Internet como canal de comunicaciones para redes clasificadas, posible solución versátil y segura para despliegues militares

Autor: González Sierra, Bernardo

Director: Zamorano Pinal, Carlos

Contacto: bgsierra@fn.mde.es

Resumen: La necesidad de despliegue de unidades militares a lo largo de toda la geografía mundial requiere de canales de comunicación versátiles, seguros y relativamente económicos. El uso de Internet, prácticamente accesible en cualquier parte del mundo, permitiría que se pudiera extender el mando a aquellas unidades situadas en lugares remotos a través de los sistemas de Mando y Control (C2). La gran capilaridad de Internet y su coste reducido podrían sustituir los canales de comunicación militares, tales como los satélites militares, las líneas dedicadas en propiedad y los radioenlaces.

Con este trabajo se pretende encontrar una solución comercial, versátil y segura que permita a los jefes de los ejércitos extender su mando y control, sin importar donde se encuentren sus fuerzas, utilizando la red de redes, siempre cumplimentando la normativa nacional sobre información clasificada.

Palabras clave: Internet, redes clasificadas, sistemas militares, canal de comunicaciones, mando y control, seguridad, DMZ

---

1. Introducción

1.1 ¿Por qué sería necesario utilizar Internet como canal de comunicación?

En la era de las nuevas tecnologías, los ejércitos necesitan sistemas de mando y control para poder extender el mando a todas sus unidades, estén cerca o lejos de los puestos de mando.

Las operaciones militares hoy en día no solo se circunscriben al campo de batalla. El auge de la guerra híbrida, unido a conflictos de pequeña intensidad, pero con gran repercusión social y humanitaria han hecho que se tengan que desplegar muchas unidades militares a lo largo de la geografía mundial para poder completar sus objetivos.

Esta cantidad de misiones implican una gran cantidad de puntos de presencia de los sistemas de mando y control militar que prestan sus servicios sobre sistemas de información clasificada. Desplegar los puntos de presencia de los sistemas clasificados conlleva la extensión de redes seguras que se suele realizar mediante soluciones militares tradicionales utilizando satélites gubernamentales o líneas dedicadas, con un coste elevadísimo y poca disponibilidad /capilaridad

1.2 Necesidad

La necesidad de despliegue de redes clasificadas en zonas de operaciones demanda el acceso a un canal de comunicaciones versátil, accesible y económico, que pueda sustituir a las conexiones a través de satélites militares o líneas dedicadas, sin disminuir el nivel de seguridad exigido.

La conexión a Internet es cada día más accesible y su cobertura es más extensa. Localizar un punto de conexión en las zonas de operaciones donde se despliegan los contingentes militares suele ser relativamente fácil, incluso en países del tercer mundo. Esta accesibilidad podría ser una solución para aquellos puntos de presencia de las redes clasificadas de mando y control de los ejércitos en zona de operaciones.

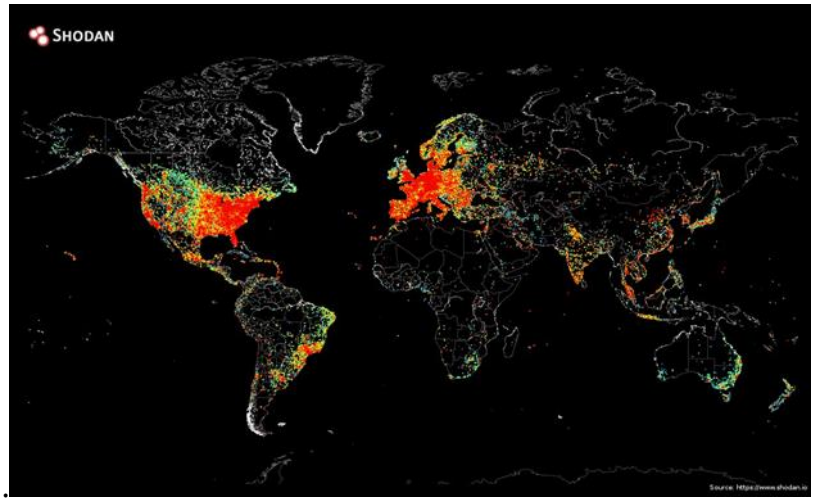

Figura 1. Mapa de “calor” de dispositivos conectados a Internet en el año 2014 (imagen obtenida de [1])

