.coit.es/noticias/una-vision-practica-de-las-redes-lpwa-en-iot.

[7] ITU-R. (2017), Report ITU-R M.2410-0. [Online]. [citado 2021 octubre. Disponible en: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf.

[8] Liberg O., (2018), LTE-M and NB-IoT meet the 5G performance requirements. [Online]. [citado 2021 diciembre. Disponible en: https://www.ericsson.com/en/blog/2018/12/lte-m-and-nb-iot-meet-the-5g-performance-requirements.

[9] 3GPP. (2018), Interim conclusions on IoT for Rel-16. [Online]. [citado 2021 diciembre. Disponible en: http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_79/Docs/RP-180581.zip.

[10] Vivier G. IoT: How 5G differs from LTE. [Online]; 2021 [citado 2021 diciembre. Disponible en: https://www.5gtechnologyworld.com/iot-how-5g-differs-from-lte/.



Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Comunicaciones en un Ejército de drones

Autor: Lorén Garay, Gonzalo
(historiagonzalo5331@gmail.com/glorgar@oc.mde.es)
Director: González Coma, José P. (jose.gcoma@cud.uvigo.es)

Resumen – En este trabajo se pretende exponer un caso hipotético, de una determinada operación militar ofensiva. Dicha operación se realizaría en un área de combate de 40 x 40 kilómetros. No es novedoso que en la actualidad estas operaciones se apoyen en drones. La novedad en este estudio, es realizar este tipo de operación solo y exclusivamente con drones dentro del área de combate. El número de drones que se calcula para llevar a cabo con éxito esa operación es de unos 5.000. Evidentemente la operación implicaría también una elevada intervención humana, pero sin que ningún humano entrara físicamente en el área de combate.

Desde el punto de vista técnico, el objetivo es atender a todos los requerimientos en cuanto a comunicaciones y posicionamiento que una operación de esta índole requeriría.

Por otro lado, se expondrán brevemente, y sin entrar demasiado en profundidad, todas aquellas cuestiones y problemas que requieren una decisión y resolución técnica, y que tienen que ver directamente con diversas asignaturas del máster.

El estudio ha tenido gran amplitud horizontal a costa de tener una limitada amplitud vertical. En él, se dan unas directrices estratégicas para acometer los diversos problemas técnicos.

Las soluciones aportadas han sido escogidas por el alumno de acuerdo a sus conocimientos (tanto los anteriores que poseía, como los adquiridos en el máster) y expuestas de forma esquemática y ordenada en un estudio de alto nivel.

Se considera que la tecnología para llevar a cabo esta operación está perfectamente asentada, y el problema principal radica en la consecución de la mezcla e implementación de las diferentes tecnologías de una forma coordinada y realista.

Palabras clave – Dron, posicionamiento, UAV, UGV, WiMAX, DTN.

1. Introducción

El objeto de este trabajo de fin de máster (TFM) es el diseño, a nivel teórico, de los sistemas de comunicación y posicionamiento de un *Ejército de drones* para una operación militar de gran envergadura.

No es novedoso el empleo de drones en el campo de batalla como auxiliar del combatiente humano. En este TFM se pretende estudiar una operación donde un bando actúe en un espacio de batalla solamente con drones, de manera que, en teoría, la operación se llevaría a cabo sin bajas humanas propias. Se pretende emplear en la operación de forma coordinada un número masivo de drones. A esto se le llama coloquialmente *enjambre*.

En la exposición del trabajo se mencionarán aspectos relativos a posicionamiento y comunicaciones. No obstante, será inexcusable tratar otros aspectos que servirán de *ambientación* para encajar la tecnología descrita en una situación real, lo cual aportará una visión de aplicación práctica de estas tecnologías. No se puede exponer la solución técnica a un problema si no se describe previamente el problema a resolver.

2. Desarrollo

2.1. Sistemas de localización y posicionamiento

Se trata la posibilidad de dotar a los drones de los sistemas de posicionamiento. Se proponen sistemas como GNSS, TACAN, DME y NDB. Normalmente los drones van a utilizar más de un sistema para que exista alternativa en caso de indisponibilidad del sistema de posicionamiento principal.

2.2. Sistemas de comunicación

Se analizan las posibilidades de las distintas comunicaciones, diferenciando los requerimientos de cada una. La obtención de la imagen de algunos drones para poderlos pilotar en tiempo real, se solventa mediante WiMAX. Otras comunicaciones que no requieran una latencia tan baja podrán implementarse sobre DTN. Al igual que en los sistemas del punto anterior algunos drones estarán equipados con más de un sistema.

2.3. Otros sistemas y consideraciones

En el estudio se tratan someramente otras cuestiones tecnológicas, como la radiogoniometría para localizar emisiones enemigas o los distintos grados de iniciativa de los drones.

Se mostrarán a continuación cuatro figuras para ilustrar este resumen. En ellas podrá verse la distribución espacial prevista, donde la condición esencial es que ninguna persona del propio ejército se acerque a la zona de combate, donde solo y exclusivamente se internarán vehículos (aéreos y

terrestres) no tripulados. En la zona humana desplegarán los medios para hacer posible el control de los drones y que estos realicen las misiones que se les encomiende desde la distancia. En las dos últimas figuras puede verse el sistema mallado que forman los drones y el detalle de uno de ellos, dentro ya de la zona de combate.

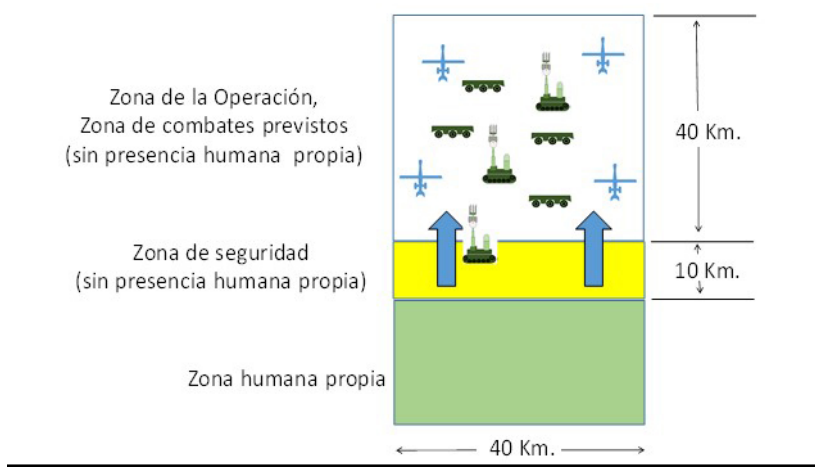


Figura 1. Ejemplo de distribución de las zonas

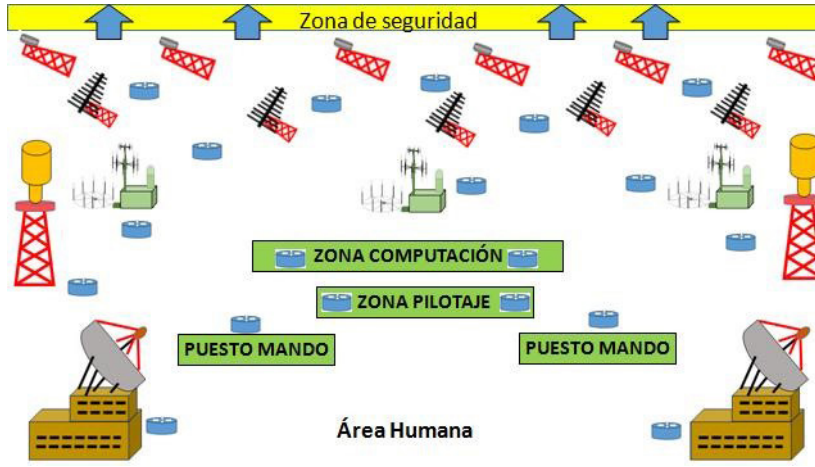


Figura 2. Detalle de la zona humana

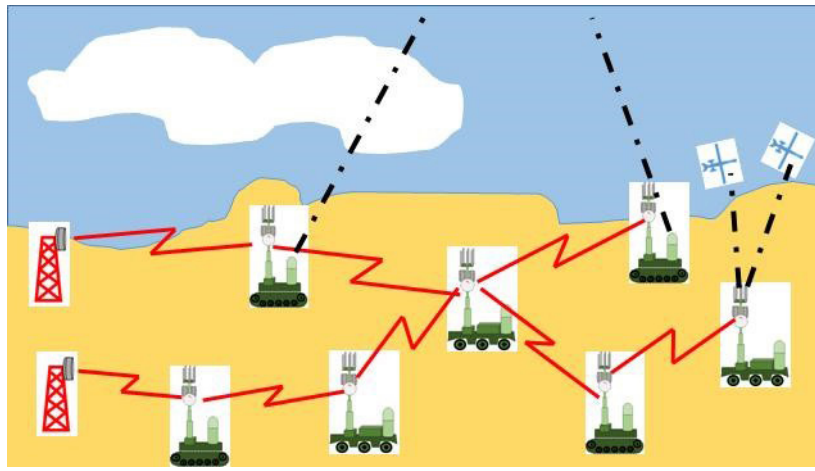


Figura 3. Despliegue de drones de comunicaciones que forman un sistema mallado a través de radioenlaces apoyados por satélite

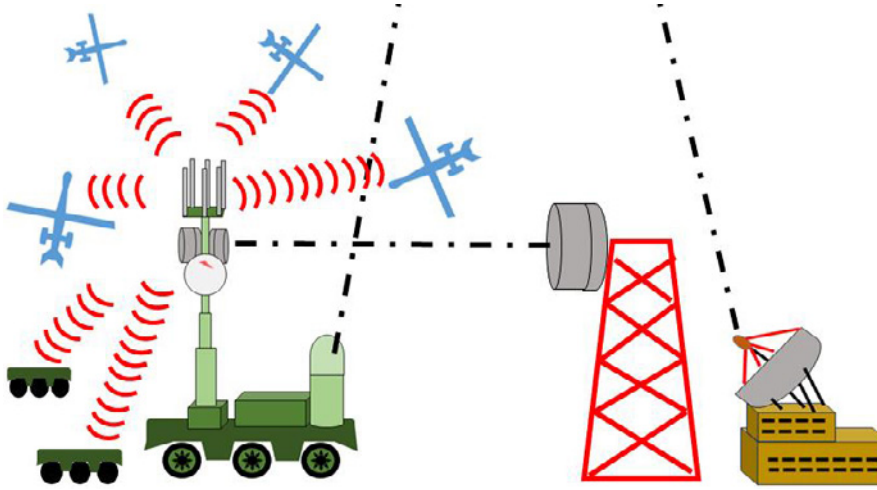


Figura 4. Detalle de uno de los drones de comunicaciones emulando a una BTS (Base Transceiver Station) de WiMAX

3. Resultados y discusión

Al comienzo del trabajo se buscaba aportar soluciones imaginativas para solventar determinados problemas. Algunos de estos problemas eran el alargamiento de la distancia de comunicaciones, saturación por concentración de drones, supervivencia y seguridad en las comunicaciones o supervivencia ante perturbaciones intencionadas en los sistemas GNSS.

Una vez que se buscaron soluciones a estos problemas, se constató que algunas tecnologías ya existentes solventaban de forma satisfactoria estos problemas. Estas tecnologías eran WiMAX, DTN, TACAN, DME o NDB.

4. Conclusiones

El autor del presente trabajo defiende que todas las tecnologías individuales y concretas para llevar a cabo este proyecto, están perfectamente en uso y han superado con creces las fases de investigación y desarrollo. Lo que queda pendiente es la labor de integración de todas ellas para llevar a cabo este proyecto.

La integración de estas tecnologías ha sido descrita en el trabajo de forma muy somera y a muy alto nivel. Si se pretendiera llevar a la práctica este proyecto se prevé que la complejidad crecería conforme se bajara de nivel y se produjera el acercamiento a lo tangible.

La información en fuentes abiertas sobre este ejército de drones es nula, pudiendo deberse esto a que ningún país está dedicando recursos a esta integración y empleo masivo, o bien a que sí lo están haciendo, pero los resultados están cubiertos y etiquetados como materias clasificadas (que sería lo lógico en este caso). Debido a esto no se ha podido completar la situación actual del estado del arte a este respecto.

Referencias y bibliografía

[1] M Cirovic, M., (1979), «Electrónica Fundamental: Dispositivos, Circuitos y Sistemas». Editorial Reverte, S.A.

[2] Huang, (2007), Hui-Min Autonomy Levels for Unmanned Systems (ALFUS) Framework. National Institute of Standards and Technology. Volumen I: Terminology / Volumen II: Framework Models.

[3] Blake, M. B., (2003), Coordinating multiple agents for workflow-oriented process orchestration. Information Systems and e-Business Management Springer-Verlag.

[4] VV.AA., (2016), Normas de la Autoridad Nacional para la Protección de la Información Clasificada. Ministerio de la Presidencia.

[5] McCoy, J. and Rawat B., Danda Software-Defined Networking for Unmanned Aerial Vehicular Networking and Security: A Survey. En Electronics 2019, 8, 1468.

[6] Briceño Márquez, J, E., (2005), Transmisión de Datos. Departamento de Electrónica y Comunicaciones de la Escuela de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Los Andes. Mérida (Venezuela).

[7] Ahmadi S., (2011), «Mobile WiMAX: A Systems Approach to Understanding IEEE 802.16m Radio Access Technology». Elsevier. Burlington (MA, USA).

[8] Documentos de WiMAX Forum:

- Release 3: WMF-T23-001-R030v02_MSP (actualización R021v02 de 20 mayo 2021).

- Release 2: Mobile Radio Conformance Tests: WMF-T25-002-R020v01 (03/08/2012)

- Release 2: Mobile Inter Operability Test: WMF-T25-003-R020v01 (03/08/2012)

[9] VV.AA., (2009), «Delay-/Disruption-Tolerant Networking: State of the Art and Future Challenges». Surrey, UK. Center for Communication Systems Research (CCSR).

[10] VV.AA., (2012), Delay Tolerant Networks: Protocols and Applications, Boca Ratón, USA. CRC Press Tylor & Francis Group, LLC.

[11] Voyiatzis, Artemios G., (2012), «A Survey of Delay- and Disruption-Tolerant Networking Applications». En Journal of Internet Engineering, Vol. 5, N.º 1.

[12] VV.AA., (2008), Global Positioning System Wide Area Augmentation System (WAAS) Performance Standard. 1th Edition. Department of Transportation (USA).

[13] VV.AA., (2008), Global Positioning System Standard Positioning Service Performance Standard. 4th Edition. Department of Defense (USA).

[14] VV.AA., (2016), Manuals Combined U.S. Navy ELECTRONICS TECHNICIAN, VOLUMES 01 – 08. Center for Surface Combat Systems.

[15] VV.AA., (2013), Navegación en condiciones de denegación de señal GNSS. En N.º 13 Monografías del SOPT (Sistema de Observación y Prospectiva Tecnológica). Secretaría General Técnica del Ministerio de Defensa.

[16] Orden ETU/1033/2017, de 25 de octubre, por la que se aprueba el cuadro nacional de atribución de frecuencias. Ministerio de Energía, Turismo y Agenda Digital. BOE 259 (27/10/2017)

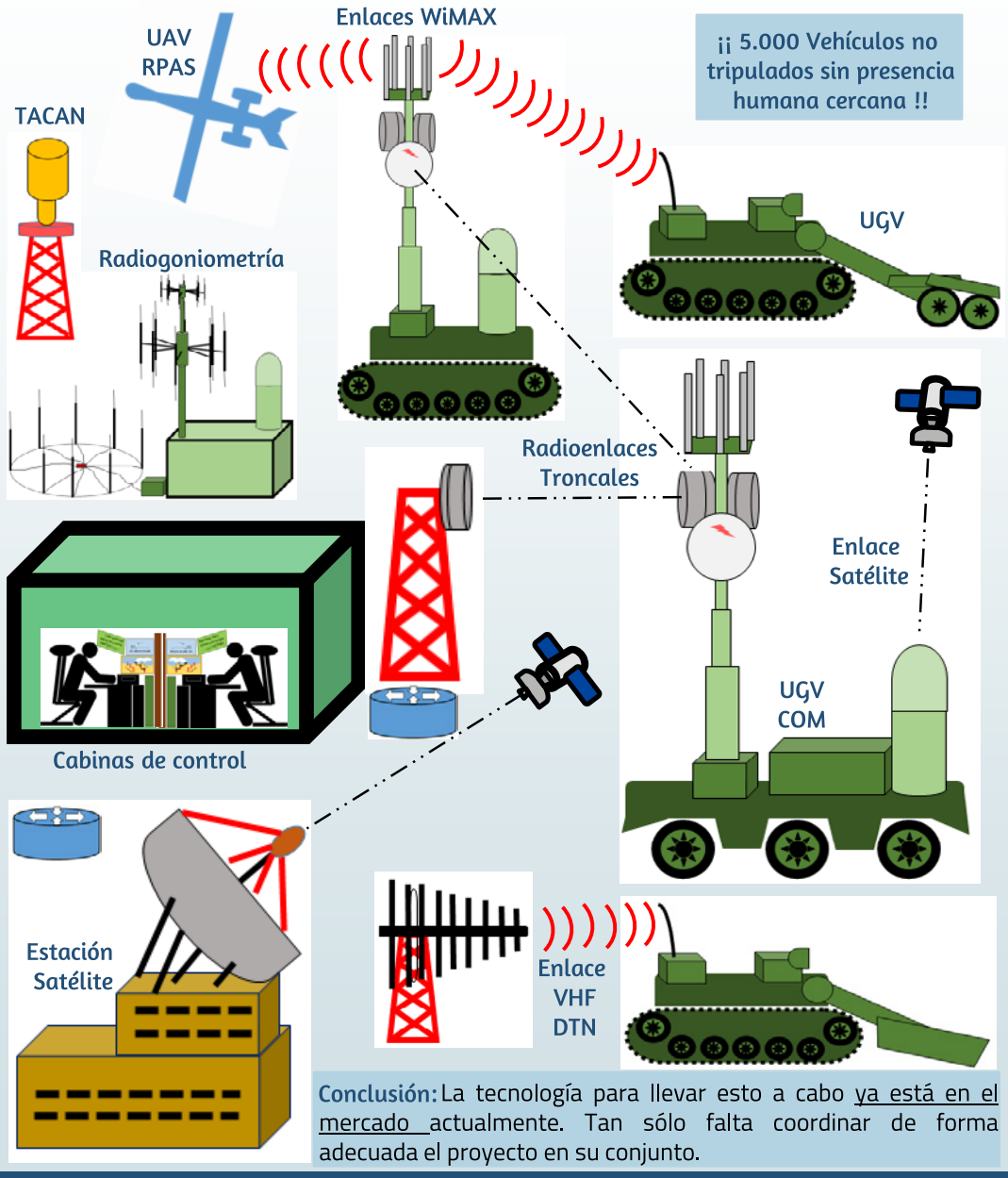
[17] Torres Portero, F. A., (2015), Estudio de WiMAX2 (IEEE 802.16m) y la factibilidad de implementación en el Ecuador. Facultad de Ingeniería de Quito.

[18] VV.AA., (2013), Performance and Capacity Evaluation for Mobile WiMAX IEEE 802.16m Standard. En Wireless and Mobile Technologies.

Comunicaciones en un Ejército de Drones

Autor: Gonzalo Lorén Garay
Director: José P. González Coma

Universidad de Vigo



Conclusión: La tecnología para llevar esto a cabo ya está en el mercado actualmente. Tan sólo falta coordinar de forma adecuada el proyecto en su conjunto.

Desarrollo de un modelo de sistema de evaluación 360° de la capacidad de liderazgo y gestión del talento en el ámbito del Ejército de Tierra

Autor: Macías Martínez, Eduardo (eduardomaciasmartinez@gmail.com)
Directores: Rodríguez Rodríguez, Fco. Javier (fjavierrodriguez@cud.uvigo.es)
y Carreño Fernández, Agustín Luis (acf@et.mde.es)

Resumen – Los líderes del Ejército de Tierra (en adelante ET) deberán desarrollar nuevas habilidades para abordar los nuevos desafíos y hacer frente a nuevos retos en los posibles escenarios, o contextos operativos de actuación del ET, en el Entorno operativo 2035 y los cambios que este deberá afrontar para adaptarse con éxito al carácter incierto y complejo de dicho entorno. Sus responsabilidades esenciales consistirán en construir equipos cohesionados y comprometidos con la misión de la institución y ser innovadores, creativos y capaces de tomar decisiones de forma ágil ante situaciones complejas. Para lograrlo, los líderes de hoy en día necesitan disponer de información precisa acerca del valor que puede proporcionar cada miembro del equipo o unidad que lidera, aquellos que consiguen reforzar el compromiso del resto de los miembros con su visión y la misión, así como identificar y gestionar el liderazgo tóxico que pueda resultar perjudicial para la institución.

La evaluación de la capacidad de liderazgo y la gestión del talento (en adelante GT) es un importante reto para el ET de cara al futuro. Para conseguir la agilidad y flexibilidad que el ET requerirá para superar el desafío que representa el horizonte 2035, este tendrá que afrontar nuevos sistemas para la evaluación de la capacidad de liderazgo de su personal y una adecuada gestión de dicho personal para posibilitar su desarrollo. El presente trabajo pretende, inicialmente abordar un estudio de las tendencias existentes actualmente en nuestras Fuerzas Armadas y el ET de los Estados Unidos (además de canalizar las conclusiones de un importante proyecto de investigación realizado referente al desarrollo del liderazgo en el ET), y posteriormente poder estudiar, desarrollar y proponer un modelo de sistema de evaluación 360º, también conocido como evaluación integral, de la capacidad de liderazgo y GT en ámbito del ET.

Palabras clave – Liderazgo, evaluación 360º, Feedback, gestión del talento, Ejército de Tierra

1. Introducción

1.1. Evaluaciones 360°

La evaluación 360° (también conocida como sistema integral de evaluación, *360-degree feedback, multi-rater feedback, multi source feedback,* o *multi source assessment*) surge durante la segunda Guerra Mundial, pero no será hasta la década de los cincuenta cuando se empezará a emplear.

Las evaluaciones de los supervisores o jefes son la forma más común de medir el desempeño de los trabajadores o subordinados. Sin embargo, en muchos trabajos, un supervisor o jefe directo no es la única persona que está en disposición de evaluar el trabajo de una persona, incluso podríamos decir que en muchos puestos de trabajo es posible que el supervisor directo ni siquiera sea el mejor posicionado para proporcionar una evaluación precisa de ciertos aspectos de la labor que realiza su trabajador o subordinado. Como resultado, muchos expertos en evaluación de personal han concluido que las calificaciones de los supervisores a veces pueden proporcionar imágenes incompletas del desempeño de los empleados [1]. Una evaluación 360º que incluye autocalificaciones y feedback de compañeros, subordinados y otros (como clientes, personas ajenas a la organización con la que deben relacionarse para el desempeño de sus cometidos, etc.) además del supervisor o superior, es una herramienta diseñada que puede ayudar a completar algunas calificaciones que los superiores no llegan a conocer.

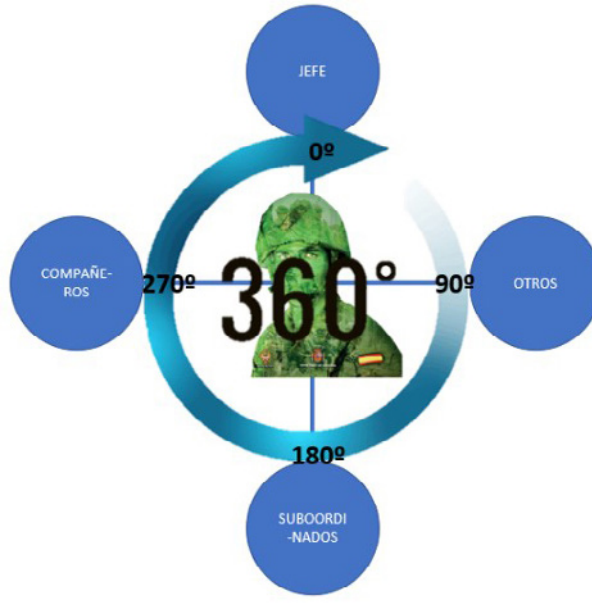


Figura 1-1. Ilustración evaluación 360º (elaboración propia)

1.2. Evaluaciones 360º en el ámbito militar

El sistema actual de evaluación a través de los informes personales de calificación (IPEC), consistente en evaluaciones de arriba hacia abajo, en las que los supervisores califican a sus subordinados, no brinda una oportunidad formal para que subordinados y compañeros de rango similar participen en la evaluación de la capacidad de liderazgo de un líder. En una organización tan jerárquica como las Fuerzas Armadas (FAS) esto podría significar que aspectos tan importantes como el desempeño profesional, prestigio o la capacidad de liderazgo quedaran parcialmente evaluados.

Una evaluación de 360 grados se convierte en un método que algunos piensan que sería útil para ayudar a llenar esos *vacíos*.

En el ámbito de las FAS existe una tendencia hacia una estrategia de liderazgo 360º y, por consiguiente, a la evaluación de este en este sentido, aunque se puede considerar que está en una fase incipiente y que requiere un profundo estudio y desarrollo del concepto de evaluación 360º para las FAS.

En relación con evaluaciones 360º cabe destacar la dilatada experiencia que tiene el Ejército de los Estados Unidos en evaluaciones MSF (Multi-Source Feedback), que a través del CALP (Center for the Army Profesional and Lidership) realiza estudios, desarrolla productos y brinda servicios para fortalecer la profesión del Ejército, mejorar el liderazgo y apoyar el desarrollo de líderes.

1.3. Evaluación actual del liderazgo en el ET

En lo que se refiere a la actual evaluación de la capacidad de liderazgo y su desarrollo en el ET, se puede decir:

- Hoy por hoy, las evaluaciones de la capacidad de liderazgo en el ET las realiza el superior jerárquico, apoyados por otros superiores (no directos) que en muchos casos no disponen de la información necesaria sobre el desempeño de cometidos del militar a evaluar. Estas calificaciones por parte de los superiores se realizan como un proceso de evaluación anual de la labor del subordinado y tienen repercusión directa en los procesos de evaluación de este.
- Las competencias y aptitudes relacionadas con la capacidad de liderazgo son medidas por un cuestionario de 17 preguntas, que corresponden a la evaluación de un concepto diferente.
- Existen condicionantes, ajenos al personal evaluador, que pueden interferir en el resultado de la evaluación y en consecuencia afectar al resultado fidedigno.
- La orientación del evaluado se limita en unos comentarios por escritos que realiza el superior en el IPEC y los derivados de la reunión con el militar al objeto de valorar el resultado. En

ocasiones esta orientación puede ser deficiente motivada por aspectos como:

- No disponer el superior de un conocimiento preciso del desarrollo del liderazgo del evaluado, al realizarse la evaluación únicamente en sentido descendente.
- La falta de aptitud del superior para llevar a cabo labores de orientación.
- El resultado de estos IPEC, y por ende de la capacidad de liderazgo incide directamente, en mayor o menor medida, según sea el sistema de ascenso en la evaluación del militar.
- Actualmente en el ET, no se analiza ni se gestiona la evolución de los conceptos de valoración del IPEC y, por ende, de la capacidad de liderazgo a lo largo de la trayectoria de un militar.

2. Desarrollo

2.1. Modelo de liderazgo en el ET

El entorno operativo en el que previsiblemente operará el ET en el año 2035 les exigirá afrontar ciertos retos, así como situaciones negativas y adversas ajenas a la institución que pueden atentar contra esta, pero también identificar oportunidades o factores positivos que se presentan en este entorno y que pueden ser aprovechados.

Entre las características de un ET bien adaptado al Entorno operativo 2035, el recurso humano, las personas, siguen siendo el elemento primordial pues es el que dirige y coordina las ideas (doctrina y conceptos) y los medios (material e infraestructuras). Esas personas que cumplen en las Fuerzas Armadas la función directiva son los mandos y para el militar el mando supone liderar y dirigir.

El modelo de liderazgo 360º se debe construir sobre la sólida base de los valores de ET y, compartiendo puntos en común con los de otras organizaciones e instituciones militares y civiles, se debe adaptar perfectamente a la realidad de una organización jerarquizada y disciplinada como es el ET. Este modelo de liderazgo aumenta el entusiasmo, compromiso individual y proactividad; facilita la colaboración, coordinación e integración del trabajo colectivo y aprovecha al máximo el potencial y talento de cada miembro del equipo.

2.2. Desarrollo actual del liderazgo en el ET

Entre junio de 2012 y marzo de 2015 la Sección de Investigación de la Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM), del Mando de Doctrina del ET (MADOC) llevó a cabo un programa de investigación del desarrollo del liderazgo en el Ejército de Tierra [2].

En base al resultado del estudio realizado se identifica un modelo de liderazgo válido para el ET definido por *once dimensiones de conductas* del líder, cuya presencia puede ser medida mediante tasas de frecuencia. El modelo ha puesto a prueba el impacto de esas dimensiones sobre *once criterios de efectividad*, lo que permite modificar y orientar a los mandos militares, en función de su nivel, hacia la adopción de aquellos estilos de mando y conductas que favorecen, entre otras: la lealtad del subordinado, la cohesión del grupo, la moral de la unidad y el compromiso con el Ejército.

Igualmente se estableció un índice de excelencia que permite conocer las características de los cuadros de mando que consiguen los mejores resultados sobre sus subordinados. La comparación de los resultados con el liderazgo excelente permitirá a los mandos del Ejército conocer qué áreas y competencias de su estilo de mando deben potenciar o, por el contrario, evitar para alcanzar la excelencia en su liderazgo, entendiendo como tal la consecución de los máximos resultados positivos del personal y unidades que dirigen, de acuerdo con las demandas de la organización.

En resumen, con dicha investigación, y a partir del método científico, se ha definido un modelo de liderazgo propio del ET. En él se describen las conductas, actitudes, preferencias y efectividad de los mandos militares en las dimensiones del liderazgo. Igualmente permite concretar en valores numéricos la magnitud de cada una de las dimensiones de conducta del líder, lo que ofrece la posibilidad de establecer comparaciones y evaluar la eficacia de las acciones que puedan llevar a cabo para el perfeccionamiento del liderazgo en el ET.

3. Resultado y discusión

El modelo de sistema de evaluación 360º de la capacidad de liderazgo y GT en el ámbito del ET propuesto en el presente trabajo pretende, por un lado, evaluar la capacidad de liderazgo del personal del ET en el desempeño de sus cometidos, participando en dicha evaluación los superiores inmediatos, compañeros y subordinados directos del militar a evaluar. Por otro lado, este modelo pretende proporcionar apoyo al personal evaluado para comprender y aceptar el resultado de sus evaluaciones 360º, así como guiarles para desarrollar sus conductas y actitudes a través de la creación de un plan de desarrollo de liderazgo individualizado.

- Los objetivos de este sistema de evaluación 360º de la capacidad de liderazgo y GT en el ámbito del ET son:
- Realizar una evaluación global, completa y objetiva de la capacidad de liderazgo del militar evaluado.
- Proporcionar al evaluado un feedback procedentes de su ámbito de trabajo (superiores, compañeros y subordinados).
- Aumentar el propio conocimiento del evaluado de su capacidad de liderazgo.

- Realizar una planificación del desarrollo de la capacidad de liderazgo del evaluado.
- Establecerse como una herramienta de apoyo a metodología del *aprendizaje cooperativo*.
- Convertirse en un catalizador del desarrollo de líderes.
- Proporcionar un elemento de juicio para posibilitar el GO o NO GO para ocupar los puestos de especial responsabilidad que se determinen.
- Ser concepto con incidencia en los procesos de evaluación del personal militar.

Para ello el sistema estará compuesto por:

- La herramienta de evaluación de 360º, que posibilita la introducción, análisis y gestión de información y generación de informes.
- Órganos de orientación y planificación para desarrollo del liderazgo.

Figura 3-1. Exposición de procesos de evaluación 360º (elaboración propia)

Una vez establecidos en detalle los requisitos del sistema por el órgano competente del ET, el diseño del sistema debería realizarse en base a la Arquitectura Global (AG) CIS/TIC [3] que constituye la principal referencia técnica para llevar a cabo la identificación y el desarrollo normalizado de todas las capacidades CIS/TIC que precisa el Ministerio de Defensa.

4. Conclusiones

4.1. Conclusiones generales

El liderazgo en el futuro de las FAS españolas merece ser considerado con una visión prospectiva, amplia, comprensiva y armónica de sus diferentes conceptos, componentes y métodos. Así, se logrará que nuestros militares adquieran una competencia en liderazgo que esté al nivel de otras capacidades morales, técnicas, tácticas y logísticas.

Las calificaciones de los supervisores o jefes son la forma más común de medir el desempeño de los trabajadores o subordinados y por tanto su capacidad de liderazgo. Estudios en evaluación de personal han notado que las calificaciones de los supervisores a veces pueden proporcionar imágenes incompletas del desempeño de los empleados. Una evaluación 360º, que incluye autocalificaciones y feedback de compañeros, subordinados y otros (como clientes, personas ajenas a la organización con la que deben relacionarse para el desempeño de sus cometidos, etc.) además del supervisor o superior, es una herramienta que puede ayudar a completar algunos vacíos de las calificaciones que realizan los superiores y no llegan a conocer.

En este aspecto, y aunque podría considerarse que aún se encuentran en fase experimental, el Ejército de Tierra, la Armada y el Ejército del Aire, empiezan a estudiar, al igual que hacen otros países de nuestro entorno militar (EE. UU.) la necesidad de contemplar el empleo de la política de evaluación de 360º.

El modelo de liderazgo 360º del ET debe interpretar al líder en su dimensión personal primero y en sus relaciones con los demás después. Este modelo prima el desarrollo de determinadas actitudes y hábitos de comportamiento que darán lugar a las capacidades que se consideran básicas para ejercer eficazmente el liderazgo y que permitirán crear conciencia de la situación, crear relaciones, crear visiones compartidas y crear valor en beneficio del grupo.

A partir del estudio realizado en el PINV 110/11 se ha identificado un modelo de liderazgo válido para el ET definido por *once dimensiones de conductas* del líder. El modelo ha puesto a prueba el impacto de esas dimensiones sobre *once criterios de efectividad*, lo que permite modificar y orientar a los mandos militares, en función de su nivel, hacia la adopción de aquellos estilos de mando que se consideren más oportunos para cada circunstancia.

En base a la necesidad de cubrir los vacíos existentes en un modelo de evaluación jerárquica existente actualmente en el ET y teniendo en cuenta los resultados y conclusiones obtenidos del PIN 110/11, se considera la necesidad de establecer un modelo de sistema de evaluación 360º de la capacidad de liderazgo y GT para el ET.

Siendo, entre otras las funciones del Centro de Sistemas de la Tecnología de la Información y las Comunicaciones (CESTIC) «el diseño, la obtención y la configuración de los sistemas y las tecnologías de la información y

las comunicaciones y de la seguridad de la información para garantizar la normalización, homologación y estandarización de dichos sistemas y su plena interoperabilidad, en el marco de la Infraestructura Integral de Información para la Defensa (I3D)», una vez desarrollado por el órgano correspondiente del ET (MADOC) el documento de especificaciones y requisitos del sistema, este debe elevarse a este órgano a través de la Jefatura de los Sistemas de Información y Telecomunicaciones y Asistencia Técnica (JCISAT) del ET, para llevar a cabo su diseño, implantación y puesta en producción del Servicio TIC/CIS siguiendo el catálogo unificado de estándares de la AG CIS/TIC.

4.2. Líneas futuras

Materializar por parte del ET el impulso necesario para fomentar la cultura de liderazgo 360º, invirtiendo para ello el tiempo y los recursos económicos necesarios, alineándose de esta manera con el proceso de cambio del ET denominado Fuerza 35. [4].

Si se decidiera implantar el modelo de sistema de evaluación 360º de la capacidad de liderazgo y GT, este debería implantarse como una evolución y no como una revolución.

4.3. Reflexión final

Actualmente son varios los programas de seguridad y defensa que están en marcha en nuestras FAS [5], con un importante presupuesto económico asignado.

¿Cuánto dinero y tiempo se estaría dispuesto a invertir en el elemento primordial que dirige y coordina las ideas (doctrina y conceptos) y los medios (material e infraestructuras), y que posibilitaría unas FAS eficientes y adaptadas al Entorno operativo 2035?

Figura 4-1. Inversión en GT en las FAS (elaboración propia)

Agradecimientos

Especial agradecimiento al siguiente personal por su apoyo para la realización del presente trabajo:

Fco. Javier Rodríguez Rodríguez (director TFM).

Tcol. de Infantería, D. Agustín Luis Carreño Fernández (Departamento Liderazgo ET).

Cte. psicólogo. Dña. María del Pilar Gallardo Rodríguez (Programa De Investigación 110/11 «Desarrollo del liderazgo en el Ejército de Tierra»).

Referencias

[1] RAND Corporation, (2015), ¿360- degree assessment, Are the right tool for USA army?

[2] MADOC, (2011), Programa de Investigación 110/11 «Desarrollo del liderazgo en el Ejército de Tierra».

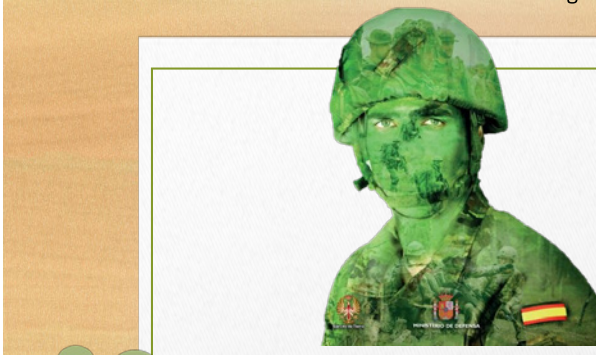
[3] Secretaria de Estado de Defensa, (2016). Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa.

[4] Ejército de Tierra, (2019), FUERZA 35, Madrid.

[5] Ministerio de Defensa, https://www.defensa.gob.es/gabinete/notasPrensa/2018/12/DGC-181214-inversion.html, fecha consulta 23/09/2021.

Desarrollo de un modelo de sistema de evaluación 360º de la capacidad de liderazgo y gestión del talento en el ámbito del Ejército de Tierra.

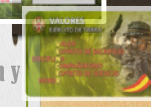
Autor: D. Eduardo Macías Martínez **Directores:** D. Fco. Javier Rodríguez Rodríguez
D. Agustín Luis Carreño Fernández



Designación de Evaluadores

1

-Subordinados
-Superiores
-Compañeros



2

Cumplimentación y validación de Evaluación

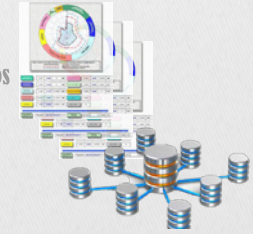
Orientación y apoyo

4

SISTEMA DE EVALUACIÓN 360°

3

Generación de informes de resultados



¿Cuánto dinero y tiempo se estaría dispuesto a invertir en el elemento primordial que dirige y coordina las ideas y los medios, y que posibilitaría un Ejército de Tierra más eficiente y adaptado al Entorno Operativo 2035?

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Estudio de comunicaciones seguras en redes de área amplia (WAN) privadas y críticas evolucionadas con SD-WAN

Autor: Martín García, Santiago José (smarga1978@gmail.com)
Directores: Carlos Zamorano Pinal (carlos.zamorano@vodafone.com)
y José María Núñez Ortuño (jnunez@cud.uvigo.es)

Resumen – Este estudio se centra en las infraestructuras de telecomunicaciones (IT) privadas tradicionales con las características de ser críticas e implementar comunicaciones seguras.

Una posibilidad de mejora de estas infraestructuras es aplicar el concepto de redes definidas por software (SDN), que tiene su aplicación en las redes de área amplia (WAN) tradicionales con la tecnología de redes WAN definidas por software (SDWAN).

Con la finalidad de sacar conclusiones concretas en el estudio, se aplica una solución de SDWAN a la infraestructura de telecomunicaciones descrita en la arquitectura global CIS/TIC del Ministerio de Defensa (AG CIS/TIC) [1], que se caracteriza por unificar dos WAN en una única, por implementar comunicaciones seguras, y por ser una infraestructura de telecomunicaciones privada y crítica.

Palabras clave – Infraestructura de telecomunicaciones, privada, crítica, seguridad, SD-WAN

1. Introducción

El estudio sigue la definición de comunicaciones seguras de la recomendación X.1205 de la UIT, que define que son aquellas que tienen por finalidad «garantizar la confidencialidad, la integridad y la exactitud de las comunicaciones de red» (UIT-T, 2008). Con ese objeto se han de emplear técnicas de encriptación para el tráfico de la organización mediante técnicas VPN en la WAN (en el alcance del trabajo se consideran IPSec y MACsec). Se considera además que en la relación de confianza entre la organización y los operadores de telecomunicaciones la VPN es implementada y operada por la organización.

Las soluciones SD-WAN desarrolladas por los fabricantes se basan en soluciones con tunelización IPSec. El carácter complementario de MACsec e IPsec requieren de un estudio particularizado para cada organización, que depende de la WAN y redes de transporte que compongan la infraestructura.

En este estudio se va a analizar la implantación de SDWAN en infraestructuras de telecomunicaciones:

- Privadas, que proporcionan conectividad entre las sedes de la organización y con el exterior de la organización. Se establece que la organización implementa VPN en propiedad, no contratadas al operador de telecomunicaciones, entre todas las sedes de la organización.
- Críticas, con requerimientos de mantener confidencialidad, integridad y disponibilidad, según el nivel de clasificación del tráfico de la organización. Se incluye en el estudio la disponibilidad de la conectividad entre sedes y la garantía del tráfico.

Dado que el SDWAN requiere de un estudio particularizado en cada organización, se aplicará el estudio a la infraestructura de telecomunicaciones del Ministerio de Defensa, definida en la arquitectura global del Ministerio de Defensa (Ministerio de Defensa, 2017), por contar con una red de área amplia, por ser un caso claro de organización que tiene una infraestructura privada y crítica, con necesidad de comunicaciones seguras, y a la que se podría aplicar el SDWAN.

La arquitectura de red de la AG CIS/TIC es comparable a la arquitectura genérica de WAN mostrada en la figura 1-1. El Ministerio de Defensa define a sus sedes o *branches* como nodos permanentes o desplegables, en función de las características de transmisión debidas a las operaciones militares.

Además, se dispone de un CPD de Defensa, como sede central de la organización, y cuenta con la defensa perimetral que da conectividad al Ministerio con internet, aunque en el caso del Ministerio de Defensa se amplía la interconexión a redes de naciones u organizaciones aliadas, el Nodo de Interconexión Clase II, o con redes desplegables, el Nodo de Interconexión Clase I.

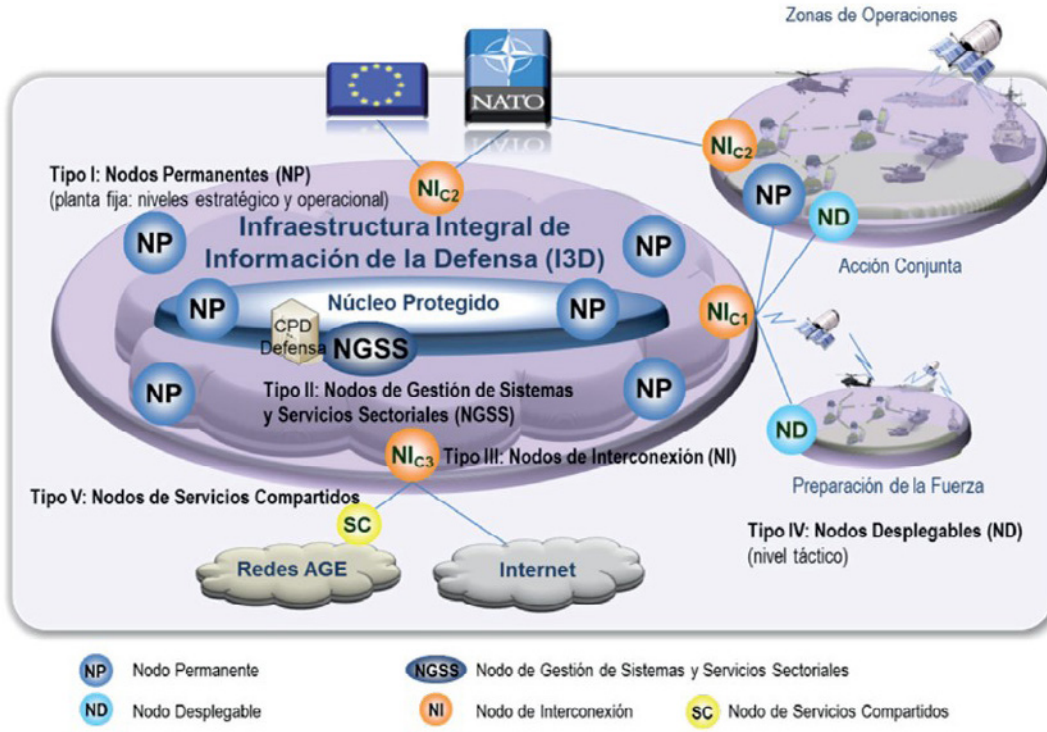


Figura 1. Arquitectura de red de área amplia del Ministerio de Defensa [2]

2. Desarrollo

En el año 2015 el Ministerio de Defensa inicia la evolución de las Redes de Área Amplia de Propósito General (WAN PG) y de Mando y Control (WAN C2), a una red de área amplia única a la que denomina Infraestructura Integral de Información (I3D) de la Defensa. Los documentos públicos de alto nivel donde se define la I3D son:

- Orden DEF/2639/2015, de 3 de diciembre, que establece la Política de los sistemas y tecnologías de la información y las comunicaciones del Ministerio de Defensa (en adelante Política CIS/TIC) y define la estructura de gobierno que permite su coordinación, control y seguimiento [3]. La Política CIS/TIC da una visión global de alto nivel estructura el gobierno de los CIS/TIC del Ministerio de Defensa, además de priorizar las capacidades CIS/TIC para las Fuerzas Armadas.
- 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 (AG CIS/TIC) [2]. En la AG CISTIC se describe a alto nivel las capacidades de la I3D, y se establecen las arquitecturas necesarias para su implantación. Se define un modelo de arquitecturas que

desarrolla la AG CIS/ITC mediante arquitecturas de referencia (AR) y objetivo (AO):

- Las AR desarrollarán las capacidades CIS/TIC identificadas en esta AG CIS/TIC, determinando los sistemas CIS/TIC necesarios para su consecución. Así mismo, son la base para el desarrollo de las arquitecturas objetivo de los citados sistemas.
- Las AO identifican en detalle los componentes CIS/TIC de los sistemas CIS/TIC determinados en las referidas AR y establecerán las bases para su especificación técnica. Además, desarrollarán dichos sistemas CIS/TIC detallando y especificando sus características, y la descomposición de los sistemas en subsistemas y equipos. Constituyen la base para el desarrollo de los proyectos y los Pliegos de Prescripciones Técnicas (PPT) para la adquisición de CIS/TIC y la contratación de servicios.

— 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 (PECIS) [4]. En cuanto a la implantación de la infraestructura de telecomunicaciones que sustituirá o evolucionará a la WAN PG y WAN C2, el documento clave para comprender las diferentes posibilidades es el PECIS. La I3D tiene varios componentes. El eje estratégico 1.1 «Avanzar hacia una única infraestructura integral de Información para la Defensa(I3D) gestionada por el CESTIC»] se especifica el diseño y despliegue de la infraestructura de telecomunicaciones de la I3D, que está compuesta por:

  - Infraestructura de telecomunicaciones terrestres (ITT).
  - Infraestructura de telecomunicaciones vía satélite (ITS).
  - Infraestructura de telecomunicaciones inalámbricas (ITI).

El objetivo estratégico (OE) 1.1 del PECIS es diseñar y desplegar las capacidades de infraestructura de telecomunicaciones de la I3D:

«La nueva I3D, deberá asegurar la provisión de Servicios CIS/TIC a los diferentes tipos de usuarios del Ministerio de Defensa en todos los emplazamientos, plataformas, puestos de trabajo y operativos en su caso. Así mismo, debe permitir el acceso a los usuarios desde emplazamientos y ubicaciones no pertenecientes al Ministerio de Defensa (redes y usuarios remotos) así como la interacción de usuarios del Departamento con otras organizaciones, nacionales e internacionales, a través de pasarelas y puntos de interconexión de Servicios CIS/TIC debidamente asegurados y normalizados. Todos los Servicios CIS/TIC de la I3D se ofrecerán de modo extremo a extremo, a través de una gestión centralizada y única, manteniendo los medios desplegables un cierto grado de autonomía en su gestión»[4. P. 30].

Además, establece que «Se debe diseñar una ITT de la I3D provista de un segmento de cableado (basado en fibra óptica) y un segmento de radiocomunicaciones (basado en radioenlaces), en algunos casos redundando el anterior segmento, que unan los emplazamientos del Ministerio de Defensa en todo el territorio nacional» [4. P. 31].

Por último, se incluye en la AG CIS/TIC un requisito propio de infraestructuras críticas, el núcleo protegido:

«la infraestructura única dispondrá de un núcleo protegido que asegure la supervivencia de determinados Servicios CIS/TIC, con el alcance necesario que posibilite el funcionamiento del Sistema de Mando y Control Militar, incluso en situaciones adversas o ante cualquier tipo de incidente que afecte a la misma» [2. P. 51].

A esta infraestructura de telecomunicaciones operada por el Ministerio de Defensa se pueden unir, como complemento para su disponibilidad y capilaridad, los servicios de telecomunicaciones contratados a un operador de telecomunicaciones.

De esta manera, contando con una infraestructura de telecomunicaciones operada por el Ministerio de Defensa complementada por la contratada a los operadores de telecomunicaciones, es posible realizar el estudio de una hipotética implantación de SDWAN con comunicaciones seguras en la infraestructura de telecomunicaciones de la I3D:

- Infraestructura privada que proporcionan conectividad entre las sedes de la organización, y con el exterior de la organización, con requerimientos de confidencialidad e integridad de la información que dependen del nivel de clasificación del tráfico. Se establece la premisa de que la I3D implementa VPN *on premise* y operadas de forma centralizada por el Ministerio de Defensa.
- Infraestructuras críticas con requerimiento de disponibilidad para posibilitar el sistema de mando y control militar en situaciones críticas. Se incluye en el estudio la disponibilidad de la conectividad entre sedes y la garantía del tráfico.

3. Resultados y discusión

Los resultados obtenidos en la práctica permiten evaluar el valor añadido por:

Disponer de conectividad WAN en capa 3 cifradas entre las sedes. Esto proporciona comunicaciones seguras en las que todo el tráfico está cifrado con los algoritmos públicos más seguros disponibles en la actualidad.

Separar el plano de gestión de la red del plano de datos, mediante la creación de un overlay sobre las distintas redes y medios físicos disponibles que trabajan de forma coordinada. Esto genera múltiples ventajas:

Mayor disponibilidad, ya que a medida que se incluyen redes distintas orientadas a dar el mismo servicio se incrementa la fiabilidad de la red overlay.

Flexibilidad de la red al permitir cursar todos los servicios de la organización en todas las sedes independientemente de la cobertura de red que haya disponible.

Ahorro de costes al incluir redes con más ancho de banda y menos coste al configurar posteriormente la capa de seguridad con la propia solución.

Optimización de la red al ser el plano de control el encargado del envío de tráfico por el mejor enlace disponible en cada momento, permitiendo su cambio a otro enlace en tiempo real en caso de degradación del enlace.

Posibilidad de comportamiento de los medios de transmisión en tiempo real.

4. Conclusiones

Se concluye que el SDWAN y las comunicaciones seguras son una opción aplicable a la AG CIS/TIC del Ministerio de Defensa, en particular a su infraestructura de telecomunicaciones del Ministerio de Defensa. La arquitectura de SDWAN estudiada es una opción viable para evaluar a gran escala:

- Supervisión centralizada y continua de la conectividad del Ministerio de Defensa.
- Uso complementario de redes propias del Ministerio de Defensa y contratadas a operador de telecomunicaciones.
- Empleo de circuitos hasta 100 Gbps en la infraestructura de telecomunicaciones. La complementariedad del uso de MACsec e IPsec permiten adaptar las comunicaciones seguras.
- Automatización del tunelizado IPsec.
- Optimización del uso del ancho de banda, permitiendo la selección de caminos a seguir por el tráfico de la organización mediante el SDWAN.

Agradecimientos

A mi familia, amigos, y compañeros, por hacer posible este trabajo.

Referencias

[1] UIT-T, 04 2008), «X.1205 Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad». [En línea]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I/es. [Último acceso: 12 10 2021].

[2] Ministerio de Defensa, (03 2017), «Arquitectura Global de sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC)». [En línea]. Available: https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html. [Último acceso: 12 10 2021].

[3] Ministerio de Defensa, (14 02 2002), «Plan Director de sistemas de Información y Telecomunicaciones». [En línea]. Available: https://boe.es/boe/dias/2002/02/20/pdfs/A06752-06756.pdf. [Último acceso: 31 10 2021].

[4] Ministerio de Defensa, (2018), Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa(PECIS).

Estudio de comunicaciones seguras en redes de área amplia (WAN) privadas y críticas evolucionadas con SD-WAN

Autor: Santiago José Martín García

Universidad de Vigo

Directores: Carlos Zamorano Pinal y Jose María Nuñez Ortuño

Introducción

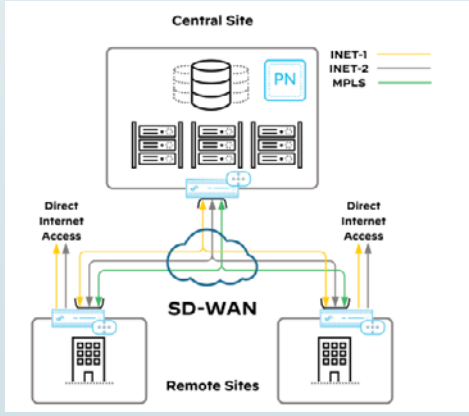
El estudio se centra en las infraestructuras de telecomunicaciones (IT) privadas tradicionales críticas que implementan comunicaciones seguras.

El concepto de Redes Definidas por Software (SDN) tiene su aplicación en las WAN tradicionales con la tecnología de redes WAN definidas por software (SDWAN).

Se aplica una solución de SDWAN a la IT descrita en la Arquitectura Global CIS/TIC del Ministerio de Defensa (AG CIS/TIC).

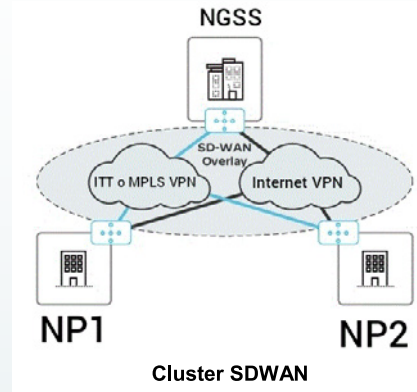
Metodología

1. Se estudia la infraestructura de telecomunicaciones de la AG CIS/TIC: la evolución de WAN PG y WAN C2 a la WAN I3D.
2. Se aplican dos tecnologías VPN a la IT: MACsec e IPsec.
3. Se modeliza la IT y se aplica la solución PAN-OS Secure SDWAN.



Arquitectura básica de PAN-OS Secure SDWAN

Resultados



Cluster SDWAN

Conclusiones

Su aplicación a gran escala dado permitiría:

- La supervisión centralizada de la conectividad de sedes y centros de procesamiento de datos.
- El uso complementario de redes propias y contratadas a operador de telecomunicaciones.
- Conectividad desde 1 Gbps a 100 Gbps.
- Automatización ante la caída de enlaces.
- Optimización del uso del ancho de banda.
- Comunicaciones seguras **con una suite criptográfica o cipher suite de GCM-AES-256 de extremo a extremo.**

Agradecimientos

A mi familia, amigos, y compañeros, por hacer posible este trabajo.

Procedimiento de acreditación de nodos de la Red SC2N-EA

Autor: Miranda Mendoza, Jorge José (jmirmen@mde.es)
Director: Rodelgo Lacruz, Miguel (mrodelgo@cud.uvigo.es)

Resumen – El SC2N es la futura red clasificada que interconectará las unidades de las FAS para ejercer el planeamiento, dirección, ejecución y control de sus operaciones y ejercicios. Estará constituida por la federación de varias redes, entre la que se encuentra su homónima específica del Ejército del Aire, el SC2N-EA.

El SC2N-EA ha obtenido la acreditación de seguridad del sistema para el manejo de información clasificada con grado *reservado nacional* en modo unificado a nivel superior. Tras la acreditación y entrada en producción, se siguen desplegando nodos en los diferentes cuarteles generales y UCO del Ejército del Aire hasta que se complete su completa implantación.

La implantación y acreditación del nodo principal del Cuartel General del Mando Aéreo de Combate (CGMACOM), así como de sus unidades dependientes, se ha materializado durante el desarrollo de este trabajo. Actualmente se están llevando a cabo los trabajos para federar esta red al SC2N.

Mediante este trabajo se pretende establecer un procedimiento que sirva de guía a las unidades usuarias para la implementación de los requisitos de seguridad de la información que permita acreditar sus nodos.

Palabras clave – seguridad de la información, información clasificada, acreditación de seguridad, SC2N-EA.

1. Introducción

1.1. El sistema de información para el Mando y Control del Ejército del Aire

El Ejército del Aire (E.A.) para poder cumplir adecuadamente con sus tareas de preparación, generación y sostenimiento de la fuerza requiere de un sistema de información para el mando y control, acreditado al nivel de seguridad correspondiente al grado de clasificación de la información que maneje, que le permita el ejercicio de la autoridad y dirección de las unidades a su mando.

Actualmente se cuenta con una diversidad de redes independientes, diseñadas para diferentes finalidades, tecnologías y con acreditaciones dispares para el manejo de información clasificada. Esto hace que los flujos de información en los diferentes niveles de planeamiento de las operaciones hayan requerido una renovación.

Como sustitución de la anterior red ICC-Nse ha implantado el Sistema de información para el Mando y Control del Ejército del Aire (SC2N-EA), que se pretende que dé conectividad global con el resto de las Fuerzas Armadas a través del futuro Sistema de Mando y Control Nacional (SC2N), permitiendo el ejercicio del planeamiento, dirección, ejecución y control de las actividades del E.A. del modo más eficiente y seguro posible.

1.2. Objetivo

En los cuarteles generales y unidades del E.A. donde se desplieguen nodos del SC2N-EA se requerirá un trabajo previo con objeto de dar cumplimiento los requisitos que impone la normativa para que dichos nodos sean acreditados para el manejo de información clasificada. Por otra parte, los ya acreditados deberán pasar periódicamente una reacreditación, tanto por caducidad de la acreditación como en aquellos casos en los que hayan cambiado las condiciones que garantizan la seguridad del nodo.

El trabajo realizado es una guía que facilite los pasos necesarios para la acreditación, o reacreditación, de un nodo del SC2N-EA, al personal encargado del mismo. Además, este procedimiento es extensible a otros sistemas, adecuándolo a las particularidades propias de estos.

2. Seguridad de la información en redes que manejan información clasificada

2.1. La información clasificada

Se considera información clasificada a toda información y material que requiere una determinada protección contra su divulgación no autorizada a la que la normativa atribuye una clasificación de seguridad. De acuerdo con lo establecido por la Orden Ministerial 76/2006, de 19 de mayo, por

la que se aprueba la política de seguridad de la información del Ministerio de Defensa, la información clasificada [1], mostrada en la figura, engloba las materias clasificadas, que están reguladas en la Ley 9/1968, de 5 de abril, sobre Secretos oficiales [2], y las materias objeto de reserva interna, reguladas en el ámbito del Ministerio de Defensa por la Orden Ministerial Comunicada núm. 1/1982, de 25 de enero, por la que se aprueban las normas para la protección de la documentación y material clasificado [3].

Figura 1. Información Clasificada

Por otra parte, la información puede clasificarse en ámbito nacional o en el de alguna de las organizaciones internacionales con los que España tiene suscritos convenios que establecen equivalencias, que se pueden ver en la, en cuanto al daño que puede provocar su filtración y a las medidas de protección exigidas. En el caso del SC2N-EA para cumplir las funciones para las que se ha diseñado requiere su acreditación para el manejo de información de grado *reservado nacional*.

Figura 2. Información clasificada y ámbitos de aplicación

2.2. Requisitos

La información durante su ciclo de vida necesita ser transmitida, almacenada, reproducida, extractada, destruida u otras operaciones sin que merme la seguridad. Para que sea posible se requiere la concurrencia de seguridad física, personal, criptológica y de la información y las comunicaciones, así como un correcto control, almacenamiento y custodia [4].

La información con grado de clasificación *reservado* se custodia por los órganos de control constituidos y autorizados para ello. Esa autorización requiere la implantación de una serie de medidas y procedimientos de protección y su acreditación por la autoridad competente. El manejo de esa información queda restringida a una ZAR acreditada a ese nivel y controlada por el órgano de control. Se debe garantizar la compartimentación de la información para que la correspondiente a diferentes grados de clasificación sea tratada exclusivamente de acuerdo a sus requisitos de seguridad, pero también para que se cumpla el principio de la necesidad de conocer. En este sentido, el SC2N-EA se ha diseñado para trabajar en modo seguro de operación *unificado a nivel superior*, que es aquel en el cual el personal que accede al sistema está autorizado para acceder al máximo nivel de clasificación de la información que maneja el sistema y no todos los usuarios tienen necesidad de conocer, motivo por el que se establecen procesos informales que garanticen una separación fiable de los datos para que se acceda de forma selectiva.

2.3. Medidas físicas

Las instalaciones que albergan al SC2N-EA deben ser ZAR de Clase I o Clase II, en función del uso. En general, los CPD o zonas en las que se instalan los servidores y la electrónica de red serán Clase I y la zona donde se ubican los terminales de los usuarios será Clase II [4]. Para la acreditación de las ZAR se requiere la elaboración de un plan de protección, compuesto por el informe de instalaciones, los procedimientos de seguridad y el plan de emergencia. Se deben asegurar los entornos siguientes [5], [6]:

- El *Entorno Global de Seguridad* (EGS) es la zona exterior general que rodea las instalaciones donde se ubica el Sistema. Este entorno actúa como una capa externa de la defensa en profundidad al suponer un primer obstáculo ante una amenaza de intrusión.
- El *Entorno Local de Seguridad* (ELS) corresponde al área interior correspondiente a la propia ZAR y la zona inmediatamente adyacente. Dependiendo del caso puede coincidir con una ZAR o bien contener una o varias ZAR. Se puede dar también el caso de que una ZAR contenga a otra o estén separadas, tal y como se muestra en la Figura 3.
- El *Entorno de Seguridad Electrónico* (ESE) debe garantizar la protección frente a escuchas, tanto pasivas, como las debidas a comunicaciones poco seguras o a través de emisiones electromagnéticas no intencionadas, como activas, que implican el uso deliberado de dispositivos de captación por parte de un tercero. Para ello los locales deberán obtener una acreditación ZONING y todo su equipamiento electrónico estará certificado TEMPEST [9].

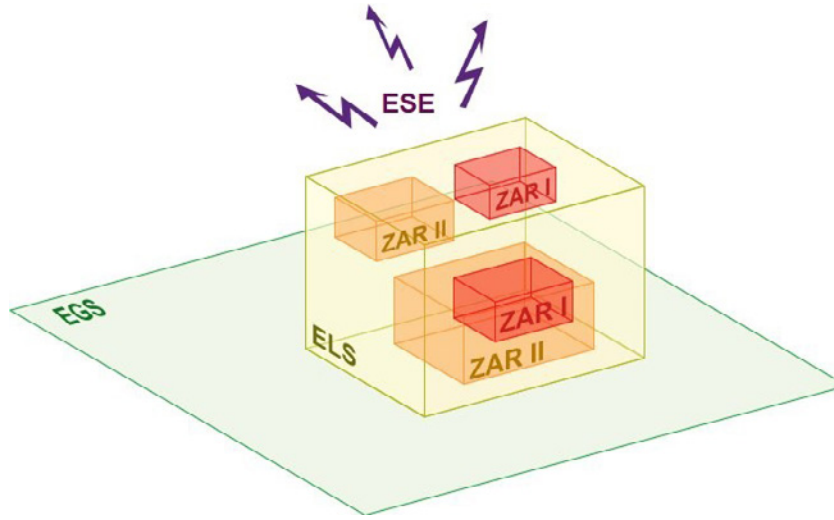


Figura 3. Posibles configuraciones de ZAR y los entornos de seguridad

2.4. Seguridad del sistema y documentación de seguridad

Además de la seguridad física, de carácter externo, se deben implementar una serie de medidas en el propio sistema. Para ello, primeramente, se realiza un *análisis de riesgos* [7], que formará parte de la gestión de riesgos. La gestión de riesgos de seguridad del sistema es un proceso completo y continuo de identificación, control y minimización de eventos potencialmente peligrosos que puedan afectar a la seguridad del sistema, que incluye, entre otros al análisis de riesgos.

Una adecuada gestión de los riesgos implicará la implementación de salvaguardas que dejen dichos riesgos por debajo de un determinado umbral, el riesgo residual, que proporcione un nivel suficiente de seguridad al sistema. El análisis de los riesgos posterior a dicha implementación sirve de evidencia documental de que dichos riesgos han sido tratados de acuerdo a las salvaguardas declaradas. Este análisis es parte obligatoria de la documentación que se envía a la autoridad acreditadora. En la implantación del SC2N-EA se ha utilizado para la Gestión de Riesgos de Seguridad la herramienta PILAR RM - Análisis y gestión de riesgos [12] que se basa en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).

Por otra parte, se debe adjuntar un paquete documental formado por tres documentos y sus respectivos anexos: el Concepto de Operación (CO), la Declaración de Requisitos Específicos de Seguridad (DRES) y los Procedimientos Operativos de Seguridad (POS) [4]. En este tipo de acreditación no es necesaria la Declaración de Requisitos de Seguridad de la Interconexión (DRSI) ni la Declaración de Requisitos de Seguridad Comunes (DRSC), pues estas tienen aplicación en el caso de interconexión de sistemas diferentes.

Figura 4. Documentación de seguridad necesaria para el proceso de acreditación

- El *Concepto de Operación* (CO) es la declaración expresa de la función del sistema, que contempla el tipo de información a manejar, las condiciones de explotación, el perfil de seguridad de los usuarios, el grado de clasificación de la información manejada, el modo seguro de operación, las amenazas a las que está sometido, la documentación de referencia y composición del sistema.
- La *Declaración de Requisitos Específicos de Seguridad* (DRES) es un documento que define lo que para el sistema es ser seguro, y especifica cómo se consigue, gestiona y controla, constituyendo un acuerdo vinculante entre la AOSTIC y la autoridad certificadora.
- Los *Procedimientos Operativos de Seguridad* (POS) recogen los procedimientos a seguir en el Sistema, así como las responsabilidades del personal, para implementar los requisitos de seguridad declarados en la DRES de acuerdo con lo establecido en el CO del sistema y las salvaguardas del análisis de riesgos.

Al tratarse de una red compuesta por nodos interconectados separados geográficamente se ha decidido redactar un DRES que contiene los requisitos específicos de seguridad comunes al sistema y en anexos los propios de cada nodo. Igualmente, los POS contienen los procedimientos comunes y entre los anexos se ha incluido a las unidades independientes. Para facilitar la gestión documental y permitir la inclusión de nuevos nodos sin tener que aprobar o modificar toda la documentación del sistema, se ha optado por el uso de anexos y apéndices a estos. De este modo, documentos como los listados de usuarios o de inventario, las certificaciones CAL, ZONING o TEMPEST de cada UCO, los diagramas de red o la organización local de la seguridad, se aprueban y anexan a la documentación general permitiendo una gestión y control de documentación más eficiente.

3. Proceso de Acreditación

El proceso de acreditación tiene como objetivo determinar oficialmente si el sistema ha alcanzado, o en su caso mantiene, los requisitos de protección de la información clasificada que establece la normativa para un determinado nivel y ámbito de clasificación. Transcurrido el periodo de validez o si en el sistema se han producido cambios que suponga una modificación relevante que afecte a las condiciones de seguridad se deberá renovar la acreditación, teniendo que comunicarse con la suficiente antelación.

3.1. Autoridades de acreditación

La ANPIC es la autoridad de acreditación de seguridad (AAS), no obstante, puede delegar esta función [4]. En el caso del E.A. el JEMA es la Autoridad de Acreditación de Seguridad Delegada (AAS-D) para los sistemas específicos del E.A. [9] que manejan información clasificada de ámbito nacional, como el caso del SC2N-EA. El JEMA es para el ejercicio como AAS-D dispone de un organismo de acreditación de apoyo en este proceso, que es la Dirección de Ciberdefensa del E.A. (DCD) [11].

3.2. Proceso de acreditación

El proceso de acreditación para sistemas específicos del E.A. que manejen información clasificada, de los requisitos establecidos por la norma CCN-STIC-101 «Acreditación de Sistemas de las TIC que manejan información clasificada» [8], tiene su propia normativa interna IT JSTCIBER/DCD 40-14 «Proceso de acreditación de sistemas de las Tecnologías de la Información y Comunicaciones que manejan información clasificada» [12], que es la que se ha seguido para el SC2N-EA, según el esquema mostrado en la figura 5.