1.3 Objetivos

Los objetivos de este trabajo son:

1. Demostrar que el uso de Internet como canal de comunicación para los sistemas C2 militares es una solución versátil y económica que puede cumplimentar los estándares de seguridad exigidos.

2. Proponer una solución técnica (DMZ) con tecnología actual que facilite el despliegue de unidades en zonas de operaciones usando Internet como canal de comunicaciones

2. Desarrollo

2.1 Requerimientos de seguridad de los sistemas clasificados

Desde el comienzo de las civilizaciones la información ha sido clave, y siempre se han buscado maneras de protegerla. Desde el empleo del bastón Skytale griego para cifrar mensajes, empleado en

el siglo V a.C., hasta la máquina Enigma, empleada por los alemanes en la Segunda Guerra Mundial, los estados han intentado proteger aquella información sensible que podía poner en peligro su poder. La necesidad de proteger aquella información sensible implica un desarrollo de normas y leyes que fijen cómo se debe emplear la información clasificada y cómo se debe proteger para evitar que llegue a manos que puedan poner en peligro la estabilidad de la nación.

La principal norma que regula los secretos oficiales en España es la Ley 9/1968, de 5 de abril (BOE. Núm. 84, de 6 de abril de 1968), sobre Secretos Oficiales (LSO), que fue modificada por la Ley 48/1978, de 7 de octubre (BOE. Núm. 243), y por el Decreto 242/1969, de 20 de febrero. El Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI), es el organismo responsable de coordinar y garantizar la seguridad de las tecnologías de la información, así como de la promulgación de las guías CCN-STIC[1] que indican las normas, instrucciones, y recomendaciones para mejorar el grado de ciberseguridad de los organismos públicos.

2.2 Soluciones militares tradicionales

Las redes de acceso a las telecomunicaciones de la Infraestructura Integral de Información para la Defensa (I3D) tienen como objeto transportar todo tipo de servicios de datos, voz y video de los sistemas de información del Ministerio de Defensa. Dichas redes se apoyan en diferentes medios de transmisión propios como son fibras ópticas oscuras e iluminadas mediante equipos de multiplexación óptica DWDM y radioenlaces distribuidos por todo el territorio nacional. Por otro lado, también utiliza otros medios contratados como son circuitos dedicados en tecnología TDM y Ethernet para el segmento terreno y alquiler de ancho de banda en los satélites Spainsat y Xtar-EUR en el segmento espacial

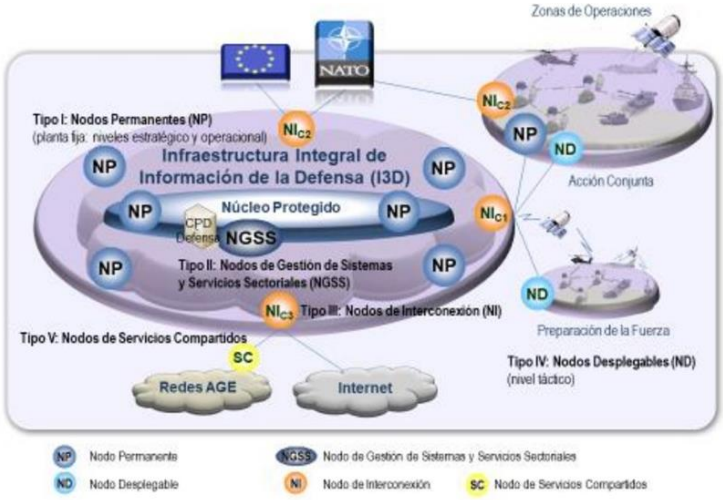

Figura 2. Esquema de las redes de acceso a la I3D (imagen obtenida de [2])