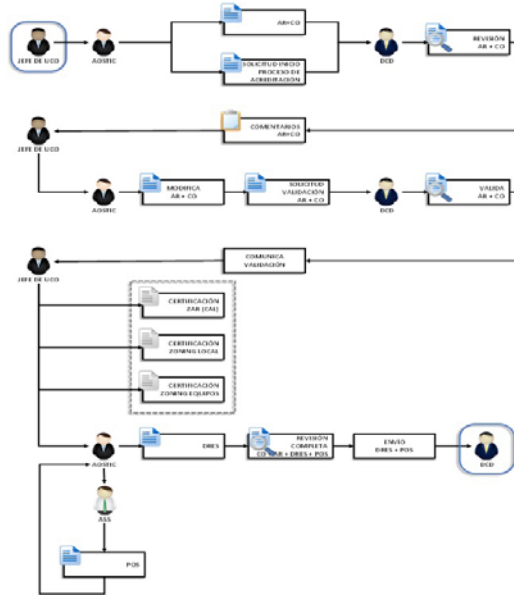


Figura 5. Proceso de acreditación anterior a la inspección

Este proceso parte del jefe de la UCO e implica la remisión de toda la documentación citada en el apartado O para su revisión, modificación si fuese necesaria, y validación. Llegado este punto se pasa a la fase de inspección / auditoría.

3.3. Inspección / auditoría

Una vez que el organismo de acreditación tiene toda la documentación de seguridad (CO, DRES, POS y AR) la verifica y, en caso de hallarla de conformidad, la valida. Dicha validación es comunicada a la UCO, que, a partir de ese momento, y bajo la responsabilidad de la AOSTIC, puede implementar en el sistema todas las medidas de seguridad reflejadas en dicha documentación. Por otra parte, el organismo de acreditación inicia los trámites oportunos, con el órgano correspondiente para la realización de la inspección/auditoría de seguridad, que se muestra en la figura 6.

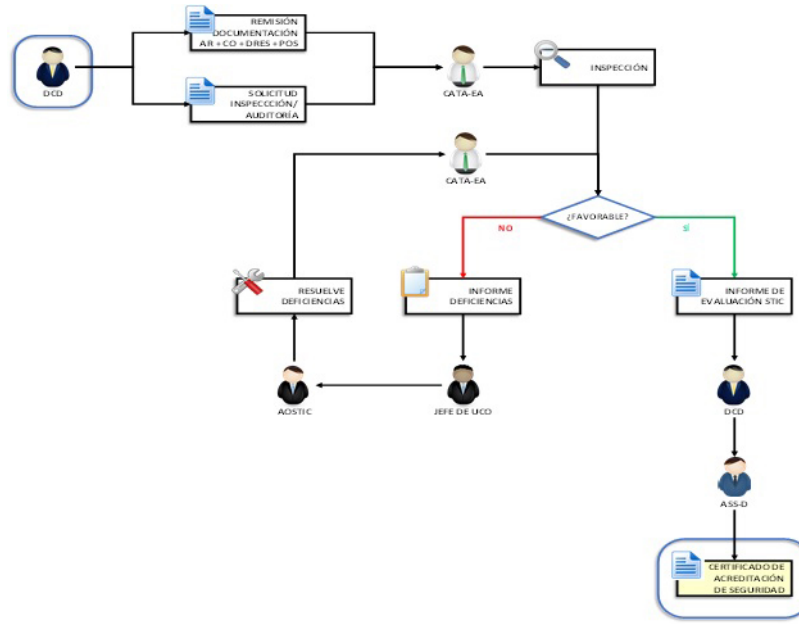


Figura 6. Proceso de inspección / auditoría y acreditación

En el caso de los sistemas específicos del E.A. que manejan información clasificada nacional dicho organismo es el Centro de Apoyo Técnico Avanzado del EA (CATA-EA).

En junio y julio de 2021 el CATA-EA realizó las inspecciones al nodo del CGMACOM, advirtiéndose una serie de no conformidades. Una vez subsanadas y trasladadas al equipo inspector / auditor, se dio como favorable la inspección/auditoría, por lo que se tramitó el Certificado de Acreditación de Seguridad.

El 27 de septiembre de 2021 el jefe de Estado Mayor del Ejército del Aire, como Autoridad de Acreditación de Seguridad Delegada (ASS-D)

firmó la acreditación del sistema y 30 de septiembre de 2021 el SC2N-EA fue puesta en producción a nivel nacional.

4. Conclusiones

En este TFM se han expuesto los conceptos fundamentales relativos al manejo de información clasificada por un sistema de información y comunicaciones que debe conocer aquel que se incorpore a algún puesto del Ejército del Aire que requiera dicha competencia. Por otra parte, se han expuesto los requisitos para poder afrontar la acreditación de una red como la SC2N-EA, de modo que pueda servir como texto básico para la instrucción del personal que deba acometer la acreditación de aquellos nuevos nodos que se establezcan en la red, así como las reacreditaciones del sistema que se deberán realizar periódicamente.

Aunque se han descrito los pasos seguidos para la acreditación de la SC2N-EA, el procedimiento es extensible a cualquier otro sistema de información y comunicaciones que maneje información clasificada, ya que se ha descrito desde un punto de vista general, sin entrar en detalles específicos, además de por la limitada extensión de este trabajo, como por la imposibilidad de ofrecer más detalles pues en su mayoría se trata de información clasificada.

Por último, cabe destacar que el mayor respaldo a la utilidad del trabajo realizado ha sido el lograr la acreditación de seguridad de la SC2N-EA.

Referencias

[1] Ley 9/1968, de 5 de abril, sobre secretos oficiales, BOE n.º 84, de 06 de abril de 1968.

[2] Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, BOD n.º 103 de 29 de mayo de 2006.

[3] Orden Ministerial Comunicada n.º 1/1982, de 25 de enero, por la que se aprueban las Normas para la Protección de la Documentación y Material Clasificado.

[4] Normas de la Autoridad Nacional para la protección de la información clasificada, Ministerio de Defensa, 2019.

[5] OR-ASIP-01-01.02 Orientaciones para plan de protección de una zona de acceso restringido (ZAR).

[6] OR-ASIP-01-02.04 Orientaciones para la constitución de zonas de acceso restringido (ZAR).

[7] CCN-STIC-001 Seguridad de las TIC que manejan información clasificada en la administración.

[8] CCN-STIC-101 Acreditación de sistemas TIC que manejan información clasificada en la Administración.

[9] CCN-STIC-104 Catálogo de Productos con Clasificación ZONING.

[10] IG-30-8 «Competencias y responsabilidades en materia de sistemas de información y telecomunicaciones (CIS) en el Ejército del Aire».

[11] IG 40-6 «Seguridad y protección de la información en el EA". Anexo G: Seguridad de la información en los sistemas de las tecnologías de la información y telecomunicaciones que manejan información clasificada».

[12] IT-JSTCIBER-DCD 40-14 «Proceso de Acreditación de sistemas de las tecnologías de la información y comunicaciones que manejan información clasificada".

[13] Herramienta PILAR. Guías y herramientas disponibles en https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html

Procedimiento de acreditación de nodos de la Red SC2N-EA

Autor: Jorge José Miranda Mendoza
Director: Miguel Rodelgo Lacruz
Universidad de Vigo

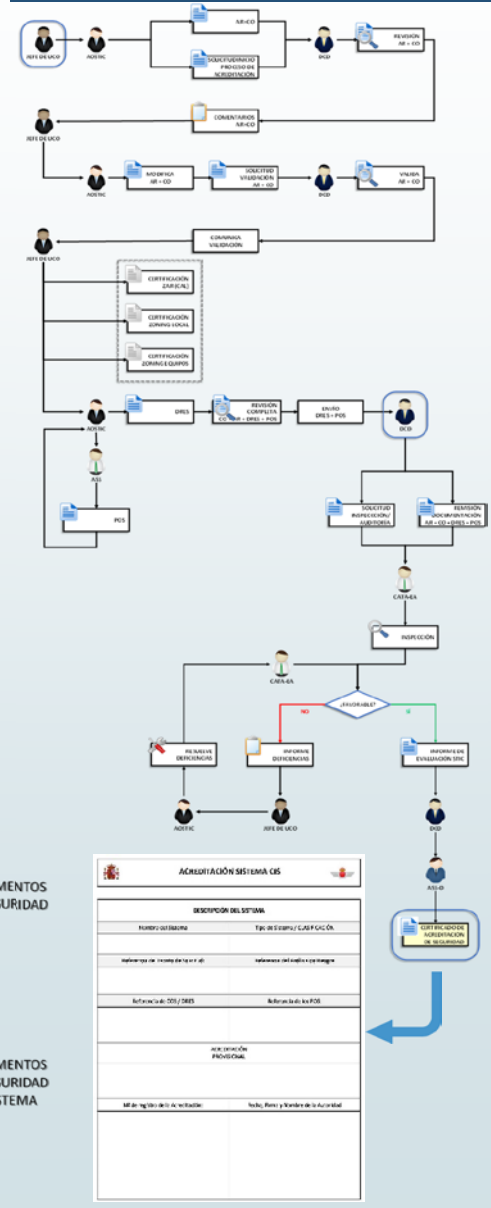
Introducción

El SC2N-EA ha sido acreditada para manejar información de grado RESERVADO Nacional en modo unificado a nivel superior. Tras la acreditación y entrada en producción, se siguen desplegando nodos en los diferentes cuarteles generales y UCOs del Ejército del Aire hasta que se complete su completa implantación.

Información Clasificada

Documentación de Seguridad

Procedimiento de Acreditación



Comunicaciones wifi seguras en entorno corporativo

Autor: Núñez García, Juan Carlos (jnungar@et.mde.es)
Directores: Zamorano Pinal, Carlos (carlos.zamorano@vodafone.com)
y Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – El objetivo principal del trabajo ha sido elaborar un documento técnico que establezca una serie directrices, pautas y guías para permitir a una organización, bajo el paraguas del Esquema Nacional de Seguridad (ENS), establecer un modelo de arquitectura de referencia para la implementación de un sistema de comunicaciones móviles basado en el estándar general 802.11 (wifi) en un entorno corporativo seguro, así como la configuración segura de la misma.

Palabras clave – wifi, Esquema Nacional de Seguridad, estándar, red inalámbrica.

1. Introducción

1.1. Breve historia de las redes inalámbricas

Desde el inicio de la era de la computación [O1] los usuarios de los primeros sistemas soñaban con entrar en sus oficinas y que sus ordenadores portátiles se conectaran *mágicamente* con una red externa que les proporcionase una fuente de información adicional.

En 1971 un grupo de investigadores bajo la dirección del Norman Abramson, en la Universidad de Hawái, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA [O2]. Esta fue la primera red de área local inalámbrica. Estos trabajos rápidamente dieron sus primeros frutos y varias empresas comenzaron a ofrecer productos basados en redes LAN (Local Área Network) inalámbricos.

Pronto se hizo necesaria la estandarización de tecnologías, de modo que el comité del IEEE (Institute Electrical and Electronic Engineers) que ya había estandarizado las redes cableadas recibió la tarea de idear un estándar para las nuevas redes inalámbricas.

El IEEE es un organismo internacional encargado de la estandarización de productos relacionados con la electricidad y la electrónica. Entre sus funciones está la innovación y la excelencia de los productos que estandariza y promociona [3].

El estándar 802.11 ha sufrido sucesivas revisiones y actualizaciones desde su primera versión en 1997. El IEEE es una organización que estandariza a nivel mundial. No obstante, la implantación depende de que los dispositivos a los que va dirigido soporten dichas actualizaciones.

1.2. Ventajas e inconvenientes de las redes inalámbricas

Las ventajas más sobresalientes de usar redes inalámbricas son las siguientes [O1]:

- Facilidad y rapidez de instalación.
- Movilidad: la libertad de movimientos es una de las ventajas más evidentes de este tipo de redes.
- Flexibilidad: capacidad para adaptarse con facilidad a las diversas circunstancias.
- Escalabilidad: facilidad de expandir la red después de su instalación inicial.
- Ahorro de costes: abaratamiento y facilidad de implantación y bajo coste de los
  dispositivos necesarios para su puesta en funcionamiento.
- Proliferación de aplicaciones y dispositivos móviles.

Sin embargo, se deben considerar algunas desventajas:

- Velocidad limitada en relación a las velocidades de las redes cableadas.
- Mayor inseguridad que las redes cableadas: el área de expansión de la red puede abarcar espacios no controlados y por tanto vulnerables.
- Interferencias: las redes wifi funcionan entre otras en la banda de 2,4 GHz y 5 GHz. Esta banda no requiere licencia administrativa por lo que es ampliamente usada en el mercado y por tanto una fuente de interferencias (por ejemplo: hornos microondas).
- Alcance: determinado por la potencia de los puntos de acceso y en constante equilibrio con la seguridad. En principio a mayor potencia de emisión mejor señal llegaría a los usuarios y por lo tanto mayor calidad de señal recibirían estos. Sin embargo, el exceso de potencia de radiación supone que la señal puede desbordar nuestras instalaciones y suponer una vulnerabilidad.

Respecto a la seguridad hay que señalar que se han implementado diferentes protocolos y métodos de protección. En este proceso de bastionado de las redes inalámbricas se han sucedido diferentes métodos, como por ejemplo la restricción de direcciones MAC (Media Access Control), y la implementación de sucesivos protocolos que han evolucionado al ritmo que han impuesto las propias debilidades, por ejemplo, del protocolo WEP (Wired Equivalent Privacy).

1.3. Seguridad en redes inalámbricas

La primera versión del estándar IEEE 802.11 [4] para conexiones inalámbricas se ratificó en el año 1997, en dicho estándar se incluyó el apartado de seguridad basado en Wired Equivalent Privacy (WEP). Dicho algoritmo de seguridad se creó para dotar de seguridad a las redes inalámbricas de la misma manera que se dotaba a las redes cableadas.

El protocolo WEP mostró su debilidad en 2001 cuando unos investigadores (Scott R. Fluher, Isik Mantin y Adi Shamir) publicaron una investigación sobre los problemas del cifrado RC4. Demostrando que en el caso de que existiese un tráfico escaso, era posible estimular la respuesta del punto de acceso y lograr la cantidad suficiente de vectores de iniciación IV para descifrar la clave WEP. Esta debilidad del RC4 invalidó al protocolo WEP como un protocolo seguro.

El protocolo WPA surgió con la condición inicial de que fuese aplicable a los dispositivos existentes como una actualización del firmware en los enrutadores y demás equipos de comunicaciones, criterio que se ha mantenido para protocolos posteriores.

Por último, se lanzó el protocolo WPA2 que ha demostrado ser mucho más robusto ante ataques que sus anteriores predecesores, aunque no ha sido inmune a otro tipo de ataques. Otro problema del protocolo WPA2 es el uso de contraseñas débiles, fácilmente descifrables mediante ataques de fuerza bruta y mediante el uso alternativo de ingeniería social para lograr que el usuario proporcione su contraseña.

1.4. Riesgos, amenazas y ataques a redes wifi

Las redes inalámbricas están expuestas a la mayoría de los riesgos que tienen las redes cableadas y, además, se añaden los riesgos y amenazas propias de la tecnología wifi.

A continuación, se muestran una serie de amenazas que afectan a las redes inalámbricas [5]:

- Debido a una vulnerabilidad no conocida, el equipo podría verse comprometido por tener habilitada la interfaz inalámbrica sin necesidad de contacto físico por parte del atacante.
- A través de la conexión inalámbrica se puede tener acceso a entornos, inalámbricos o no, que estén en contacto con el primero.
- La propagación por espacio libre hace que las comunicaciones puedan ser interceptadas en modo pasivo sin contacto físico con la red y sin posibilidad de detectar dicha captura.
- Se pueden realizar ataques tales como denegación de servicio (DoS) a través de inhibidores de frecuencia, paquetes maliciosos, etc.
- Despliegue de equipos maliciosos, tales como puntos de acceso falsos (rogue AP) y suplantación de los equipos legítimos con el objeto de exfiltrar información.
- Se puede obtener acceso a información realizando un análisis forense de un equipo legítimo, previamente sustraído.
- En el caso de que haya redes federadas o conectadas a la nuestra, se puede obtener acceso a través de las mismas, ya que estas podrían tener otras vulnerabilidades susceptibles de ser explotadas.
- Se puede obtener información de la entidad propietaria y de los dispositivos de usuario recolectando datos abiertos de fácil captura, por ejemplo: SSID, direcciones MAC, etc.

Las amenazas arriba indicadas tratan de menoscabar los principales activos de seguridad que deben protegerse en toda red [6]:

- Confidencialidad: característica que consiste en que la información solo debe ser revelada a usuarios autorizados.
- Integridad: asegura que la información no ha sufrido modificaciones no autorizadas que perturben la veracidad u originalidad de la misma.

- Disponibilidad: la información debe estar a disposición de aquellos usuarios autorizados que deban de tener acceso a la misma cuando se requiera.
- Autenticidad: propiedad que garantiza la procedencia de la información.
- Trazabilidad: propiedad que nos permite efectuar un seguimiento de los usuarios autorizados que han tenido acceso a la información.

Estas propiedades se verán afectadas por comportamientos inapropiados, maliciosos o descuidados por parte de personal legítimo o atacantes.

1.5. Esquema Nacional de Seguridad (ENS)

Debido al auge que en los últimos años ha experimentado la ciberseguridad debido al aumento de ciberataques a nivel mundial, se han creado organismos nacionales cuya función es regular y combatir el cibercrimen. En España, entre otros se han creado el INCIBE (Instituto Nacional de Ciberseguridad), el MCCE (Mando Conjunto del Ciberespacio) y el CCN (Centro Criptológico Nacional).

El CCN [10] es el órgano responsable de coordinar la acción de los diferentes organismos de la Administración Pública, para que utilicen medios y procedimientos de cifra y garantizar la seguridad de las tecnologías de la información en ese ámbito. Las redes bajo su responsabilidad son las correspondientes a las Administraciones Públicas (nacional, autonómica y local), así como las correspondientes al sector público, organismos autónomos dependientes de la Administración y aquellas empresas declaradas de interés estratégico para la seguridad nacional y para el conjunto del país.

El CCN se rige por el Esquema Nacional de Seguridad (ENS) que tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Para el cumplimiento de los objetivos previstos en el Esquema Nacional de Seguridad se definen y valoran los fundamentos que van a permitir categorizar sistemas y servicios. Esto supone que dependiendo de la categoría se deberán implementar unas medidas de seguridad u otras, exigiéndose requisitos más restrictivos en función de la información a proteger.

Una red inalámbrica se considera de manera similar a cualquier otro sistema de información. Formado por hardware y software y cuya misión fundamental es dar acceso a recursos, información y servicios de la organización.

Para la determinación de la categoría de la red inalámbrica como sistema de información dentro del Esquema Nacional de Seguridad, hay que tener en cuenta la criticidad de los recursos y servicios de la organización que se establecen y la criticidad de la información que fluye a través de sus conexiones.

La criticidad se establece atendiendo al grado en que se cumple y se protege la información, garantizando, en todo momento, la confidencialidad, disponibilidad, autenticidad, trazabilidad y disponibilidad de la misma.

Así mismo, la valoración del impacto negativo que ocasionará para la organización la pérdida o compromiso de los puntos citados en el párrafo anteriores determinará que la red sea catalogada como *básica, media o alta*.

2. Desarrollo

El vicerrectorado de Planificación académica de la Universidad de Extremadura, ha decidido instalar un sistema de conexión inalámbrica para facilitar el trabajo entre sus trabajadores. Dicho servicio wifi también estará disponible para los ciudadanos dentro de sus instalaciones con las limitaciones pertinentes.

El edificio al cual se ha de dotar de wifi está compuesto por una sala diáfana con zonas públicas que se destinarán a zona de espera de los estudiantes y visitas

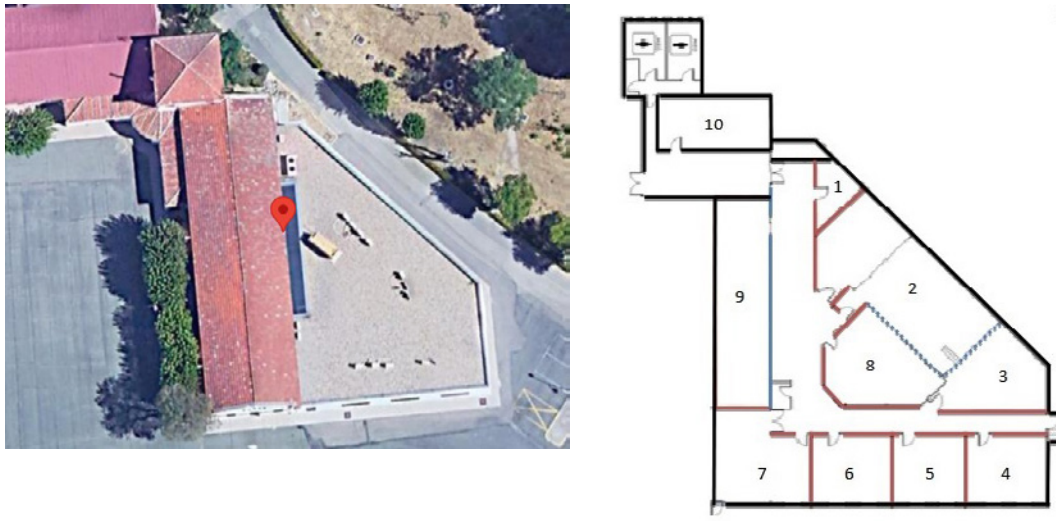


Figura 1. Vista aérea y distribución de la instalación [8]

El propósito, por lo tanto, es dotar de un acceso de calidad a usuarios, empleados y visitas. Dicha red inalámbrica completará a la red cableada existente en la instalación. Así mismo, la red inalámbrica estará conectada con la red cableada con el objeto de disponer de conexión con el resto de redes de la universidad y con Internet.

Para la configuración de la red se ha tenido en cuenta que se trata de una red de uso en una dependencia de la administración universitaria y por lo tanto la configuración se realizará en base al Anexo I de la guía CCN-STIC-803 *Valoración de los Sistemas en el ENS* [9], adoptando las medidas establecidas para una red de categoría *media*, en base a la criticidad de los recursos e información y de los servicios de la organización que se establecen a través de dicha red.

Los requerimientos de seguridad están basados en la Guía CCN-STIC-816 *Seguridad de Redes Inalámbricas* en el Esquema Nacional de Seguridad y estarán divididos en varios apartados:

- Requerimientos técnicos:
  - Normativa de seguridad.
  - Procedimientos de seguridad y proceso de autorización.
  - Configuración de seguridad.
- Requisitos operacionales:
  - Arquitectura de red.
  - Método de autenticación o control de acceso a la red corporativa.
- Requisitos de Explotación:
  - Inventario de activos
  - Protección de los equipos corporativos
  - Protección de los puntos de acceso
  - Servidor de autenticación
  - Registro y trazabilidad de actividades
  - Gestión del personal
- Requerimientos de protección de datos

Para la implantación de la red wifi propuesta se ha elegido un rúter de banda ancha inalámbrico sobre el que se implantarán las medidas obligatorias y recomendadas en la guía CCN-STIC-816 *Seguridad en las redes inalámbricas*. Así mismo, la guía CCN-STIC-105 *Catálogo de productos STIC* recomienda el uso de dispositivos de red que proporcionen un mínimo de seguridad. Dicha guía recomienda que la adquisición de productos TIC, en aquellas redes que vayan a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información. Dentro del catálogo de productos TIC, se ha elegido el producto certificado RUCKUS WIRELESS R610 como punto de acceso de referencia y sobre el que se va a configurar el despliegue de la red inalámbrica.

Sobre dicho rúter se implementan las medidas de seguridad que establece el Esquema Nacional de Seguridad para una red con un nivel de seguridad tipo medio.

Posteriormente se procede al despliegue físico de la red con la determinación de la ubicación ideal de los puntos de acceso, teniendo en cuenta la composición física del edificio, su taquicado interior y ajustando la potencia de emisión para evitar un exceso de radiación fuera del área de interés. Para ello procedemos al estudio del área de interés con un software que mostrará a través de un mapa de calor la ubicación ideal de los puntos de acceso.

Figura 2. Colocación de los puntos de acceso [10]

Así mismo, se realiza un estudio de la saturación electromagnética en la zona de interés a través de la herramienta AcrylicWi-Fi Home.

Una vez determinada la ubicación de los puntos de acceso, así como estudiada la saturación radioeléctrica de la zona de interés se procede a valorar la mejor opción de despliegue y se decide la conexión inalámbrica entre puntos de acceso con el objetivo de conseguir una máxima velocidad y estabilidad en la red, mejorando asimismo la saturación radio de la zona de interés.

Procedemos al bastionado de la red. La configuración de fábrica de los puntos de acceso y la configuración realizada posteriormente sobre el gestor de configuración web han proporcionado una seguridad mínima sobre la infraestructura. La red inalámbrica planteada en el proyecto necesita de un nivel de seguridad adicional que la permita adaptarse a lo especificado en la guía CCN-STIC-804 *Medidas de implantación del ENS*.

Por último, procedemos a la instalación y configuración de un servidor Radius que nos permitirá la autenticación segura de usuarios y su correspondiente base de datos de referencia. Asimismo, se va a dotar al administrador de un sistema de detección de intrusos basado en el software Kismet, que le permitirá tener un control mínimo de la red.

3. Resultados y discusión

Una parte importante del trabajo ha sido el estudio del área de interés, principalmente desde el punto de vista del reparto interno de ubicaciones y por otra parte, los limites que el edificio proporciona y por tanto limitan el área en la cual estamos interesados en dar servicio. A través de software libre se ha estudiado el área de interés y su composición, decidiéndose las ubicaciones más beneficiosas para la instalación de los puntos de acceso y se ha configurado la potencia de transmisión para que la señal radiada fuera del edificio fuese la mínima.

En base a los requerimientos de seguridad que establecen las guías CCN-STIC_816 *Seguridad en Redes Inalámbricas en el ENS* y en el anexo I de la guía CCN-STIC_803 *Valoración de los sistemas en universidades*, se considera que se han implementado las medidas de seguridad necesarias para conseguir el nivel de seguridad requerido.

4. Conclusiones

El objetivo principal del trabajo ha sido elaborar un documento técnico que permita a una organización bajo el paraguas del Esquema Nacional de Seguridad establecer un modelo de arquitectura de referencia para la implementación de un sistema de comunicaciones móviles basado en el estándar general 802.11 wifi seguro en un entorno corporativo.

Para la distribución de los puntos de acceso se realizó un mapa de calor en el cual se especificaban los materiales de construcción del área a abarcar y la posible atenuación que dichos materiales producían en la cobertura wifi. Se redujo la potencia de transmisión de los mismos para evitar una excesiva cobertura de radiación.

Posteriormente, se ha procedido con la complicada labor de configurar una red inalámbrica corporativa, complementada con una red de invitados. En dicha configuración se ha pretendido sintetizar y mostrar aquellos apartados que se han considerado más importantes.

Por último, se han realizado algunas pruebas pertinentes para comprobar y valorar que las medidas implementadas son efectivas, obviándose una serie de pruebas que darían un enfoque más amplio al proyecto.

Agradecimientos

Para mi familia, que estoicamente ha soportado mis malos momentos y me ha apoyado para la realización de este máster con paciencia.

Para mis compañeros de máster, su compañerismo, buen hacer y generosidad me han motivado para continuar y mejorar cada día.

Por supuesto, para mis tutores don Norberto y don Carlos, que me han guiado en este camino, a veces oscuro y tenebroso.

Referencias

[1] Tanenbaum S. y D. J. Wetherall, (2012), Redes de computadores, Editorial Pearson. ISBN 9780132126953.

[2] Historia de las redes inalámbricas [en línea] Enlace:https://histinf.blogs.upv.es/2010/12/02/historia-de-las-redes-inalámbricas/ [Último acceso: 05/01/2022]

[3] Institute of Electrical and Electronics Engineers [en línea] Enlace: https://www.ieee.org/ [Último acceso: 05/01/2022]

[4] Caos en la seguridad wifi [en línea] Enlace: https://www.xataka.com/seguridad/caos-enla-seguridad-wifi-un-repaso-a-las-vulnerabilidades-de-wep-wap-y-wap2 [Último acceso: 05/01/2022]

[5] Ataques en redes LAN [en línea] Enlace: https://www.redusers.com/noticias/ataques-enredes-lan-que-es-y-como-funciona-el-sniffing/ [Último acceso: 05/01/2022]

[6] CCN-CERT_BP_11_Recomendaciones redes WIFI [en línea] Enlace: https://www.ccncert.cni.es/informes/informes-ccn-cert-publicos/3143-ccn-cert-bp-11-recomendacionesredes-wifi-corporativas-1/file.html [Último acceso: 05/01/2022]

[7] Guía CCN-STIC-804 Medidas de implantación del ENS [en línea] Enlace:https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html [Último acceso: 05/01/2022]

[8] Ubicación geográfica de las instalaciones [en línea] Enlace: https://www.google.es/maps/@40.4010803, -3.8091817,68m/data=!3m1!¿1e3? hl=es [Último acceso: 05/01/2022]

[9] Guía CCN-STIC-803 Valoración de los sistemas [en línea] Enlace: https://www.ccncert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2509-ccn-stic-803-valoracion-de-sistemas-en-el-ens-anexo-i-universidades/file.html [Último acceso: 05/01/2022]

[10] Mapas de calor, Acrylic [en línea] Enlace: ttps://www.acrylicwifi.com/programassoftware-herramientas-wifi/análisis-cobertura-wifi-acrylic-heatmaps-mapas-de-cobertura/ [Último acceso: 05/01/2022]

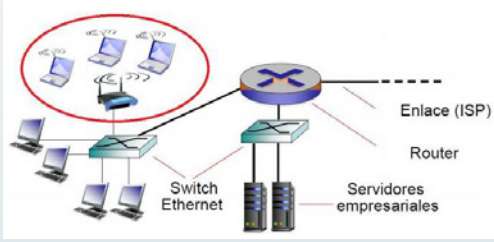
Comunicaciones WiFi seguras en entorno corporativo

Autor: Juan Carlos Núñez García
Directores: Norberto Fernández García y Carlos Zamorano Pinal
Universidad de Vigo

Estado del Arte

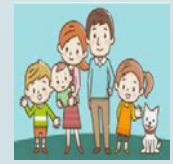
Desarrollo del TFM

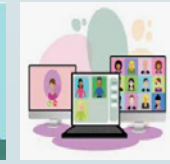
Despliegue de la red

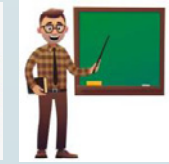


Conclusiones y Valoración

Agradecimientos







Metodología para la gestión de servicios en un Centro de Explotación CIS de la Armada

Autor: Rendón Fernández, Manuel (manrend@hotmail.com))
Directores: Ares Tarrío, Miguel Ángel (matarrio@gmail.com)
y Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – En este trabajo se propone una metodología genérica, flexible y eficiente, aplicable a cualquier Centro de Explotación CIS (CECIS) de la Armada, para proveer los servicios CIS/TIC de su responsabilidad a las unidades de su ámbito geográfico, siguiendo estándares y paradigmas de buenas prácticas, conocidos y probados, como son ITIL e ISO.

A partir de la Organización CIS/TIC de Defensa y de la Armada y de sus servicios, se fundamentará la necesidad de emprender este TFM con el objetivo de implementar el resultado en un CECIS como el último escalón en la provisión y gestión de los servicios CIS/TIC en la Armada.

En su desarrollo se expone la estructura de la Armada y la gestión del conocimiento y la información en Defensa, algunas de las tecnologías, normativas e iniciativas relevantes en la gestión de servicios, procedimientos y modelos actualmente en práctica en entidades nacionales e internacionales, así como herramientas informáticas específicamente diseñadas para la gestión de servicios con el fin de aportar valor al cliente con unos resultados de calidad. Finalizando el proyecto con una propuesta de metodología de trabajo aplicable siguiendo una estructura de Acuerdos de Nivel (Service Level Agreement - SLA), apoyada por una robusta herramienta informática de gestión, y realizando previamente una reestructuración funcional en el seno del propio CECIS para establecer la adecuada atención a la provisión de servicios.

Palabras clave – metodología, gestión, servicio, explotación, ITIL.

1. Introducción

En el trabajo se exponen conceptos y normas preestablecidas que nos permitirán conocer el marco regulador en el que se encuentran los CECIS de la Armada y cómo ejercen las funciones de su competencia, y así poder proponer una metodología acorde a referencias y estándares de buenas prácticas (ITIL e ISO).

A partir de la normativa y del conocimiento del estado del arte y dinámica de trabajo actual de nuestros CECIS, se realiza el esfuerzo por definir una metodología real y creíble que mejore lo existente, y que está orientada hacia tres claros objetivos o pilares: proponer una estructura organizativa interna en los centros que aporte mayor valor a los clientes, en definitiva los usuarios finales de redes y sistemas, con la creación de una célula de mantenimiento preventivo que siga las pautas que ITIL e ISO marcan a nivel internacional, trabajando con una herramienta de gestión de servicios consistente y bien extendida en todas nuestras unidades, y por último documentando toda relación de provisión de servicios a las Unidades de la Armada sobre SLA.

Finalmente se valorará si los citados objetivos han sido alcanzados, o al menos son alcanzables con los medios a disposición a día de hoy, y se trazarán unas posibles líneas futuras que podrían mejorar el resultado con el tiempo.

1.1. Organización CIS de la Armada

En la Organización de la Armada se establecen los Órganos de Apoyo a la Acción Orgánica (OAAO), bajo la autoridad del 2.º AJEMA, con la responsabilidad de proporcionar los servicios y apoyos de su competencia para facilitar la acción orgánica en la estructura de la Armada, como técnicos en su materia específica y asesorando al Estado Mayor de la Armada (EMA) en la elaboración de las políticas de su ámbito.

Como OAAO CIS/TIC tenemos la Jefatura de Sistemas de la Información y Telecomunicaciones (JECIS), que gestiona y proporciona servicios CIS en el nivel adecuado de eficacia, relacionados con los sistemas de información y telecomunicaciones de su ámbito de responsabilidad, a las unidades y organismos de la Armada, supervisa la aplicación de la normativa de seguridad de la información (SEGINFO), la protección de datos personales y garantía de derechos digitales, y dirige y gestiona la adquisición y empleo de la capacidad de ciberdefensa en la Armada.