En la figura 2 se muestran todas las redes, las no clasificadas (Red de propósito general o WANPG) y las clasificadas (Núcleo Protegido). En el caso de las redes clasificadas que competen a la realización de este trabajo, se emplean medios de transmisión propietarios, bien sea mediante fibra óptica, radioenlaces o empleando la parte gubernamental de los satélites Spainsat y Xtar-EUR. El principal

[1] Centro Criptológico Nacional – Seguridad de las Tecnologías de la Información y Comunicaciones

sistema de transmisión en los despliegues de unidades en las zonas de operaciones es el uso de sistemas satelitales dada la complejidad y carestía que supone desplegar medios de transmisión propietarios fuera del territorio nacional. Siguiendo la normativa nacional vigente, todas las transmisiones de las redes clasificadas deberán estar cifradas, usando cifradores hardware publicados en la guía CCN-STIC-105 "Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación".

2.3 Elementos de interconexión. Los Sistemas de Protección de Perímetro (SPP)

Un Sistema de Protección de Perímetro (SPP) consiste en una combinación de recursos hardware y/o software denominados Dispositivos de Protección Perimetral (DPP), cuya finalidad es intervenir el tráfico de entrada y salida en los puntos de interconexión de los sistemas, en especial en aquellos que se encuentran en la frontera de la red.

Un DPP según el CCN es "el hardware y/o software, cuya finalidad es mediar en el tráfico de entrada y salida en los puntos de interconexión de los sistemas" y según el NIST "un dispositivo (p. Ej., gateway, enrutador, firewall o túnel cifrado) que facilita la adjudicación de diferentes políticas de seguridad del sistema para los sistemas conectados o proporciona protección de límites. El límite puede ser el límite de autorización de un sistema, el límite de la red organizativa o un límite lógico definido por la organización" [3].

2.4 Sistemas de cifrado

La criptografía es la ciencia que mediante métodos y herramientas matemáticas puede cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando para ello dos o más claves, logrando en algunos casos la confidencialidad, en otros la autenticidad o bien ambas simultáneamente. Consiste en la conversión de datos en un mensaje codificado para que sea ilegible. Se transforma un mensaje en algo inteligible que solo puede ser leído si se dispone de la clave secreta [8].

Todos los sistemas de cifrado deben cumplir la función Dk (Ck(m)) =m, es decir, que si se tiene un mensaje m, se cifra empleando la clave K y luego se descifra empleando la misma clave, se obtiene el mensaje original m.

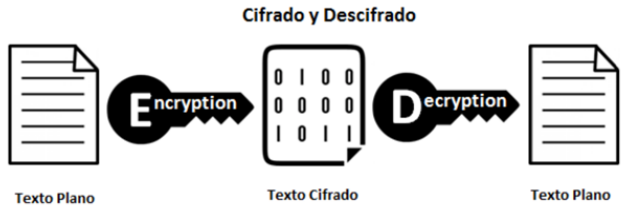

Figura 3. Esquema de un sistema de cifrado (imagen obtenida de [4])

2.5 Zona desmilitarizada o DMZ

La DMZ o zona desmilitarizada es una red perimetral que protege la LAN interna de una organización del tráfico no confiable. Es una subred que se encuentra entre la Internet pública y las redes privadas. Expone los servicios externos a redes que no son de confianza y agrega una capa

adicional de seguridad para proteger los datos confidenciales almacenados en las redes internas utilizando firewalls para filtrar el tráfico.

El objetivo final de una DMZ es permitir que una organización acceda a redes que no son de confianza, como Internet, al tiempo que garantiza que su LAN permanezca segura. Las organizaciones suelen ubicar los servidores para el sistema de nombres de dominio (DNS), protocolo de transferencia de archivos (FTP), correo, proxy, protocolo de voz sobre Internet (VoIP) y servidores web en la DMZ.

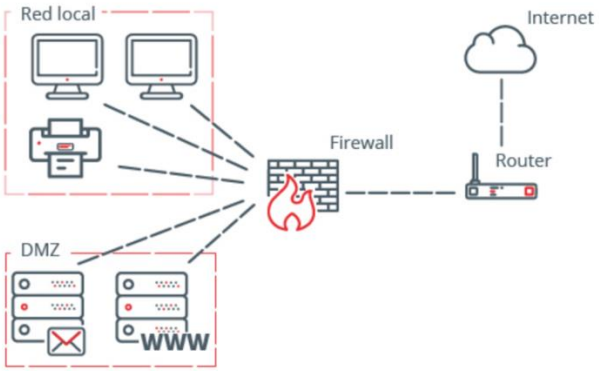

Figura 4. Esquema de una DMZ (imagen obtenida de [5])

2.6 Solución técnica propuesta

Para los sistemas C2 clasificados empleados en zona de operaciones que se quieran unir a la red usando canales de comunicaciones inseguros, se necesita una alta protección tal y como indica la normativa nacional, no siendo necesario romper la continuidad de los protocolos. Usando distintos dispositivos de defensa perimetral. En este caso se propone el uso de una DMZ en ambos emplazamientos para garantizar la triada CIA[2] del sistema.

En la figura 5 se materializa el concepto general de la solución y para evitar los riesgos inherentes al uso de una red insegura como es Internet, se incrementa la protección de las DMZ con cifradores dado la sensibilidad de la información que se transitará por estas redes.

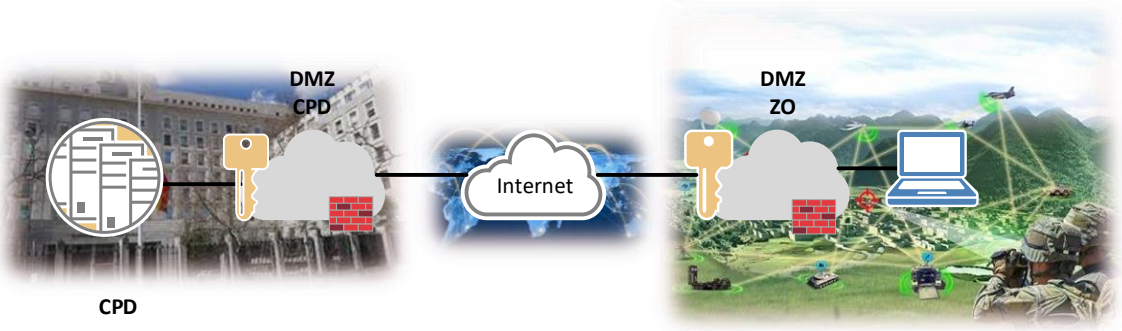

Figura 5. Diagrama conceptual de la solución técnica propuesta

La solución que se propone es la instalación de dos DMZ. Una en la zona de operaciones donde el router con acceso a Internet tendría una VPN con túnel IPSec con el router conectado con Internet en el CPD. La función de ese túnel es enmascarar el tráfico cifrado que se intercambiaría entre los cifradores, teniendo que ser cifradores hardware por requerimiento de seguridad establecido en distintas guías CCN-STIC. Ambas DMZ estarían provistas de un firewall exterior que protege a los

[2] Confidencialidad, Integridad y Disponibilidad (CIA, de sus siglas en inglés)

cifradores hardware. Después de los cifradores se instalaría otro firewall interior que protege los activos que se despliegan en zona de operaciones o en la DMZ del CPD, estos firewall deberán ser de un fabricante diferente a los exteriores para permitir la defensa en capas y evitar un único punto de fallo.