Dentro de la JECIS tenemos el Grupo de Centros de Explotación de Sistemas de Tecnología de Información y Telecomunicaciones (GRUCECIS), figura 1-1, que proporciona los servicios CIS/TIC de apoyo a las unidades de la Armada implementando y manteniendo los requisitos de seguridad aprobados. Gestiona, controla y explota los CIS/TIC de su entorno de

responsabilidad, corporativos y conjuntos, dando asesoramiento técnico CIS. Entre sus cometidos:

- Dirige y controla la actividad de los CECIS para la correcta explotación de los CIS/TIC de la Armada y los corporativos del MDEF en nuestro ámbito.
- Genera, difunde y controla la ejecución de la normativa técnica a aplicar por los CECIS.
- Coordina y gestiona las peticiones y necesidades que los CECIS requieren de otros órganos CIS de ámbito conjunto y en la Armada.
- Elabora y mantiene el catálogo e inventario de la configuración de los componentes hardware y software de los sistemas CIS/TIC, y coordina la distribución de este material informático a los CECIS.

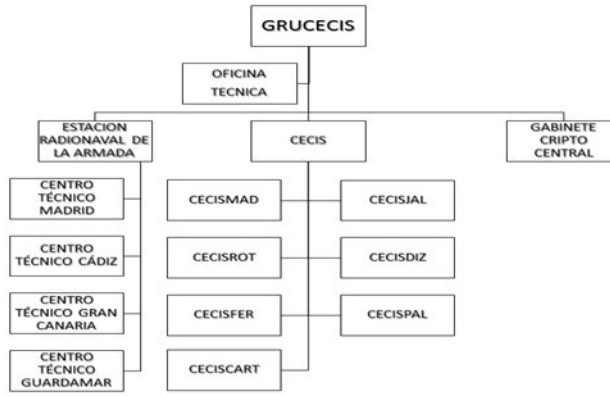


Figura 1-1. GRUCECIS y Centros de Explotación CIS establecidos

Y ya en particular, los CECIS facilitan a las unidades de su localización geográfica los servicios CIS, el acceso a los sistemas para el ejercicio de sus funciones y el apoyo técnico para su empleo. Reparten sus competencias en dos departamentos, el Centro de Comunicaciones (CECOM) y el Centro de Sistemas de Información (CESIN). Entre sus cometidos se contempla:

- Asegurar la continuidad de los enlaces entre sistemas y usuarios garantizando rapidez, seguridad, confianza y flexibilidad.
- Apoyar a las unidades en la instalación, configuración y actualización de los sistemas CIS prestando asesoramiento técnico CIS.
- Controlar, administrar y distribuir el equipamiento informático hardware y software, manteniendo el inventario actualizado.
- Prestar servicios de cifra, distribuir y controlar el material cripto y apoyar en el mantenimiento del equipamiento criptográfico.
- Colaboran en la definición de los requisitos de los nuevos sistemas, en la elaboración de la doctrina sobre su empleo, en la realiza-

ción de pruebas y estudios para su implantación y en el desarrollo de nuevas aplicaciones informáticas.

- Mantener los niveles de servicio adecuados de los sistemas CIS propios y colaborar con los del MDEF.

2. Desarrollo

Information Technology Infraestructure Library (ITIL) es una amplia publicación que contiene *buenas prácticas* orientadas a la gestión de servicios de TI, que facilitan a las organizaciones la gestión de sus infraestructuras TI y dan apoyo a sus objetivos de negocio. Como manual nació en los años 80 en el sector público británico y hoy en día es una herramienta aplicable a cualquier organización para la gestión de materias como la seguridad de la información, los niveles de servicio, gestión de sus activos, software y aplicaciones, tratando de crear un punto de unión entre la gestión de la TI y la gestión empresarial, en relación con otros estándares como son ISO (International Organization for Standardization) o el EFQM.

Desarrollado sin derechos de propiedad, es de uso libre y público, y está en continuo crecimiento con otras buenas prácticas recopiladas por expertos y profesionales del sector, favoreciendo la estandarización internacional de terminología, lenguaje y documentos. Está en vigor su versión 4, compuesta por 5 libros o volúmenes que definen el ciclo de vida ITIL (figura 2-1), organizados en 34 procesos o *conjuntos de recursos organizacionales diseñados para realizar un trabajo o lograr un objetivo*, para dar soporte y valor al negocio desde un punto de vista TI. No todos tienen por qué realizarse en una organización, principal diferencia con ISO, donde todos ellos son imprescindibles para lograr la certificación.

Figura 2-1. ITIL lifecycle

Los libros son *Estrategia, Diseño, Transición, Operación y Mejora Continua del Servicio*, donde se dan consejos para la gestión de la cartera y catálogo de servicios, de la demanda, de los niveles, de la disponibilidad, de los proveedores, de la capacidad y la continuidad, del cambio, configuración, versiones y despliegues. Gestión del Centro de servicios, de incidencias, problemas y errores.

2.1. Herramientas de Gestión de Servicios CIS

Son diferentes las aplicaciones o herramientas software disponibles en el entorno del MDEF y en el sector civil, diseñadas específicamente para la gestión de incidencias y peticiones, la solicitud de apoyo y soporte y para la administración y control del parque informático en cada entorno, además de comunicación directa con su Centro de Atención al Usuario (CAU). En el desarrollo del trabajo se dan a conocer en detalle las siguientes:

- SCANS (Sistema de Control de acuerdos de nivel de servicio) del MDEF para la red de propósito general no clasificada (WAN PG),
- I-CIS para la gestión de servicios IT en el Ejército de Tierra (ET),
- GISMI (Gestión de incidencias y saldos de mantenimiento de informática) como herramienta de gestión del mantenimiento hardware también en el ET,
- Proactivanet, como herramienta en estado de pruebas en el ámbito del Estado Mayor de la Defensa (EMAD) sobre la red clasificada de mando y control (C2) SIJE.

3. Resultados y discusión

Para el adecuado funcionamiento de los servicios, el CECIS debe poseer un área o núcleo de provisión de servicios que siga cada solicitud y supervise todas las peticiones asociadas, altas, modificaciones, traslados, bajas parciales o totales. Además, deberá comprobar que el cliente tiene instalada la solución a su incidencia/petición, revisando la configuración e informando al cliente de las acciones realizas tanto a nivel datos/redes como radio. También explicará a los CISPOC de las unidades las dudas que pudieran tener sobre el servicio, para que puedan en ciertas ocasiones autogestionar la resolución de incidencias internas, ya sea facilitándoles manuales o el acceso a una base de conocimiento con preguntas frecuentes (FAQ), por ejemplo.

El CECIS tendrá un CAU capaz de atender incidencias vía telefónica, por email y con una completa y robusta aplicación de gestión de incidencias y peticiones, derivando las entradas al área de competencia y al propio responsable del servicio tratado según su organigrama. Todo con el fin de recuperar los servicios en el menor tiempo posible, de acuerdo al nivel de servicio acordado y en base a unos indicadores clave de rendimiento definidos (Key Performance Indicators – KPI) y medidos generalmente en horas para su resolución según el horario de atención del CECIS.

Como epicentro de la política de mejora continua del CECIS se propone perfeccionar la prestación de servicios de mantenimiento, entendiendo este concepto no como la reparación y subsanación de incidencias a posteriori, sino como la ejecución de tareas proactivas y diarias para mantener el servicio operativo y en niveles de entrega satisfactorios en previsión a posibles fallos.

La atención de solicitudes, incidencias, averías y problemas diarios alcanza cifras altísimas y los tiempos de resolución se incrementan a medida que se trata de clientes individuales y aislados, frente a casos de afección genérica. Afrontar cada incidencia de manera reactiva, actuando exclusivamente en situaciones de averías a nivel de red, líneas, aplicaciones, etc., a la larga, demuestra que el tiempo de dedicación, la atención a los clientes y en general el nivel de satisfacción empeora.

En el trabajo se instaura internamente en el CECIS una Célula de mantenimiento que desarrolla una gestión proactiva de los servicios, atendiendo a las consultas, incidencias, averías y solicitudes, aportando valor al usuario con atención inmediata vía telefónica y telemática, mejorando el valor estratégico del CECIS, alineando las peticiones con el tratamiento adecuado, y mejorando los tiempos y niveles de resolución.

Esta célula será capaz de gestionar el conocimiento de todos sus integrantes, quienes afrontan las incidencias y deben tener la información necesaria para poder solucionarlas y la experiencia en su tratamiento y escalado; siendo capaz de adaptarse a múltiples escenarios cambiantes. En el detallado plan de implementación propuesto para esta célula en el seno del CECIS, se proponen en el trabajo numerosas acciones, siguiendo las buenas prácticas ITIL ya vistas, y otras decisiones específicas para su Operación, comenzando con:

- Designar un coordinador global de la actividad, con responsabilidad en la redacción de informes de seguimiento de la actividad y que actúe ante las incidencias muy críticas y de máxima prioridad y aquellas que superen el margen de tiempo de resolución convenido.
- Establecer un grupo de soporte a operadores y de apoyo al coordinador del CECIS, responsable también de la recopilación de información para los informes antes indicados. Número de operadores que dependerá del número de unidades a atender en la zona.

Esta nueva célula trabajará con un manual de cabecera para todas y cada una de sus acciones en relación a la prestación de servicios; los Acuerdos de Nivel de Servicios (SLA) que especifiquen cómo actuar y la atención a proporcionar ante incidencias, los tiempos de resolución según servicios y prioridades, periodos de atención y método a seguir según el horario laborable, días hábiles o inhábiles. En el trabajo no se incluye un modelo completo y fijo de SLA, sino que se muestra con ejemplos los diferentes conceptos vistos a lo largo de estudio, siguiendo los procesos de gestión

y buenas prácticas de ITIL e ISO, y que deberán detallarse en el acuerdo entre las partes involucradas.

Se trata de un documento tan extenso y desarrollado como se desee puntualizar la relación entre las partes, y que se propone que incluya:

- las diferentes referencias en las que estará basado el acuerdo entre las partes, como por ejemplo normativa de Organización de la Armada y su Estructura CIS, las relaciones de dependencia de la unidad apoyada y los servicios de voz y datos que debe disponer,
- los contratos vinculantes establecidos con proveedores de servicios externos,
- el plan anual de ejercicios y operaciones en los que la unidad participará y que supondrán servicios, dedicación y prioridades extra por parte del CECIS,
- las necesidades de adiestramiento del personal CIS de la unidad y que serán impartidas por el personal de la Célula de Mantenimiento del CECIS,
- un listado de servicios centralizados por el CESTIC y fuera del ámbito de este SLA particular o con un mínimo nivel de apoyo por parte del CECIS como intermediario o interlocutor con su proveedor.
- listado de servicios propios de la Armada que el CECIS provee en su entorno geográfico,
- desglose del equipamiento hardware entregado a las unidades, según catálogo de servicios,
- listado de prioridades establecidas por la unidad apoyada, el cliente, con una atención específica según los parámetros pactados, indicando para cada servicio su código, nombre, unidad, urgencia e impacto de la incidencia, nivel de prioridad y condición/es para ser atendida según el acuerdo,
- un capítulo de términos y condiciones del acuerdo que recogerá entre otros detalles, el horario y tipo de atención según días de la semana, comienzo y duración, representantes de las partes y sus roles y responsabilidades, informes a rendir y participación de las partes,
- niveles de apoyo según la dificultad y extensión de las incidencias, cortes e interrupciones programadas y el proceso de monitorización, medidas e informes de nivel y calidad de servicios a rendir en base a KPI (Performance) y KQI (Quality).

Finalmente, para la gestión de incidencias y control de inventario se comenzó a probar en el segundo semestre de 2021 una herramienta de gestión totalmente compatible con ITIL en el ámbito de la Armada y que hasta el momento solo estaba disponible en la red de mensajería oficial SACOMAR.

Esta herramienta, GLPI (Gestión Libre del Parque Informático), es una solución software libre de código abierto para gestión de incidencias e inventario de una plataforma informática completa, aportando múltiples funcionalidades:

- Inicio y seguimiento de incidencias, fallos, averías y solicitudes de servicio sobre el equipamiento.
- Comunicación y seguimiento de problemas generales en la red informática.
- Planificación y programación de actuaciones sobre la red, permitiendo el control de la configuración y de las distintas versiones SW a integrar en la red.
- Creación de roles estructurables al objeto de escalar incidencias, peticiones, problemas.
- Comienzo y desarrollo de informes de estado y seguimiento.
- Facilidad de integración con otras herramientas para la automatización de los catálogos e inventarios.
- Creación y alimentación de una base de datos del conocimiento (GIC), conteniendo la mayor cantidad de información y referentes para la resolución de problemas rápida y eficiente. Además, con un banco de preguntas frecuentes disponible para los usuarios, que cada vez requieren un acceso más rápido a las soluciones y reforzará el apoyo de nivel O (self-service).

Será GLPI la aplicación propuesta a utilizar como herramienta de trabajo del CECIS en su entrega de servicios de calidad a las unidades apoyadas, quedando instalada en los servidores principales de las redes propias y que en el desarrollo del trabajo se exponen las particularidades que la hacen especial e idónea para su empleo en el entorno Armada.

4. Conclusiones

Como conclusión de este trabajo se confirma que los objetivos propuestos de inicio son alcanzables e implementables, estando a día de hoy disponible una herramienta capaz de centralizar toda la gestión de servicios que facilitan nuestros Centros de Explotación CIS (GLPI para nuestro caso), siendo totalmente viable la reestructuración funcional interna de los CECIS de la Armada configurando una *célula de mantenimiento* preventivo que aporte valor al usuario velando por el correcto funcionamiento de redes y sistemas con antelación suficiente a posibles incidencias y problemas; y por último documentando y normalizando su dinámica de trabajo y servicio en un marco legal establecido por acuerdos de nivel con las unidades apoyadas y terceros, a través de los conocidos como Service Level Agreement – SLA.

Agradecimientos

A mi tutor, Miguel Ángel, por su disponibilidad, orientación y suministro de material e ideas para la investigación.

A mis compañeros de máster y de unidades como el CESTIC, la JECIS y el CECISDIZ, por facilitarme documentación, ejemplos y sugerencias para afrontar esta complicada tarea.

Y finalmente a mi familia, esposa e hijas, por su paciencia y apoyo constante, a quien les debo las horas disponibles para superar este proyecto.

Referencias

[1] Instrucción General 01/10 del Componente CIS del Sistema de Mando y Control Militar (SMCM), de enero de 2010, del JEMAD.

[2] Instrucción Técnica para la Gestión de la Calidad del Servicio en la Red IPC2 del STM, de 13 de julio de 2015, del JESPREMAD.

[3] Acta del Pleno de la Junta CIS (JUCIS) de la Armada, de mayo de 2021 sobre la nueva Organización CIS de la Armada.

[4] Concepto de Operaciones (CONOPS) del CESTIC, de enero de 2020.

[5] Orden Defensa 2639/2015, sobre Política CIS/TIC del MDEF, de 10 de diciembre.

[6] Instrucción 37/2019, para la Coordinación de la gestión de la información y el concimiento (GIC), de 9 de julio, del SEDEF.

[7] Instrucción 06/17, de Control del Catálogo e Inventario del material informático de la Armada, del JEGRUCECIS.

[8] Instrucción 01/17, Cambio 1 sobre Procedimiento de adquisición de material informático para la red de propósito general y redes clasificadas, del JEGRUCECIS.

[9] Instrucción técnica 01/20, de la Gestión de la Demanda, del CESTIC.

[10] Norma 03/21, de la Gestión del Servicio de red wifi de asistencia al personal, del CESTIC.

[11] Instrucción Operativa para la Gestión de Incidencias y Peticiones en las redes RAPNA y SAPZO, del CESTIC.

[12] Manual Integro ITIL v3 de B-able, *Biable Management, Excellence and Innovation*.

[13] *ITIL for dummies*, edición de 2011, de Peter Farenden, publicación de John Wiley and Sons, Ltd.

[14] Norma Española UNE-ISO/IEC 20000-1, de diciembre 2018, del Comité Técnico CTN71 Tecnología de la Información.

[15] *Enterprise Information and Communicaction Technology Service Delivery Model*, de 30 de noviembre de 2016, de la NATO *Communications and Information Agency* (NCIA).

[16] *Enterprise Service Delivery Model Implementation Plan 2019*, de 17 de octubre de 2018, de NCIA.

[17] Manuales de las aplicaciones de Gestión de Servicios SCANS, iCIS, ARIET y GISMI extraídos de la Red Corporativa de Propósito General (WANPG).

[18] Manual de la aplicación de Gestión de Servicios Proactivanet, de Gartner Peer Insights.

[19] Manual de la aplicación de Gestión de Servicios GLPI extraído de la red de mensajería oficial de la Armada, SACOMAR.

[20] ITIL. Apuntes y clases magistrales de la asignatura COM3 del Máster DIRETIC 2020-2021 del Centro Universitario de la Defensa (CUD).

Metodología para la Gestión de Servicios en un Centro de Explotación CIS de la Armada

Autor: Manuel Rendón Fernández

Directores: Miguel Angel Ares Tarrío y José María Núñez Ortuño

Introducción

Los Centros de Explotación CIS de la Armada apoyan a las unidades en la instalación, configuración y actualización de los medios CIS y administran, distribuyen y controlan el equipamiento TIC necesario.

En el desarrollo de sus cometidos no existe actualmente un procedimiento o metodología basada en procesos ni una herramienta de gestión de servicios facilitadora de su actividad.

Son varios los estándares internacionales, ITIL e ISO fundamentalmente, que versan como guías de buenas prácticas y maneras, con el objetivo de impulsar el valor de estas acciones reportando mayores beneficios a los usuarios de los sistemas.

Metodología

A través del estudio de la numerosa documentación referente a la organización y funcionamiento CIS de Defensa y la Armada, así como de los procedimientos ya establecidos en el ámbito de las TIC, se plantea una Metodología genérica, flexible y eficiente para la Gestión de Servicios en un Centro de Explotación CIS de la Armada, siguiendo los estándares antes mencionados y con tres claros pilares:

- Una reestructuración interna que aporte más valor a los clientes.
- Una herramienta de trabajo y gestión consistente y extendida en la Institución.
- Un marco regulador de servicios en base a acuerdos de nivel (*Service Level Agreement* – SLA).

Resultados

Son alcanzados los objetivos propuestos, a través de la implementación de una Célula de Mantenimiento preventivo en el seno de nuestros Centros de Explotación CIS, que domina una potente y versátil herramienta de gestión de servicios (se propone GLPI – Gestión Libre del Parque informático) y dentro de un paradigma de trabajo materializado por Acuerdos de Nivel de Servicios con las Unidades apoyadas, que facilitan, automatizan y en definitiva responden a las necesidades de los clientes y del proveedor.

Conclusiones

La información, el conocimiento y los sistemas son esenciales para la consecución de la propuesta planteada, pero sin duda vuelve a ser el aspecto personal, la disponibilidad de una plantilla dimensionada dotada de efectivos con conocimiento y experiencia en los Centros de Explotación y en la cadena de mando CIS/TIC el ingrediente fundamental para su implementación y obtención del máximo rendimiento.

Agradecimientos

Aprovecho la oportunidad para agradecer su colaboración en el presente TFM a mi tutor como guía, a los compañeros de trabajo y Máster como facilitadores de conocimiento, y finalmente a mi familia por su apoyo y fuerza en el desarrollo.

Desarrollo de un sistema de exploración *off-line* del espectro radioeléctrico, basado en el análisis de datos goniométricos

Autor: Rey Alameda, Javier (jreyala@et.mde.es)
Director: Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – Actualmente, la exploración del espectro radioeléctrico con la finalidad de escuchar, interceptar y localizar emisiones radioeléctricas de interés, se realiza en base a receptores de banda ancha, los cuales de una manera on-line presentan la actividad existente en tiempo real. Esto supone que, aquellas emisiones que no se traten en el preciso momento de su interceptación, se perderá su información, a no ser, que puedan ser tratadas a posteriori.

Igualmente, no existe un sistema que posibilite el análisis del comportamiento en el tiempo de esas emisiones captadas.

Por estos motivos y basado en la información goniométrica proporcionada por un sistema de guerra electrónica (EW), este trabajo pretende implantar las bases de un modelo de sistema que posibilite:

— Almacenar la información goniométrica proporcionada por un sistema de EW, en un ancho de banda determinado, así como en un margen de tiempo.

— Poder llevar a cabo un análisis de manera conjunta (tiempo y frecuencia de emisión) para convertir orígenes de datos goniométricos, sin relación entre sí, en información coherente, interactiva y atractiva visualmente.

— Mostrar la información goniométrica que se determine en un Sistema de Información Geográfica (GIS).

— Posibilitar en el contexto radioeléctrico y en base al análisis de Big Data de captaciones radioeléctricas, la realización de Machine Learning para detección de anomalías.

Palabras clave – guerra electrónica (EW), sistemas de radiogoniometría, Big Data, Machine Learning, detección de anomalías.

1. Introducción

1.1. EW

La guerra electrónica (abreviado, EW, del inglés *Electronic Warfare*) [4] consiste en una actividad tecnológica y electrónica con el fin de determinar, explotar, reducir o impedir el uso hostil de todos los espectros de energía, por ejemplo, el electromagnético, por parte del adversario y a la vez conservar la utilización de dicho espectro en beneficio propio.

Dada la complejidad de las operaciones militares, la EW se divide en tres partes elementales:

- Medidas de apoyo de guerra electrónica (ESM).
- Contramedidas electrónicas (ECM).
- Medidas de protección electrónica (EPM).

Las que nos interesan son las medidas ESM. Son actividades encaminadas a buscar, interceptar e identificar las emisiones electromagnéticas, así como a localizar su procedencia. La finalidad de estas actividades es la obtención de conocimiento acerca de la situación electromagnética del enemigo (Orden de Batalla Electrónico OBE), y el reconocimiento inmediato de la amenaza. Dada su naturaleza, la ESM comparte muchas características comunes con las actividades realizadas para la obtención de inteligencia. Dichas actividades se suelen clasificar en las siguientes categorías:

— Inteligencia de comunicaciones o COMINT (*Communications Intelligence*), consiste en la obtención de información a partir de las emisiones realizadas por sistemas de comunicaciones.

— Inteligencia electrónica o ELINT (*Electronic Intelligence*), comprende las actividades dirigidas a obtener información técnica y de inteligencia a partir de emisiones realizadas por sistemas de no-comunicaciones (radares, perturbadores, etc.).

— Inteligencia de señales o SIGINT, (*Signals Intelligence*), agrupa a COMINT y a ELINT. Se utiliza este término cuando no se quiere distinguir entre las dos. Dada su naturaleza, las actividades ESM comparten muchas características con las actividades SIGINT, siendo la principal diferencia entre ambas su finalidad y el uso que se haga de la información obtenida (apoyo a decisiones tácticas a corto plazo —ESM—, o a decisiones estratégicas a largo plazo —SIGINT—).

Técnicas ESM [6]. Se puede generalizar que un sistema ESM realiza todas o parte de las siguientes tareas:

— Exploración. Utilizando sensores que captan las señales del entorno electromagnético. Los sensores constan de equipos receptores y antenas. Normalmente se dispone de receptores de banda ancha que cubren o exploran a gran velocidad un margen más o menos amplio del espectro, con el fin de detectar actividad en él.

- Interceptación. Cuando, durante la fase de exploración, se descubre una frecuencia que está emitiendo, pudiéndose grabar su frecuencia o no.
- Medida de parámetros. Los parámetros de los pulsos (señales de no comunicaciones) y de las señales de comunicaciones son medidos y digitalizados para su proceso posterior.
- Análisis y clasificación. Mediante HW y SW específico se analizan las señales captadas identificando sus parámetros técnicos, y se clasifican. En el caso de las trasmisiones de comunicaciones digitales, se utilizan equipos para decodificarlas. El contenido de las comunicaciones se obtiene mediante operadores humanos, o bien mediante sistemas automáticos de reconocimiento del habla.
- Registro. Las señales captadas pueden ser registradas mediante equipos de grabación para su conservación o análisis posterior en laboratorio (*off-line*).
- Identificación. En equipos ESM de no comunicaciones, reuniendo los datos obtenidos del análisis de las señales se realiza una identificación automática o asistida por el operador. En sistemas ESM de comunicaciones se utilizan los datos del análisis de señal, el contenido de las transmisiones de comunicaciones, y la localización de los emisores para realizar una identificación de emisores basado principalmente en la experiencia del operador. Se apoyan en bases de datos obtenidas y depuradas mediante captaciones anteriores a lo largo de tiempo.
- Localización. Se utilizan equipos que permiten obtener de forma más o menos precisa la localización geográfica del emisor. Se consigue mediante radiogoniómetros, que son receptores capaces de determinar el ángulo de llegada de la señal. Utilizando varios de esos equipos situados en localizaciones suficientemente separadas, o bien un único equipo en movimiento, se puede obtener la localización por triangulación. También, existen sistemas que, para ciertos casos, además del ángulo en azimut determinan también el ángulo de elevación. Con ellos se puede obtener, en determinadas circunstancias, la localización utilizando un solo sensor.

Esta localización se basa en la radiogoniometría, cada vez más utilizada, ya que con las nuevas técnicas de transmisión de espectro ensanchado (SS), es casi imposible conocer el contenido de la información transmitida, pero, gracias a la radiogoniometría, se puede conocer la fuente de origen de la emisión. La principal técnica de radiogoniometría utilizada, suele ser la interferometría. El principio básico del interferómetro correlativo consiste en comparar las diferencias de fase medidas, con las diferencias de fase obtenidas por el sistema, utilizando un ángulo de onda conocido. La comparación se realiza calculando el error cuadrático o el coeficiente de correlación de los dos conjuntos de datos.

2. Desarrollo

La primera necesidad que nos surge es la de tratar la ingente cantidad de señales radioeléctricas y goniometrías recibidas (Big Data) a posteriori de su recepción (*off-line*), en una base de datos (BBDD) ágil que permita a un usuario analizar esa cantidad de información basándose en alarmas y logs que detectarán el cambio de patrón seguido por las señales durante un determinado tiempo de muestreo.

Para el tratamiento, filtrado y representación de resultados se puede utilizar una herramienta de análisis de datos comercial que pueda manejar la ingente cantidad de datos de salida (Big Data). El análisis de datos es un proceso que consiste en inspeccionar, limpiar y transformar datos con el objetivo de resaltar información útil, para sugerir conclusiones y apoyo en la toma de decisiones. Se centra en la inferencia estadística, la cual permite tomar una decisión de forma sencilla con un grado de confianza determinado, identificando y analizando tanto datos como patrones de comportamiento.

Habría que crear una herramienta *ad-hoc* que analizase los datos para proporcionar visualizaciones interactivas y poder crear a sus usuarios informes. A falta de esa herramienta particular, se ha adoptado y *customizado* la herramienta Power BI. Se necesitan que las máquinas sean capaces de realizar una variedad de acciones que no están implementadas en esta herramienta como: avisar cuando, entre una ingente cantidad de datos, alguno o algunos de ellos se salgan de la norma, es decir, cuando los datos entrantes sean diferentes a los patrones considerados normales. Se necesita un programa que establezca unas alarmas cuando:

- Exista un incremento o disminución anormal de emisiones en el éter.
- Cuando una plataforma emisora haya cambiado de azimut.
- Cuando haya habido un cambio en las horas de emisión de una plataforma conocida.
- Cuando una plataforma conocida cambie de frecuencia de emisión.

Para ello se necesita dotar al *sistema de exploración off-line*, de una herramienta de detección de anomalías basada en inteligencia artificial (IA) y más concretamente en la técnica *Machine Learning*.

Machine Learning [2] utiliza dos tipos de técnicas, figura 1:

- Aprendizaje supervisado, el cual desarrolla modelos predictivos basados en datos conocidos de entrada y salida.
- Aprendizaje no supervisado, donde los datos se agrupan y se interpretan basándose solamente en los datos de entrada.

El algoritmo usado en el aprendizaje no supervisado se utiliza para analizar los datos conocidos y ser capaz de encontrar patrones escondidos. Los algoritmos de detección de anomalías no supervisadas sirven para detectar anomalías. Esta detección de anomalías no deja de ser una

técnica de minería de datos que permite el reconocimiento de nuevos patrones con comportamiento inusual, los cuales pueden ser traducidos como acciones no válidas o anómalas sobre los datos.

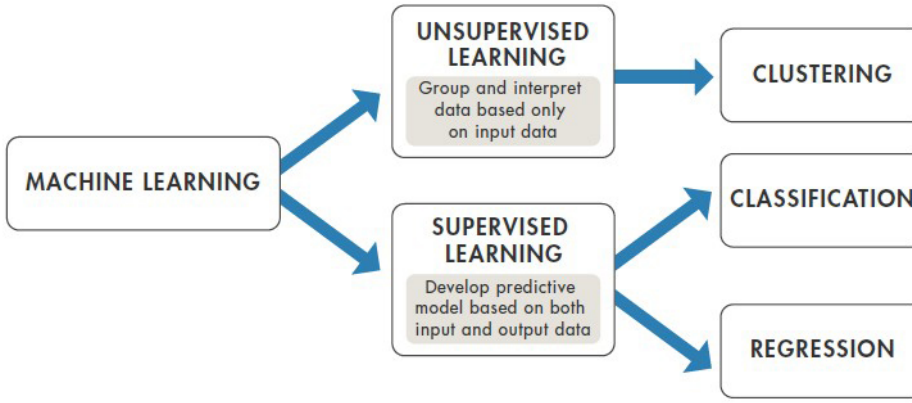


Figura 1. División de tipos de aprendizaje y algoritmos

3. Resultados y discusión

Los sistemas actuales de EW [1] están formados por una base goniométrica, es decir, conjunto de sensoras (varias antenas receptoras omnidireccionales distantes geográficamente entre sí), que, junto con un SW de tratamiento de señal y presentación, permiten a los operadores explorar el espectro electromagnético para detectar una emisión, figura 2-1, y localizarla utilizando el método de radiogoniometría descrito anteriormente (interferometría).

Para crear un sistema flexible y rápido se debería trabajar la selección de los datos en origen, en cada goniómetro utilizado, de tal forma que mediante una serie de algoritmos se extraigan los datos de interés según las misiones designadas.

El sistema debería constar de tres bases de datos (BBDD) diferentes. La BBDD de mando y control que sería la encargada de almacenar y distribuir la configuración común, la configuración individual de cada goniómetro, así como la de las misiones asignadas.

Los procesadores goniométricos enviarían los resultados obtenidos a la BBDD intermedia y a la BBDD histórica. Esta última recibiría los datos de la misión y los parámetros de configuración asignados a cada goniómetro en el momento de ejecución de la misión, al objeto de poder reproducir con fiabilidad todos los datos iniciales y los resultados obtenidos en cualquier momento temporal.

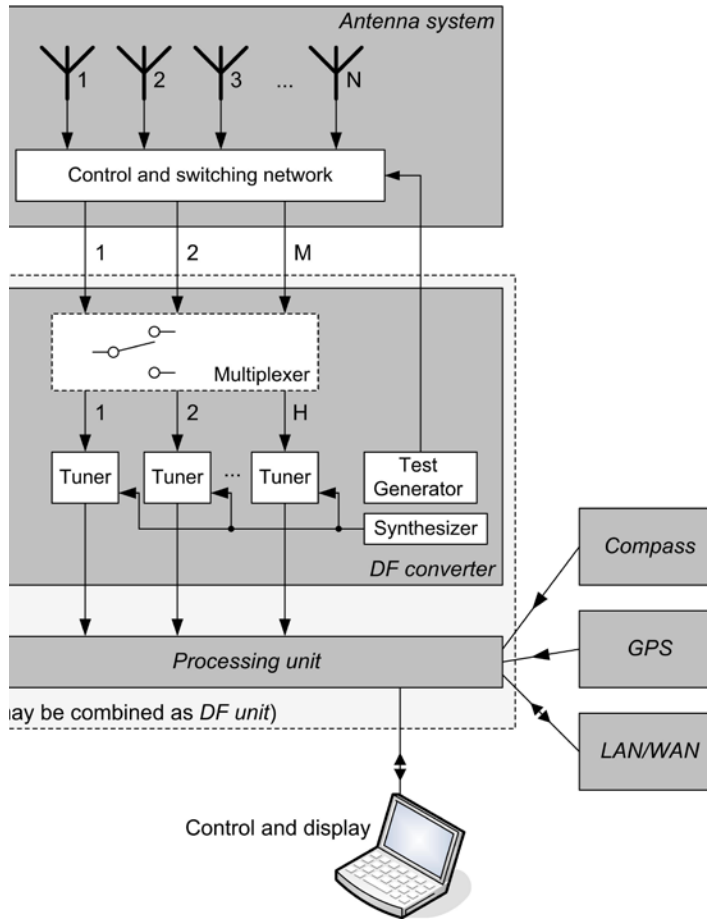


Figura 2. Componentes de un sistema de radiogoniometría (figura tomada de R&S DDF550 manual)

La BBDD Intermedia sería la encargada de la recogida de los datos obtenidos por cada goniómetro según los parámetros de configuración y las misiones asignadas en curso, de esta forma proporcionará las interceptaciones obtenidas al equipo en tiempo útil. Este SW utilizará la estadística que proporcione la BBDD histórica.

Se debe ejecutar en un equipo que recoja la posibilidad de activar las siguientes alarmas y análisis, utilizando las técnicas anteriormente descritas referentes a *Machine Learning* y detección de anomalías:

- Alarmas sobre aumento de actividad de las frecuencias asignadas de interés.
- Alarmas sobre la disminución de actividad de las frecuencias asignadas de interés.
- Alarmas sobre la actividad de las frecuencias propias.
- Alarmas sobre cambio de horas habituales de comunicaciones.

4. Conclusiones y líneas futuras

En definitiva, para poder abordar el problema de la exploración *off-line* y detección de alarmas, se debería emplear una arquitectura cliente-servidor flexible [5] que proporcionara un conjunto completo de herramientas para llevar a cabo la vigilancia por radio. Este sistema debería adquirir y describir rápidamente cualquier señal radio, y posteriormente realizar un análisis detallado de señales específicas de interés, tanto en tiempo real como *off-line*. El análisis debería incluir la detección, localización, clasificación y archivo de las actividades radioeléctricas. Cuando se detectase una señal, el sistema determinaría automáticamente la dirección de la fuente de energía y todos los demás parámetros, y presentaría esa información al operador. Esta información se archivaría automáticamente para análisis futuros (*off-line*) o se podría pasar simultáneamente en tiempo real a las estaciones de trabajo del cliente (operador).

Este sistema debería constar de los siguientes subsistemas, figura 3:

- Array de antena de control/DF y distribución de RF.

  Para la radiogoniometría, el sistema se debería poder configurar para operar con una variedad de antenas interferómetro.

- Adquisición de señal de canal de banda ancha y procesador DF.

  Cada canal constaría de un preselector de banda ancha, un digitalizador de alta velocidad y un procesador de señal digital. Estos procesadores detectarían simultáneamente la actividad de la señal en cada canal y realizarían goniometrías en los canales activos. La actividad espectral y los datos DF se enviarían al controlador para su posterior procesamiento.

- Adquisición y recopilación de señales.

  El controlador administraría el acceso de los clientes a los procesadores DF, además registraría los resultados sin procesar (en crudo) para almacenarlos en una BBDD local privada.

- Estaciones de trabajo para tareas del sistema y análisis de señales en tiempo real y *off-line*

- Interfaz de sistema externo y multisitio.

Este sistema debería integrar una interfaz gráfica de usuario que detectase y catalogase automáticamente todas las señales, para que el operador pueda examinar todas las detecciones o buscar señales específicas de interés utilizando una lista integrada, un espectrograma y mapas. Se debería poder limitar los resultados mostrados a solo señales de interés deseadas, además de poder realizar una búsqueda para encontrar instantáneamente señales similares por frecuencia, huella espectral o geolocalización.

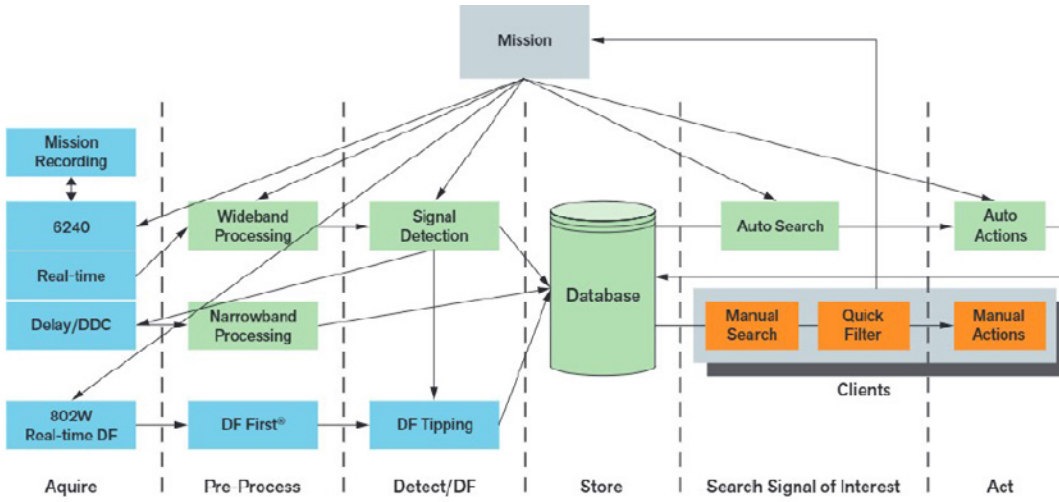


Figura 3. Esquema de subsistemas (figura tomada de 802W Wideband HF COMINT system)

Esta interfaz debería permitir evaluar automáticamente las interceptaciones entrantes según unos criterios de búsqueda. Las intercepciones que fueran coincidentes deberían desencadenar acciones automatizadas como *alertas* del operador, etiquetado, clasificación de la modulación, grabación en tiempo real, grabación inteligente (grabación basada en criterios de modulación de señal) y geolocalización. Estas tareas de automatización ayudarían a los operadores notificando *alarmas*. Los operadores deberían poder definir áreas de interés para buscar señales por geolocalización.

En relación con líneas futuras, se vislumbran:

- SDR/CR. Aprovechar la flexibilidad que ofrece la radio definida por software (SDR) aplicada a receptores, y más concretamente las radios cognitivas (CR) para mostrar mejores prestaciones en cuanto a reconfiguración de la frecuencia de las antenas y filtrado de ruido [7]. Se propone un enfoque cognitivo, llamado selección de antena cognitiva (CASE), para cambiar secuencialmente los elementos del array de antenas en función de observaciones anteriores.
- Metamateriales. Materiales inteligentes dotados de propiedades electromagnéticas inusuales [8], que se podrían aplicar para fabricación de antenas receptoras utilizando cristales electromagnéticos (antenas de cristal) que permite la eliminación de espúreos en filtros de microondas.
- Receptores fotónicos. Convierten las ondas electromagnéticas en fotones que viajan a la velocidad de la luz. Al procesar la información en fotones en lugar de electrones se pueden extraer y analizar más señales y más rápido [9].

Referencias

[1] Manual del sistema R&S DDF550, wideband direction finder.

[2] Mathworks machine learning ebook «Introducing machine learning», 2016.

[3] Radiomonitoring & radiolocation, catalog 2016, de Rohde & Schwarz.

[4] Monografías del SOPT, octubre 2009. La guerra electrónica en España.

[5] Ficha de características técnicas del 802W Wideband HF COMINT system, 2016.

[6] Documentación del II Curso de Analista de Información Electrónica del E.T.

[7] https://www.researchgate.net/publication/224263423_On_antennas_for_Cognitive_Radios

[8] www.mundodigital.net/metamateriales-los-materiales-inteligentes/

[9] https://www.dasphotonics.com/defense/

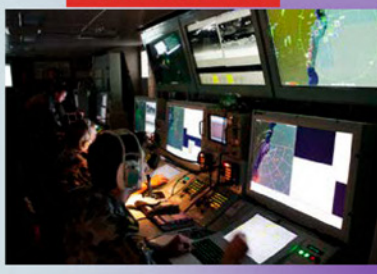
Desarrollo de un sistema de exploración off-line del espectro radioeléctrico, basado en el análisis de datos goniométricos

Universidad de Vigo

Autor: Javier Rey Alameda

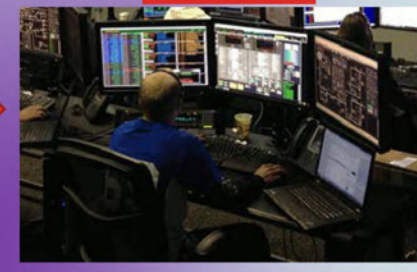
Director: Jose María Nuñez Ortuño

OPERADORES EW



BIG DATA

ANALISTA EW



MACHINE LEARNING

¿Se puede aplicar Inteligencia Artificial para analizar y alertar de patrones inusuales en datos recogidos por estaciones de interceptación y localización de señales radioeléctricas?

- Aumento de actividad
- Disminución actividad
- Cambio horas Tx
- Cambio de azimut

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

Mecánica cuántica aplicada a procesado y comunicaciones: implicaciones presentes y futuras

Autor: Sánchez Jiménez, Ricardo (ric@coit.es)
Directores: Fernández Gavilanes, Milagros (mfgavilanes@cud.uvigo.es)
y Fernández García, Norberto (norberto@cud.uvigo.es)

Resumen – El objetivo de este trabajo es demostrar el enorme desarrollo que han experimentado las tecnologías cuánticas en las últimas décadas, haciendo una amplia revisión de su estado actual y estimando cuál podrá ser su evolución.

Cuando los ordenadores cuánticos alcancen la supremacía cuántica, se podrán ejecutar algoritmos que disminuirán los tiempos de resolución de problemas actualmente complejos. Estos hitos no tendrían mayor trascendencia si no fuese porque se mina la confianza en la que se basan los sistemas actuales de criptografía asimétrica. Como consecuencia, se está discutiendo el estándar de una familia de sistemas criptográficos no basados en la física cuántica, pero que se espera que sean lo suficientemente complejos de resolver por ella. No existen estándares de cifrado cuántico, pero se estudia la aplicación de sistemas de comunicaciones cuánticas en protocolos que permiten establecer con máxima seguridad un secreto compartido. Estas comunicaciones, encuentran también un nicho de oportunidad en el desarrollo de generadores cuánticos de números aleatorios, aumentando la entropía de los generadores actuales. Relacionado con el avance de la computación y de los algoritmos cuánticos, se estudia su impacto en los métodos de aprendizaje automático, con un potencial a considerar en su uso en aplicaciones de seguridad, como los sistemas de detección de intrusiones en red.

En definitiva, la definición de casos de uso basados en las diferentes tecnologías cuánticas será el detonante para su desarrollo a nivel académico, al aumentar los presupuestos de investigación. También es esperable un crecimiento de la inversión privada, dadas las múltiples aplicaciones de estas tecnologías.

Palabras clave – cúbit, estados cuánticos, criptografía PQ, QKD, QML.

1. Introducción

1.1. Contexto histórico

En el primer cuarto del siglo XX se asentaron las bases de la nueva física cuántica, aconteciendo lo que se ha conocido como la primera revolución cuántica, en la que se obtiene la capacidad para acceder a estados cuánticos discretos en los sistemas. Se comienza a hablar de la *cuantización* y del efecto túnel, con el desarrollo a partir de la mitad del siglo XX, de tecnologías que se basan en el carácter discreto de la naturaleza. Encontramos ejemplos como el del diseño del primer transistor, el primer láser o las células fotovoltaicas.

Posteriormente, a partir de los años 80 llegamos a la segunda revolución cuántica, que podemos considerar que pervive hasta hoy. Se dispone de la capacidad de preparar y controlar los estados cuánticos a voluntad, gracias a propiedades como la superposición y el entrelazamiento cuántico. De esta forma, durante la última década se ha desarrollado enormemente la investigación en las tecnologías cuánticas que son objeto de este trabajo, principalmente la computación y las comunicaciones cuánticas, dado que el resto de disciplinas podemos considerarlas como una consecuencia de los avances de estas dos primeras.

1.2. Objetivos

A lo largo del presente documento se pretende transmitir al lector la relevancia del extenso concepto de las tecnologías cuánticas, poniendo de manifiesto el gran potencial que tienen desde el punto vista técnico y estratégico, obteniendo unas capacidades y unos niveles de seguridad muy superiores a los obtenidos por los métodos tradicionales.

Para conseguirlo, se hará un estudio pormenorizado de la situación actual de los ordenadores cuánticos, que van a ser del detonante del desarrollo de las otras tecnologías cuánticas, ya sea de forma directa o indirecta. Esto aplica especialmente al caso de la criptografía postcuántica (PQ) o del aprendizaje automático cuántico (QML). Podemos considerar que en el caso de las comunicaciones cuánticas y de los generadores cuánticos de números aleatorios (QRNG), están evolucionando de forma (más) independiente, pero siempre en base a las propiedades cuánticas de los elementos que manipulan, generalmente fotones de luz.

2. Motivaciones y necesidades para su desarrollo

Desde principios del siglo pasado, la física cuántica ha venido estudiando el comportamiento de las partículas de tamaño atómico, intentando explicar su comportamiento con fenómenos difícilmente explicables desde el punto de vista de la física clásica. Sin embargo, ha sido en los últimos 20 años cuando han convergido los estudios teóricos conocidos hasta la fecha, con un enorme desarrollo técnico en la implementación de los ordenadores

cuánticos, que ha permitido ir demostrando uno a uno todos los postulados definidos por los físicos teóricos durante el siglo XX. Al ir pasando los estudios paulatinamente del plano teórico al escenario real, se ha vuelto a despertar el interés no solo de la comunidad científica y la sociedad en general, sino de diferentes consorcios empresariales y agencias gubernamentales dado el enorme potencial que ofrece esta tecnología. Han entrado en el campo de juego múltiples jugadores no tradicionales, dadas las derivadas geopolíticas entre los países del bloque occidental y China, principalmente. Gartner [1] prevé que, en 2023, un 20 % de las organizaciones contemplarán en su presupuesto partidas para proyectos de computación cuántica, frente al 1 % de las organizaciones que lo presupuestaron en 2019.

Según la consultora de negocios BCG [2], puede haber 3 causas que expliquen el vertiginoso aumento de inversión, que va ligado a la actual carrera de investigación y desarrollo en el campo de las tecnologías cuánticas:

- Alcanzar la ansiada supremacía cuántica, ya anunciada un par de veces de manera un tanto controvertida tanto por Google [3] como por un grupo de investigación de la Universidad de Ciencia y Tecnología de China en Hefei [4]).
- Disponer de una hoja de ruta que fije hitos rupturistas a diez años vista.
- Definir casos de uso que hagan despertar el interés comercial de la industria.

3. Tecnologías cuánticas

3.1. Ordenadores cuánticos

Comenzamos haciendo referencia al concepto de supremacía cuántica, comentado al final del apartado anterior. Esta idea fue presentada por Preskill en 2012 [5]. Según su artículo, la supremacía se alcanzará cuando seamos capaces de realizar tareas con sistemas cuánticos controlados, de una complejidad mayor que las tareas más complejas que se pueden conseguir con ordenadores digitales clásicos. En el caso de Google, en 2019 [3] anunciaron que habían alcanzado la supremacía cuántica después haber superado un reto muy complejo para los ordenadores actuales. Lo consiguieron con un ordenador cuántico de 53 cúbits, denominado Sycamore. Desde el punto de vista de IBM [6], este reto se podía haber completado en un par de días mediante su propio superordenador clásico Summit, poniendo en discusión la autoproclamada supremacía cuántica y rebajándola a tan solo una *ventaja* cuántica.

Posteriormente, Preskill presentó un concepto en 2018 [7], utilizado para describir el punto de situación en el desarrollo de los actuales ordenadores cuánticos, en la vertiginosa carrera de investigación existente. Son los llamados ordenadores NISQ (*noisy intermediate scale*

quantum). Vienen caracterizados por su gran sensibilidad respecto del ambiente que los rodea (*noisy*), lo que perturba el estado de sus cúbits. Su número de cúbits (en un orden de entre 50 y unos pocos cientos) sigue en pleno crecimiento, pero lejos de representar un valor diferenciador (*intermediate scale*). Aun así, proporciona una pequeña ventaja cuántica de procesamiento respecto de los ordenadores actuales (*quantum*).

En la figura 1 podemos ver las diferentes apuestas que lideran varias corporaciones TIC. Destacamos los ordenadores cuánticos basados en bucles de superconductores, apuesta tecnológica de IBM, Google y Amazon. Consiguen los mejores resultados basándose en la superposición de corrientes que discurren simultáneamente alrededor de un conductor. El coste de fabricación es bajo, pero requieren de un gran esfuerzo en mantener temperaturas extremadamente bajas, para extraer la entropía introducida por el ruido [5]. Otra dificultad es el valor tan bajo del tiempo de coherencia que consiguen, del orden de milisegundos.

Sin embargo, se va consolidando la idea de un escenario híbrido altamente eficiente, en el que los ordenadores actuales pueden complementar el papel de los simuladores cuánticos. Preskill [7] hace mucho hincapié en no perder de vista el esfuerzo de I+D de puertas cuánticas con una menor tasa de error que, junto con el diseño de algoritmos cuánticos resilientes al ruido ambiente, nos permitan construir sistemas de mayor volumen cuántico. Por tanto, la motivación principal que debe marcar la investigación en la búsqueda de un ordenador cuántico debe ser obtener un sistema perfectamente aislado del mundo exterior, medible y gestionado [5].

	Superconductors	Ion traps	Photonics	Quantum dots	Cold atoms
% of potential users who consider technology "promising"	61%	35%	34%	26%	16%
Qubit quality[1] — *Qubit lifetime*	~1 ms	~50+ s	N/A	~1-10 s	~1 s
Gate fidelity	~99.6%	~99.9%	~99.9%	~99%	~99%
Gate operation time	~10-50 ns	~1-50 µs	~1 ns	~1-10 ns	~100 ns
Connectivity	Nearest neighbors	All-to-all	All-to-all[2]	Nearest neighbors	Near neighbors
Strengths	✓ Engineering maturity ✓ Scalability[3]	✓ Stability ✓ Gate fidelity ✓ Connectivity	✓ Horizontal scalability ✓ Established semiconductor tech	✓ Stability ✓ Established semiconductor tech	✓ Horizontal scalability ✓ Connectivity
Challenges	× Near absolute zero temperatures × Connectivity limitation in 2D	× Gate operation times × Horizontal scaling beyond one trap	× Noise from photon loss	× Requires cryogenics × Nascent engineering	× Gate fidelity × Gate operation time
Example players	IBM, Google	Honeywell, IonQ	PsiQuantum, Xanadu	Intel, SQC	ColdQuanta, Pasqal

Figura 1. Tabla resumen de las tecnologías usadas en los ordenadores cuánticos [2]

3.2. Distribución cuántica de claves

Si bien todavía no existe ningún estándar de cifrado propiamente cuántico, sí que existe un escenario de comunicaciones cuánticas basado en el transporte de fotones de luz. Empleando protocolos de distribución cuántica de claves, se puede establecer con seguridad una clave de cifrado compartida entre emisor y receptor en un canal no seguro. Se abre un campo enorme de investigación en el que se intenta reutilizar infraestructuras de comunicaciones de fibra óptica, o bien desplegar sistemas de comunicaciones ópticas en el espacio libre con línea de visión directa.

Los diferentes métodos desarrollados se han basado en transmitir fotones manipulados en función de la información codificada a transmitir. Esa manipulación ha consistido tradicionalmente bien en una polarización del fotón (en dos o cuatro bases no ortogonales, que entenderemos como orientaciones diferentes), o bien en el entrelazamiento de una pareja de fotones. Lo que se implica establecer una clasificación muy relevante, que se plasmará en los diferentes protocolos propuestos. En el caso del protocolo desarrollado en 1984 por Bennett y Brassard (BB84) [8], hace uso de fotones polarizados por el emisor y receptor, mientras que el protocolo desarrollado por Ekert en 1991 (E91) [9], hace uso de fotones entrelazados que se encuentran correlados de forma complementaria (anticorrelados, en los que al realizar una medida colapsa su estado y adquieren valores contrarios).

De forma similar a como se ha diferenciado tradicionalmente el mundo analógico del mundo digital, en la comunicación cuántica se puede distinguir el uso de valores continuos o valores discretos. Los primeros protocolos de QKD se basaron en la transmisión de señales discretas, normalmente en forma de pulsos de luz. Estos métodos son conocidos como DV-QKD, más sencillos de implementar y con un mayor alcance, acompañados de una mejor tolerancia a fallos. En el otro extremo están los métodos basados en el envío de señales continuas (CV-QKD), propuestos por Ralph en 1999 [10]. Transmiten con una polarización fija, son más complejos, pero tienen la gran ventaja de poder compartir el canal de comunicación con otras señales existentes, lo que evita disponer de canales de comunicaciones dedicados en exclusiva para su funcionamiento. Esto favorecerá su despliegue, así como su integración en redes de comunicaciones ópticas existentes multiplexadas, como una señal más.

3.3. Criptografía poscuántica (PQ)

El desarrollo e implementación de equipos que permitan ejecutar algoritmos, que puedan representar un riesgo para la mayoría de los sistemas de cifrado actuales, es cada vez más cercano. Podemos estimar un periodo incierto de 15 años hasta el momento más crítico en el que se rompan los sistemas de cifrado vulnerables. Debido a esto, se requiere iniciar urgentemente un periodo de investigación y desarrollo, que evite

la continua exposición de secretos cifrados con los algoritmos actuales. Apremia comenzar a migrar toda la infraestructura de los sistemas de cifra vigentes a nuevos estándares resistentes a dichos ataques. Estos futuros estándares son conocidos por el nombre de sistemas criptográficos poscuánticos (PQ).

En el caso de los sistemas de cifrado en bloque, que emplean claves de cifra simétrica como por ejemplo en el AES, gracias al algoritmo de Grover [11] es posible encontrar un resultado en una lista desordenada de N elementos (en este caso claves), reduciendo su complejidad (computacional) al caso en el que la lista tuviese la raíz cuadrada de N elementos. A efectos prácticos, la seguridad se reduciría de manera equivalente, al hecho de realizar un ataque clásico por fuerza bruta con una clave de la mitad de bits. Por lo que se recomienda seguir usando una longitud de clave de 256 bits, pero con la vista puesta en el avance de los ataques.

Por otro lado, la aplicación [12] del algoritmo de Simon [13] en ataques basados en la búsqueda de colisiones, posibilita acelerar su cómputo de manera exponencial. Esto permite romper diversos algoritmos de cifra simétricos empleados en autenticación y cifrado autenticado, tales como: CBC-MAC, PMAC, GMAC, GCM, y OCB, algoritmos que se pueden considerar completamente rotos.

En el caso de los sistemas de cifrado de clave pública, esta situación es considerablemente más preocupante según la aplicación del algoritmo de Shor [14], dando por neutralizada la complejidad computacional de la solución al problema de logaritmo discreto y de la factorización de números primos grandes. Ambos constituyen la base de los sistemas de cifra de clave pública, como es el caso de los sistemas de curvas elípticas (EC) y RSA.

La comunidad criptográfica lleva años estudiando la aplicación de sistemas alternativos de cifrado y firma digital, que no se basen en los problemas comentados y que eviten ser rotos por los futuros ordenadores cuánticos, al menos con el conocimiento matemático del que se dispone hoy en día. Se están estudiando algoritmos basados en:

- Retículos
- Teoría de códigos
- Isogenias
- Resúmenes
- Ecuaciones multivariables.

Ante la problemática existente, el Instituto Nacional de Estandarización y Tecnología americano (NIST), publicó un concurso en el año 2016 para buscar algoritmos alternativos a sus estándares de firma digital [15] y de establecimiento de claves [16] [17], que sean resistentes a futuros ataques producidos con ordenadores cuánticos. Se pretende que los esquemas ganadores puedan modificar los protocolos potencialmente afectados (IKE, TLS, DH, IPSec, DNSSEC, etc.), para completar una transición a los nuevos algoritmos en un plazo de 10 años.

3.4. Generadores cuánticos de números aleatorios (QRNG)

Los QRNG [18] son capaces de generar secuencias aleatorias con un alto nivel de entropía, aprovechándose de las propiedades de la física cuántica, que proporcionan unas condiciones de aleatoriedad perfectas para este fin. El mero hecho de medir el estado de un sistema cuántico provoca que colapse de forma única, aleatoria e impredecible, de acuerdo con el teorema de no clonación. A esto se añade el hecho de que el sistema, tras realizar la medición, continuará evolucionando de forma probabilística.

Idealmente se basarán en soluciones hardware, pero pueden verse reforzados por complementos software, p.ej. para aumentar la tasa de generación de la secuencia de salida hasta valores del orden de gigabytes/s. En caso contrario, dado que normalmente usarán dispositivos de medida como detectores de fotones, el resultado vendrá condicionado por la capacidad de medida del detector, limitando su rendimiento al orden de los megabytes/s.

3.5. Aprendizaje automático cuántico (QML)

Los algoritmos de aprendizaje automático tradicionalmente procesan grandes cantidades de información para tareas en las que se interpretan datos. Generalmente hay dos tipos de aproximaciones de algoritmos de ML al ámbito de QML [19]:

- Desarrollo de nuevas versiones de algoritmos (cuánticos) que puedan sustituir a antiguos algoritmos (clásicos) para solucionar un problema, p.ej. en los casos de búsqueda de los k-vecinos más cercanos (*k-nearest neighbour*), agrupación de datos (*data clustering*) o reconocimiento de patrones (*pattern recognition*), donde el pesado cálculo de distancias puede ser acelerado en un ordenador cuántico.
- Utilizar la descripción probabilística de la física cuántica para traducir aquellos procesos estocásticos, como la teoría de decisión bayesiana o los modelos ocultos de Markov, a los nuevos lenguajes de programación.

Adicionalmente, hay otros modelos de ML como el caso de las redes neuronales o los árboles de decisión, que todavía siguen esperando una versión cuántica eficiente. Se pueden considerar prometedores los algoritmos cuánticos que han demostrado ser muy eficientes, como HHL o QPCA, en su aplicación para métodos de reconocimiento de patrones.

Tradicionalmente se han empleado técnicas de ML para aplicaciones de detección de intrusiones en red, conocidas como NIDS (*network intrusión detection system*), dado que se puede plantear la detección de una anomalía como un problema de clasificación para detectar un comportamiento anómalo entre otros correctos. Se puede extender la aplicación de métodos QSVM (*quantum support vector machines*) para este propósito [20].

4. Conclusiones

A lo largo del presente trabajo se ha intentado transmitir al lector una idea lo suficientemente amplia sobre el mecanismo de las diferentes tecnologías cuánticas, su capacidad, y cuál será probablemente su hoja de ruta en función de los avances que vayan obteniendo sus investigadores.

En el caso de los ordenadores cuánticos, se ha destacado el concepto presentado por Preskill acerca de los ordenadores NISQ que, aunque siguen presentando problemas de ruido y no ofrecen una gran capacidad, ofrecen una funcionalidad suficiente para que otras disciplinas puedan seguir evolucionando. Existen diferentes arquitecturas de aproximación al ordenador cuántico, con diferente grado de evolución. Podemos destacar como muy prometedora la apuesta *topológica* liderada por Microsoft, pero siendo realistas, las referencias que más están destacando incluyen diseños basados en bucles de superconductores.

Para hacer realidad una de las grandes promesas cuánticas, como ejecutar el algoritmo de Shor, siguen existiendo trabas técnicas que imposibilitan en la actualidad implementar sistemas con suficientes cúbits tolerantes a errores. Sin embargo, son muy relevantes las advertencias que hace Michele Mosca [21] cuestionando si nuestros sistemas estarán preparados a tiempo para cuando llegue ese momento.

La distribución cuántica de claves, independiente del aumento de capacidad de computación, es una tecnología a tener muy en cuenta, y prueba de ello son las inversiones multimillonarias y los grandes avances que están consiguiendo los centros de investigación chinos. Sin ninguna duda, uno de los grandes retos de QKD va a ser su integración en escenarios SDN, conjugado con ofrecer un servicio de distribución de claves como servicio (KaaS). Para que esto se pueda llevar a cabo, se considera casi imprescindible el desarrollo de un sistema basado en valores continuos (CV-QKD), con el que se asegure una compatibilidad y una convivencia con los actuales medios de transmisión de fibra óptica.

En cuanto a los sistemas cuánticos de aprendizaje automático, tras revisar la literatura existente se puede considerar que, de todas las tecnologías cuánticas, esta es la que se encuentra en un estado más inmaduro, pero no implica que no se esté investigando ampliamente sobre la adaptación de sus múltiples variantes al ámbito cuántico. Hay que destacar el anuncio hecho por IBM [22] en el que declaraba haber obtenido una ventaja polinómica de cómputo en los métodos QSVM.

En definitiva, las conclusiones a las que hemos llegado y los retos planteados, vendrán muy influenciados por la inversión en I+D que se dedique en estos campos. Actualmente nos encontramos en un periodo dorado gracias a la promesa de alcanzar un hito rupturista que, con el aliciente de anuncios como los ya comentados de alcanzar la supremacía

cuántica, permiten ir definiendo en mayor medida casos de uso para la industria. Lo que afortunadamente nos devuelve a la casilla de salida, incentivando la inversión privada y, en algunos casos, hasta la inversión pública.

Referencias

[1] Gartner.com: The CIO's Guide to Quantum Computing [Internet]. [09 Ene 2022]. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-quantum-computing.

[2] Boston Consulting Group: ¿What Happens When 'If' Turns to 'When' in Quantum Computing? [Internet]. [09 Ene 2022]. https://www.bcg.com/publications/2021/building-quantum-advantage?linkId=124924149.

[3] Arute et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019; 574: 505-511.

[4] Yulin Wu et al. (2021), Strong Quantum Computational Advantage Using a Superconducting Quantum Processor Phys. Rev. Lett. 127, 180501.

[5] Preskill J. (2012), Quantum computing and the entanglement frontier. arXiv; 1203.5813.

[6] IBM.com: On «Quantum Supremacy». [Internet]. 2019. [10 Ene 2022]. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[7] Preskill J., (2018), Quantum Computing in the NISQ era and beyond. Quantum; 2: 79.

[8] Bennett CH., Brassard G., (2014), Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science; 560: 7–11.

[9] Ekert A. Quantum Cryptography Based on Bell's Theorem. Phsysical review letters. 1991; 67 (6): 661-663.

[10] Ralph TC. Continuous Variable Quantum Cryptography. arXiv quant-ph. 1999; 9907073.

[11] Grover L., (1996), A fast quantum mechanical algorithm for database search. Proceedings, STOC; 212-219.

[12] Kaplan et al., (2016), Breaking Symmetric Cryptosystems using Quantum Period Finding. arXiv; 1602.05973: 1-31.

[13] Simon D., (1997), On the power of quantum computation. SIAM journal on computing; 26(5): 1474–1483.

[14] Shor P., (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing; 26(5): 1484-1509.

[15] NIST. Digital Signature Standard (DSS). FIPS. 2013; 186-4: 1-130.

[16] Barker et al., (2018), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography Digital Signature Standard (DSS). NIST-SP; 800-56A: 1-139.

[17] Barker et al., (2019), Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. NIST-SP; 800-56B: 1-131.

[18] Jacak M., (2021), Quantum generators of random numbers. Nature Scientific Reports; 11(16108): 1-21.

[19] Schuld et al., (2014), An introduction to quantum machine learning. arXiv; 1409.3097: 1-19.

[20] Gouveia A., Correia M., (2020), Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection. IEEE 19th International Symposium on Network Computing and Applications (NCA); 1-8.

[21] Mosca M., (2018), Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy; 16 (5): 38-41.

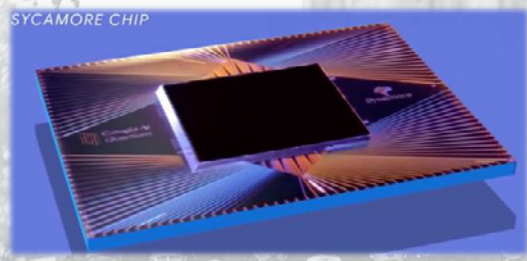
[22] Liu et al., (2020), A rigorous and robust quantum speed-up in supervised machine learning. arXiv; 2010.02174: 1-27.

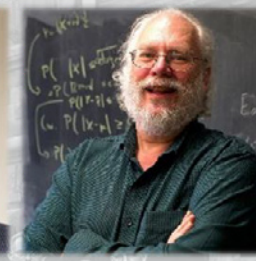
Mecánica cuántica aplicada a procesado y comunicaciones: implicaciones presentes y futuras

Autor: Ricardo Sánchez Jiménez

Directores: Milagros Fernández Gavilanes, Norberto Fernández García

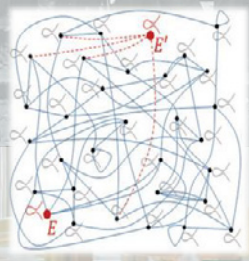
Universidad de Vigo

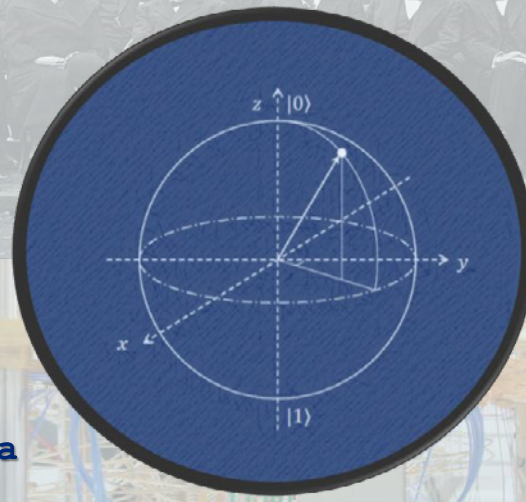


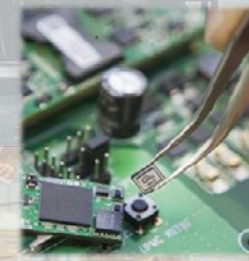


Ordenadores cuánticos

Grover & Shor

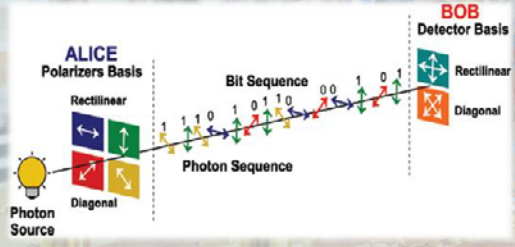


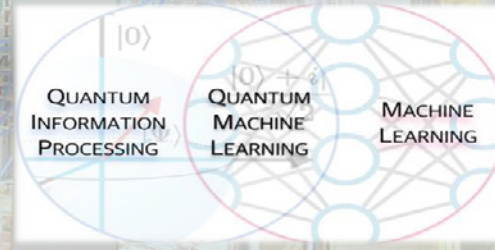




Criptografía post cuántica

QRNG





Distribución cuántica de claves

QML

Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Evolución de las telecomunicaciones satélite militares en las Fuerzas Armadas

Autor: Sierra García, Rafael (rafael.sierra@alumnos.uvigo.es; rsierrag2012@gmail.com)
Directores: Troncoso Pastoriza, Francisco (ftroncoso@cud.uvigo.es) y Núñez Ortuño, José María (jnunez@cud.uvigo.es)

Resumen – Por estar en su fase final de operación los dos satélites militares geoestacionarios, como proveedor de servicios de telecomunicaciones a las Fuerzas Armadas (FF.AA.) españolas, en este trabajo se estudiará desde un punto de vista teórico, la evolución de las telecomunicaciones satélite militares durante la vida útil de ambos satélites identificando los indicadores de evolución más determinantes que permitan sobre un nuevo escenario basado en los satélites de nueva generación de 2025, concluir acerca de las previsiones de empleo de la carga gubernamental tanto en el segmento espacial como en el segmento terreno.

Para realizar el estudio, tras un capítulo que explicará los fundamentos de las telecomunicaciones por satélite a nivel general, en el capítulo de desarrollo, con datos adaptados al trabajo basados en las tablas de registro de autorizaciones de acceso a satélite de los satélites actuales, plantearemos cuatro escenarios de telecomunicaciones y un futuro quinto escenario de telecomunicaciones con los próximos satélites de nueva generación. Posteriormente, los datos de empleo registrados en los escenarios actuales los trataremos y, según unas premisas, de información obtenida, extraeremos los indicadores más determinantes que, comparados entre sí, contribuirán a proyectar la evolución de empleo en el escenario futuro.

Finalmente, completaremos las conclusiones del estudio, añadiendo algunos otros aspectos identificados a lo largo del trabajo, relativos a las mayores funcionalidades de los satélites de nueva generación y al proceso de evolución de las redes a la Infraestructura Integral de Información para la Defensa (I3D).

Palabras clave – proveedor de servicios, indicadores de evolución, satélites de nueva generación, carga gubernamental, escenarios de telecomunicaciones, Infraestructura Integral de la Información para la Defensa (I3D).

1. Introducción

España en 1989 inició el camino para disponer de su propio sistema de telecomunicaciones por satélite militares al principio de la década de los 90, a través del programa del Sistema Español de Comunicaciones Militares Satélite (SECOMSAT) para garantizar la extensión de las comunicaciones nacionales a zonas de interés estratégico y operativo, adquiriendo elevada experiencia y desarrollo tecnológico a nivel empresarial y profesional.