Para incrementar la seguridad, también se desplegará un IDS/IPS en ambas DMZ que reportarán sus logs a un sistema SIEM centralizado en el CPD. Puesto que los despliegues en zona de operaciones son más vulnerables y susceptibles de sabotajes, ataques, etc., se implementarán thin/zero clients desprovistos de medios de almacenamiento interno que puedan ser sustraídos, minimizando los riesgos de pérdida de información sensible. En la DMZ del CPD se ubicará un Unified Access Gateway y un call manager que harán de "proxy" entre los escritorios VDI y los teléfonos desplegados y los servicios prestados por el CPD en territorio nacional. Un último firewall en la DMZ del CPD protegerá todos los servicios del CPD.

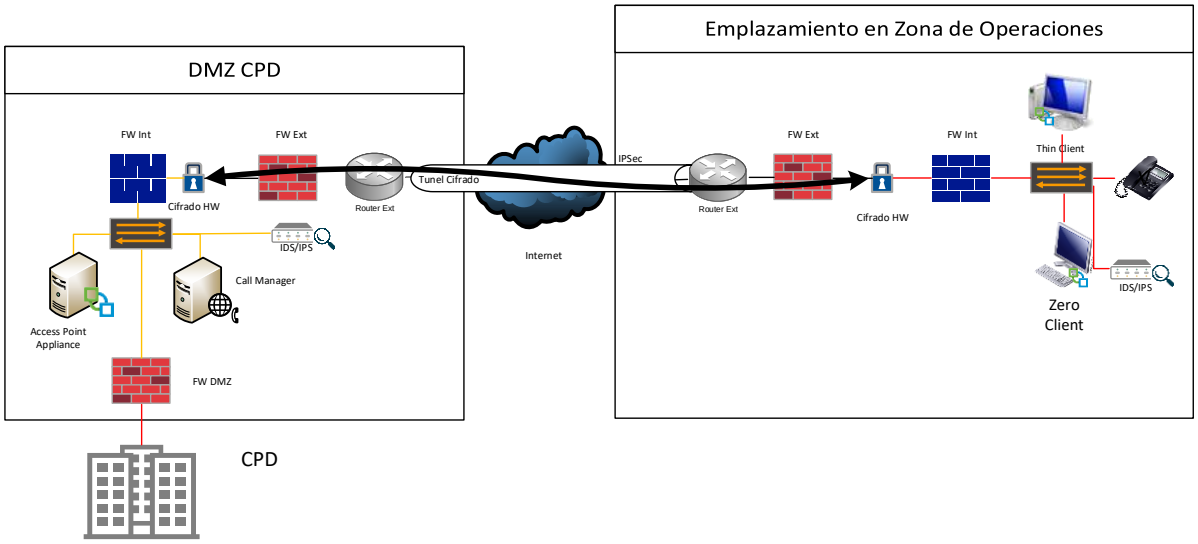

Figura 6. Diagrama de alto nivel de la solución técnica propuesta

3. DMZ vs. soluciones militares tradicionales

En este punto se comprobará la bondad de la solución técnica propuesta en este trabajo con las soluciones militares tradicionales empleadas actualmente para dar servicio a todos los nodos de las redes clasificadas desplegadas fuera de territorio nacional.

3.1 Seguridad

La seguridad es un elemento imprescindible en cualquier sistema clasificado. Los principios necesarios para cumplir con los objetivos de seguridad en los sistemas clasificados son: análisis y gestión del riesgo, mínima funcionalidad, mínimo privilegio, nodo autoprotegido, defensa en profundidad, control de configuración, verificación de la seguridad, vigilancia y respuesta a incidentes, monitorización y resiliencia [6]. La normativa vigente establece unos criterios estrictos y claros a la hora de determinar los procedimientos y sistemas para proteger la información clasificada, recogidos en las guías CCN-STIC. La solución técnica propuesta cumple con los requisitos establecidos, estando en línea con lo requerido en las guías CCN-STIC en vigor, destacando el empleo de cifradores IP hardware certificados, que a su vez están protegidos mediante una DMZ. Aun cumpliendo con todos los requisitos de seguridad la solución propuesta en este trabajo, las soluciones militares tradicionales, que emplean redes no expuestas, son más seguras al reducir los riesgos inherentes que conlleva el empleo de redes públicas.

3.2 Disponibilidad

La disponibilidad es la cualidad o condición de la información que permite, a las personas o procesos autorizados, acceder a ella cuando se demande de acuerdo a los requisitos establecidos [6]. En el caso de la solución técnica propuesta la disponibilidad depende íntegramente de los proveedores de Internet contratados en zona de operaciones para suministrar la red de transporte. Esta dependencia de los ISP puede poner en peligro la disponibilidad de la red clasificada, mientras que en las soluciones tradicionales, principalmente a través de satélites militares, dependería de la accesibilidad a la constelación de satélites militares por parte del receptor en zona de operaciones, normalmente solo condicionada por la situación meteorológica.

3.3 Capilaridad

La capilaridad o capacidad de poder desplegarse en distintas ubicaciones es una cualidad a tener en cuenta a la hora de destacar unidades a lo largo y ancho de la orografía mundial. La solución técnica propuesta es más ventajosa que las soluciones tradicionales ya que el despliegue de un nodo dependería de poder acceder a Internet, siendo esto relativamente sencillo. El 57% de la población global tiene acceso a Internet [7] y en todos los países donde hay unidades desplegadas actualmente hay proveedores de Internet disponibles.

En el caso de las soluciones tradicionales la capilaridad dependería principalmente de la cobertura de los satélites gubernamentales, no siendo ésta global, y que además disponen de un ancho de banda bastante limitado que debe ser compartido con todos los terminales desplegados, tanto en zona de operaciones como en territorio nacional.

3.4 Coste

El coste aunque en menor medida, también tiene cierta importancia a la hora de desplegar sistemas clasificados dependientes del Ministerio de Defensa. Los recursos económicos son limitados y últimamente esta carencia es cada vez más significativa. En la tabla 1 se puede apreciar una comparativa del gasto necesario para implementar una solución tradicional y la solución técnica propuesta. Esta tabla es un resumen de los datos recopilados y en ella se puede apreciar que la inversión en la solución técnica propuesta es sustancialmente más económica

CAPEX	**Solución Tradicional**	**Solución Técnica Propuesta**
CPD	113.774,36 €	148.235,57 €
Nodo desplegado	471.926,13 €	22.487,04 €
TOTAL	**585.700,49 €**	**170.722,61 €**

Tabla 1. Tabla comparativa CAPEX de la solución tradicional y la solución técnica propuesta

En lo referente al acceso a la red de transporte. En el caso de la solución propuesta el precio de acceso a Internet es relativamente asequible en los lugares donde hay desplegadas unidades de las fuerzas armadas, con un promedio de aproximadamente 18,00 €/Mbps. Es difícil hacer una comparación económica entre la solución técnica propuesta y las soluciones tradicionales, ya que fuera de territorio nacional el despliegue de las redes clasificadas se realiza casi exclusivamente mediante el empleo de satélites militares, cuyos gastos se sufragan de una manera conjunta, pero con importes significativamente mayores. No obstante y de una manera general se puede afirmar que las conexiones

a Internet a través de proveedores locales tendrían un coste más reducido que la conexión a un satélite gubernamental.

3.5 Ancho de banda (BW) y tiempo de despliegue

Los despliegues de satélites militares se mueven entre los 2 y 4 Mbps de ancho de banda, pudiendo llegar a los 8 Mbps para los terminales con mayor capacidad, mientras que las ofertas de los ISP en las zonas de despliegue de las unidades españolas oscilan entre 0,5 y 500 Mbps, con un promedio de aproximadamente 48 Mbps a precios relativamente asequibles, como se constató en el punto anterior.