Tras casi 30 años de experiencia en este campo, actualmente está en fase final de explotación la segunda generación de satélites con carga gubernamental:

- El satélite XTAR-EUR (29E), en órbita desde el 12 de febrero de 2005 y en operación desde marzo del mismo año.
- El satélite SPAINSAT (30W), en órbita desde el 11 de marzo de 2006, y en operación desde abril del mismo año.

Próximos a finalizar su vida útil, nos encontramos en un momento clave de diseño y desarrollo de los satélites militares SPAINSAT de nueva generación (NG) I y II que sustituirán a los actuales SPAINSAT y XTAR-EUR respectivamente (HISDESAT, s.f.).

Paralelamente, en base a la Política CIS/TIC del Ministerio de Defensa, las FF.AA. están inmersas en un proceso de evolución de las telecomunicaciones y los sistemas de información hacia una Infraestructura Integral de Información para la Defensa (I3D) que también afectará al escenario de telecomunicaciones por satélite (Ministerio de Defensa, 2015).

1.1. Objetivo

Como proveedor de servicios de telecomunicaciones satélite militares en carga gubernamental del Ministerio de Defensa, definir desde un punto de vista teórico el escenario de telecomunicaciones aplicable a los satélites de nueva generación, identificando los indicadores de evolución más determinantes derivados de escenarios anteriores que nos permitan concluir a cerca de las previsiones de empleo de la carga gubernamental tanto en el segmento espacial como en el segmento terreno.

1.2. Fundamentos

Las telecomunicaciones por satélite se remontan a 1960 utilizando la luna como repetidor de señal pasivo, y marcando el inicio del desarrollo de los primeros sistemas satélite, a nivel general y militar en particular, hasta nuestros días.

Es en la Conferencia mundial de 1963 cuando, por parte de la Unión Internacional de Telecomunicaciones (UIT), se reguló por primera vez este

nuevo campo de las comunicaciones (Escuela de Especialidades Antonio Escaño, Curso de especialización TCI PE-TCI.601-(B)).

Como denominador común, la arquitectura se basa en la existencia de los segmentos espacial y terreno para todo tipo de misiones, y de un tercer segmento de usuario para los sistemas satélite de radiodifusión y radionavegación.

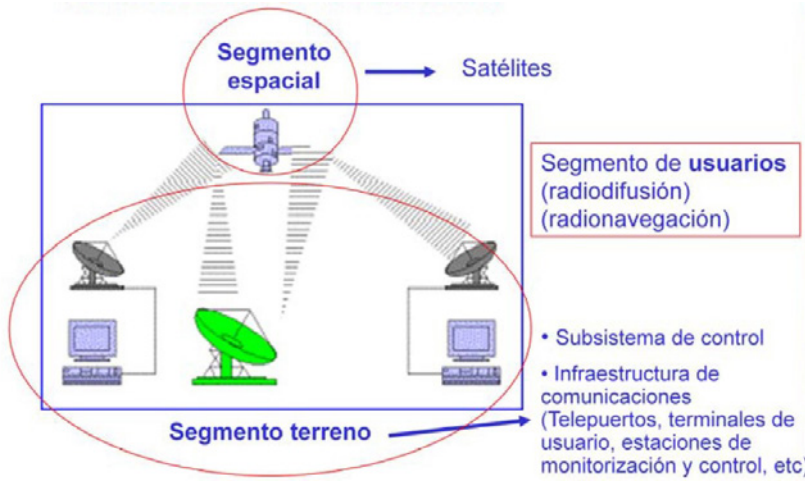


Figura 1. Segmentos de un sistema satélite (UPM, ETSI, Máster en Sistemas de Comunicación e Información para la Seguridad y la Defensa , 2013)

El segmento espacial, está constituido por el satélite o conjunto de satélites de la misión y por los Centros de Control del Satélite. Aunque forman parte del segmento espacial, los Centros de Control del Satélite están desplegados en tierra para las funciones de seguimiento, recepción de la telemetría y comando del satélite o satélites según la misión de la que se trate.

Forman parte del segmento terreno las estaciones de telecomunicaciones de los usuarios, las estaciones de anclaje o telepuertos y, cuando el servicio requiera gestión especializada del tráfico y de los accesos, los Centros de Control de Red.

Se trata de enlaces digitales a través de satélites en órbita geoestacionaria con transpondedores transparentes que retransmitirán en enlace descendente a tierra los enlaces enviados al satélite por las estaciones de comunicaciones transmisoras del segmento terreno (enlace ascendente).

Por ser enlaces de naturaleza digital, al hablar de las estaciones de comunicaciones, en el trabajo se exponen brevemente los procesos aplicados a la señal analógica y digital en las *cadenas* de transmisión y de recepción, encuadrándose en subsistemas de: alta frecuencia, frecuencia

intermedia, banda base, monitorización y control, y resto de subsistemas ligados a la infraestructura.

Para finalizar, además de unas nociones de propagación de los enlaces satélite, se enumeran y explican brevemente las técnicas de acceso múltiple aplicables. A destacar, los enlaces con preasignación de recursos de frecuencia portadora (SCPC), clásicamente empleada en los enlaces militares SECOMSAT, y las técnicas de acceso múltiple de asignación bajo demanda (DAMA).

2. Desarrollo

Aplicando las nociones que se indicaron en 1.2, en el trabajo, modificando algunos parámetros que pudieran ser sensibles, se describe el *potencial* de los segmentos espacial y terreno del sistema actual y futuro relativo a la capacidad o carga gubernamental asociada al Ministerio de Defensa para su gestión y operación por parte del Centro de Sistemas de Tecnologías de la Información y las Telecomunicaciones (CESTIC) como proveedor de comunicaciones a través de los satélites militares a los ámbitos.

Para ser *precisos*, por haber modificado algunos parámetros, a lo largo del trabajo los satélites SPAINSAT y XTAR-EUR pasan a denominarse *Atlántico* e *Índico* y, los futuros SPAINSAT NG I y II, *Atlántico NG* e *Índico NG* respectivamente.

En paralelo, para hacer un estudio predictivo del empleo de los futuros satélites militares, del periodo de explotación de los actuales, se extraen datos de hasta 22.691 entradas de autorizaciones con 14 campos cada una y se maneja información de hasta 842 entradas de tipos de terminales. Una vez tratados y depurados los datos, eliminando duplicidades y los no aplicables, los datos quedaron reducidos a 20.700 entradas de 14 campos relativas a autorizaciones satélite y 596 entradas relativas a terminales o también llamados estaciones de comunicaciones.

Posteriormente, teniendo en cuenta el potencial de cada segmento actual y futuro y con todos los datos de empleo disponibles, bajo las siguientes premisas, se procederá a identificar los escenarios de telecomunicaciones, y a sentar las bases de estudio/ análisis predictivo posterior.

Las premisas relativas a los satélites actuales son las siguientes:

- Se consideran los escenarios desde el año 2006 por ser el año a partir del cual el segmento espacial estaba constituido por los dos satélites Atlántico e Índico en operación.
- Se considera que ambos satélites estarán operativos hasta su sustitución por los satélites de nueva generación.
- Por ser SCPC el principal método de acceso múltiple empleado, para determinar los niveles de ocupación de cada canal de los satélites en ancho de banda, en cada escenario se aplicará la modulación y codificación más representativa en SCPC.

- El nivel de consumo de potencia en el canal se considerará proporcional y equilibrado con el consumo de ancho de banda.
- Se considerarán enlaces permanentes aquellos cuya ventana de enlace sea superior a medio año. Suelen ser enlaces de destacamentos de zona de operaciones o de infraestructura de red. El resto de enlaces tendrán consideración de temporales.
- Los accesos múltiples con asignación dinámica DAMA se tratan meramente como subredes definidas por un ancho de banda y potencia, sin profundizar en los detalles técnicos que les caracteriza.
- La información de base de cada uno de los escenarios, ha sido recopilada del registro de autorizaciones de acceso a satélite del CGS desde el 2006 al 2021, habiendo sido tratada para su uso didáctico sin alterar la información que es de interés para cumplir con el objetivo de este trabajo (Ministerio de Defensa, SEDEF CESTIC, 2016 a 2021) (Ministerio de Defensa, EMAD JESEMAD (CGS), 2006 a 2016).

Las premisas aplicadas al escenario de nueva generación:

- Se considera que se cumplen las previsiones de puesta en órbita y entrada en operación de los dos satélites en 2025.
- Definiremos coberturas similares a las proporcionadas por los satélites Atlántico e Índico, siendo conservadores a la hora de prever nuevos escenarios de despliegue en todas las bandas, designando como:
  - *Fija*, a la cobertura de los transpondedores asociados a los canales C1-C1 de los satélites actuales o a la cobertura regional de banda X y al spot de Ka orientado al centro de España en los satélites de nueva generación.
  - *Móvil 1*, a los transpondedores aplicados a los canales con cobertura móvil C2 en alguno de los enlaces ascendente o descendente de los satélites actuales, o similar en los satélites de nueva generación.
  - *Móvil 2*, a los transpondedores aplicados a los canales con cobertura móvil C3 en alguno de los enlaces ascendente o descendente de los satélites actuales, o similar en los satélites de nueva generación.
  - *Global*, cuando alguno de los enlaces ascendentes o descendentes es del global G1 de los satélites actuales o global en banda X, semiglobal en banda Ka y global en UHF en los satélites de nueva generación.
- Se considerará SCPC como el principal método de acceso múltiple empleado en las bandas X y Ka, y, si fuera necesario, para determinar los niveles de ocupación de cada canal de los satélites en ancho de banda, según corresponda, se aplicará la modulación y codificación más representativa del escenario 4 por ser el escenario actual y más próximo al escenario futuro.

- El nivel de consumo de potencia en el canal se considerará proporcional y equilibrado con el consumo de ancho de banda.
- Los accesos múltiples con asignación dinámica DAMA se seguirán tratando meramente como subredes definidas por un ancho de banda y potencia, sin profundizar en los detalles técnicos que les caracteriza.
- Para poder hacer previsiones en base a los datos de empleo, se plantea un modelo continuista en cuanto a las tecnologías de banda base existentes en las estaciones de anclaje y en las estaciones de comunicaciones.

2.1. Escenarios de telecomunicaciones

Los escenarios de telecomunicaciones que finalmente se identifican, en función del potencial de los segmentos satélite y terreno a lo largo de la vida útil de los dos satélites en operación son:

- Escenario de telecomunicaciones número 1. Desde el 1 de enero de 2006 al 31 de diciembre de 2006. Predominio del modo de acceso SCPC. También se dispone del modo de acceso DAMA CDMA (DAMA FAS). Los terminales se integran con banda base TDM de 1990. Solo se emplea la banda X polar.
- Escenario de telecomunicaciones número 2. Desde el 1 de enero de 2007 al 31 de diciembre de 2009. Predominio del modo de acceso SCPC. Continúa el modo de acceso DAMA CDMA (DAMA FAS), y se incorpora la UME con el sistema DAMA FDMA (VIPERSAT). Los terminales se integran con banda base TDM de 1990 y TDM Fleximux. Solo se emplea banda X.
- Escenario de telecomunicaciones número 3. Desde el 1 de enero de 2010 al 23 de abril de 2021. Predominio del modo de acceso SCPC. Sigue DAMA CDMA (DAMA FAS) y DAMA FDMA (VIPERSAT) y se suma DAMA TDMA (iDirect). Se extiende y afianza el empleo de terminales con tecnología IP. Se emplea la banda X y la banda Ka.
- Escenario de telecomunicaciones número 4. Desde el 24 de abril de 2021 hasta el fin de la vida útil. Segmento espacial basado en la totalidad de la carga útil de los dos satélites. Predominio de modo de acceso SCPC y con accesos DAMA CDMA (DAMA FAS) y DAMA FDMA (VIPERSAT) y DAMA TDMA (iDirect). Se empiezan a probar los pilotos de I3D apoyándose en la tecnología IP de los terminales y de las estaciones de anclaje. Se emplea la banda X y la banda Ka.

Sobre cada escenario, en el trabajo quedan reflejados todos los detalles de las capacidades por segmento espacial y terreno, la tecnología de los subsistemas y las medias de empleo diarias según diversos conceptos como: el número de enlaces, las velocidades binarias de enlace, la tecnología de banda base empleada, los tipos de acceso DAMA o SCPC, el carácter

temporal o permanente de los enlaces, los enlaces contra estaciones de anclaje o intrateatro, las bandas de frecuencia de acceso en X o Ka, el desglose de terminales y datos anteriores por ámbito que establece el enlace, desgloses por coberturas.

El escenario de telecomunicaciones número 5, se define desde el momento en que se alcance la capacidad de operación completa de los dos satélites NG. Para ello, previamente, las estaciones de anclaje habrán evolucionado al menos los recursos mínimos necesarios de todos sus subsistemas para permitir, cada una, el anclaje de las estaciones de comunicaciones en las tres bandas: X (en polar y contrapolar), Ka y UHF a través de los dos satélites de nueva generación.

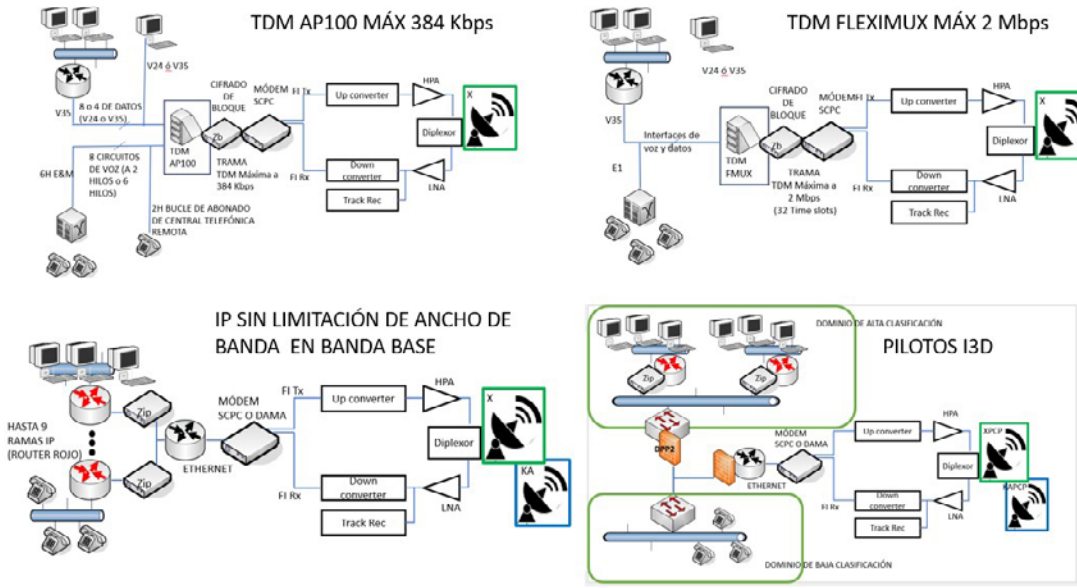


Figura 2. Arquitectura de las estaciones de comunicaciones según la tecnología de banda base (elaboración propia)

3. Resultados

Para hacer el análisis predictivo de empleo en el escenario de telecomunicaciones número 5, aplicando una función de tendencia lineal donde sea preciso. En el capítulo 4 se presenta la información en tablas y gráficos, según los siguientes apartados:

- Número de autorizaciones de acceso satélite anuales registradas hasta septiembre de 2021.
- Evolución del espectro disponible en carga gubernamental para cada banda X, Ka y UHF.
- Volumen de enlaces medios diarios en carga gubernamental.

- Velocidad binaria media diaria de los enlaces SCPC en carga gubernamental.
- Porcentajes medios diarios de ocupación del espectro.
- Número de enlaces SCPC medios diarios según terminal destino.
- Número de enlaces SCPC medios diarios contra estaciones de anclaje según tecnología de banda base.
- Empleo medio diario de la tecnología de banda base SCPC por ámbitos.
- Recursos medios diarios asociados a subredes DAMA en estaciones de anclaje según su tecnología de acceso.
- Evolución de las estaciones de comunicaciones según su banda de frecuencias.
- Evolución de las estaciones de comunicaciones según su modo de acceso al satélite.

Para analizar la tendencia creciente/ decreciente y las estimaciones de capacidad, del análisis que se realiza se extraen hasta 88 indicadores de evolución en una matriz de resultados que apoyará a las conclusiones y líneas futuras del trabajo.

4. Conclusiones

Aplicando el modelo continuista sobre las capacidades en banda X y Ka, mientras predominen los enlaces SCPC como el principal método de acceso a los satélites NG, se registrarán valores anuales de autorizaciones de enlace similares a los ya registrados desde el año 2013 en el escenario 3 (entre 1.500 y 1.600). Este modo de acceso podría cambiar su tendencia conforme se incremente el empleo de subredes DAMA del tipo FDMA (VIPERSAT) en la UME o DAMA TDMA (iDirect) en el resto de ámbitos.

En las coberturas regionales/ fijas, la ocupación de ancho de banda seguirá siendo superior a la ocupación del resto de las coberturas móviles o global de los satélites.

Las velocidades binarias medias diarias de los enlaces SCPC muestran una clara tendencia creciente en las bandas X y Ka (600 Kbps en banda X, 2,7 Mbps en banda Ka). Potenciará su crecimiento en ambas bandas el disponer de: dos satélites con capacidades gubernamentales similares desde el principio, el incremento de las coberturas definibles, y el mayor espectro de la banda X en polar y contrapolar multiplicando por 4 la capacidad de los tres primeros escenarios, y por 34 la de la banda Ka.

Hay una tendencia creciente a la ocupación de los recursos satélite de forma permanente (de más de medio año de duración) frente a enlaces satélite con asignación de recursos de forma temporal.

Desaparecerá la tecnología TDM sobre multiplexores AP1OO, y el ritmo de evolución de los terminales hacia la arquitectura I3D, determinará el ritmo de reducción de los enlaces TDM sobre Fleximux.

La banda UHF, igual que en su momento lo fue la banda Ka en los satélites actuales, es novedosa. Se empleará para establecer mallas radio semidúplex a bajas velocidades con cobertura global. Deberá determinarse qué arquitectura basada de enlaces SCPC o DAMA deberá aplicarse en función de las necesidades operativas de las unidades.

Paralelamente, para llegar al escenario de telecomunicaciones futuro número 5, el segmento terreno deberá evolucionar: las estaciones de anclaje para disponer de capacidades a través de los dos satélites NG: en banda UHF, Ka y X contrapolar, y el Sistema de Control y Supervisión de Red (COSRED) del Centro de Control de Red bajo la dirección del CESTIC, para automatizar los procesos que le permitan aplicar a través del Centro de Control del Sistema las nuevas funcionalidades ofrecidas por los satélites NG relativas a:

- Aplicar la mayor flexibilidad en la configuración de coberturas y en la asignación de potencia a las bandas X y Ka.
- Aplicar la mayor flexibilidad de asignación y distribución del espectro de frecuencias incluyendo la reutilización de frecuencias en diferentes coberturas (SDMA) en las bandas X y Ka.
- Autorizar y aplicar el establecimiento de enlaces entre estaciones de comunicaciones distribuidas en coberturas no convencionales mediante *beam-hopping* en banda X.
- Solicitar la geolocalización de interferencias en tierra en la banda X.
- Aplicar la inhibición de frecuencias interferentes en banda X y Ka.
- Aplicar la generación de nulos *nulling* en banda X.
- Autorizar y aplicar la difusión de información mediante *multicast* para retransmitir la señal de enlace ascendente de un canal por varios canales de enlace descendentes simultáneamente en las bandas X y Ka.
- Solicitar el servicio de obtención de datos de monitorización del espectro de los enlaces ascendentes y descendentes de cualquiera de las tres bandas.
- Autorizar y habilitar la aplicación de *cross-banding* entre enlaces ascendentes y descendentes de las bandas X y Ka.

Agradecimientos

A mis directores del trabajo de fin de máster por su disponibilidad y asesoramiento.

A mi unidad ACETEL de la DIVOPER del CESTIC con su coronel, mis comandantes, capitanes, subtenientes e ingeniero de ISDEFE. Su apoyo incondicional ha sido fundamental.

A mi familia, mi motivación constante.

Referencias

[1] Escuela de Especialidades Antonio Escaño, Curso de especialización TCI PE-TCI.601-(B). (s.f.). Comunicaciones por Satélite. Escuela de Especialidades Antonio Escaño.

[2] HISDESAT. (s.f.). PROGRAMA SPAINSAT NG. Obtenido de https://www.hisdesat.es/wp-content/uploads/2021/11/SPAINSAT-NG_ES.pdf

[3] Ministerio de Defensa. (2015). Política CIS/TIC del Ministerio de Defensa.

[4] Ministerio de Defensa, EMAD JESEMAD (CGS). (2006 a 2016). Registro de Autorizaciones de Acceso a Satélite.

[5] Ministerio de Defensa, EMAD, JESEMAD (CGS). (2005). Presentación SECOMSAT.

[6] Ministerio de Defensa, SEDEF CESTIC. (2016 a 2021). Registro de Autorizaciones de Acceso a Satélite.

[7] UPM, E. D. (2008). Programa de postgrado en comunicaciones por satélite 2008 (10.ª edición), segmento terreno (tomo 2).

[8] UPM, ETSI, Máster en Sistemas de Comunicación e Información para la Seguridad y la Defensa. (2013). Comunicaciones, localización y radionavegación por satélite.

[9] UPM, EUIT de telecomunicación. (2008). Programa de postgrado en comunicaciones por satélite 2008 (10.ª edición), El enlace satélite (tomo 3).

[10] UPM, EUIT de telecomunicación. (2008). Programa de posgrado en comunicaciones por satélite 2008 (10.ª edición), segmento espacio (tomo 1).

Evolución de la telecomunicaciones satélite militares en las Fuerzas armadas

Autor: Rafael, Sierra, García
Director/es: Francisco, Troncoso, Pastoriza y José María, Núñez, Ortuño
Universidad de Vigo

Introducción

Visión como proveedor de servicios de telecomunicaciones satélite militares en carga gubernamental (CESTIC)

2005 XTAR-EUR (29E) (OPERATIVO)
Banda X
2006 SPAINSAT (30W) (OPERATIVO)
Banda X y Ka

Red de Telecomunicaciones Defensa

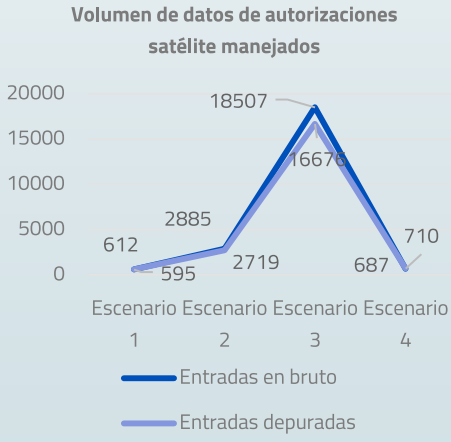
2025 SPAINSAT NG I y II (29E y 30W)
Banda UHF, X y Ka

Infraestructura Integral de Información para la Defensa (I3D)

Metodología

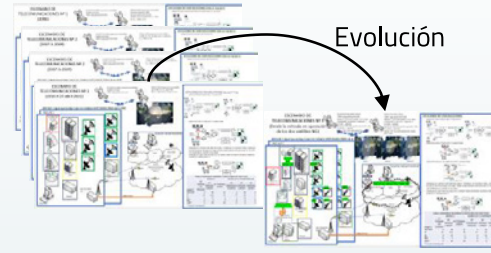
Análisis predictivo sobre datos de autorizaciones satélite en cuatro escenarios telecomunicaciones a lo largo de la vida útil de los dos satélites.

Previsiones: Aplicación de tendencia lineal inter-escenarios en los gráficos de información media diaria de empleo más determinantes.



Resultados

Dada la flexibilidad de los satélites de nueva generación se aplican premisas en la identificación de los cuatro escenarios de telecomunicaciones sobre los satélites actuales y en la definición de quinto escenario futuro sobre los satélites NG.



Conclusiones

Se mantiene en X y Ka el volumen anual de enlaces SCPC. Cambio de tendencia conforme se incremente el empleo de las subredes de acceso bajo demanda.
Novedosa la banda UHF.
Tendencias crecientes de medias de empleo diario destacables en:

- Velocidades binarias de los enlaces, potenciado además por disponer de dos satélites con carga gubernamental, más flexibilidad y coberturas en bandas X y Ka multiplicando por 4 la capacidad de los tres primeros escenarios, y por 34 la de la banda Ka.
- Ocupación de los recursos satélite de forma permanente y de las cobertura fija o regional.

Desaparecerá TDM sobre AP100 (tecnología de los 90) y TDM Fleximux según proceso de cambio a I3D.
Evolucionar: Estaciones de Anclaje al escenario 5 y el COSRED del CESTIC para automatizar el empleo de nuevas funcionalidades NG.

Agradecimientos

A mis directores del TFM por su disponibilidad y asesoramiento.
A mi unidad ACETEL de la DIVOPER del CESTIC, su apoyo incondicional ha sido fundamental.
A mi familia, mi motivación constante.

La gestión del talento y la motivación en entornos de Administración Pública: análisis técnico y propuestas estratégicas de actuación

Autora: Silvent Aparicio, Cristina (cristina.silvent@gmail.com)
Director: Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – La motivación es el motor que nos impulsa a acometer acciones para obtener resultados y se puede aplicar, de forma transversal, a todos los aspectos de nuestra vida. Se han realizado muchos estudios relacionados con la motivación y multitud de psicólogos han escrito teorías y análisis sobre ella.

En el ámbito laboral la motivación es un aspecto imprescindible: sin su existencia no se obtendrían resultados, objetivo final de cualquier actividad empresarial. Por ello, mantener la motivación de los empleados de una organización es indispensable, y para esto es clave que las empresas tengan una gestión del talento como factor estratégico organizacional.

En el caso particular de la Administración Pública, una de las motivaciones para convertirse en empleado público es la de tener un trabajo de por vida del que no te pueden despedir. Pero, una vez conseguido, ¿cómo se mantiene esa motivación inicial? Teniendo en cuenta las limitaciones que tiene —por ejemplo, a nivel presupuestario—, ¿qué herramientas puede implementar la Administración para conseguir mantener a sus funcionarios motivados y que los servicios que ofrecen sean excelentes y óptimos? ¿Cree la Administración necesaria implementar planes de retención del talento?

Estas son algunas de las preguntas que se intentarán responder en este TFM y, para poner en relieve todos estos conceptos, se ha analizado el caso de los militares que han decidido abandonar las Fuerzas Armadas para trabajar en Amazon, donde se justifica que el motivo principal que les ha llevado a tomar esta decisión ha sido la falta de motivación.

Palabras clave – motivación, Administración Pública, gestión del talento, retención del talento, Amazon.

1. Introducción

Históricamente, la imagen que se ha tenido de la Administración Pública no siempre ha sido la mejor. Las cosas han cambiado mucho desde el artículo de Mariano José de Larra, titulado *Vuelva usted mañana*, nada menos que datado en el año 1833, en el que describió de forma particular la escasa diligencia de los empleados de la Administración Pública. Desde entonces, la Administración ha evolucionado y ha implementado planes de mejora y modernización que todavía están en curso. Sin embargo, tiene muchas tareas pendientes, como la mejora de la gestión del talento.

Así pues, este estudio se centra especialmente en la motivación de los trabajadores públicos y, sobre todo, en cómo podría la Administración mejorar esa motivación y retener su talento.

Todo esto teniendo en mente a las nuevas generaciones, que al fin y al cabo formarán parte de los funcionarios del futuro, cuyos perfiles son muy diferentes a los de los trabajadores que han copado el mercado laboral hasta ahora: el concepto de estabilidad no les interesa, han nacido inmersos en una sociedad ya transformada digitalmente que cambia de forma muy rápida —concepto contrario al relacionado tradicionalmente con la Administración— y donde reina la concepción del ya y el ahora.

Así pues, ¿cómo podrán los nuevos funcionarios mantener la motivación en sus puestos? ¿Cómo podrá la Administración retener el talento de aquellos profesionales que están empezando a optar por abandonar sus puestos estables y prestar sus servicios en la empresa privada? Este TFM pretende agrupar estas y otras preguntas y plantear posibles respuestas y estrategias de actuación.

2. Cambios contextuales

Para realizar un análisis correcto de la gestión del talento y la motivación en la Administración Pública es necesario previamente señalar los cambios contextuales que se han ido sucediendo en nuestra sociedad. La gestión de recursos humanos ha quedado atrás para dar paso a la gestión del talento, pero esto se ha debido a que la sociedad ha cambiado y entre otras, con la llegada de la tecnología, la forma de trabajar, que ha dado un giro de 360º en muchos sectores. La Administración Pública entre ellos.

Precisamente la tecnología es la que ha impulsado dichos grandes cambios que están viviendo las generaciones. Las nuevas generaciones no conciben un mundo sin tecnología, han nacido rodeadas de teléfonos móviles y sistemas inteligentes y esto ha motivado un cambio en su forma de pensar, vivir y por supuesto, de trabajar. Las futuras generaciones están muy formadas y la oferta laboral que tienen por delante es tan amplia que no dudarán en saltar de trabajo en trabajo hasta encontrar el que más les motive, les ofrezca proyectos más interesantes o presente un plan estratégico que encaje con su forma de pensar.

Estas nuevas generaciones son las que tendrán que cubrir los puestos, en los próximos años, que los miles de funcionarios en edad de jubilación

van a dejar. Pero, ¿es la Administración Pública suficientemente atractiva para ellos? La respuesta ahora mismo es claramente que no.

Por lo que es posible que, de la misma forma que está ocurriendo en los Ejércitos y la Armada con los militares que se van a trabajar a la empresa privada, como se verá más adelante cuando se habla del caso de Amazon, después de un tiempo sin grandes cambios en sus puestos, sin un plan de carrera y sin posibilidad de ser escuchados para cambiar o mejorar las cosas, decidan abandonar la estabilidad soñada de sus padres que les ofrece la Administración por puestos en el ámbito empresarial que sí respondan a sus necesidades.

Frente a este panorama la Administración Pública no tendrá otra opción que la de evolucionar y crecer a imagen y semejanza a como lo hace el mundo que le rodea. Si no es capaz de hacerlo, se encontrará sin talento necesario para afrontar el entorno turbulento actual mediante decisiones de adaptación y con empleados poco motivados.

3. La gestión del talento como factor estratégico organizacional

La visión tradicional de la gestión de personas se ha centrado en lo que se ha denominado Gestión de Recursos Humanos, sin embargo, en esta visión tradicional no se ha tenido en cuenta el talento. Así pues, es imprescindible considerar la gestión del talento como factor estratégico organizacional en un entorno turbulento como el que vivimos. Los factores que han propiciado la aparición de dicho entorno, también denominado entorno VUCA (traducción al inglés de volatilidad, incertidumbre, complejidad y ambigüedad), son la globalización, la política mundial, la revolución tecnológica, la innovación, los nuevos tipos de organización, etc. y esto no solamente afecta a las empresas privadas, sino que también lo hace a la Administración Pública.

La visión que han de poseer los empresarios, directivos y mandos es la de participar en lo que se puede denominar guerra por la captación del talento. Y no únicamente se trata de captarlo, sino de identificarlo previamente, atraerlo, desarrollarlo y, por último, retenerlo para que permanezca en la organización, tal y como se muestra en la figura 1 a continuación:

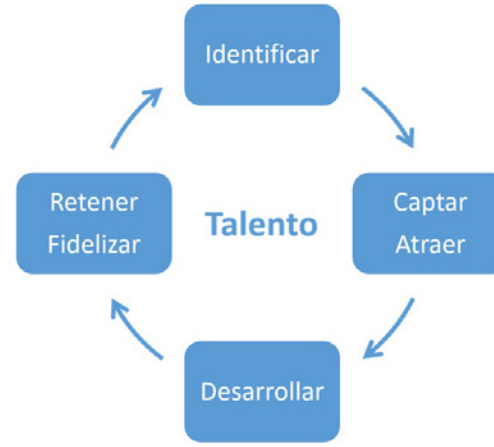


Figura 1. El proceso continuo de la gestión del talento [elaboración propia a partir de los apuntes de COM1 – asignatura impartida en el máster DIRETIC]

El campo de batalla para la guerra por el talento es complejo, pero en la medida en la que cada organización sepa identificarlo, buscarlo en otros lugares y construya compromiso con sus empleados tendrá una clara ventaja competitiva respecto al resto [1].

4. Propuestas estratégicas de actuación

Se enumeran a continuación algunas de las propuestas estratégicas planteadas en el TFM, unas más asequibles y realizables que otras, que podrían mejorar la situación de los funcionarios y por ende su motivación, que podría conllevar a una mejora del servicio prestado y a una optimización de los recursos:

• **Creación de planes de captación de talento**. La Administración Pública debe empezar a diseñar la futura fuerza de trabajo, establecer los procesos precisos para incorporar los perfiles y el talento que van ser necesarios en los próximos años. Es imprescindible dejar a un lado políticas de recursos humanos cortoplacistas o de simple reposición de los efectivos para compensar las crecientes jubilaciones. La estructura del sector público que se necesita para afrontar los retos del futuro no es la misma que la que se diseñó en los años 90 [2].

Las pruebas de acceso a la función pública, así como las de promoción interna, basadas fundamentalmente en evaluar la capacidad para memorizar una serie de contenidos, deberían adaptarse para incorporar los nuevos perfiles necesarios. Las entrevistas tradicionales y los típicos test psicotécnicos que, por supuesto, pueden ser necesarios para ciertos puestos, no deberían utilizarse como herramientas únicas de selección puesto que no permiten valorar lo más intangible del talento: las cualidades, las competencias y la capacidad de compromiso [1].

Por otra parte, la Administración Pública tiene la necesidad de abordar estrategias de *Employer Branding*: crear un buen lugar para trabajar y posteriormente promocionarlo para atraer a aquellos profesionales con el talento, conocimiento y habilidades que la organización necesita para alcanzar sus planes estratégicos y objetivos.

• **Creación de una relación directa entre las retribuciones y el esfuerzo percibido para alcanzarlas, así como tener sistemas retributivos orientados a los resultados, no a la categoría ni al puesto.** Se propone implantar un método para establecer un sistema de retribuciones ligado al desempeño. Aunque cada nivel de la Administración posea una retribución específica de base, se deberían tener en consideración otros aspectos como la experiencia previa, el número de personal al cargo de funcionario, el grado de responsabilidad (al mando de servicios críticos o no), los horarios (existencia de guardias o turnicidad), etc. En este sentido, se podrían asignar complementos específicos para cada uno de estos factores u otros que se consideraran.

• **Mantener una correspondencia entre las expectativas individuales y las aspiraciones de la Administración.** Aunque un funcionario está destinado a servir las necesidades de la Administración, esto se puede realizar de muchas maneras. Y evidentemente será mejor hacerlo motivando al empleado público, aspecto que pasa por conocer en todo momento cuáles son sus expectativas. Para esto, la Administración tendría que dar cabida a los ascensos por especialización, al movimiento de personas en función de sus intereses y a la formación continua. Es evidente que no siempre se podrán satisfacer las aspiraciones puntuales de todos los funcionarios, pero lo que no es normal es que nunca se consiga hacerlo.

• **Establecer políticas de evaluación del rendimiento individual como forma de integrar las aspiraciones de individuo y organización que sean claras y objetivas.** Según el artículo 20 —la evaluación del desempeño— de la Ley del Estatuto Básico del empleado Público [3], «los sistemas de evaluación del desempeño se adecuarán, en todo caso, a criterios de transparencia, objetividad, imparcialidad y no discriminación y se aplicarán sin menoscabo de los derechos de los empleados públicos».

Aquello que no se mide difícilmente se gestiona y si el talento se está convirtiendo en el activo más estratégico de las compañías, es lógico que sea necesario medirlo —si es necesario utilizando herramientas de software para la evaluación del desempeño—, y para ello es esencial establecer objetivos o metas que resulten alcanzables, cuantificables y realistas, que no sean a muy largo plazo sino asumibles y que puedan lograrse en un tiempo razonable. Lo contrario puede desmotivar muy fácilmente [4].

Por otra parte, dichas evaluaciones tienen que ser transparentes y objetivas y mantenerse en todo momento a disposición del funcionario, además de ir acompañadas de entrevistas personales en las que se comuniquen correctamente las decisiones tomadas para evaluar. Esto permitirá que el funcionario entienda en todo momento su proceso y pueda tomar acciones para mejorar si fuera necesario, o para saber que está trabajando de la forma que se espera.

• **Desarrollar un plan de carrera orientado en función de la valía y de los intereses de los funcionarios.** La planificación de carreras implica para el empleado público la posibilidad de ocupar puestos mejores, ir adquiriendo mayores habilidades y responsabilidades y progresar, retributivamente hablando. Probablemente, esta sea una de las herramientas más importantes que tiene la Administración para motivar a su fuerza de trabajo y para proveerse de talento altamente especializado y competente [5].

Si se desarrollara un plan de carrera claro, se le daría al funcionario la capacidad de escoger hacia dónde quiere dirigir su carrera profesional, su futuro. Si dispone de ciertas libertades para marcar su camino laboral, sus niveles de motivación crecerán. Si por otro lado se le impone cierta carrera que se aleja de sus intereses, su motivación caerá en picado. Así pues, hay

que tener en cuenta el potencial motivador de un plan de carrera correcto frente a la desmotivación que generaría uno mal desarrollado.

Según Byars y Rue [6], el plan de carrera debe contener etapas sucesivas de acción, de manera sostenida y permanente. Ellos establecen cuatro etapas en el desarrollo de un plan de carrera:

1. Valoración por el individuo de sus capacidades, intereses y objetivos de carrera.
2. Valoración de la organización de las capacidades y potencialidades del individuo.
3. Comunicación de las opciones y oportunidades de carrera existentes dentro de la organización.
4. Orientación sobre la carrera con el fin de establecer objetivos y planes realistas para su logro.

• **Implantar el teletrabajo.** Se deben desarrollar las medidas y herramientas necesarias para implantar de forma paulatina, y allí donde las circunstancias lo permitan, sistemas de teletrabajo. En septiembre de 2020, y motivado por la pandemia que indujo a quedarse en casa a la población mundial, se actualizó el artículo 47 bis —teletrabajo— de la Ley del Estatuto Básico del empleado Público [3]. Así pues, la Administración Pública ya está teniendo en cuenta está nueva situación que, aunque pareciera en un primer momento temporal, ha venido para quedarse.

• **Ofrecer salario emocional**. Como se ha visto en puntos anteriores, las motivaciones por el trabajo son, inicialmente, las de satisfacer las necesidades más básicas, sin embargo, el salario emocional tiene una gran cabida e impacto en la motivación de los trabajadores. A las nuevas generaciones les importan aspectos que hasta ahora no eran relevantes para las empresas, como por ejemplo el medioambiente o la responsabilidad social corporativa, que se pueden incorporar al *Employer Branding* de la Administración.

• **Ofrecer formación continua.** La formación es un instrumento de motivación ya que, a medida que aumenta la competencia del personal, también aumenta directamente su sensación de autoestima y de satisfacción personal. La formación cobra su sentido en el momento que sirve para actualizar las capacidades, actitudes, conocimientos y técnicas de un profesional de la Administración. Esta actividad debe estar planificada y alineada con las metas de la Administración Pública [5].

• **Impartir formaciones de liderazgo para mandos que gestionan personas.** Actualmente existen muchos programas de liderazgo destinadas a mejorar las capacidades en gestión de personas y el desarrollo del talento. En ocasiones, especialmente para los puestos de nivel A1 de la Administración, un funcionario se encuentra gestionando equipos —más o menos numerosos— sin disponer de la experiencia ni el

conocimiento para hacerlo. Y la gestión de personas no es algo trivial, sino que se trata de una ciencia complicada que, aunque pueda resultar innata en algunas personas, también es una competencia que se puede aprender.

• **Estudiar la viabilidad de realizar intercambios temporales con la empresa privada para tener una retroalimentación en cuanto formas de trabajar.** Debido a su naturaleza, la Administración Pública siempre irá un paso atrás si se compara con las empresas grandes y punteras, a todos los niveles: uso de tecnología, optimización de procesos, gestión del talento en todas sus vertientes, etc. Es por ello que una estrategia que se podría llevar a cabo para que la Administración obtenga de primera mano información sobre cómo mejorar y aprender de las acciones que plantean las empresas privadas es la de establecer relaciones con organizaciones nacionales de renombre de las que poder asimilar este conocimiento directamente.

5. El caso Amazon

Aunque no es la primera vez que un miembro de las Fuerzas Armadas las abandona para trasladar su carrera al mundo civil, en los últimos años alrededor de 50 oficiales han sido contratados por Amazon, y lo mismo ha sucedido en el ámbito de los suboficiales. Aunque otras organizaciones como Frontex e ICRC - Comité Internacional de la Cruz Roja también constituyen destino de personal de las FAS, es el gigante de la logística el que más militares ha contratado en el último año.

Uno de los factores condicionantes que inducen a esta organización empresarial como destino lo constituye el programa de captación de talento dedicado a militares llamado Militar Hiring que ofrece Amazon. Esta es una iniciativa que otras empresas privadas no han realizado y que viene precedida por una situación habitual en Estados Unidos, que es la de contratar personal de las Fuerzas Armadas.

Amazon les pide como objetivo principal que desarrollen, apliquen y consigan implantar y desarrollar la cultura de liderazgo que han aprendido en los Ejércitos y la Armada, y que en las plantillas de operaciones de Amazon no existe por diferentes motivos.

La investigación concluye que lo que llevó a estos oficiales a dar el paso de saltar a la vida civil no fue principalmente ni el sueldo, ni la conciliación, ni la falta de interés profesional —aunque por supuesto, estos factores ayudaron a tomar la decisión de realizar el cambio— si no la falta de criterio en el desarrollo de sus trayectorias profesionales, la arbitrariedad y una política de gestión del talento inexistente que trata al oficial como un número y no como una persona con sus fortalezas y debilidades, con experiencia, formación y circunstancias personales particulares.

6. Conclusiones

Hasta ahora, la Administración Pública no ha desarrollado una gestión estratégica de gestión del talento: no ha implementado planes de captación, retención y desarrollo porque no lo ha necesitado. Durante mucho tiempo esto ha generado un descenso de la motivación de los funcionarios que ha influido directamente en su productividad, generando malas opiniones en la sociedad en general del trabajo de los funcionarios en algunos sectores de la función pública.

Pero a la Administración no le preocupaba, puesto que los servicios se seguían ofreciendo y, aunque no fuera de la mejor manera, seguía funcionando. Sin embargo, en la actual era del talentismo, para hacer frente al entorno turbulento en el que vivimos, la gestión del talento se ha convertido en un factor estratégico para las organizaciones y ahora la Administración Pública también debe tenerlo en cuenta.

Una de las mayores motivaciones para ser funcionario era tener un trabajo estable y de por vida. Sin embargo, las generaciones han cambiado, el mundo ha evolucionado y el mencionado entorno turbulento caracterizado por la volatilidad, la incertidumbre, la complejidad y la ambigüedad, han cambiado las reglas del juego. El talento que tienen los jóvenes profesionales no se retiene ofreciéndoles estabilidad. Hay que ir más allá, y, por ello, se ha de focalizar la atención en establecer planes estratégicos de gestión del talento donde propiciar un entorno laboral motivador sea uno de los principales objetivos.

Para ello deberá ofrecerles planes de carrera adecuados, claros y que se cumplan; facilitando la formación de personal experto, por un lado, que pueda ascender de forma horizontal, y de personal que ascienda verticalmente por otro.

La flexibilidad será otro de los puntos que deberá adoptar, incluyendo la capacidad de actuar rápidamente frente a la necesidad de cambios de personal y de generación de vacantes.

Hay que dejar de mirar al pasado, donde un puesto como funcionario era algo envidiable por la estabilidad que conllevaba, y empezar a analizar las generaciones futuras, cuyo interés, como ha puesto de manifiesto el desarrollo del presente trabajo, ha dejado de ser la estabilidad y se posicionan en el lado contrario: valoran la asignación a proyectos de interés, la movilidad periódica, la conciliación personal, la formación y desarrollo continuos y sobre todo la rapidez en obtener resultados. Y, por encima de todo, que se les escuche y que se materialicen sus ideas.

La Administración ha empezado a ver la necesidad del cambio y tiene varios proyectos en marcha, pero debería realizar más estudios sobre su evolución, tal y como se hizo en el 2012 por la Comisión para la Reforma de las Administraciones Públicas [7]. En este contexto, debiera

de abordar, de modo decisivo, actuaciones encaminadas a la gestión del talento, profundizando y estudiando qué cambios, alineados con la gestión estratégica del talento se pueden realizar.

Por último, debería preocuparle que su personal abandone sus puestos para dirigirse a la empresa privada, ya que es un indicio de que existen ámbitos susceptibles de mejorarse; aunque, por otra parte, podría resultar interesante el retorno de este personal para que implementen todos sus nuevos conocimientos y se sientan lo suficientemente motivados como para quedarse.

Referencias

[1] Jericó P., (2008), La nueva gestión del talento. Construyendo compromiso. Madrid: Pearson Educación S.A.

[2] Pastor Bermúdez A. y Nogales Fuentes P., (2019), El futuro del trabajo en la Administración Pública. ¿Estamos preparados? IVAP Estudiosx. N.º 3: 34-51.

[3] Boletín Oficial del Estado; Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. [Internet] 2015 [Consultado en enero de 2022]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2015-11719.

[4] Padilla Ruiz P., (2013), La gestión del reconocimiento en la Administración Pública. Revista de trabajo y seguridad social, n.º 364.

[5] Ortega Pérez C. A., (2018), La motivación en el trabajo de la administración. Madrid: Formación Alcalá.

[6] Byars L. L. y Rue L. W., (1997), Gestión de Recursos Humanos. McGraw-Hill Interamericana de España S.L.

[7] Gobierno de España - Presidencia del Gobierno; Transparencia y CORA. [Internet]. [Consultado en diciembre de 2021]. Disponible en: https://www.lamoncloa.gob.es/espana/historico/eh15/transparenciaycora/Paginas/index.aspx

La gestión del talento y la motivación en entornos de Administración Pública: análisis técnico y propuestas estratégicas de actuación

Universidad de Vigo

Autora: Cristina Silvent Aparicio - Director: Francisco Javier Rodríguez Rodríguez

Propuestas estratégicas para mejorar la motivación y gestionar el talento

- Crear planes de captación y retención del talento
- Desarrollar Planes de Carrera
- Establecer políticas de evaluación del rendimiento individual claras y objetivas
- Ofrecer formación continua
- Realizar intercambios temporales con la empresa privada
- Implantar el teletrabajo
- Mantener equilibrio entre expectativas individuales vs aspiraciones de la Administración
- Ofrecer salario emocional
- Impartir formaciones de liderazgo

Fases de la gestión del talento

Identificar → Atraer → Desarrollar → Retener

Estudio de redes definidas por software y su implantación en redes privadas

Autor: Tafalla Pemán, Alfonso (alfonsotafalla@yahoo.es)
Directores: Fernández García, Norberto (norberto@cud.uvigo.es)
y Suárez Lorenzo, Fernando (fsuarezl@gmail.com)

Resumen – SDN son las siglas de redes definidas por software. La definición más sencilla y directa de esta arquitectura es la separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red. Con ello, se favorece la implementación de servicios de red de forma ágil, dinámica y escalable, estando la lógica de control en un dispositivo común denominado controlador.

El paradigma SDN mejora la seguridad de la red, ya que se proporciona una total visibilidad de la misma, realizando análisis continuos y dando respuesta de una forma proactiva, propagando políticas de seguridad desde el controlador de forma ágil y dinámica, a todos los dispositivos de la red.

SDN y en concreto la SD-WAN (redes de área amplia definidas por software), está evolucionando a otra solución denominada SASE (acceso seguro de servicios de borde) en el que incluye la propia SD-WAN, pero se añaden servicios en la nube en relación a control de accesos, funciones de seguridad y cortafuegos.

En este trabajo se estudian las redes definidas por software y su implementación en redes privadas, con diferentes soluciones propietarias de diversos fabricantes posicionados en el cuadrante mágico de Gartner, como líderes en infraestructuras frontera en redes de área amplia. A modo de práctica se realiza una simulación de la solución Cisco ACI, con su controlador Cisco APIC, observando la facilidad y sencillez en la implementación, monitoreo y gestión de una arquitectura *spine-leaf* en centros de datos.

Palabras clave – SDN, Openflow, NFV, Overlay y Underlay.

1. Introducción

1.1. Introducción a las redes definidas por software

SDN son las siglas de Software Defined Networking o redes definidas por software, la definición más sencilla y directa de esta arquitectura nos la da la Open Networking Foundation (ONF) [1], organización impulsada por los usuarios cuyo fin es promover la estandarización y comercialización de SDN a través del desarrollo de estándares abiertos. Esta organización define SDN como:

> «La separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red» [1]

Básicamente esto significa que vamos a reducir la carga del plano de control en los equipos de red y se le otorgará a un elemento de la red (plataforma de gestión) que, de manera centralizada, no solamente gestionaría un equipo, sino que lo hará con un conjunto completo de varios equipos de forma dinámica y efectiva. Es por ello que una red definida por software es una arquitectura ideal para los entornos de red en los que en el día a día se debe responder de manera oportuna a la creciente demanda de servicios por parte de sus clientes.

Entre las características más destacables, al integrar una red con SDN le proporcionamos la capacidad de ser directamente programable. Ahora podemos aprovechar las fortalezas del software para hacer que nuestra red sea fácil de gestionar, configurar y operar. Otra de sus características es que, dado su dinamismo, es una arquitectura ágil donde podemos programar software o aplicaciones que realicen distintas tareas de acuerdo con ciertos parámetros o comportamientos de la red.

SDN utiliza controladores centralizados para la gestión de los dispositivos de la red, haciéndola bastante flexible y escalable y permitiendo configurar, gestionar y optimizar los recursos de red de manera dinámica. El controlador centralizado se encargará de tomar las decisiones y gestionar el comportamiento de los equipos de red, siendo su arquitectura compuesta de tres capas, tal y como se ve en la figura 1-1.

Lo primero que se puede lograr con este paradigma es tener un control centralizado y más efectivo de la red, pudiendo mejorar significativamente la gestión y la detección de eventos no deseados en la red, lo que luego permitirá tomar las mejores decisiones y tener un mayor rendimiento. Se pueden desplegar conmutadores/enrutadores virtualizados en cortos periodos de tiempo y, por último, se puede automatizar el comportamiento de la red mediante la creación de políticas.

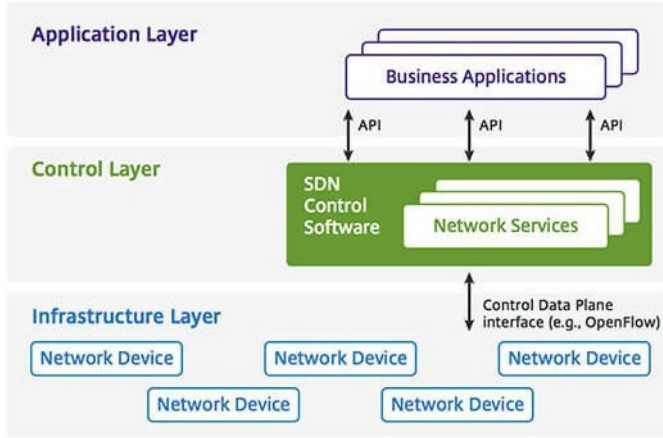


Figura 1-1. Arquitectura SDN (fuente [1])

2. Desarrollo

2.1. Soluciones comerciales SDN

Una vez introducido el paradigma SDN, se van a exponer diversas soluciones SDN actuales, basándose en el cuadrante mágico de Gartner, en relación a las infraestructuras de borde en redes WAN, íntimamente ligadas a la tecnología SD-WAN. En la figura 2-1 se observa dicho cuadrante [2].

Figura 2-1. Cuadrante de Gartner WAN Edge Infrastructure (septiembre 2021) (fuente [2])

Las mejores soluciones SDN del mercado (zona de líderes en el cuadrante), en este caso más concretamente SD-WAN, las aportan las siguientes empresas:

- Fortinet
- VMware
- Versa Networks
- Palo Alto Networks
- Cisco
- HPE (Aruba y Silver Peak)

2.2. Fortinet

La solución SD-WAN de Fortinet está implementada en el hardware de los equipos que comercializan, en el sistema operativo de los cortafuegos de nueva generación denominados Fortigate, permitiendo simplificar las operaciones de red y seleccionar los mejores caminos hacia un destino, con la capacidad de tener múltiples conexiones a distintas sucursales de una organización y seleccionar automáticamente cuál es la mejor alternativa para conectarnos de extremo a extremo, visualizando qué aplicaciones están corriendo por la red y dando prioridad a las más críticas.

Todos los equipos Fortigate tienen unos circuitos integrados con tecnología patentada por Fortinet (ASIC) que realizan el procesamiento de tráfico y el procesamiento de seguridad independientemente al procesamiento principal, es decir, los equipos tienen una CPU como cualquier equipo informático, pero además tienen un procesador dedicado para el tráfico de red y un procesador dedicado para el tráfico de seguridad, siendo esto una innovación de Fortinet, consiguiendo con ello alcanzar muy altas velocidades de procesamiento.

2.3. VMware

La solución de la empresa VMware de SD-WAN se denomina VMware SD-WAN de Velocloud, su lanzamiento se produjo en 2019 conectando más de 200 oficinas remotas de MD Anderson, una extensión de la Universidad de Texas, localizada en Houston, dedicada al campo de la medicina. VMware SD-WAN introdujo la automatización y la visibilidad en las oficinas remotas, lo que permitió una implementación rápida y eficiente. Con el aprovisionamiento de cero toques (ZTP), los trabajadores de oficinas remotas pueden instalar VMware SD-WAN Edge ellos mismos. El dispositivo se conecta automáticamente a la herramienta de administración central basada en la nube, denominada Orquestador VMware SD-WAN. Esto conecta inmediatamente al trabajador a la red corporativa y los administradores de red pueden ver los bordes individuales de VMware SD-WAN activados, pudiendo solucionar problemas desde la sede central.

2.4. Versa Networks

La solución de SD-WAN forma parte de la solución SASE de Versa Networks. Característica de la solución es la superposición (overlay) cifrada o no cifrada vía MPLS, GRE (Generic Routing Encapsulation), VXLAN, etc.

La tecnología de Secure SD-WAN de Versa Networks se diferencia de otros fabricantes o proveedores de SD-WAN porque implementa capacidades que permiten una arquitectura de SASE, incluyendo visibilidad del tráfico que recorre la red entre los usuarios, las aplicaciones y los dispositivos independientemente de su ubicación.

2.5. Palo Alto Networks

Palo Alto Networks tiene varias soluciones SD-WAN entre las cuales las más extendidas son CloudGenix SD-WAN y Prisma Access.

CloudGenix SD-WAN es una solución en la nube que opera a nivel de sesión y flujo de aplicaciones, a diferencia de los conmutadores y enrutadores de las SD-WAN tradicionales, que lo hacían en capa 2 y 3.

Prisma Access es otra solución, que consigue una mayor seguridad y protección donde sea necesario, tanto en sedes, como para cualquier trabajador de la organización en movilidad, ya que se trata de una evolución de SD-WAN a un servicio de acceso seguro de borde (SASE), que proporciona seguridad a todos sus usuarios y aplicaciones.

2.6. Cisco

Cisco tiene la solución SD-WAN de empresa, anteriormente denominada Viptela. En ella están implementados todos los componentes principales de la solución Cisco SD-WAN consistiendo en el sistema de administración de red vManage (plano de administración), el controlador vSmart (plano de control), el orquestador vBond (plano de orquestación) y el enrutador WAN Edge (plano de datos).

Todos los componentes se basan en software salvo el enrutador WAN Edge que está disponible como dispositivo de hardware o enrutador basado en software y se ubica en un sitio físico o en la nube, proporcionado conectividad segura en el plano de datos entre los sitios a través de uno o más transportes WAN.

2.7. HPE (Aruba y Silver Peak)

La arquitectura de SD-WAN de Silver Peak se denomina Aruba EdgeConnect SD-WAN, donde hay un orquestador centralizado que controla, monitoriza y gestiona los equipos EdgeConnect, que son dispositivos de infraestructura de borde, los cuales se pueden implementar

en tres modalidades (físicos, virtuales o en la nube), dependiendo de los requerimientos de la organización o empresa.

El orquestador se puede ejecutar de forma local *on premise*, en la nube o como un servicio, todo dependerá de las necesidades de la empresa. De manera opcional, se puede implementar un dispositivo denominado Boost WAN Optimization, para acelerar los procesos y optimizarlos. Si un usuario ejecuta una aplicación, la misma se almacena en la memoria caché del EdgeConnect, de tal forma que cuando otro usuario quiera disponer de ella, lo haga con menos latencia.

3. Prueba y validación

3.1. Arquitectura *spine-leaf*

Durante años, los centros de datos se han construido en una arquitectura de tres niveles (capa de núcleo, capa de agregación/distribución y capa de acceso). Pero con los centros de datos integrados, la virtualización y el surgimiento de sistemas hiperconvergentes, una nueva arquitectura de red, *spine-leaf* [3], se ha convertido en la implementación actual de la red de los centros de datos, superando algunas limitaciones de la arquitectura tradicional de tres niveles. Con esta arquitectura se consigue una latencia mejorada, los cuellos de botella reducidos y el ancho de banda ampliado.

La arquitectura de red *spine-leaf* se está imponiendo hoy en día en grandes centros de datos o redes en la nube debido a su escalabilidad, fiabilidad y un mejor rendimiento. El diseño de *spine-leaf* solo tiene dos capas, la capa *spine* y la capa *leaf*. La capa *spine* está formada por conmutadores para el proceso de enrutamiento, siendo la columna vertebral de la red. Por otro lado, la capa *leaf* consta de conmutadores a los que se conectan dispositivos finales, de almacenamiento, servidores, etc. Cada conmutador *leaf* está conectado con todos los conmutadores *spine* (entre ellos no conectados), por lo tanto, para que un dispositivo final se comunique con otro dispositivo conectado en otro conmutador *leaf*, solo habrá una ruta posible a través del conmutador *spine* que conecta dos conmutadores *leaf*.

El simulador Cisco ACI proporciona un software del controlador Cisco APIC con funciones completas, junto con una infraestructura de estructura simulada de conmutadores *spine* y *leaf* en un servidor físico. Se puede usar para comprender las funciones, ejercitar las API e iniciar la integración con sistemas y aplicaciones de orquestación de terceros.

El simulador de Cisco ACI incluye conmutadores simulados, por lo que no puede validar una ruta de datos. Además, el simulador Cisco APIC permite la simulación de fallos y alertas para facilitar las pruebas y demostrar funciones.

3.2. Instalación del simulador Cisco ACI

Para el desarrollo de la práctica es preciso la instalación del simulador Cisco ACI. Para ello es necesario descargar el archivo de extensión ova de su máquina virtual, de la página web de Cisco [4]. Una vez dentro de la web de descarga, se elige la versión del simulador ACI más actualizada. Dicha versión se compone de seis archivos, que posteriormente se unirán para recomponer el archivo ova de la máquina virtual del simulador.

Para ejecutar el archivo ova de la máquina virtual del simulador hay que disponer del software hipervisor de VMware Workstation, ya que la citada máquina virtual no es compatible con el hipervisor VirtualBox. Dependiendo de la versión de sistema operativo Windows 10 (Pro o Enterprise) que se tenga instalado, será necesaria una versión de VMware Workstation compatible.

3.3. Práctica del simulador de Cisco ACI

Una vez que se ha cargado la web del simulador Cisco ACI, con el usuario/contraseña que definimos en la instalación del mismo, lo abrimos, implementamos los dispositivos *spine-leaf* y configuramos los parámetros básicos que nos solicita para su funcionamiento (figura 3-1):

- Fabric Membership. Se configuran y registran los dispositivos que el propio simulador detecta que están conectados a la red (por diseño e instalación del simulador solo se dispondrá de un conmutador *spine* y dos conmutadores *leaf*).
- BGP. Configuración de los conmutadores *spine* que van actuar con el protocolo BGP, para comunicar entre sí a los conmutadores *leaf* que consideremos oportuno para el buen funcionamiento de la solución (por diseño e instalación del simulador solo se dispondrá de un conmutador *spine*).
- NTP. Configuración de servidores NTP (Network Time Protocol) para el uso del controlador Cisco APIC (solo uno en esta implementación) y los conmutadores *spine-leaf*.
- DNS. Configuración de servidores DNS para el uso del controlador Cisco APIC y los conmutadores *spine-leaf*.
- Proxy. Configuración de servidores proxy para el uso del controlador Cisco APIC.
- Out of Band Management. Configuración de la interfaz de gestión para nodos vía IP que se conecten a la red de gestión OOB (*Out of Band*).
- Global Configurations. Configuraciones generales recomendadas.

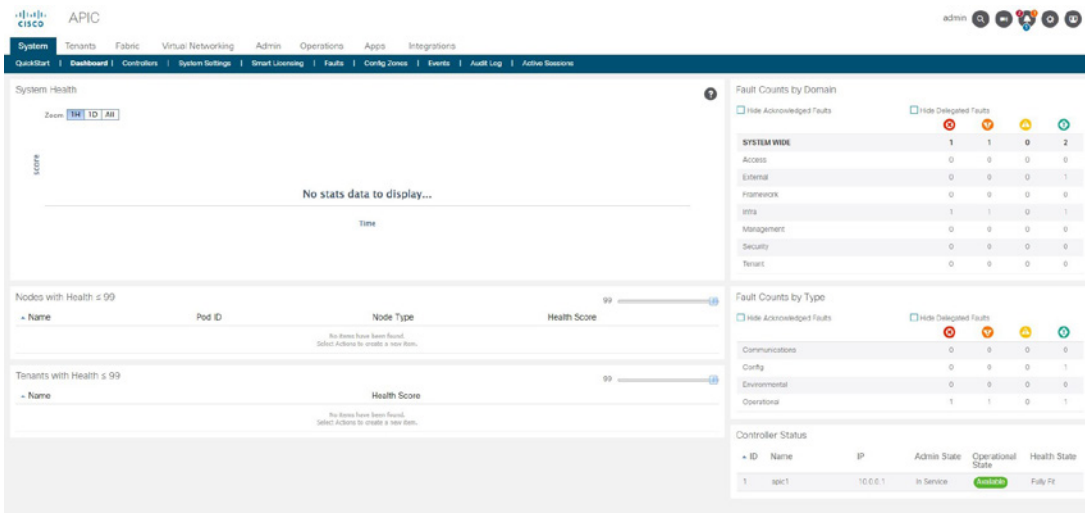


Figura 3-1. Simulador APIC (fuente propia)

Una vez en funcionamiento la solución Cisco ACI se pueden recorrer los innumerables menús de la misma, configurando y personalizando nuestros requerimientos. Se pueden hacer diversas configuraciones, mostrar la topología, crear nuevos tenant o grupos de usuarios con sus perfiles (por defecto el simulador crea tres), configurar las actualizaciones de *firmware* (con un solo clic de ratón), visualizar todos los puertos de los conmutadores o la configuración de roles de acceso y su autenticación entre otros.

4. Conclusiones

Como hemos visto en el trabajo, SDN son las siglas de Software Defined Networking o redes definidas por software. La característica principal de este paradigma es la separación física del plano de control del plano de datos o reenvío y donde el plano de control gestiona distintos dispositivos de red.

Este paradigma favorece la implementación de servicios de red de forma ágil, dinámica y escalable, estando la lógica de control en un dispositivo común a toda la red denominado controlador, desde el cual se gestionan todos los componentes de la red de forma centralizada, descargando de este trabajo al propio hardware de los dispositivos.

Con la característica del control centralizado y de programabilidad de la red en SDN, se puede implementar de forma más sencilla y dinámica la seguridad de los dispositivos de red, pero, por otro lado, el controlador se convierte en un potencial objetivo debido a su papel fundamental en una red definida por software.

Se han mostrado en el desarrollo de este trabajo multitud de soluciones y tipos de SDN, de fabricantes que en estos momentos lideran este

campo, según lo indicado en el cuadrante mágico de Gartner, con las cuales cualquier organización puede actualizar sus redes para el cumplimiento de los requisitos que sean necesarios en la misma.

En beneficio de la seguridad, SDN está evolucionando a otro paradigma denominado SASE (Acceso Seguro de Servicios de Borde) en el que incluye SD-WAN, pero complementándolo con servicios en la nube en relación a control de accesos, funciones de seguridad y cortafuegos.

Como conclusión final, resulta beneficiosa la implementación del paradigma SDN, además de para mejorar la seguridad, para hacer más dinámicos otros procesos de red, ya que tiene muchas ventajas sobre las redes tradicionales y en la mayoría de las soluciones se puede realizar la transición al nuevo modelo de forma progresiva, coexistiendo las dos, de forma conjunta.

Referencias

[1] Web de Open Networking Foundation (ONF), [en línea]. Disponible: https://opennetworking.org/ [Último acceso enero 2022].

[2] Web de Bafing, [en línea] Disponible: https://www.bafing.com/infraestructura-wan-edge-de-fortinet-lider-en-gartner-2021/ [Último acceso enero 2022].

[3] Web de FS community [en línea] Disponible: https://community.fs.com/es/blog/leaf-spine-with-fs-com-switches.html [Último acceso enero 2022].

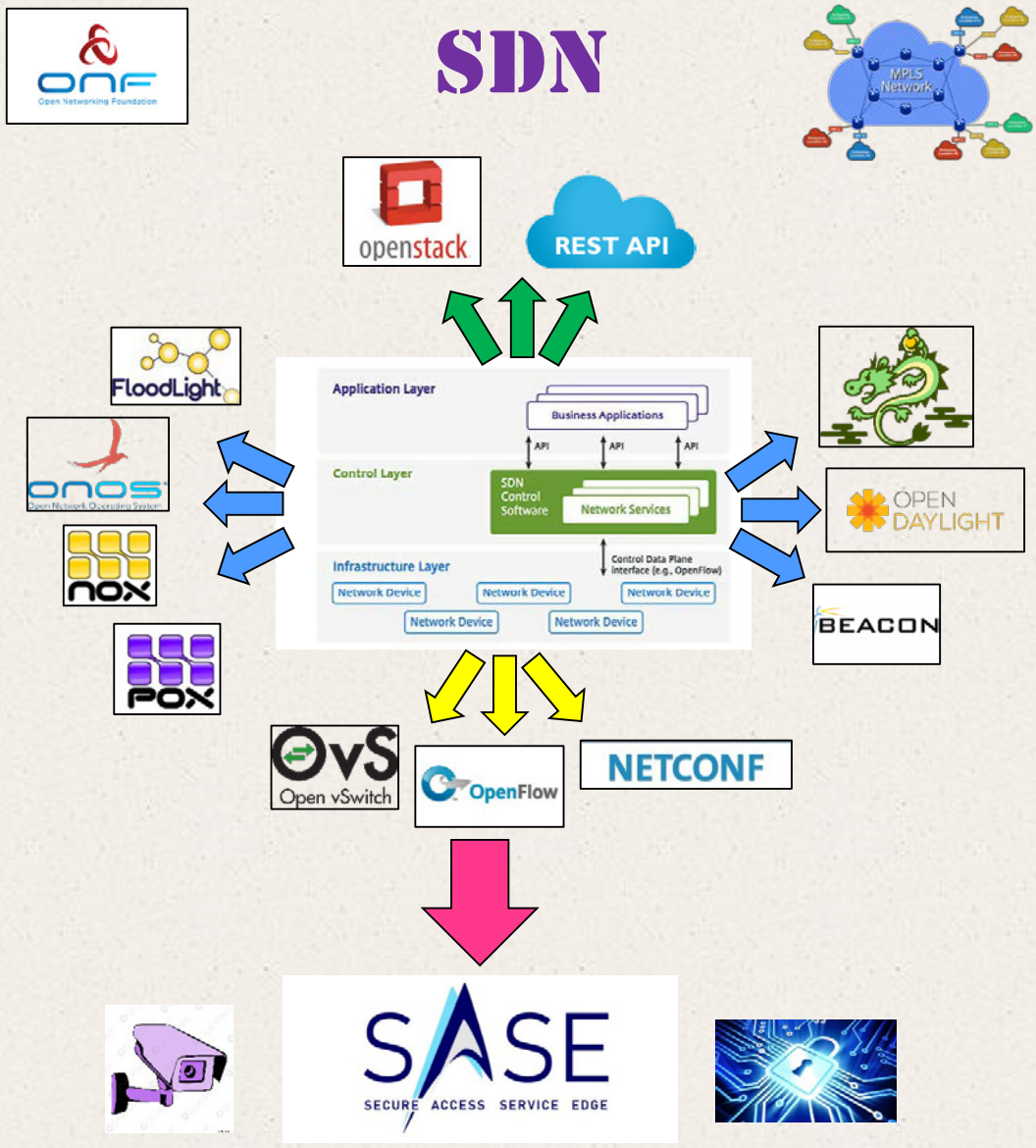
[4] Web de Cisco sobre simulador Cisco ACI, [en línea] Disponible: https://www.cisco.com /c/en/us/products/cloud-systems-management/application-centric-infrastructure-simulator [Último acceso enero 2022].