En cuanto al tiempo de despliegue, la solución tradicional es más ventajosa ya que tanto el terminal como el personal que lo opera se despliegan con las tropas en la zona de operaciones, pudiendo establecerse la conexión en pocas horas una vez establecida su base. La contratación de una conexión de Internet a través de proveedores locales puede demorarse, si tenemos en cuenta que el tiempo de aprovisionamiento de una conexión a Internet en España oscila entre 3 y 15 días, las barreras idiomáticas y la forma de pago (necesidad de una cuenta bancaría local, cambio de moneda, etc.).

4. Conclusiones

Teniendo en cuenta lo presentado en este trabajo, se puede afirmar que el uso de Internet como canal de comunicaciones para redes clasificadas podría ser una solución versátil y segura para los despliegues militares fuera de territorio nacional. La solución técnica propuesta cumple con los estándares de seguridad exigidos por la normativa vigente para sistemas clasificados y cuenta con la enorme ventaja que tiene el despliegue mundial de Internet con su gran capilaridad, permitiendo un acceso a la red de transporte en cualquier parte de del mundo con un ancho de banda aceptable a un coste razonable.

El coste del equipamiento necesario en la solución técnica propuesta es casi cuatro veces más económica que las soluciones tradicionales y el precio por Mbps también es más ventajoso.

El gran hándicap de esta solución es la disponibilidad debido a la total dependencia de los proveedores de los servicios de Internet y al tiempo de aprovisionamiento, sumado a que en las zonas de operaciones suele haber conflictos que pueden degradar o inutilizar el acceso a Internet. Los servicios de las redes clasificadas se pueden ver interrumpidos o degradados sin previo aviso y la prioridad de su restablecimiento está fuera de las capacidades de las fuerzas desplegadas.

Ante estos hechos, se considera que la solución técnica propuesta es apropiada para el despliegue de unidades en zona de operaciones, pero debería tener como respaldo una solución tradicional, es decir, acceso a satélites gubernamentales o con varios proveedores de Internet diferentes que hicieran de backup.

Agradecimientos

A Susana, Pablo y Álvaro, por permitirme robarles tiempo en familia para dedicarme a la realización de este máster y a todos aquellos que nunca han querido dejar de aprender. El conocimiento no es el fin, es el comienzo.

Referencias

[1] P. Engel, «Bussiness Insider,» 14 septiembre 2014. [En línea]. Available: https://www.businessinsider.com/this-world-map-shows-every-device-connected-to-the-internet-2014-9. [Último acceso: 27 agosto 2020].

[2] J. M. N. García, «En marcha la nueva red de telecomunicaciones de Defensa por 33,4 millones de euros,» 9 septiembre 2020. [En línea]. Available: https://www.defensa.com/espana/marcha-nueva-red-telecomunicaciones-defensa-33-4-millones-euros. [Último acceso: 12 diciembre 2020].

[3] Joint Task Force, «NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations Rev. 5,» U.S. Department of Commerce, Gaithersburg,, MD, 2020.

[4] A. d. l. Cruz, «Criptografía, métodos de cifrado y hashing: cómo las empresas PCI almacenamos datos de forma segura,» 14 febrero 2019. [En línea]. Available: https://paynopain.com/actualidad-fintech/post-experto-fintech/criptografia-metodos-de-cifrado-y-hashing-como-las-empresas-pci-almacenamos-datos-de-forma-segura/. [Último acceso: 4 enero 2021].

[5] «Qué es una DMZ y cómo te puede ayudar a proteger tu empresa,» INCIBE, 19 septiembre 2019. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa. [Último acceso: 12 Octubre 2020].

[6] CCN, «CCN-STIC-001 "Política de Seguridad de las TIC",» Gobierno de España. Ministerio de la Presidencia, Madrid, 2016.

[7] «Key Internet Statistics to Know in 2020 (Including Mobile),» [En línea]. Available: https://www.broadbandsearch.net/blog/internet-statistics. [Último acceso: 7 enero 2020].