Estudio de redes definidas por software y su implantación en redes privadas

Universidad de Vigo

Autor: Alfonso Tafalla Pemán

Director/es: Norberto Fernández García / Fernando Suarez Lorenzo



Máster Universitario en Dirección TIC para la Defensa (Máster DIRETIC), 2021/2022

Gestión de talento en organismos CIS/Ciber del MINISDEF

Autor: Tormos Fernández, Vicente (vtorfer@et.mde.es)
Director: Rodríguez Rodríguez, Francisco Javier (fjavierrodriguez@cud.uvigo.es)

Resumen – Hoy en día consideramos activos de una organización a sus bienes inmuebles, construcciones, infraestructuras, máquinas, vehículos, equipos tecnológicos o sistemas informáticos, pero también otros menos tangibles o tal vez menos clásicos como la información que la empresa posee o gestiona, su imagen,... y el recurso humano, las personas que trabajan en y para ella.

Desde hace unos años parece haberse asentado y asumido en el ámbito laboral en general, y en el sector empresarial en particular, la importancia trascendente del recurso humano en el correcto y eficaz funcionamiento de la organización. Por tanto, si tan alto es el valor que aporta, entonces requiere de una dedicación especial, principalmente porque históricamente ha sido un hermano menor, secundario, en las preocupaciones y por tanto en las atenciones de las instituciones.

Actualmente y con el auge de las nuevas tecnologías y la dependencia que de ellas tiene el MINISDEF se hace más necesario que nunca una adecuada y moderna gestión de los recursos humanos, como base imprescindible de la estructura de la organización y por ende como gestores de los sistemas que utilizan esas nuevas TI (tecnologías de la información).

Esta vertiginosa evolución tecnológica implica en el ámbito del personal una especialización de los perfiles para los distintos puestos de los organismos, que se hace mucho más acuciante en las UCOS (unidades, centros, organismos) de carácter técnico y que poseen relación con la gestión de los CIS (sistemas de telecomunicación e información) del MINISDEF.

A la queja endémica de falta de personal, y sobre todo con el perfil adecuado en particular, por parte de un elevado porcentaje de las empresas y otras organizaciones de nuestra sociedad se ha de responder con una acertada actuación estratégica relativa a la gestión de recursos humanos, en los diversos aspectos que contempla: búsqueda, captación, identificación, formación, incentivación, retención. Y, si es necesario, cambiar el tradicional paradigma de gestión de personal o recursos humanos por el más moderno de gestión de talento.

Parece ser una realidad ineludible que el satisfactorio cumplimiento de las misiones que la sociedad encomienda a nuestras Fuerzas Armadas y que pasa por alcanzar su máxima operatividad, posee una gran dependencia de sus sistemas de información y telecomunicaciones. La correcta gestión de nuestro ámbito ciberespacial tiene además un impacto directo sobre las operaciones en los otros ámbitos, terrestre, marítimo, aeroespacial y cognitivo.

El personal adecuado en cantidad y calidad es la base de la estructura. La situación actual y la tendencia, reflejan que el factor cantidad puede estar limitado por aspectos presupuestarios, de plantillas, de priorización para otras necesidades. Hagamos el esfuerzo de estudiar e implementar el factor calidad de este valiosísimo activo de la organización a través de una acertada *gestión del talento*, orientada a los puestos, funciones y las capacidades profesionales.

Palabras clave – recursos humanos, gestión de talento, búsqueda y detección, captación, formación y desarrollo, fidelizar, perfil y función, trabajo en equipo.

1. Introducción

Por mi experiencia en distintos puestos de la estructura del MINISDEF, y más concretamente en algunos de carácter técnico y en otros relacionados con la gestión de personal, he podido observar en primera persona las carencias y deficiencias históricas y endémicas en esta gestión. En ocasiones esta mala praxis no es achacable a las propias unidades, ni por supuesto a los responsables de la gestión de personal de las unidades, sino que es consecuencia de una política general del departamento en materia de gestión de personal, de la escasez presupuestaria o de la ausencia o mal diseño de lo que definiremos como Plan Estratégico de Gestión de los Recursos Humanos.

He comprobado con frustración lo que cuesta formar a un especialista, un analista de un área técnica, reflejados en ejemplos relevantes como: investigador forense de incidentes o eventos en redes y sistemas CIS, administrador de una de estas infraestructuras, analista de imágenes, o de señales electromagnéticas, etc. Además, para la consolidación en un puesto de estas características se requieren periodos largos (de dos a cuatro años).

En este sentido, con desesperación veía y sigo viendo que cuando hemos conseguido formar mínimamente a un técnico en una de estas áreas, no podemos retenerle, porque no somos capaces de ofrecerle incentivos suficientes que compitan con las oportunidades que se le brindan en otros ámbitos (puestos en el extranjero, sector privado, unidades con mayor proyección profesional...).

También soy testigo de la dificultad de cubrir adecuadamente muchos de estos puestos. La actual cantera de personal, que son los propios componentes de las FAS y del Ministerio de Defensa, no está resultando suficiente para satisfacer, en número y calidad, la demanda de este tipo de perfiles.

La relevancia del importante activo que para nuestra organización representa el personal (y cualquier otra), se ilustra con lo que nuestro jefe del Estado Mayor de la Defensa (JEMAD), comandante de la estructura operativa de las Fuerzas Armadas, ya exponía en 2017 en su concepto de ciberdefensa destacando algunas ideas clave que se repiten tanto en el mundo empresarial como en el militar: «*El factor humano constituye la clave del éxito*. No solo el personal técnico y operativo involucrado en las actividades descritas en este documento, sino con carácter general, el conjunto del personal del MDEF como usuarios de los servicios proporcionados por redes y sistemas. En este sentido, la concienciación, la formación y el adiestramiento, el alistamiento de los efectivos necesarios, el reclutamiento, así como la experiencia del personal, su nivel de conocimiento y su motivación son aspectos determinantes»

> «El personal formado en este ámbito es *un recurso escaso*», «*Identificación temprana del talento y su captación*», «Reclutamiento y *retención del personal técnico:* un aspecto cada vez más importante, puesto que en los próximos años existirá una competencia cada vez mayor con el mundo civil. Siendo conscientes de que el MDEF no podrá competir con los salarios que se ofrecen en otros ámbitos, se deben ofrecer a cambio otros incentivos que incrementen el atractivo de servir en el MDEF, y que mantenga alta la motivación del personal: un modelo de carrera definido y atractivo, una formación actual y de calidad, medios tecnológicamente avanzados, cometidos interesantes, adiestramiento realista, retos constantes, etc. «La definición e implantación de un perfil de carrera» «integración de personal civil» «La cíberreserva estratégica,...».

Parecen las mismas ideas, conceptos y tendencias que se imponen en la organización privada, y se plasman en las publicaciones y bibliografía de expertos y estudiosos de esta materia. Solo cambia en el documento del JEMAD la utilización de cierta jerga militar. El objetivo por parte de la política de personal del MINISDEF debe ser llevarlas a cabo e implementarlas correctamente.

Asimismo, creo firmemente que el fin último del Ministerio de Defensa debe ser conseguir la mayor operatividad posible de sus Fuerzas Armadas, para cumplir con las misiones que la sociedad a través de su Gobierno nos asigna. Y no podremos cumplir con este mandato sin una correcta base de la estructura. Luego le doy una importancia capital, por delante incluso, de otras capacidades (como los medios materiales o las infraestructuras...).

Me consta que es un tema que está en pleno debate en muchos foros militares (como el Taller 2035, o los estudios del Instituto Español de Estudios Estratégicos,), pero también veo que no pasamos de los conceptos teóricos y las nuevas corrientes filosóficas empresariales, que pienso ya tenemos asumidas y aceptadas y toca proponer soluciones imaginativas para implementarlas.

2. Desarrollo

2.1. Objetivos

En los últimos tiempos, muchas publicaciones sobre este tema desechan el concepto de Gestión de Recursos Humanos en beneficio de la tendencia actual de Gestión de Talento. Desde mi punto de vista no son incompatibles. Es más, creo que la gestión de talento es un aspecto más o al menos una estrategia, que puede ser nuclear incluso, de los Departamentos de Recursos Humanos. Cuestión aparte es si se ha estado

realizando correctamente y si como parece, adoptar ese nuevo enfoque tiene margen de mejora. Parece evidente, a priori que así es.

En definitiva, me ha atraído el nuevo paradigma sobre la gestión de talento en las organizaciones porque creo tal y como expresan los expertos que debe estar alineado con los intereses estratégicos de aquellas y que redundará en beneficio de la consecución de sus objetivos. Hemos intentado a lo largo del trabajo acomodar cada fase del nuevo modelo de gestión de talento a las circunstancias particulares de las Unidades CIS/Ciber del MINISDEF, proponiendo soluciones para su implantación: identificar, captar, desarrollar y retener.

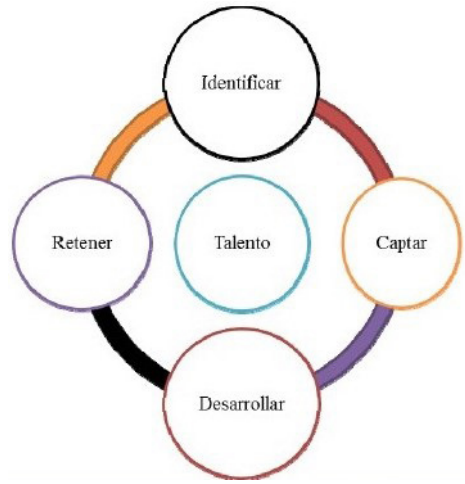


Figura 1. Un esquema modelo de la gestión de talento. Apuntes Máster DIRETIC, COM1

2.2. Estudio del recurso humano como activo esencial en un entorno imprevisible

En los últimos años parece haberse consolidado y asentado el concepto del recurso humano, las personas, como un activo importante de cualquier organización. Y como tal activo de importancia extraordinaria hay que cuidarlo y gestionarlo con la debida implicación y acierto. La adecuada gestión de las personas que componen una organización se hace más necesaria, si cabe, en instituciones que requieran una especialización por parte de su personal. El éxito o fracaso en alcanzar los objetivos de la misma depende de un modo claro de la correspondiente aportación de las personas que lo componen.

Por otra parte, todas estas realidades debemos enmarcarlas en un entorno operativo, aplicando la terminología militar, que es complejo, dinámico e impredecible (turbulento) y que requiere cada vez más una especialización técnica elevada y concreta para cada organización y puesto. A este entorno habrá que saber adaptarse para tener oportunidades de

éxito, objetivo que se materializa con el cumplimiento de la misión que la sociedad encomienda a sus FAS. Este entorno operativo se enmarca, por tanto, en el concepto denominado VUCA.

Asimismo, debemos analizar cómo pueden adaptarse e implementarse las modernas teorías aplicadas al ámbito de la Gestión del Talento en nuestra organización o qué variaciones requieren para adecuarlas a la especial idiosincrasia y estructura del MINISDEF y de sus Fuerzas Armadas.

2.3. Análisis y desarrollo del ciclo de Gestión del Talento. Identificación del talento

La necesidad de talento se vuelve más perentoria en ámbitos donde se requiera una elevada especialización técnica de su personal como puedan ser aquellos objetos de este trabajo: Unidades CIS y Ciber de este Ministerio. Es decir, aquellas que trabajan y llevan a cabo sus operaciones y actividades en el ámbito ciberespacial. Parece evidente que antes de intentar captar a las personas talentosas para mi organización debo desarrollar un estudio de los puestos, individuales y de equipo, necesarios para el cumplimiento de las misiones y objetivos estratégicos de la empresa; esto es, definir las competencias profesionales técnicas y transversales requeridas.

El éxito radicará en tener la suficiente agilidad para, al detectar a alguien con las capacidades adecuadas, integrarlo en la organización y posteriormente ubicarlo en el puesto más idóneo a sus características.

Y en este punto descubrimos una de las diferencias fundamentales entre los dos modelos de gestión: la tradicional, que gira en torno a las plantillas como elemento nuclear, y el nuevo modelo, que lo hace en relación a las personas que poseen las capacidades, el talento que mi organización necesita.

2.4. Búsqueda, detección y captación de talento

Una de las claves de una correcta gestión se sitúa en *conseguir que las personas con el talento más alineado a nuestros objetivos estratégicos sean las que quieran entrar en nuestra organización*.

En el actual escenario, ante las perspectivas de dificultad de cubrir los puestos, y la previsión de que la situación no vaya a cambiar en un futuro a medio plazo, es necesario buscar soluciones imaginativas, innovadoras.

Y en este punto debemos acudir, por un lado, a la búsqueda del talento y de los perfiles técnicos y específicos que la Unidad CIS/Ciber requiere en fuentes ajenas y externas al propio Ministerio (universidad, Formación

Profesional, sector privado, reservistas voluntarios...) y, por otro lado, a la adopción y empleo de nuevas técnicas empresariales que mejoran este proceso del ciclo: externalización y *outsourcing*; digitalización del proceso de búsqueda y captación; empleo de nuevas tecnologías como inteligencia artificial (por ejemplo la orientada en *chatbots*) para las entrevistas y selección de candidatos para los mejores para cada proceso, técnicas de posicionamiento SEO en las páginas web de las UCO del Ministerio de Defensa (aplicando una política de comunicación que vaya orientada a la mejora de la imagen de marca denominada marca del empleador o *employer branding*), empleo de expertos como *Headhunters* o cazatalentos, y otros procedimientos como estrategias de *e-Recruiting*,...

En este contexto, a pesar de que la retribución económica es el primer incentivo para las personas que buscan trabajo (aspecto sobre el que poco podemos intervenir desde el MINISDEF o las unidades y sus órganos de gestión de personal, ya que los presupuestos son limitados y las remuneraciones están preestablecidas y no es un parámetro que podamos modificar), existen otros factores valorados por los encuestados sobre los cuales sí podemos intervenir para que sean un reclamo para la captación de talento: conciliación, buen ambiente laboral, seguridad y estabilidad personal y profesional, flexibilidad, movilidad y la propia imagen de marca de la empresa u organización.

2.5. Proceso de incorporación. Selección de personal. Procesos de evaluación. Encuadramiento

Esta es una fase importante para una correcta Gestión del Talento, que, aunque no está excesivamente tratada en las publicaciones de expertos en esta materia, no hay que olvidar, pues va a contribuir a, una vez captado el personal, ubicarle en el puesto de la organización donde mejor desarrolle sus capacidades, esté satisfecho con su trabajo y, en definitiva, la organización saque el máximo partido de él.

Todas estas actividades deben incluirse en el necesario (y a día de hoy inexistente como tal en nuestro MINISDEF) Plan Estratégico de Recursos Humanos de la organización. Su contenido, desde una perspectiva transversal que contemple como elemento nuclear el talento del personal, debe adecuarse en cada caso a las características de la empresa, pero de forma genérica podemos afirmar que ha de contemplar y abordar los siguientes factores condicionantes: análisis del entorno, plantilla de puestos, reclutamiento, diseño del plan de incorporación, contratación retribuciones, disponibilidad económica, formación especializada, promociones, motivación, enriquecimiento del puesto, rotación, plan de riesgos laborales, política de atención al empleado, vacaciones, promociones...

Figura 2-1. Cuadrante de Gartner WAN Edge Infrastructure (septiembre 2021) (fuente [2])

En los necesarios planes de incorporación y procesos de tutorización y evaluación del personal, vuelven a proponerse de nuevo estrategias actuales del mundo empresarial como el *mentorig* o el *coaching* y otras actividades que de forma parcial, podrían importarse para nuestra organización (pruebas colectivas de evaluación de capacidades como el conocido Método Grönholm).

2.6. Formación y desarrollo del talento

Parece fuera de toda duda y debate la necesidad de cultivar y evolucionar el talento inicial y aplicando nuestra innovadora fórmula matemática de Talento= Componente innato + trabajo (esfuerzo, desarrollo).

Se requiere, por tanto, una oferta formativa amplia para satisfacer esta necesidad.

Quizás es en este punto donde a nivel ministerial, y en concreto en el ámbito de UCO CIS/Ciber, existen menos carencias con un abanico muy amplio y variado de oferta formativa, una parte de la cual se expone a título ilustrativo en uno de los anexos del trabajo.

Como aspectos de mejora, o al menos de focalización, destacamos que podríamos centrar más la formación hacia el intercambio o la participación de actividades con el sector civil y en especial la propia y específica formación en materia de Gestión de Recursos Humanos y Gestión de

Talento para el personal destinado en las primeras secciones o direcciones de personal de las UCO, del MINISDEF en general y de nuestras Unidades CIS en particular.

Se advierte previamente una carencia en la formación y actualización de los responsables y gestores de personal de los distintos organismos del Ministerio.

A este respecto existe a día de hoy un amplísimo abanico de posibilidades en el mercado para mejorar las capacidades de nuestro personal encargado de la Gestión de Recursos Humanos (ponemos como ejemplo un Máster Universitario en Dirección y Gestión de Recursos Humanos).

2.7. Retención del talento de la organización. Fidelización

Muchas de las actividades, condiciones, procesos y estrategias, que hemos mencionado y analizado en las fases anteriores de forma indirecta, en especial en el proceso de captación (pero también en las de encuadramiento, formación), influyen en los incentivos que la organización ofrece a sus empleados talentosos para conseguir retenerlos, fidelizarlos.

Y aquí nuevamente aparecen alternativas de mejora dentro de nuestro Ministerio. Algunas más complicadas de adoptar, como la retribución flexible o la remuneración por objetivos, otras más factibles (pero que requieren la adaptación de las estructuras y planificación de misiones y objetivos) como la movilidad geográfica o el teletrabajo y otras *gratuitas* pero que implican un cambio radical en la organización y planteamientos del Ministerio:

- Cambio de la normativa en vigor de Evaluación y Clasificación para los ascensos, de forma que la permanencia prolongada en los destinos no esté penalizada (estabilidad necesaria en puestos de carácter técnico).
- Igualmente, los destinos fuera de la estructura orgánica de los Ejércitos (MCCE, CESTIC) deben dejar de penalizarse para la proyección de ascensos.
- Actualmente los cupos numéricos que cada Ejército puede ceder a los organismos del Órgano Central y del EMAD, en numerosos empleos, impiden que personal con el adecuado perfil pueda optar por puestos en esta estructura.
- Necesidad de creación de una comunidad ciberespacial en base a un cuerpo, especialidad o al menos trayectoria, de tal manera que se pueda desarrollar la actividad profesional a lo largo de toda la carrera en unidades del hipotético cuerpo del ciberespacio, fomentando así el principio de necesidad de permanencia y estabilidad.
- Permitir, incentivar y facilitar la movilidad geográfica, apoyada en el teletrabajo o en las nuevas tecnologías materializadas en VPN para acceso remoto al puesto de trabajo, videoconferencias, o presencia física en la ubicación de otra UCO en el lugar de residencia.

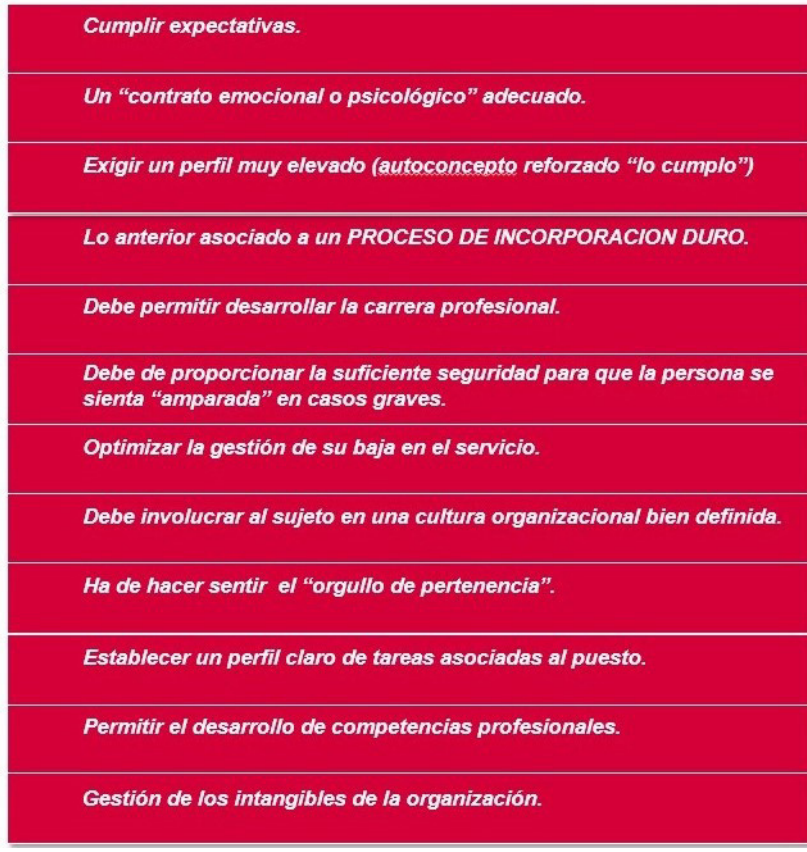


Figura 3. Algunas herramientas, estrategias, condiciones para la fidelización del personal desde un estudio psicológico. (Presentación sobre gestión de personal en el ámbito del EMAD)

3. Cuestión para debate y discusión. ¿Por qué Gestión de Recursos Humanos vs Gestión de Talento?

En mucha bibliografía consultada se plantea que la *nueva y actual* tendencia de Gestión de Talento destierra y se opone a la *antigua y obsoleta* Gestión de Recursos Humanos.

Ya solo ha de hablarse de la dirección de personas (DP) o dirección de personas basada en el talento (DPT) en vez de los mal llamados recursos humanos (RRHH).

Sin embargo, el recurso humano existe. El término en sí mismo es una evidencia. Es un activo más de la organización. Tal vez el más importante. ¿Por qué evitar esta terminología? Lo que hay que hacer es enfocar la Gestión del Recurso Humano a gestionar el talento que las personas poseen y ejecutar eficazmente los procesos.

Los Departamentos de Recursos Humanos en las empresas existen y se encargan precisamente de eso, de la gestión de ese activo. ¿Es necesario entonces cambiarle el nombre a Departamento de Gestión de Talento? No parece necesario ni procedente, ni es la corriente que impera en el mundo empresarial. De hecho, la gestión del talento de las personas que forman parte o van a formar parte de la organización es un aspecto más de toda gestión del recurso humano. Tal vez sea, o deba ser el núcleo de esta, pero en todo caso una parte del todo.

Se trata en definitiva de que la Gestión del Recurso Humano pivote sobre la Gestión del Talento de las personas, como medio para conseguir los fines de la organización.

A pesar de todo, parece fuera de toda duda que existen una serie de nuevas tendencias y una evolución a nivel empresarial en la Gestión de Recursos Humanos que nuestros departamentos, direcciones y secciones de personal deben ir introduciendo en la medida que sea posible, sorteando las trabas administrativas y agilizando y flexibilizando la normativa.

Y aquí introducimos algunas ideas susceptibles de incorporarse a nuestra gestión del recurso humano:

- Romper con las estructuras jerárquicas y encaminarse a modelos centrados en el trabajo entre equipos.
- Nuevos enfoques como el *design thinking* y el *employee journey maps*.
- Encaminarse a nuevos modelos de gestión como el Performance Management, adoptando metodologías *team-centric*, que se focalizan en el trabajo en equipo.
- Digitalización del Departamento de Recursos Humanos.

Como ya se ha mencionado, actualmente las plantillas constriñen la incorporación de personas talentosas a la organización. Se requiere agilidad y flexibilidad para ser capaces de incorporar al talento detectado en la estructura de la organización y adecuar las plantillas a las capacidades de las personas y no al revés.

4. Conclusiones, otras ideas fuerza y líneas futuras

El Recurso Humano es un activo capital para cualquier organización y constituye la base sobre la que se sustentan todas las demás estructuras y actividades; por lo tanto, requiere una especial y prioritaria atención, y si es necesario, un esfuerzo extra en materia presupuestaria anteponiéndolo a otras necesidades.

En el escenario VUCA (convulso, cambiante, incierto) en el que nos encontramos, el factor y límite presupuestario supone uno de los principales obstáculos con los que nos enfrentamos para una exitosa gestión del

personal. Limita los efectivos de las Fuerzas Armadas, las posibilidades de contratación externa (tanto de personal técnico como de empresas colaboradoras) y en general todas las actividades sobre las que giran las distintas fases del teórico ciclo de la gestión de talento: identificar, captar, desarrollar y retener.

No obstante, a pesar de tales inconvenientes existen caminos para mejorar la Gestión del Talento como factor estratégico organizacional. Las nuevas tecnologías y tendencias del mundo empresarial abren una puerta a la evolución en la Gestión del Talento, al que hay que tratar como un objetivo central dentro de la gestión de los recursos humanos de la organización, con cuyos objetivos estratégicos además debe estar alineada. Estas nuevas tecnologías facilitan estrategias como la mejora de la imagen de la empresa (lo que los gurús de la gestión de talento llaman marca del empleador o *employer branding*), la digitalización de los procesos de captación, *e-recruitment*, selección y evaluación del personal, el teletrabajo como incentivo laboral...

La Gestión de Talento no se opone a la Gestión de Recursos Humanos, ni al contario, sino que debe ser un componente de esta, correctamente desarrollado.

Las limitaciones de efectivos nos obligan a la búsqueda de talento en el sector civil y a incorporarlo de forma permanente en la organización.

También la colaboración con empresas especializadas en el sector de los Recursos Humanos y de las TI parece ser un camino imprescindible para mejorar la gestión.

Existen herramientas y soluciones parciales que sin grandes incrementos de costes mejoran la gestión del personal.

Se ha de poseer la capacidad de integrar en las unidades a las personas más idóneas y que las plantillas se adecúen a ellas y no al contrario, y conseguir, en última instancia, que las personas con mayor talento quieran formar parte de nuestra organización.

No obstante, somos conscientes que la mejora de la Gestión del Talento constituye un impacto en toda la organización y requerirá un cambio de algunas de sus estructuras y políticas, tanto a nivel militar como ministerial y que requiere, asimismo, la implicación firme y convencida de la cúpula del departamento.

El recurso económico, es decir, el capítulo presupuestario, es clave para posibilitar los medios necesarios para una correcta gestión, donde predomine la eficacia, del Recurso Humano.

A pesar de estas servidumbres se pueden emprender líneas de acción imaginativas, innovadoras y ambiciosas (ya empleadas en el ámbito empresarial), que mediante un reducido coste económico supongan mejoras sensibles en la Gestión del Talento de la organización.

En relación con las posibles líneas de investigación para proseguir este estudio, se propone abordar inicialmente la implementación de las siguientes medidas y su posterior evaluación:

- La revisión y adecuación de los planes de formación en los centros de enseñanza militar para la inclusión desde la base de los correspondientes créditos/módulos CIS/CIBER.
- La formación de un Grupo de Estudio multidisciplinar (expertos en planes, RRHH, jurídicos, logistas...) para la creación de un arma/especialidad fundamental ciberespacial.
- El desarrollo de normativa y la habilitación de créditos que posibiliten la contratación de personal civil, con el adecuado perfil técnico, procedente de universidades, Formación Profesional, empresas civiles del ámbito de las TIC, para que puedan integrarse con carácter permanente en la organización.
- El estudio e implementación de la oferta de formación que existe en el sector civil y empresarial para la capacitación y actualización de nuestros responsables y gestores de los RR.HH. y del talento que este activo atesora.

Referencias

[1] Entorno Operativo 2035 y trabajos y conclusiones del Grupo de Trabajo, PAC 5, Gestión de Talento.

[2] La Gestión de Talento en las FAS. Una decisión estratégica. Documento de investigación del Instituto Español de Estudios Estratégicos.

[3] La nueva gestión del talento. Pilar Jericó.

[4] Gestión del talento. Roberto Lunas Aroca.

[5] Normativa de gestión de personal del EMAD.

[6] Información consultada de interés obtenida de diversas páginas web:

https://www.universia.net/es/actualidad/empleo/10-competencias-transversales-mas-valoradas-empleadores-1139319.html

https://cybersecuritynews.es/falta-talento-en-ciberseguridad/

https://bloggrupoledo.com/2021/03/06/cual-es-la-diferencia-entre-outsourcing-y-tercerizacion/

http://www.infodefensa.com/es/2020/11/20/opinion-presupuestos-defensa-numero-consistencias-inconsistencias.php

https://www.iebschool.com/blog/desmotivacion-laboral-relaciones-laborales/

https://www.gestiopolis.com/remuneracion-desempeno-objetivos/

https://empresas.infoempleo.com/hrtrends/diferencias-mentoring-coaching

https://www2.deloitte.com/es/es/pages/human-capital/articles/10-tendencias-gestion-RRHH.html

Gestión de talento en organismos CIS/Ciber del MINISDEF

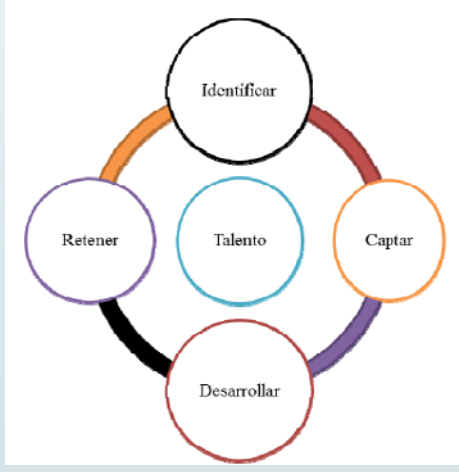
Autor: Vicente Tormos Fernández
Director: Francisco Javier Rodríguez Rodríguez

Introducción

- ✓ El Recurso Humano como activo fundamental de las organizaciones.
- ✓ Atendámoslo adecuadamente.
- ✓ Busquemos el talento de las personas
- ✓ Dentro de un entorno operativo incierto, volátil y en permanente evolución
- ✓ Apliquemos soluciones imaginativas

Metodología

1.-Estudio y análisis de las distintas fases del ciclo de gestión de talento



2.-Adecuar las nuevas tendencias a nuestros actuales procesos y estructuras

Resultados

Que las personas con más talento quieran formar parte de mi organización.

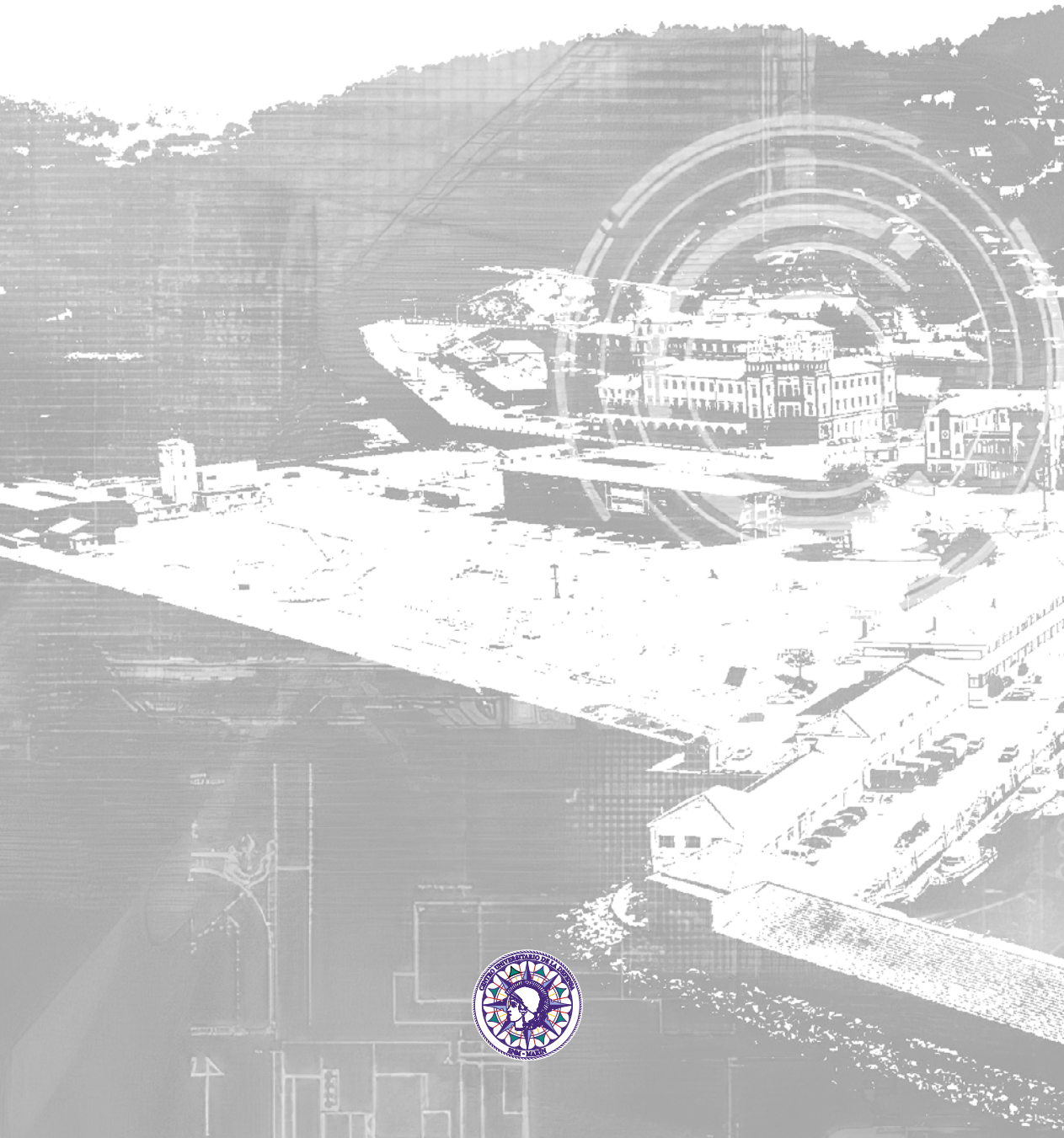
Conclusiones

- ➢ **Romper con las estructuras obsoletas y encaminarse a los nuevos modelos centrados en el trabajo en equipo**
- ➢ **Aprovecharse de las nuevas TI,s**
- ➢ **Acudir a fuentes externas de talento**
- ➢ **Incentivar**
- ➢ **Que la gestión del personal gire en torno al TALENTO**

Agradecimientos

GRACIAS!:

- A mi tutor por su ayuda y orientación. Muchas horas dedicadas a este TFM
- A mi familia por su apoyo y comprensión por el tiempo que les he robado en la elaboración de este trabajo
- A tantos y todos los compañeros que han colaborado con sus ideas e información



PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL