Trabajo Fin de Grado

Acceso cliente de forma segura a los servicios de un PCMAAA a través de la tecnología inalámbrica

Autor

Juan Luis Flores Muñoz

Directores

D. Manuel Montes Menéndez
Dr. Fernando De León-Pérez

Centro Universitario de la Defensa-Academia General Militar
Año 2018

Resumen

La implantación de tecnología inalámbrica en el ámbito militar es un reto debido a que ofrece muchas ventajas y a la vez requiere de un nivel de seguridad más elevado que las redes convencionales.

Uno de los escenarios posibles en la implantación de redes inalámbricas son los Puestos de Mando, en los cuales existen numerosos equipos que requieren conectividad.

En este trabajo se ofrece una alternativa a la conexión por cable que actualmente se utiliza para que, los equipos cliente de un Puesto de Mando del Mando de Artillería Antiaérea, puedan acceder al servicio de red del Ministerio de Defensa y al servicio para el mando y control del Ejército de Tierra. La propuesta de red realizada se basa en una red en formato inalámbrico, evitando así el empleo de gran cantidad de cable dentro del Puesto de Mando, y facilitando el movimiento dentro de dicho Puesto de Mando.

En la primera parte de la memoria se investiga el estado del arte de las redes inalámbricas y la conectividad dentro de los puestos de mando. Los resultados de la investigación se desglosan de la siguiente forma. En primer lugar, se ofrece una visión de las redes inalámbricas, su composición y funcionamiento. A continuación, se abordan las amenazas que atañen a las redes inalámbricas, los tipos que existen y el modo en que operan. Seguidamente, se trata el tema de la seguridad en este tipo de redes, desde la configuración recomendada para los equipos hasta la importancia del componente humano en el empleo de las redes. Tras lo anterior se detalla la configuración y disposición actual de un Puesto de Mando en el acceso a los servicios que se pretenden migrar a conectividad inalámbrica.

En la segunda parte de la memoria, con el asesoramiento de una serie de expertos, se realiza una propuesta de red siguiendo una metodología compuesta por: una encuesta (para decidir los aspectos más importantes a evaluar de los dispositivos), un análisis multicriterio (para decidir qué dispositivos son los más adecuados) y un análisis de riesgos (para identificar los riesgos principales de una red inalámbrica)

En la memoria se concluye que es posible la implantación funcional y segura de la red propuesta. Se añaden las pautas que se deben seguir en el futuro para implementar esta propuesta.

Abstract

The implementation of wireless technology in military networks is a challenge for it potential advantages demand a level of security much higher than in conventional networks.

One of the possible scenarios for the implementation of wireless networks are the Command Posts, due to the large number of devices that should be interconnected within this army unit.

This paper offers an alternative to the standard wired connection that is currently used by the client devices of an Antiaircraft Artillery Command Post in order to access the network service of the Ministry of Defense and the command and control service of the Army. Our proposal is based on a wireless network, that would avoid the large amount of cable used inside the Command Post, improving in this way the mobility inside this unit.

The first part of the paper researches the state of the art of wireless networks and the main features of the connectivity within Command Posts. Main results are presented in the following way. First, we give a global view of wireless networks, their composition, and ways of operation. Next, we address the threats that affect wireless networks. Main kinds of known threats are identified and their behavior is described. Next, security in this type of networks is discussed. Our analysis extends from the recommended configuration for the equipment to the importance of the human component in the use of networks. Finally, we detail the current configuration and given arrangement of those services of a Command Post that are intended to migrate to wireless connectivity.

On the second part of the paper, we make, after the advice of a series of experts, a network proposal that follows a methodology composed of: a survey (to decide which relevant features of the devices are going to be evaluated), a multicriteria analysis (to choose the appropriate device) and a risk analysis (to identify the main risks of a wireless network).

We conclude that a functional and safe implementation of the proposed network is possible. Future unavoidable steps toward a first prototype are added to the main conclusions of the paper.

Agradecimientos

El presente proyecto no habría podido desarrollarse con éxito sin la ayuda y colaboración de:

- Dr. Fernando de León-Pérez (tutor académico): su disponibilidad para la supervisión de éste proyecto ha sido constante, de calidad y muy satisfactoria. Sus orientaciones han permitido guiar la realización de la presente memoria por el camino más adecuado, buscando en todo momento la perfección en cada fase.
- Capitán D. Manuel Montes Menéndez (tutor militar): sus conocimientos y orientaciones han hecho posible que el trabajo de investigación haya seguido el camino adecuado, habiéndose mostrado dispuesto a colaborar y facilitado la elaboración de dicho trabajo en todo momento.
- Al Centro Universitario de la Defensa: por la formación proporcionada durante cuatro años, sin los cuales no habría sido posible llegar a formarse adecuadamente como futuro Oficial del Ejército de Tierra.
- Teniente D. Rodrigo De Dios García: por su permanente disponibilidad a resolver dudas y su gran conocimiento de la materia. Cabe destacar los buenos modos y la excelente respuesta en todo lo que se le ha solicitado.
- Teniente D. Alberto Buena Jorge: por utilizar su dilatada experiencia en sistemas de información para aclarar cualquier tipo de duda que haya podido surgir en el transcurso del presente proyecto.
- A la 1ª Compañía de la Unidad de Transmisiones del Mando de Artillería Antiaérea por su constante predisposición a colaborar en todo lo que se le ha solicitado.

Índice

Índice de figuras

Índice de tablas

Lista de Acrónimos

AAA	Authentication, Authorization and Accounting
AGM	Academia General Militar
CC	Criterios Comunes
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSfC	Commercial Solutions for Classified
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
CUD	Centro Universitario de la Defensa
DOS	Denial of Service
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EEUU	Estados Unidos
EIGRP	Enhanced Interior Gateway Routing Protocol
ENS	Esquema Nacional de Seguridad
ET	Ejército de Tierra
IEEE	Institute of Electrical and Electronics Engineers
IPSEC	Internet Protocol Security
ITSEC	Information Technology Security Evaluation Criteria
MINISDEF	Ministerio de Defensa
MITM	Man In The Middle
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OC-CCN	Órgano de Certificación del Centro Criptológico Nacional
PC	Puesto de Mando
PCMAAA	Puesto de Mando de Artillería Antiaérea

PSK	Pre-shared Key
RFC	Request for Comments
RFS	Requisitos Fundamentales de Seguridad
RIP	Routing Information Protocol
SIMACET	Sistema para el Mando y Control del Ejército de Tierra
SSH	Secure Shell
SSID	Service Set Identifier
TCSEC	Trusted Computer System Evaluation Criteria
TFG	Trabajo Fin de Grado
TIC	Tecnologías de la Información y la Comunicación
TLS	Transport Layer Security
VM	Valor de Modelo
VPN	Virtual Private Network
WANPG	Red de Propósito General
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

Capítulo 1. Introducción

Las tecnologías en el ámbito de las comunicaciones han experimentado un enorme avance en los últimos años. Las infraestructuras de telecomunicaciones de hace una década requerían de conexiones mediante cables como única posibilidad para interconectar equipos. Actualmente la tecnología inalámbrica se ha impuesto a las conexiones cableadas debido a que ofrece una serie de ventajas claras. Como la de proporcionar una alta flexibilidad y simplificar enormemente las tareas de montaje y desmontaje de las redes.

En el ámbito militar, las comunicaciones inalámbricas suponen un reto, debido a que el carácter confidencial de la información implica establecer un nivel de seguridad adecuado en el espectro electromagnético, que es el medio de propagación que utilizan las conexiones inalámbricas. Dicho nivel de seguridad es mucho más complejo de alcanzar en este medio que en una conexión mediante cables.

En una maniobra es vital que las comunicaciones fluyan de forma adecuada y segura para que las Unidades que haya desplegadas en el campo de batalla reciban las órdenes emitidas desde los Puestos de Mando (PC).

El establecimiento de las comunicaciones dentro del PC debe ser lo más rápido y eficiente posible. La rapidez de su puesta en funcionamiento puede implicar o marcar la diferencia entre el éxito o el fracaso de la misión. La implantación de tecnología Wi-Fi proporcionaría una gran flexibilidad, ya que permitiría realizar cambios en la disposición interna del PC sin necesidad de realizar nuevas instalaciones de cable o de modificar las ya establecidas.

El reto principal de las comunicaciones Wi-Fi en el ámbito militar reside en la capacidad de dotar de una seguridad adecuada a las redes, de manera que la transferencia de información clasificada y no clasificada sea segura.

1.1. Propósito

Existen dos propósitos principales en la elaboración de este trabajo.

Uno de los propósitos de este trabajo es simplificar las labores del montaje físico del PC mediante **la eliminación total del cableado físico en los enlaces** entre un dispositivo cliente (ordenador portátil) y los servidores de un Puesto de Mando de Artillería Antiaérea (PCMAAA), y sustituyendo dicho cableado por dispositivos inalámbricos **que permitan una comunicación segura**.

En segundo lugar, se persigue **dotar al terminal cliente de libertad de movimiento dentro del PC de forma que no sea necesario que su ubicación dentro del PC sea fija.** La conexión inalámbrica permitirá realizar cambios en la disposición de los elementos que conforman el PC sin necesidad de realizar cambios físicos en la red, debido a la ausencia de cableado.

1.2. Objetivos

Para cumplir los propósitos anteriores definiremos los siguientes objetivos. Primero, realizar una revisión bibliográfica en fuentes especializadas, que permita obtener toda la información necesaria sobre redes inalámbricas, seguridad y amenazas existentes.

Segundo, seleccionar los dispositivos adecuados que conformen una red con la seguridad y fiabilidad adecuadas. En este punto es imprescindible el asesoramiento experto que valide las decisiones que tomaremos. Las tareas para llevar a cabo la toma de decisiones se basan en una primera fase de encuesta a expertos y una segunda de análisis comparativo de dispositivos mediante un método multicriterio.

Tercero, analizar y cuantificar los riesgos con vistas a identificar las debilidades de una red sin cables y facilitar la actuación ante la futura aparición de alguno de los riesgos registrados. El enfoque experto también es un elemento clave para la elaboración de este análisis de riesgos.

1.3. Alcance

La propuesta que se realiza en este trabajo pretende servir como base en el inicio del empleo de las comunicaciones inalámbricas en el interior de un Puesto de Mando, comenzando por el Puesto de Mando del Mando de Artillería Antiaérea y pudiendo, en un futuro, ser extrapolado a Puestos de Mando de otras Unidades, adaptando la red a las particularidades de cada Unidad.

Con este proyecto se persigue lograr una mejora sustancial en el empleo de material y en la movilidad dentro de un Puesto de Mando.

1.4. Ámbito de aplicación

Este proyecto se desarrolla en un momento en el que las tecnologías inalámbricas están presentes en casi todos los ámbitos de la vida. En los ejércitos más poderosos del mundo ya se están implantando sistemas de comunicaciones vía Wi-Fi. Para estar a la vanguardia de los mejores ejércitos es necesario que, en España, se lleven a cabo acciones de cara a una pronta implantación de tecnologías inalámbricas seguras que permitan agilizar y facilitar las maniobras en curso y lleven a un éxito más probable de la misión.

1.5. Estructura del trabajo

El presente trabajo se estructura en seis capítulos y cuatro anexos. Los tres primeros capítulos introducen al tema y resumen el estado del arte. En los capítulos 4-6 se describe y evalúa nuestra propuesta de red inalámbrica.

Capítulo 1. Se realiza una breve introducción a la memoria del trabajo, así como una presentación de la estructura de la memoria, los objetivos y propósito que se persiguen, y el alcance y ámbito de aplicación del proyecto.

Capítulo 2. Este capítulo versa sobre generalidades de las redes inalámbricas, las amenazas que se pueden presentar en una red sin cables y el concepto de seguridad en este tipo de redes.

Capítulo 3. Se lleva a cabo una explicación de los servicios que se han de proveer a los clientes de un Puesto de Mando de Artillería Antiaérea.

Capítulo 4. En este capítulo se detalla el proceso de selección de dispositivos de red y la elaboración de una propuesta de red inalámbrica segura.

Capítulo 5. Se desarrollan los riesgos asociados a la implantación de una red inalámbrica y las medidas que se han de tomar en cada caso.

Capítulo 6. Se exponen las conclusiones a las que se llegan tras la elaboración del proyecto.

Anexo I. Se expone un esquema de montaje de la red y un ejemplo de direccionamiento IP mediante el simulador Packet Tracer.

Anexo II. Contiene la tabla utilizada para realizar el análisis de riesgos.

Anexo III. Contiene la encuesta de expertos.

Anexo IV. En este anexo se muestran todas las especificaciones técnicas de los dispositivos que se comparan, así como una breve descripción de las características más importantes.

Capítulo 2. Redes inalámbricas

2.1. Generalidades

2.1.1. Definición

Una red inalámbrica ("*Wireless"* en inglés), es aquella en la que los dispositivos se interconectan mediante ondas electromagnéticas que viajan por el aire. La tecnología inalámbrica actual permite el establecimiento de redes muy complejas y con gran número de usuarios de una forma mucho más sencilla que una red similar en la que sus conexiones se estableciesen mediante cableado tradicional

2.1.2. Tipos de redes inalámbricas

Las redes sin cables se clasifican en función del área de aplicación (ver Figura 2.1) y del alcance de la señal. Atendiendo a este criterio se diferencian cuatro grupos [1]:

- Wireless Personal Area Network (WPAN)
- Wireless Local Area Network (WLAN)
- Wireless Metropolitan Area Network (WMAN)
- Wireless Wide Area Network (WWAN)

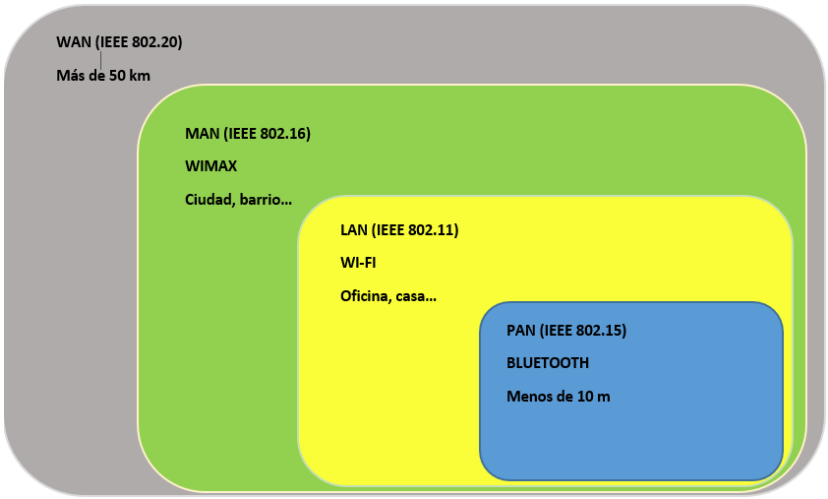


Figura 2.1. Tipos de redes inalámbricas y sus estándares

Las redes WLAN se basan en el estándar 802.11 del *Institute of Electrical and Electronics Engineers* (IEEE 802.11) [2]. Este tipo de redes proporcionan una cobertura de hasta cien metros. Las características de las redes WLAN las hacen ideales para proporcionar comunicaciones en entornos como viviendas, oficinas, instituciones públicas…

La entidad de un PC es similar a los entornos anteriormente citados, por lo que el tipo de red inalámbrica ideal para un Puesto de Mando es una Red de Área Local. La idoneidad de estas redes se debe a que en un PC todos los dispositivos cliente (que requieren conexión) se encuentran en un radio inferior a cien metros, por lo que una red WLAN proporciona una zona de cobertura adecuada.

2.1.3. Topologías de red

Una red sin cables puede funcionar en dos modos diferentes atendiendo al grado de control, de seguridad y a la finalidad que vaya a tener la red. Los tipos de arquitecturas de red son los siguientes [3]:

Modo AD-HOC

Los dispositivos se comunican directamente entre sí, sin ningún dispositivo intermedio. Carecen de Punto de Acceso (PA, ver descripción detallada en el siguiente apartado) y son el tipo de red más sencillo.

Modo Infraestructura

En el modo infraestructura es necesaria la existencia de al menos un PA para poder conectar los dispositivos inalámbricos a la red cableada. La gestión y configuración están centralizadas, lo que proporciona una seguridad mayor que en una red Ad-Hoc.

En una red en la que existe tráfico de información de carácter confidencial, el modo infraestructura dota de los medios para implantar medidas de seguridad adecuadas. La gestión y configuración centralizada de una red, en este caso militar, posibilita al

administrador de la red el poder llevar a cabo una supervisión que permita detectar con mayor rapidez las amenazas existentes en las redes sin cables.

2.1.4. Arquitectura de una red Wi-Fi

Una red inalámbrica Wi-Fi requiere de una serie de dispositivos concretos. A continuación, se exponen los componentes necesarios para establecer una red Wi-Fi [3].

Punto de Acceso (PA)

Un PA es un dispositivo cuya función es la interconexión entre un dispositivo inalámbrico y una red cableada. El PA es el nexo de unión fundamental en una red Wi-Fi ya que, sin él, la red inalámbrica no podría establecer flujos de datos con las redes cableadas tradicionales. Generalmente, un PA dispone de un puerto "Ethernet" para realizar la conexión a la red cableada. Por otro lado, emite señales de radiofrecuencia que permiten a los dispositivos inalámbricos llevar a cabo la conexión al Punto de Acceso.

Existen PA inteligentes, los cuales son capaces de llevar a cabo las labores de gestión de los dispositivos que están conectados de forma inalámbrica a ellos y las tareas de cifrado de la información. Por otro lado, se encuentran los PA simples. En el caso de disponer en la red de PA simples, la gestión de dispositivos y las labores de cifrado se llevan a cabo de forma centralizada, por lo que los PA no almacenan las claves criptográficas.

Dispositivos cliente

Los dispositivos cliente son los equipos que se conectan a los PA mediante medios inalámbricos como puede ser una tarjeta de red.

Para que una red inalámbrica funcione únicamente son necesarios los dos dispositivos descritos anteriormente, sin embargo, existen diversos sistemas que pueden ser necesarios según el tipo de red que se esté montando y las características que deba poseer dicha red.

En el ámbito militar serán podrían ser necesarios elementos como cifradores que se encarguen de encriptar los datos o servidores que provean de diferentes servicios a los usuarios. Los sistemas concretos que precisa un Puesto de Mando de Defensa Antiaérea se concretarán en el Capítulo 3.

2.2. Amenazas en una red inalámbrica

En una red inalámbrica aparecen una serie de peligros nuevos ante los que es necesario establecer medidas de seguridad para prevenir cualquier tipo de daño o acceso no autorizado en la red. Pero para poder aplicar medidas es necesario conocer que amenazas existen y cuáles son sus características.

Según Waliullah, M. y Gan, D. [4] las amenazas presentes en una red WLAN se clasifican en dos tipos:

Por un lado, están las amenazas pasivas. En ellas el atacante trata de obtener información que está siendo transmitida o recibida en la red. Las amenazas pasivas son

muy difíciles de detectar debido a que el ataque no produce ningún tipo de cambio en la red, simplemente se logra captar la información de forma pasiva. Las amenazas pasivas más importantes son el Análisis del tráfico y el denominado "*Eavesdropping*". Éste último se traduce como "escuchas" y se encarga de interceptar tráfico sin ser detectado, con el objetivo de conseguir información transmitida en claro.

Por otro lado, las amenazas activas son aquellas en las que, al producirse un ataque a la red, el atacante no sólo trata de obtener la información deseada, sino que dicho ataque también producirá cambios en la red. Estos cambios pueden consistir en alteraciones en la información o incluso en la creación de información falsa que es introducida en la red con el objetivo de provocar un caos generalizado. Las amenazas activas más a tener en cuenta son: Acceso no autorizado, Punto de acceso no autorizado, ataques "Man in the middle" y Denegación de servicio (DoS). Las características de estos dos últimos ataques se describen debajo.

De acuerdo a los principios de Confidencialidad, Integridad y Disponibilidad de la información los tipos de ataques pueden ser [5]:

2.2.1. Ataques contra la confidencialidad

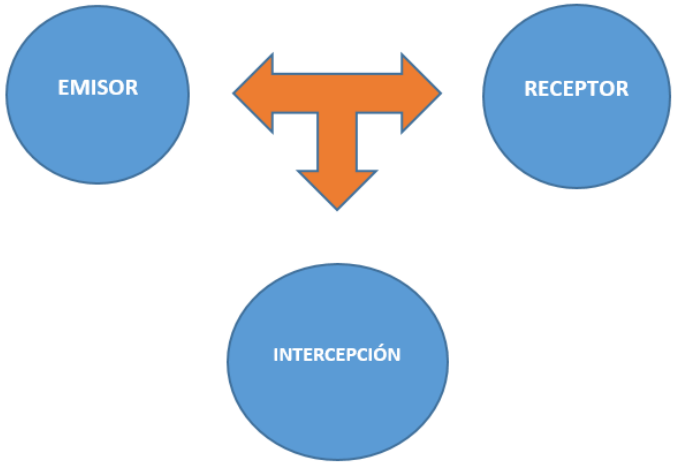


Figura 2.2 Esquema de ataques contra la confidencialidad

En este tipo de ataques, se trata de interceptar información sensible que está siendo transmitida de manera inalámbrica por el medio aéreo, independientemente de que dicha información viaje encriptada o en claro, ver esquema en la Figura 2.2.

El atacante puede llevar a cabo acciones de análisis del tráfico, que pueden llegar a proporcionarle información sobre el número de paquetes transmitidos, el tamaño de éstos y las direcciones de la fuente y el destino de la información. Este tipo de ataques son sencillos de llevar a cabo, ya que existen herramientas de software libre como

"*Netstumbler*" o "*Kismet*"[1] que permiten al atacante configurar su tarjeta de red en modo promiscuo para lograr conseguir la información que se está transmitiendo.

2.2.2. Ataques contra la integridad

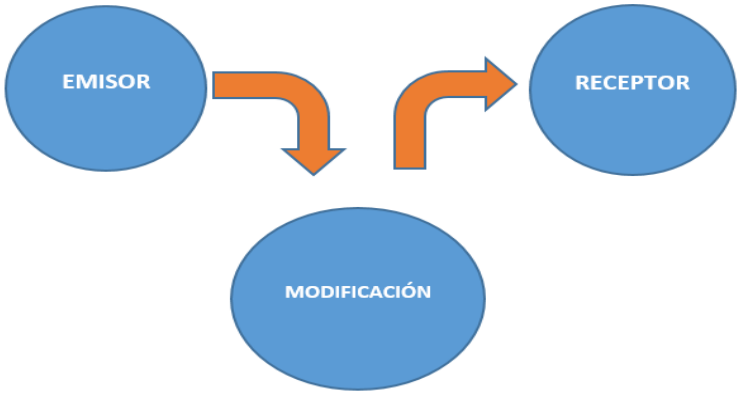


Figura 2.3 Esquema de ataques contra la integridad

Un ataque contra la integridad, ver esquema en la Figura 2.3, es aquél que es capaz de alterar la información transmitida ya sea introduciendo nueva información, eliminando parte de la transmisión o modificando los datos que son transmitidos.

Considerados ataques contra la integridad son los denominados "ataques *Man in the Middle (MITM)*". En este tipo de ataques se persigue leer o modificar la información que es interceptada, así como introducir nueva información falsa. Una de las técnicas de protección frente a ataques MITM es el uso de redes privadas virtuales (VPN) que permiten el establecimiento de túneles de datos en los que la información viaja cifrada (mediante protocolos IPsec). Además, las VPN impiden averiguar de dónde procede la información y a quién va dirigida.

[1] A diferencia de "Netstumbler", que sólo funciona en Windows, "Kismet" está disponible para varios sistemas operativos incluyendo Windows y Linux.

2.2.3. Ataques contra la disponibilidad

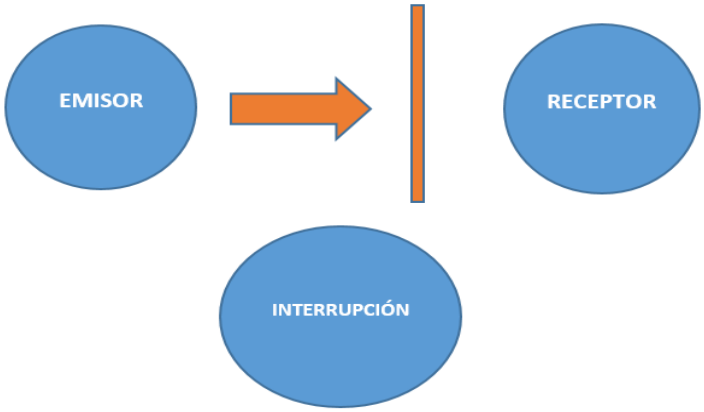


Figura 2.4 Esquema de ataques contra la disponibilidad

En un ataque contra la disponibilidad, cuando el cliente legítimo trata de acceder a la información el acceso le es denegado, ver esquema en la Figura 2.4.

Las amenazas de Denegación de Servicios (DoS) o Denegación de Servicios Distribuida (DDoS) son las más comunes en los ataques contra la disponibilidad. Los ataques DoS consisten en que un equipo lanza peticiones a un servidor de forma constante con el objetivo de acabar saturándolo y bloqueándolo, ver esquema en la Figura 2.5. Los ataques DDoS siguen el mismo principio de los DoS, la diferencia reside en que en los DDoS las peticiones al servidor se realizan desde varios equipos a la vez.

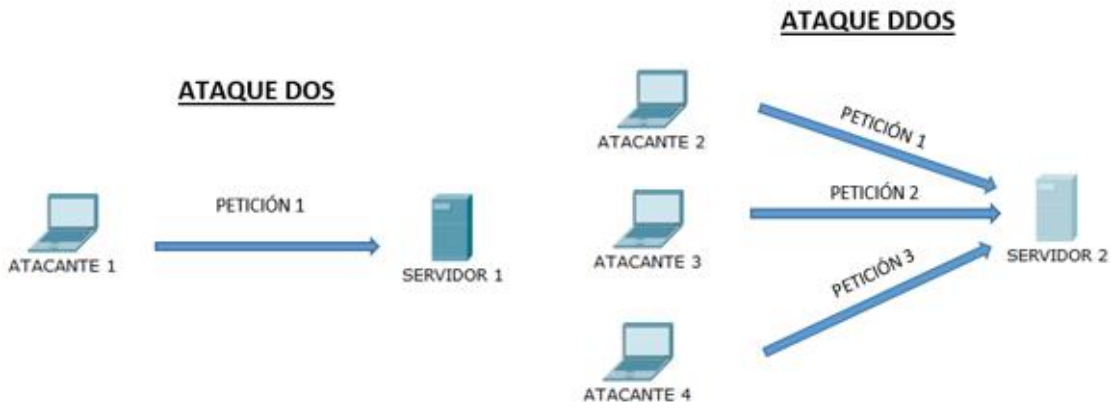


Figura 2.5 Ataques DoS y DDoS

2.2.4. Ataques contra la autenticación en una red

En este tipo de amenaza el atacante trata de obtener las credenciales de los usuarios legítimos para acceder a la red. El peligro de un ataque fructífero de este tipo está en que puede llevar tiempo el detectar que unas credenciales de usuario están siendo utilizadas por alguien ajeno a ese usuario legítimo. Existen dos tipos:

Los ataques de diccionario consisten en una base de datos que almacena posibles contraseñas y/o usuarios. Las combinaciones existentes se van probando para lograr alguna coincidencia. Si las credenciales correctas no se encuentran registradas en la base de datos, el acceso será imposible debido a que este método sólo compara las palabras almacenadas en su base de datos (diccionario).

Por otro lado, se encuentran los ataques de fuerza bruta. Éstos consisten en ir probando todas las combinaciones posibles de caracteres hasta hallar las credenciales correctas. Este tipo de ataques puede llevar gran cantidad de tiempo, pero con el suficiente, son capaces de averiguar cualquier clave.

2.3. Seguridad en redes inalámbricas

En una red inalámbrica cuyo propósito es el envío seguro de información clasificada es necesaria la implantación de las medidas de seguridad adecuadas.

A nivel nacional, la entidad encargada de coordinar la utilización, por parte de la Administración, de medios y procedimientos en las Tecnologías de la Información y la Comunicación (TIC) es el Centro Criptológico Nacional (CCN).

Dentro del CCN se encuentra el Organismo de Certificación del CCN (OC-CCN), ver Figura 2.6, que es el encargado de expedir las certificaciones de seguridad de productos y sistemas de Tecnologías de la Información según lo establecido en Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información y las Comunicaciones [6].

Figura 2.6. Dependencia OC-CCN del CNI

En 1990, a nivel internacional, se crearon los Criterios Comunes (CC) [7]. Estos criterios tienen el objetivo de armonizar los requerimientos de seguridad para los equipos y dispositivos TIC de forma que sean válidos en varios países. Actualmente los CC se encuentran estandarizados mediante la serie de normas ISO/IEC 15408: ISO 15408-1,2005 [8], ISO 15408-2,2008 [9] y ISO 15408-3,2008 [10].

El origen de los CC se encuentra en los criterios utilizados por diferentes países para la evaluación de la seguridad en productos TIC. Los CC aúnan los criterios de tres publicaciones:

Trusted Computer System Evaluation Criteria (TCSEC) [11]: Conocido como el "Libro naranja de la seguridad informática", se componía de los requisitos de seguridad establecidos por el Departamento de Seguridad de EEUU.

Information Technology Security Evaluation Criteria (ITSEC) [12]: Publicado unos años más tarde que el TCSEC, es el homólogo europeo de éste.

Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [13]: Es la publicación usada en Canadá. Estaba conformada en su mayor parte por los criterios recogidos en TCSEC y ITSEC.

Los CC suponen un aumento del abanico de posibilidades a la hora de adquirir un equipo seguro, ya que todos los países que forman parte de la organización aportan nuevos medios acreditados de forma constante. A pesar de lo anterior, cuando se trata información militar clasificada cabe tomar medidas más seguras que si de otro tipo de datos de la Administración Pública se tratase. Esto es debido, fundamentalmente, a que una filtración de información clasificada podría comprometer la seguridad nacional.

Para llevar a cabo la instalación de una red inalámbrica segura para el ámbito militar en el Ejército Español (ET) los requisitos no podrán basarse únicamente en el estándar ISO/IEC 15408. Los dispositivos deberán cumplir los criterios establecidos por el OC-CCN, que es la entidad a nivel nacional en España que se encarga de la certificación de seguridad de productos TIC.

Para proporcionar un nivel de seguridad adecuado a una red inalámbrica dentro de un PC se van a aplicar los criterios y requisitos de seguridad establecidos en el Esquema Nacional de Seguridad (ENS). El ENS está regulado por el Real Decreto 3/2010, de 8 de enero [14].

El ENS establece una serie de medidas con el objeto de proveer de la máxima seguridad posible a una red inalámbrica. Las medidas se clasifican en medidas organizativas, operacionales y de protección [15] [3]. Las diferentes medidas serán descritas en los apartados siguientes.

2.3.1. Medidas organizativas

Las medidas organizativas exponen que las redes inalámbricas deben estar presentes en elementos clave de una institución.

Uno de estos elementos clave es la **normativa** propia, debido a que una red inalámbrica es un sistema complejo y crítico que requiere de una serie de normas concretas para su buen funcionamiento. Las normas creadas para regular la red inalámbrica se incluirán dentro de la normativa general de la institución. A modo de ejemplo, quedarán definidos los requisitos de seguridad que la red ha de tener. Los requisitos se refieren a la asignación de responsabilidades para la dirección, gestión y

explotación de la red; se determinará qué tipo de información (clasificada, no clasificada, secreta…) podrá ser transmitida en la red. Otro aspecto que debe quedar claro en la normativa son los requisitos de seguridad física de los equipos, así como la configuración a aplicar y los métodos de protección de la red (claves de acceso, autenticación, pasarelas…).

Por otro lado, las redes inalámbricas también poseen **procedimientos** propios que son necesarios plasmar en el conjunto de procedimientos de la organización o institución. Algunos de estos procedimientos son la operación y mantenimiento de la red, la gestión de eventos y los procedimientos a adoptar ante ataques o pérdidas de información.

Los **procesos de autorización** de acceso a la red también deberán ser parte de los procesos de la institución. En una red se conoce por procesos de autenticación aquellos que proveen de autorización a usuarios y sistemas para el acceso y explotación de la red.

Uno de los puntos clave para la seguridad de una red que debe quedar plasmado en la normativa de la organización es el establecimiento de evaluaciones o auditorías de seguridad de manera periódica.

2.3.2. Medidas operacionales

Las medidas operacionales que determina el ENS son aquellas en las que se especifican que características de seguridad debe tener una red inalámbrica.

Arquitectura

El ENS establece dos medidas de seguridad. La primera hace referencia a la ubicación física de los PA. Deberá tenerse en cuenta tanto la ubicación física como la potencia radiada el PA con el objetivo de que la cobertura de la red inalámbrica no alcance el exterior del PC, o lo haga lo menos posible. Esta medida es vital debido a que cuanto más se acote la zona de cobertura de la red inalámbrica, más fácil resultará su control. La segunda medida establece que la red se establecerá en modo infraestructura, ya que de esta manera la configuración de la red se encuentra centralizada y es más sencillo llevar a cabo un control efectivo de la red.

Autenticación

Se establecen también medidas de autenticación. Dentro de estas medidas se abarcan tres aspectos que han de quedar definidos:

- Tipo de autenticación: Según el ENS, se debe implantar el método 802.1X/EAP. Además, requiere de la existencia de servidores de autenticación (RADIUS).
- Mecanismo: En caso de que la información tenga carácter clasificado, deberá emplearse una autenticación de doble factor. El nivel de fortaleza de claves y contraseñas frente a ataques de diccionario y fuerza bruta deberá ser muy alto. Además, debe establecerse una política que regule y controle que las contraseñas empleadas tengan un nivel alto de seguridad, así como establecer renovaciones periódicas de las contraseñas.

- Método "*Extensible Authentication Protocol"* (EAP): para una transmisión de datos no clasificados, deberá usarse un método EAP que aplique **todas las características obligatorias** del "*Request for Comments*" (RFC 4710). En el caso de información clasificada, el método EAP debe proporcionar tanto **las características obligatorias como las recomendadas en su totalidad**.

Administración y gestión de Puntos de Acceso

En los PA sólo podrá llevar a cabo labores de administración el personal autorizado expresamente para ello, debiendo quedar registrado todo lo que sucede durante dichas labores.

Configuración de seguridad

Cada tipo de dispositivo en una red inalámbrica deberá disponer de una configuración de seguridad propia. En una red inalámbrica se diferencian tres tipos de dispositivos.

- Clientes: En el ámbito de un PC los clientes deben configurarse de forma que cada uno sólo pueda acceder a los recursos que le corresponden.
  Las conexiones automáticas a la red y las conexiones duales deberán estar deshabilitadas.
  El cliente debe emplear el mismo método EAP que haya sido definido en las medidas de autenticación de la red (ver Autenticación).
- Red y Puntos de Acceso: Los PA deben tener la capacidad de crear redes privadas virtuales (VPN) para asegurar la comunicación entre el PA y el servidor de autenticación.
  No deben permanecer los parámetros por defecto en las configuraciones.
  El PA debe ocultar el Service Set Identifier (SSID) de la red, de manera que un dispositivo sólo se podrá conectar si introduce de manera manual el SSID correcto en su configuración.
  Al igual que en los dispositivos cliente, el método EAP que deben utilizar los PA deberá ser el mismo especificado para la red (ver Autenticación).
  El direccionamiento de la red debe ser estático de modo que no se podrán utilizara protocolos de direccionamiento dinámico como DHCP, RIP, EIGRP…
- Servidores AAA (Authentication, Authorization and Accounting): Los servidores de autenticación deberán estar protegidos con las medidas de seguridad adecuadas para evitar la intrusión, mediante la red inalámbrica, de usuarios no autorizados.

Intrusión en la red

La monitorización ante posibles intrusiones no autorizadas en la red deberá llevarse a cabo mediante los denominados *Wireless Detection Intrusion Systems* (WIDS) [16]. Estos sistemas constan de una serie de sensores cuya función es la de capturar tráfico de la red inalámbrica y analizarlo en buscar de ataques. Los WIDS deben ser capaces de detectar dispositivos no autorizados, dispositivos con configuraciones diferentes a la propia de la red, patrones anormales de uso de la red, ataques de denegación de servicio, de suplantación y ataques del tipo *man in the middle.*

2.3.3. Protección de redes inalámbricas

Tan importante es disponer de una red inalámbrica con las configuraciones de seguridad adecuadas como llevar a cabo una protección efectiva de la red en los siguientes aspectos.

Es de vital importancia que a toda persona que vaya a realizar algún tipo de tarea en la red se le haya proporcionado una formación adecuada respecto a su uso. Asimismo, es importante que la formación del personal sea constante debido al creciente número de amenazas que surgen.

2.3.4. Destrucción de datos

En la tabla extraída de, CCN-STIC-804[15] (basada en las medidas del National Institute of Standards and Technology (NIST) SP 800-88 [17]), que se muestra a continuación, se detalla el proceso a seguir para la destrucción de datos en función de su naturaleza:

Medio	Procedimiento	Tareas
Papel	Destruir	• Triturar en tirar de 2mm
Móviles y PDA,s	Borrado manual	• Agenda • Mensajes • Llamadas • Resetear a la configuración de fábrica
Routers	Borrado manual	• Tablas de encaminamiento • Registros de actividad • Cuentas administrativas • Resetear a configuración de fábrica
Impresoras y fax	Borrado manual	• Resetear a configuración de fábrica
Discos reescribibles	Reescribir sobre ellos	• Reescribirlos tres veces: con unos, con ceros y con datos aleatorios
Discos de sólo lectura	Destruir	• Trituradora 5mm

Tabla 2.1 Criterios de destrucción de datos

2.3.5. Seguridad criptográfica

Tanto para el envío de datos de carácter clasificado como para datos no clasificados la suite criptográfica a utilizar será *Counter Mode Cipher Block Chaining Message Authentication Code Protocol* (CCMP), que es uno de los algoritmos criptográficos acreditados por el CCN.

Los dispositivos inalámbricos deberán implementar *Wi-Fi Protected Access 2* (WPA2).

Para el envío de datos clasificados los dispositivos deberán contar con la certificación correspondiente de "Producto Aprobado" expedida por el OC-CCN. Los productos aprobados son aquellos aptos para el envío de información clasificada.

Capítulo 3. Las comunicaciones en el entorno de un PC

Hasta ahora las comunicaciones en los PC se han establecido por medio de cables. El uso de tecnologías inalámbricas en el ámbito militar está muy poco estudiado debido al mayor número de amenazas que este tipo de tecnología presenta. A pesar de lo anterior se han llevado a cabo algunos pasos en este ámbito.

En las acciones que se han llevado a cabo en el ámbito de las comunicaciones sin cables se pueden diferenciar dos tipos: por un lado, está la implantación de redes inalámbricas en entornos controlados y, por otro, su implantación en entornos no controlados. La razón de ello es que no es igual de sencillo proporcionar niveles de seguridad adecuados dentro de una zona segura (dentro de un PC), que proporcionarla en zonas en las que el enemigo pueda interceptar las comunicaciones.

En este proyecto se aborda la instalación de una red segura dentro de un entorno controlado como es un PC, el cual está dotado de medidas de seguridad en su totalidad.

Antes de llevar a cabo la proposición de un modelo de red inalámbrico para el acceso a los servidores de un PCMAAA es necesario saber cuál es el sistema que se emplea actualmente para acceder a dichos servidores desde un dispositivo cliente.

Dentro de un PC se provee a los clientes de diferentes servicios dependiendo de la función que desempeñen. En un PC de pequeña entidad no existen complicaciones sustanciales respecto a la cantidad de conexiones físicas a realizar. Sin embargo, cuando el PC adopta una entidad considerable, la infraestructura de red se hace muy compleja. Una infraestructura de red que esté compuesta por gran cantidad de cableado físico provoca una gran cantidad de problemas. El principal está en el tiempo necesario para llevar a cabo el montaje y desmontaje de las comunicaciones del PC, ya que establecer todas las conexiones físicas y proceder a la posterior organización y ocultación de todo el cableado es una tarea compleja y que requiere de una cantidad de personal determinada. Otro inconveniente importante reside en que la utilización de cableado implica un deterioro del mismo. Esto provoca que cada cierto tiempo sea necesario proveer de material nuevo al PC con el gasto que ello conlleva.

La utilización de conexiones físicas también reduce en gran medida la movilidad dentro del PC, ya que, si es necesario el movimiento de un cliente, se deben llevar a cabo labores de desconexión de cableado para volverlo a conectar en la nueva ubicación del cliente. En los PC actuales la movilidad es un factor muy importante, debido a que, el hecho de tener un PC que pueda desplegarse y replegarse en poco tiempo dota a la maniobra de mayor fluidez y una probabilidad más alta de éxito.

En un PCMAAA existen dos servicios cuya transformación a la tecnología inalámbrica provocaría una enorme disminución del cableado requerido debido a que poseen un número de usuarios considerable.

Por un lado, se propone proveer de acceso inalámbrico a los servidores de acceso a la red de propósito general (WANPG). En este caso se trata de que el cliente sea capaz de acceder mediante un ordenador portátil a la red del Ministerio de Defensa (MINISDEF). En dicha red la información no tiene carácter clasificado.

Por otro lado, está el servicio de acceso a servidores del Sistema para el Mando y Control del Ejército de Tierra (SIMACET). Este servicio implica la transmisión de información de carácter clasificado, por lo que todos los dispositivos de red utilizados deberán ser acreditar las medidas de seguridad adecuadas.

Dentro de un PCMAAA existen más servicios, sin embargo, dado el escaso número de clientes que tiene el resto de servicios (pueden ser uno o dos) no se considera necesaria la instalación de una red inalámbrica para dichos servicios que, además, no están presentes siempre (a diferencia de WANPG y SIMACET).

En un PCMAAA los clientes (tanto los de WANPG como los de SIMACET) están conectados físicamente a un switch mediante un cable RJ45 (Ethernet). Debido a ello los PC deben disponer de gran cantidad de cable por dos motivos. El primero de ellos es que la presencia de más de 40 clientes conectados de forma física implica el uso simultáneo de más de 40 cables. El segundo motivo es que la presencia de cableado implica posibles fallos o roturas debido a diferentes factores (trato inadecuado, un vehículo que pisa un cable…) ante los cuales es necesario disponer de repuestos de forma que un cliente no quede anulado de forma permanente por un fallo en un cable RJ45.

Además de lo anterior, todo el cable necesario para una maniobra debe ser transportado, ocupando espacio en unos vehículos, la mayoría de veces, escasos.

RED	TIPO DE INFORMACIÓN	NÚMERO DE USUARIOS
WANPG	No Clasificada	Más de 20
SIMACET	Clasificada	Más de 20

Tabla 3.1 Comparativa WANPG/SIMACET

Aunque se aparta del objetivo de esta memoria, es conveniente destacar que en algunas Unidades del ET se han comenzado a dar pasos hacia la incorporación de le conectividad inalámbrica al ámbito militar, ejemplo de ello es la Compañía de Transmisiones de la Brigada “GALICIA VII”. Esta Unidad está estudiando la posibilidad de establecer comunicaciones inalámbricas entre Puestos de Mando de forma segura. Esto consiste en sustituir las antenas de radiofrecuencia tradicionales por antenas Wi-Fi. Un ejemplo de los dispositivos en estudio son las antenas de la marca Ubiquiti. El empleo de las antenas anteriormente citadas implicaría la creación de una red Wi-Fi que conectaría las redes cableadas de dos Puestos de Mando.

Debido a los requisitos de seguridad de las comunicaciones militares, en la Brigada "GALICIA VII" se está estudiando la posibilidad de conectar las antenas a un cifrador para que, de esta forma, las comunicaciones que viajan por el aire vayan cifradas y no puedan ser entendidas por el enemigo en caso de intercepción. A pesar de ello, el estudio se encuentra aún en una fase muy temprana y aún no ha sido propuesto para ser acreditado por el OC-CCN.

A diferencia de lo que ocurre en la Compañía de Transmisiones de la Brigada "GALICIA VII", **lo que se propone en este trabajo no es establecer una comunicación Wi-Fi entre varios PC sino dentro del propio PC**. La ventaja de la propuesta realizada en este proyecto respecto al estudio mencionado es que, la existencia de una red inalámbrica entre dos PC implica dotar de seguridad al espectro electromagnético en toda la zona que exista entre ambos PC (pudiendo ser de más de 10km), mientras que la existencia de una red Wi-Fi dentro de un PC sólo precisaría de seguridad en el entorno del propio PC, que es donde se localiza la red en su totalidad.

Soluciones comerciales disponibles

Existe gran cantidad de dispositivos en el mercado, sin embargo, el tipo de información con el que se trabaja en el ámbito militar hace que no ellos sean válidos.

La información clasificada transmitida en un PC implica que, para establecer una red inalámbrica, sea necesario el empleo de dispositivos de red que cumplan con las más altas exigencias de seguridad establecidas para este tipo de información. La red a implantar deberá contener los dispositivos de red necesarios para un funcionamiento correcto y seguro, por lo que es necesario la existencia de los siguientes:

- Enrutadores: serán los dispositivos encargados de interconectar la red de clientes con la de servidores. Para que esta conexión sea segura se debe establecer una VPN creada mediante protocolos IPsec y utilizando el "modo túnel", pues son requisitos del CCN para el establecimiento de redes seguras.
- Punto de acceso: este dispositivo será el que proporcione la conectividad inalámbrica al cliente.
- Firewall WIPS: es el encargado de controlar el acceso no autorizado. Existen enrutadores que ya incluyen firewall en el mismo dispositivo, sin embargo, los firewalls integrados suelen tener unas capacidades inferiores.
- Servidor de autenticación: este servidor será contra el que se autenticarán los usuarios para poder acceder al sistema.
- Servidor WANPG/SIMACET: Son los servidores que proveen del servicio concreto requerido por los clientes de un PC.
- Cliente: se trata de ordenadores portátiles normalizados del ET.

En el mundo hay ejércitos que ya implementan soluciones inalámbricas en el ámbito de la información clasificada. En este caso el país de referencia es Estados Unidos (EEUU).

La *National Security Agency* (NSA) de EEUU dispone de un programa de certificaciones para dispositivos de red. Se trata del programa *Commercial Solutions for*

Classified (CSfC)[18]. Este programa contiene un gran número de dispositivos entre los que se pueden encontrar enrutadores, servidores AAA, puntos de acceso y sistemas WIPS aptos para la transmisión de datos clasificados.

Debido a la inexistencia actual de una alternativa de similar magnitud al CSfC en España, la red propuesta estará realizada en base a dispositivos aprobados por la NSA en el CSfC.

A continuación, se muestra en una tabla los diferentes medios que cumplen con las características de seguridad necesarias para el envío de información clasificada aprobados por la NSA. Los medios que se citarán en la tabla son los **únicos** acreditados por la NSA en el CSfC. Se expondrán medios de las siguientes categorías: enrutadores, puntos de acceso, dispositivos WIDS/WIPS y servidores de autenticación.

ENRUTADORES [19]	PUNTOS DE ACCESO [20]	FIREWALL WIDS/WIPS	SERVIDOR AAA [21]
• Cisco Familia 3900 (3945E, 3925E). • Cisco Familia 2900[22] (2901, 2911, 2921, 2951) • Cisco Familia 1900 (1921, 1941)	• Cisco Aironet Familia 1500 (actualmente descatalogada por Cisco) • Cisco Aironet Familia 1600 (1602E, 1602I) • Cisco Aironet Familia 3500 (3502E, 3502I) • Cisco Aironet Familia 3600 (3602E, 3602I, 3602P)	• Cisco ASA 5505[23] • Cisco ASA 5510 • Cisco ASA 5512-X • Cisco ASA 5515-X	• Aruba Clearpass Policy Manager • Cisco Identity Services Engine (ISE)

Tabla 3.2 Soluciones comerciales existentes

La Tabla 3.2 muestra cómo, para el caso de los routers, los dispositivos acreditados pertenecen a tres familias de dispositivos: la 1900, la 2900 y la 3900. Entre paréntesis se especifica cuáles son los modelos concretos que poseen la acreditación de la NSA. El resto de la tabla se interpreta de igual forma a la explicada para los routers.

En España, para que un dispositivo sea adecuado en materia de seguridad debe disponer de una serie de acreditaciones que le hayan sido proporcionadas por el CCN.

El CCN tiene disponible para su consulta y descarga el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) [24], en el que se encuentran dispositivos concretos que cumplen con los criterios de seguridad establecidos por el CCN. Todos los productos que aparecen cumplen con los CC y los Requisitos Fundamentales de Seguridad (RFS). En función de las certificaciones previas

de que disponga un equipo concreto, puede ser o no necesarias una serie de evaluaciones para su posterior inclusión en el catálogo.

CERTIFICACIONES PREVIAS	EVALUACIONES REQUERIDAS[7]	
	EVALUACIONES ADICIONALES	EVALUACIÓN CRIPTO
Certificación Common Criteria con TODOS RFS.	-	Validación algoritmos. Conformidad algoritmos de uso en el ENS.
Certificación Common Criteria no incluye TODOS RFS.	Recertificación Common Criteria o Evaluación STIC	
Sin Certificación Common Criteria	Certificación Common Criteria con todos RFS	

Tabla 3.3 Certificaciones previas y evaluaciones requeridas [25]

La Tabla 3.3 muestra que, para un dispositivo que cumple los CC incluyendo todos los RFS, no es necesaria ninguna evaluación adicional. Sin embargo, sí será necesaria una validación por parte del ENS de los algoritmos que utilice el dispositivo

Dentro del CPSTIC los dispositivos se dividen en dos tipos. Por un lado, se encuentran los **dispositivos cualificados**[2], que son aquellos aptos para el envío de información sin clasificar. Por otro lado, están los dispositivos que cumplen las medidas de seguridad más estrictas, son los **dispositivos aprobados**. Éstos últimos tienen las características requeridas para llevar a cabo la transmisión de datos de carácter clasificado.

El motivo de que la propuesta esté realizada en base a productos del CSfC es que, basándose en el CPSTIC, no puede establecerse una red inalámbrica segura para el envío de datos clasificados debido a que dentro de los productos aprobados no existen enrutadores, sistemas WIPS, puntos de acceso ni servidores AAA. Para que ello fuera posible, deberían someterse a evaluación dispositivos de las categorías anteriormente mencionadas, y tras ello, deberían obtener las correspondientes certificaciones de seguridad.

A pesar de que los dispositivos del CSfC cumplen con los más altos estándares de seguridad, incluyendo los exigidos por el CCN, los dispositivos deben ser evaluados por el CCN ser incluidos en el CPSTIC y, posteriormente, utilizados en la creación de una red inalámbrica segura.

[2] El CCN publica una guía [28] que detalla el proceso de inclusión de un producto dentro de los medios TIC cualificados.

Capítulo 4. Fundamentación de la propuesta de red

En este capítulo se expondrán los procedimientos utilizados para llegar a la propuesta de red que se realiza al final del mismo.

4.1. Diseño de la red

Para llevar a cabo el diseño de la red inalámbrica que se quiere implantar es necesario plantear la red más sencilla que sea posible, de forma que cumpla con todos los requisitos de seguridad y esté compuesta por todos los dispositivos necesarios.

Se propone como diseño la creación de una sola red en la que se establezca como umbral de seguridad el máximo requerido, esto es, el nivel de seguridad que requiere la transmisión de datos clasificados. En este planteamiento la información que posee requisitos de seguridad inferiores será enviada, también, a través de una red segura.

Otra opción de diseño es crear dos redes totalmente independientes. Cada una constaría de los dispositivos de red con el nivel de seguridad adecuado al tipo de información que se transmite. Sin embargo, establecer dos redes físicas independientes implicaría disponer por duplicado de dispositivos que desempeñan la misma función (cada uno con el nivel de seguridad correspondiente).

Para evitar duplicidades de dispositivos y economizar medios se establece la creación de una única red como la solución ideal.

4.2. Topología de red propuesta

La topología de red que se propone es una red en modo infraestructura (ver **Modo Infraestructura** en el apartado 2.1.3) Este modo es el exigido por el ENS. Para llevar a cabo la elección de los modelos concretos se ha seguido una metodología compuesta por una encuesta de expertos y un análisis multicriterio:

1. Encuesta de expertos (ver Anexo III. Encuesta de expertos): se ha elaborado una encuesta en la que se pide a tres expertos que clasifiquen según su criterio la importancia de cada una de las características de los dispositivos a implementar. Los expertos consultados han sido:
   - **Capitán D. Manuel Montes Menéndez**: Jefe de la 1ªCompañía de la Unidad de Transmisiones del Mando de Artillería Antiaérea (UTMAAA).
   - **Teniente D. Rodrigo de Dios García**: Jefe de la Sección RBA de la UTMAAA.
   - **Teniente D. Alberto Buena Jorge**: Jefe de la Sección de Puesto de Mando de la UTMAAA.

   Para rellenar la encuesta los expertos lo han hecho por consenso (una única encuesta para los tres expertos), debido a que el fin de la encuesta no es obtener

una estadística de su valoración individual sino ordenar los atributos de cada dispositivo por orden de relevancia. Dado que el número de características es alto, los expertos aconsejan realizar la comparativa posterior en base a las especificaciones a las que han asignado mayor valor (se escogen alrededor de la mitad del total). En el Anexo IV se proporciona una descripción de las características más valoradas por los expertos.

Los expertos han asignados valores desde '1' en adelante (siendo '1' la más valorada) a las diferentes especificaciones en función de la importancia que ellos consideran. En caso de haberse considerado dos características como iguales en importancia se les asigna a ambas el mismo valor (los valores aparecen reflejados en el Anexo III.

A continuación, se muestran qué características han sido las más valoradas por los expertos para cada tipo de dispositivo.

ROUTERS	PUNTOS DE ACCESO	FIREWALL	SERVIDOR DE AUTENTICACIÓN
• Precio • Slots ISM • Interfaces EHWIC • Puertos USB • Memoria SDRAM	• Estándares Wi-Fi • Autenticación RADIUS • Configuración remota • Precio • Beamforming	• Precio • Velocidad • Paquetes por segundo • Creación de redes VLAN	• Compatibilidad • Precio • Formato

Tabla 4.1 Características seleccionadas por los expertos

En la Tabla 4.1 se observan, por orden (de mayor a menor importancia) qué características han sido consideradas más importantes por los expertos. Destaca el precio como una característica común que se considera importante en todos los casos. Debido a que los dispositivos tienen un coste elevado, se ha considerado que, dentro de los dispositivos que cumplan los requisitos de seguridad necesarios, el precio es vital a la hora de tomar una decisión.

En los router se han valorado más las características de conectividad, en los firewall y puntos de acceso las de seguridad y en los servidores de autenticación las características físicas y de software.

2. Análisis Multicriterio (ver Anexo IV.): Para obtener el modelo de dispositivo más adecuado se ha llevado a cabo un análisis multicriterio que sirva como herramienta de evaluación de las diferentes opciones y que permita tomar, finalmente, la decisión de optar por uno u otro modelo de dispositivo en base a unos criterios. En dicho análisis se han asignado ponderaciones a las características más importantes (previamente seleccionadas por los expertos). Las ponderaciones se expresan en forma porcentual, y su valor corresponde a la

importancia relativa entre las especificaciones a evaluar que los expertos han considerado.

También se han asignado Valores de Modelo (VM), en forma de fracción, a cada dispositivo en cada característica. La atribución de valores en cada característica se ha realizado, en base al asesoramiento experto, de la siguiente forma:

$$VM = \frac{numerador}{nº\ de\ niveles}$$

Nº de niveles

En primer lugar, se identifican los niveles que hay dentro de una misma característica. Los niveles son los diferentes valores que puede tomar una característica en el conjunto de los dispositivos en estudio. Ejemplo: En el caso del precio de los routers, existen siete precios diferentes, por lo que existen siete niveles. En el caso de la memoria SDRAM de los routers, existen dispositivos con 1Gb o 512Mb de memoria, por lo que existen dos niveles. El número de niveles existentes en una característica constituye el denominador de la fracción.

Numerador

El numerador del VM se asigna desde el valor '1' hasta el número de niveles. Por ejemplo, en la característica "Precio", se asigna el valor '1' (en el numerador del VM) al router con un precio más desfavorable (el de mayor precio). A continuación, se asigna el valor '2' al router que tenga un precio inmediatamente inferior (el siguiente más favorable).

En el caso de que dos dispositivos coincidan en una característica se les asigna el mismo valor. Ejemplo: si dos router tienen el mismo precio, y además es el precio más alto, ambos tendrán el valor '1' (en el numerador del VM) en esa característica.

Resultados

Tras asignar los valores, el modelo más adecuado será el que tenga un VTM más alto. El VTM se calcula según la siguiente fórmula y se expresa en forma porcentual:

$$(\mathbf{PC1} * \mathbf{VM1}) + (\mathbf{PC\ 2} * \mathbf{VM2}) + \cdots + (\mathbf{PCn} * \mathbf{VMn}) = \boldsymbol{VTM}$$

Siendo:

- PC#: ponderación de la característica #
- VM#: valor asignado al modelo de dispositivo en la característica #
- VTM: valor total del modelo

A continuación, se muestran las tablas con los valores asignados:

Características	Interfaces EHWIC	Slots ISM	Puertos USB	SDRAM	Precio		
Ponderación	15,00%	20,00%	10,00%	10,00%	45,00%	100,00%	VTM
Modelos							
3945E	2/3	1/2	1	1	1/7		46,33%
3925E	2/3	1/2	1	1	2/7		52,77%
2951	1	1	1	1/2	2/7		62,87%
2921	1	1	1	1/2	4/7		75,70%
2911	1	1	1	1/2	1		95,00%
2901	1	1	1	1/2	3/7		69,31%
1941	1/3	1	1	1/2	6/7		78,52%
1921	1/3	1/2	1/2	1/2	5/7		57,08%

Tabla 4.2 Análisis multicriterio routers

En la Tabla 4.2 se observa que las características evaluadas en el caso de los Routers han sido cinco: interfaces EHWIC, slots ISM, puertos USB, memoria SDRAM y precio. Tras asignar los valores a la tabla, se observa en la columna "VTM" que el router más adecuado es el modelo "2911" por haber obtenido un VTM del 95%. El modelo 2911 posee mejores características en todas las características evaluadas, excepto en la memoria SDRAM, por ello obtiene la mayor valoración.

En segundo lugar, se aprecian dos modelos que han obtenido un VTM muy similar, son el modelo "1941" con un valor del 78,52% y el modelo "2921" con un valor del 75,7%.

Características	C. Remota	Estándares Wi-Fi	A. RADIUS	Beamforming	Precio		
Ponderación	20%	25%	25%	10%	20%	100%	VTM
Modelos							
Aironet 1600	1/2	2/3	1/2	1/2	1		64%
Aironet 3500	1/2	2/3	1	1	1/2		72%
Aironet 3600	1	1	1	1	1/4		85%
Aruba RAP-100	1/2	1/3	1/2	1/2	3/4		51%

Tabla 4.3 Análisis multicriterio Puntos de Acceso

En la Tabla 4.3 se observa que las características evaluadas en el caso de los Puntos de Acceso han sido cinco: configuración remota, estándares Wi-Fi, autenticación RADIUS, beamforming y precio. Tras asignar los valores a la tabla, se observa en la columna "VTM" que el Punto de Acceso más adecuado es el modelo "Aironet 3600" por haber obtenido un VTM del 85%, con una ventaja considerable respecto al segundo dispositivo más adecuado (Aironet 3500).

El dispositivo de Aruba ha sido el que ha obtenido menor calificación debido a que, en las dos características consideradas más importantes (estándares Wi-Fi y autenticación RADIUS), dicho dispositivo tiene unas especificaciones inferiores a sus rivales.

En este caso, las características que se han considerado más importantes han sido las relacionadas con la seguridad, ya que el Punto de Acceso será el encargo de proveer la conexión inalámbrica, directamente, al cliente.

Características	Velocidad	Redes VLAN	Paquetes por segundo	Precio		
Ponderación	25%	10%	25%	40%	100%	VTM
Modelos						
ASA 5505 / Security Plus	1/4	1/2	1/4	1		57,50%
ASA 5510 / Security Plus	2/4	1	2/4	3/4		65,00%
ASA 5512-X / Security Plus	3/4	1	3/4	1/4		57,50%
ASA 5515-X	1	1	1	2/4		80,00%

Tabla 4.4 Análisis multicriterio Firewall

En la Tabla 4.4 se observa que las características evaluadas en el caso de los Firewall han sido cuatro: velocidad, redes VLAN, paquetes por segundo y precio. Tras asignar los valores a la tabla, se observa en la columna "VTM" que el Firewall más adecuado es el modelo "ASA 5515-X" por haber obtenido el mayor VTM (80%). El modelo elegido es superior a sus competidores en todo excepto en precio.

También se observa que existen dos modelos (5505 y 5512-X) que son los menos adecuados, habiendo obtenido ambos el VTM más bajo (57,5%).

Características	Formato	Compatibilidad	Precio		
Ponderación	15%	65%	20%	100%	VTM
Modelos					
Aruba Clearpass Policy Manager	1	1/2	1/2		58%
Cisco Integrated Services Engine	1/2	1	1		93%

Tabla 4.5 Análisis multicriterio Servidor AAA

En la Tabla 4.5 se observa que las características evaluadas en el caso de los Servidor AAA han sido tres: formato, compatibilidad con otros dispositivos y precio. Tras asignar los valores a la tabla, se observa en la columna "VTM" que el Servidor AAA más adecuado es el modelo "CISCO Integrated Services Engine" por haber obtenido un VTM del 93%.

En comparación con la solución de Aruba (con un VTM del 58%), el dispositivo CISCO es mucho más adecuado, ya que la compatibilidad con otros dispositivos es un factor clave.

A continuación, se exponen cuáles son los modelos concretos de dispositivos de red que se emplearán en la propuesta en base al VTM obtenido en el análisis multicriterio y se citarán sus características más importantes, así como su precio aproximado[26]:

- Enrutador: Se empleará el modelo Cisco 2911. Dispone de 4 interfaces EHWIC, 1 Slot ISM, 2 puertos USB, 512 Mb de memoria SDRAM y un precio de 400 dólares.
- Punto de Acceso: el PA a utilizar será un Cisco Aironet 3600. Dispone de autenticación RADIUS, cumple con todos los estándares Wi-Fi (incluyendo 802.11i), capacidad de enviar más cobertura en una dirección concreta

(Beamforming), puede ser configurado remotamente y tiene un precio de 850 dólares.

- Firewall WIPS: el modelo Cisco ASA 5515-X. Dispone de una velocidad de 1,2 Gbps, capacidad para crear hasta 100 VLAN, un procesamiento de 500.000 paquetes por segundo y un precio de 1400 dólares.
- Servidor de Autenticación: en este caso la solución a implementar será Cisco Identity Services Engine. Este servidor es de tipo software. Es compatible con dispositivos de otros fabricantes y tiene un precio de unos 1750 dólares.
- Switches: Switch Cisco 3650 Catalyst. En este caso no se ha llevado a cabo una comparativa entre los diferentes switches debido a que éstos dispositivos no tienen funciones de seguridad asignadas en la red propuesta. El precio unitario de estos dispositivos es de 1500 dólares.

A continuación, se muestra la red propuesta en base a los dispositivos que han sido seleccionados mediante el Análisis Multicriterio anterior:

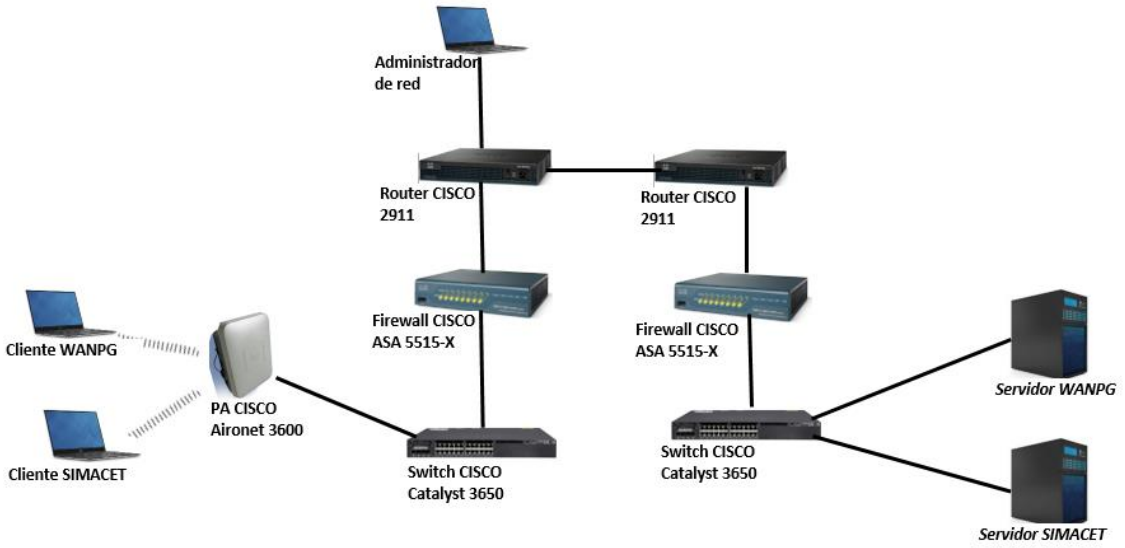


Figura 4.1 Esquema de red propuesto

La Figura 4.1 es una representación gráfica de las conexiones entre los diferentes dispositivos que componen la red propuesta.

Se muestran tres ordenadores portátiles. Uno corresponde al cliente de la red WANPG y otro al cliente SIMACET, ambos se conectan de forma inalámbrica al PA.

El tercer ordenador es el del administrador de la red. La función de este cliente será la supervisión y gestión de la red, por ello se conecta mediante cable directamente al router.

La red posee también dos switches. Uno de ellos interconecta los servidores WANPG y SIMACET con el router. El otro switch interconecta el PA con el dispositivo Firewall. Éste último no es estrictamente necesario en el modelo propuesto, sin embargo, su presencia proporciona la posibilidad de añadir dispositivos adicionales antes del Firewall.

Entre el router y el PA se sitúa un dispositivo Firewall para evitar y prevenir que los ataques externos puedan alcanzar el router y los servidores.

4.3. Ubicación de dispositivos en un PCMAAA

Junto a los expertos se determina la siguiente ubicación física de los componentes de la red en el PCMAAA:

- Interior del PCMAAA: se ubicarán los clientes y el PA. El único cableado físico que existirá será el que una el PA con el switch.
- Exterior del PCMAAA: en el exterior se ubicarán el resto de dispositivos. Los dispositivos de red estarán situados dentro de un vehículo en el exterior del PCMAAA.

El planteamiento anterior permitirá que el número de dispositivos a instalar cada vez que el PCMAAA despliegue o se repliegue sea el mínimo. Sólo será necesario ubicar dentro del PC los clientes y el PA. El PA estará conectado mediante un único cable al vehículo (donde se encuentran el resto de dispositivos de red).

4.4. Costes económicos de la propuesta

El establecimiento de la red propuesta implica la compra de todos los dispositivos, ya que se ha realizado el estudio en base a productos acreditados por la NSA para el envío de información clasificada. A continuación, se muestra una tabla con los costes aproximados de cada dispositivo, así como el coste total de la red.

	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
Router CISCO 2911	2	400 dólares	800 dólares
Punto de Acceso Cisco Aironet 3600	1	850 dólares	850 dólares
Firewall Cisco ASA 5515-X	2	1400 dólares	2800 dólares
Servidor Autenticación CISCO ISE (software)	1	1750 dólares	1750 dólares
Switch CISCO Catalyst 3650	2	1500 dólares	3000 dólares
Cableado de interconexión de dispositivos*	-	-	-
Costes de personal**	-	-	-
TOTAL			9200 dólares

Tabla 4.6 Desglose de costes de implementación de la red

*No se considera el coste del cableado necesario para interconectar los dispositivos debido a que la UTMAAA ya dispone de dicho cableado, por lo que no es necesaria su compra.

**No se contemplan costes de personal, ya que, desde su compra, los dispositivos son operados y puestos en funcionamientos por personal propio de la UTMAAA. Por ello no existen costes de personal asociados a la puesta en marcha de la red.

Los precios han sido consultados en la web CNET.

Capítulo 5. Análisis de Riesgos

En el estudio previo a la instalación de una red inalámbrica no puede faltar la realización de un análisis de riesgos en el cual se plasmen los riesgos más significativos que existen en el entorno de una red sin cables.

En el análisis se han considerado cuatro categorías de riesgo: bajo, medio, medio-alto y alto. En la categoría de riesgos bajos no se ha considerado ninguno. A continuación, se detallan cuáles han sido los riesgos concretos de cada categoría, sus causas y las medidas a tomar para su control o supresión.

En el Anexo II. Análisis de riesgos se muestra el modelo de análisis de riesgos empleado. Se ha empleado el modelo de análisis de riesgos [27] impartido en la asignatura Oficina de Proyectos, correspondiente a cuarto curso de la Academia General Militar (AGM). Los riesgos que han sido considerados en dicho anexo se han obtenido mediante la técnica de "Brainstorming" realizada en conjunto con los expertos citados en el apartado 4.1 ha permitido elaborar este análisis.

A continuación, se describen los diferentes riesgos considerados, agrupados en los niveles correspondientes. La descripción presentada es equivalente a los resultados mostrados en el Anexo II.

RIESGOS MEDIOS.

Configuración defectuosa de los routers: Todos los equipos han de estar debidamente configurados, especialmente los routers, ya que se encargan de la comunicación entre redes. Para evitar **fallos sistemáticos** en la configuración de los routers será necesario que el personal encargado de configurar estos dispositivos haya recibido una formación adecuada previamente. No se considera en este tipo de riesgo los fallos puntuales que el administrador de la red pueda cometer en la configuración.

Perturbación del espectro electromagnético: Existen equipos que tienen la capacidad de perturbar el espectro electromagnético y entorpecer la conexión entre el cliente y el punto de acceso, por ello podrían ser usados por el enemigo. Para evitar esta situación se han de utilizar sistemas WIPS que escaneen constantemente el espectro y tomen medidas en caso de detectar alguna deficiencia.

Conexión a Punto de Acceso falso: La presencia de un punto de acceso fraudulento puede provocar que el cliente se conecte a él creyendo que se trata de un Punto de Acceso legítimo, y se produzca un robo de datos del cliente.

RIESGOS MEDIOS-ALTOS

Acceso no autorizado: Para evitar que un dispositivo no autorizado acceda de forma inalámbrica a la red y se produzcan robos de información será necesario establecer mecanismos de seguridad en el control de acceso a la red. Uso de sistemas firewall y servidores de autenticación.

Pérdida de credenciales: Si se produce la pérdida de las credenciales de acceso por parte del usuario tendrá que iniciarse el procedimiento de recuperación de claves. El encargado de este proceso será el administrador de la red, por lo que mientras esté realizando este procedimiento no podrá atender otros asuntos de la red. Para disminuir esta situación (evitarlo completamente es casi imposible) es necesario concienciar a los usuarios de la importancia de conservar y actualizar sus credenciales.

Avería del cliente: En caso de que el equipo cliente se estropee o deje de funcionar es necesario disponer de equipos de reserva debidamente configurados y dotados de autorización de acceso a la red para que en caso de necesidad puedan ser puestos en funcionamiento a la mayor brevedad posible.

Área de cobertura externa al PC: La situación y orientación del Punto de Acceso es muy importante de cara a evitar que exista un área de cobertura amplia fuera del Puesto de Mando. Por ello será necesario orientar el Punto de Acceso de forma que la máxima cobertura se proporcione hacia los lugares donde se sitúan los usuarios de la red.

RIESGOS ALTOS

Saturación de la red: El riesgo más importante que se ha identificado es la posible saturación de la red debido a un uso inadecuado de ella por parte de los usuarios autorizados. Se considera un riesgo de nivel alto debido a que se pueden producir cortes en la red o su ralentización, por lo que toda la maniobra en curso podría retrasarse también. La probabilidad de que un usuario haga un uso inadecuado de la red es muy alta debido a que, consciente o inconscientemente, el usuario puede utilizar el equipo para acceder a contenido como periódicos o similares que no corresponde al contenido autorizado para la maniobra. La forma más efectiva de combatir este riesgo es concienciar a todo el personal de llevar a cabo un uso adecuado de la red.

Capítulo 6. Conclusiones

Tras el estudio realizado, se concluye es posible la implantación de tecnologías inalámbricas seguras dentro de un PCMAAA. Para ello es necesario utilizar medios adecuados en el ámbito de la seguridad. Por el anterior motivo, la propuesta se ha realizado en base a dispositivos acreditados por la NSA en el catálogo CSfC. El empleo de dispositivos del CSfC proporciona la confianza de que dichos elementos cumplen los más altos estándares de seguridad, y son por ello, adecuados para transmitir información clasificada de forma segura.

También debe asegurarse al personal que administra la red una formación rigurosa y actualizada que permita mantener el nivel de seguridad del conjunto.

Si se aplican conjuntamente la red propuesta y el personal formado adecuadamente, se dispondrá de una red con un nivel de seguridad máximo a través de la cual podrá enviarse información clasificada de forma segura.

Si bien, toda red inalámbrica es susceptible de ser atacada de forma efectiva, por lo que cumplir los más altos estándares de seguridad no exime de la posibilidad de que esa seguridad sea, en algún momento, vulnerada. Es por ello que la actualización constante debe ser primordial para mantenerse a la vanguardia de la seguridad y disminuir al mínimo los riesgos.

Para que en el Ejército de Tierra pueda implantarse la red propuesta, ésta debe ser acreditada por el CCN en su totalidad. Actualmente el CCN no tiene dispositivos inalámbricos acreditados para la transmisión de información clasificada por vía inalámbrica, por lo que la red propuesta no podría ser acreditada debido al componente inalámbrico que contiene.

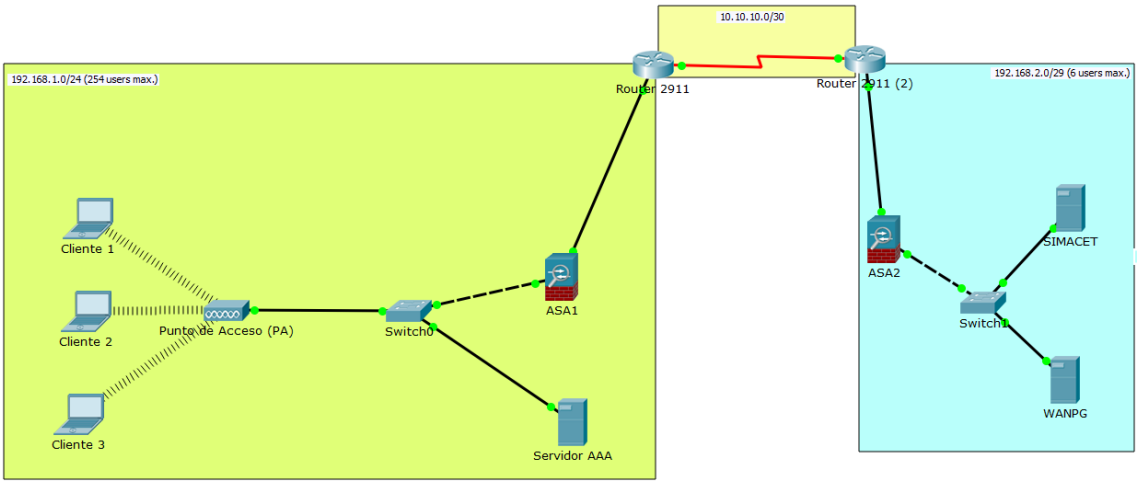
Para que la propuesta de red pudiera ser sometida a las correspondientes pruebas para su acreditación es necesario que en el CPSTIC sean incluidos dispositivos de red inalámbricos, ya que es una condición imprescindible que los elementos utilizados estén contenidos en dicho catálogo **para garantizar que España reconoce como seguros los estándares de seguridad empleados por dichos dispositivos**.

La implementación de la red propuesta implicaría una inversión, relativamente, pequeña. Sin embargo, sería fundamental incidir en la formación de los operadores y administradores de la red, que constituye un gasto durante todo el tiempo que la red esté operativa. Debido a la evolución constante de las redes inalámbricas sería necesario **asumir la responsabilidad** de mantener al personal constantemente actualizado en este tipo de redes. Por lo que el proyecto de implementación de este tipo de red no es algo puntual, sino que sería algo constante.

Para concluir se afirma que los dos propósitos de este proyecto se alcanzan con la propuesta realizada. Por un lado se elimina gran cantidad de cableado físico del interior de un PC y se sustituye por medios inalámbricos seguros, y por otro lado se dota al PC de mayor flexibilidad en su configuración física y se aumenta su movilidad para facilitar su adaptación a un entorno de constante cambio como pueden ser una misión real o unas maniobras.

Anexo I. Topología de red propuesta

A continuación, se muestra un esquema de la red que se propone implantar para un PCMAAA.



En el modelo de red de la imagen se han establecido 3 redes diferentes dentro del PC.[3]

La red 192.168.1.0 corresponde a los dispositivos cliente, el PA, el router 2911, el servidor AAA y el firewall situado entre los dos dispositivos anteriores. Se establece una máscara de red /24 cuyo número máximo de direcciones utilizables es 254. De esta manera no existirán problemas a la hora de incorporar nuevos clientes y dispositivos de red.

En esta red se encuentran los equipos que se conectan de forma inalámbrica debido a que es la red que se encuentra dentro del PC, que es donde se pretende proporcionar conexión Wi-Fi.

La red 192.168.2.0 se compone del servidor SIMACET, el servidor WANPG, el firewall y el router 2911(2). En esta red se establece una máscara /29 que proporciona 6 usuarios ya que el número de servidores no aumenta ni disminuye.

La red 10.10.10.0 conecta los dos routers. La máscara de red en este caso será /30 ya que esta máscara sólo permite asignar dos direcciones IP, que son las dos direcciones correspondientes a los routers. En esta red se establece un túnel VPN con protocolo IPsec.

A continuación, se muestra una tabla que contiene la información relativa a las direcciones IP asignadas a cada dispositivo:

[3] El direccionamiento mostrado es un ejemplo. En la realidad las direcciones a utilizar serán las que se asignen y determine el administrador de la red. Se han elegido las que se muestran para facilitar la comprensión de la red.

	192.168.1.0	192.168.2.0	10.10.10.0
Router 2911	192.168.1.1		10.10.10.1
Cliente 1	192.168.1.2		
Cliente 2	192.168.1.3		
Cliente 3	192.168.1.4		
Servidor AAA	192.168.1.5		
Router 2911 (2)		192.168.2.1	10.10.10.2
Servidor SIMACET		192.168.2.2	
Servidor WANPG		192.168.2.3	

Anexo II. Análisis de riesgos

Centro Universitario de la Defensa Zaragoza

Análisis de riesgos

ID	Descripción riesgo	Categoría riesgo	Causa del riesgo	Impacto (bajo, medio, alto)	Probabilidad (1,2,3)	Clase riesgo	Efectos riesgo	Medida	Responsable
1	Configuración defectuosa en los routers	Configuración	Falta de formación de personal encargado de configurar los equipos	H	1	1H	Imposibilidad de establecer la red	Asegurar la formación del personal encargado de cada equipo	Jefe Unidad
2	Acceso inalámbrico no autorizado a la red	Acceso a red	Falta de mecanismos de seguridad ante el acceso de dispositivos ajenos a la red	H	2	2H	Ataques o robos de información confidencial	Control de acceso a la red con firewall y servidor de autenticación	Jefe Unidad
3	Perturbación del espectro electromagnético	Espectro electromagnético	Dispositivos ajenos a la institución emiten ondas para perturbar el espectro electromagnético	M	1	1M	Los equipos cliente no logran conectarse al Punto de Acceso o se interrumpe la conexión	Control del espectro mediante sistemas WIPS	Jefe Unidad
4	Pérdida de credenciales de acceso	Usuario	El usuario pierde u olvida su usuario o contraseña de acceso al equipo cliente	M	3	3M	Administrador tiene que proporcionar nuevas claves al usuario pudiendo producirse retrasos en la maniobra	Incidir durante la formación en la importancia de mantener y actualizar las claves las claves	Jefe Unidad
5	Conexión a Punto de Acceso falso (Rogue AP)	Configuración	Un Punto de Acceso fraudulento intenta engañar al cliente para que se conecte a él.	H	1	1H	Los datos del cliente pueden ser interceptados por el Punto de Acceso falso	Control de acceso mediante servidor de autenticación	Jefe Unidad
6	Equipo cliente deja de funcionar	Funcionamiento equipos	Algún componente del equipo se estropea por el uso o tiempo de vida que tenga	H	2	2H	El usuario no dispone de equipo para conectarse a la red	Disponer de equipos sin asignar que estén autorizados a formar parte de la red	Jefe Unidad
7	Disponer de cobertura fuera del perímetro del Puesto de Mando	Espectro electromagnético	Mala orientación del Punto de Acceso	H	2	2H	Un equipo autorizado o no podría conectarse desde un área no autorizada	Disponer los elementos radiantes de forma que la cobertura externa sea mínima	Jefe Unidad
8	Saturación de la red	Usuario	Uso inadecuado de la red	H	3	3H	Bloqueo o ralentización de la conexión	Formación y concienciación de uso de los equipo sólo para el fin establecido	Jefe Unidad

Anexo III. Encuesta de expertos

Para establecer qué características de cada dispositivo debían ser evaluadas en el análisis multicriterio se solicitó a tres expertos que rellenasen por consenso una encuesta (1 único formulario para los tres) cuyo resultado se muestra a continuación:

ENCUESTA CARACTERÍSTICAS MÁS DESTACABLES

ROUTERS									
Puertos WAN Integrados	Interfaces EHWIC	Slots ISM	Puertos USB	Memoria flash por defecto	Memoria SDRAM por defecto	Cortafuegos Stateful	Hardware VAM (VPN Acceleration Module)	Filtro de contenido	Precio
7	3	2	4	5	4	6	9	8	1

Puntos de Acceso												
Emplazamiento	Velocidad Wi-Fi	Estándares Wi-Fi	Bandas de frecuencia	Configuración Remota	Beamforming	POE	TKIP	Cifrado AES	WPA2	Autenticación RADIUS	Memoria	Precio
5	3	2	7	10	3	4	6	6	6	8	9	1

Firewall WIDS/WIPS									
Velocidad de procesamiento	Sesiones simultáneas	Conexiones por segundo	Paquetes por segundo	Procesamiento de redes VPN	Sesiones de usuario VPN	Redes VLAN (enlaces troncales habilitados)	Switch Integrado	Puertos Gigabit Ethernet	Precio
2	6	5	2	4	9	3	8	7	1

Servidores de autenticación					
Formato	Autenticación Pasiva	Estándares AAA	Active Directory	Compatibilidad con dispositivos de otros fabricantes	Precio
3	6	5	4	1	2

Instrucciones:

Evaluar por orden de importancia las características de los dispositivos. Se asignarán valores a partir del '1', siendo ésta la característica considerada más importante.

Se podrá asignar la misma importancia a varias características.

De las valoraciones asignadas se seleccionan aproximadamente la mitad de las más importantes para asignarles ponderaciones y evaluar los dispositivos mediante un análisis multicriterio.

Anexo IV. Características técnicas

En el presente anexo se muestra una tabla para cada tipo de dispositivo, en la que se encuentran todas las características técnicas de que disponen. Debajo de cada tabla se localiza una breve descripción de las características que los expertos han considerado más importantes

ROUTERS

	3945E	3925E	2951	2921	2911	2901	1941	1921
Puertos WAN Integrados	4 Gigabit Ethernet	4 Gigabit Ethernet	3 Gigabit Ethernet	3 Gigabit Ethernet	3 Gigabit Ethernet	2 Gigabit Ethernet	2 Gigabit Ethernet	2 Gigabit Ethernet
Interfaces EHWIC	3	3	4	4	4	4	2	2
Slots ISM (Integrated Services module)	0	0	1	1	1	1	1	0
Puertos USB	2	2	2	2	2	2	2	1
Memoria flash por defecto	256 MB	256 MB	256 MB	256 MB	256 MB	256 MB	256 MB	256 MB
Memoria SDRAM por defecto	1 GB	1 GB	512 MB	512 MB	512 MB	512 MB	512 MB/	512 MB
Cortafuegos Stateful	Si	Si	Si	Si	Si	Si	Si	Si
Hardware VAM (VPN Acceleration Module)	Si	Si	Si	Si	Si	Si	Si	Si
Filtro de contenido	Si	Si	Si	Si	Si	Si	Si	Si
Precio	2000 dólares	1400 dólares	1400 dólares	800 dólares	400 dólares	900 dólares	560 dólares	600 dólares

Características técnicas de los routers

Ponderaciones

Las ponderaciones asignadas a cada característica se deben a:

- Precio: se le asigna la ponderación más alta debido a que el ET dispone de recursos económicos reducidos. Asignar mayor valor a esta característica no implica una menor calidad ni seguridad, ya que todos los dispositivos han pasado los estándares de seguridad y calidad de la NSA.
- Slots ISM: Son módulos que permiten reforzar la seguridad de los túneles VPN IPsec (empleado en el enlace entre los dos routers de la propuesta realizada). Se considera la segunda más importante debido a que es una característica de seguridad.
- Interfaces EHWIC: estas ranuras proporcionan conexiones ethernet (RJ45) de alta velocidad. Cuantas más tenga el router más dispositivos podrán conectarse de cara a instalar nuevos equipos. Se considera la tercera característica más importante debido a que permite la conexión de dispositivos que pueden ser de

mucha utilidad en un PC. Sin embargo, el precio y la seguridad siempre serán más importantes que esto.

- Memoria SDRAM: se trata de la cantidad de memoria de la que un router dispone para las tareas en ejecución en cada momento. Se borra cada vez que se reinicia el router. No se considera tan importante como las anteriores características debido a que 512MB es una cantidad más que de sobra para llevar a cabo las tareas de un router en un PC.
- Puertos USB: pueden usarse para establecer impresoras de red o servidores de archivos. Se considera que su importancia es similar a la cantidad de memoria SDRAM.

PUNTOS DE ACCESO

	Aironet 1600	Aironet 3500	Aironet 3600	Aruba RAP-100 Series
Emplazamiento	Interior	Interior	Interior	Interior
Velocidad Wi-Fi	300 Mbps	450 Mbps	1.3 Gbps	300 Mbps
Estándares Wi-Fi	802.11a/b/g/n/i	802.11a/b/g/n/i	802.11ac/a/b/g/n/i	802.11a/b/g/n
Bandas de frecuencia	2,4GHz / 5 GHz	2,4GHz / 5 GHz	2,4GHz / 5 GHz	2,4GHz / 5 GHz
Configuración Remota	NO	NO	SI	NO
Beamforming	NO	SI	SI	NO
POE	SI	SI	SI	SI
TKIP	SI	SI	SI	NO
Cifrado AES	SI	SI	SI	NO
WPA2	SI	SI	SI	NO
Autenticación RADIUS	NO	SI	SI	NO
Memoria	256 MB	128 MB	256MB	
Precio	300 dólares	700 dólares	850 dólares	650 dólares

Características técnicas de los puntos de acceso

Ponderaciones

Las ponderaciones asignadas a cada característica se deben a:

- Precio: se importante debido a que el ET dispone de recursos económicos reducidos.
- Estándares Wi-Fi: Un dispositivo será más apropiado cuantos más estándares Wi-Fi cumpla, ya que es vital tener un dispositivo que vaya implementando los estándares más recientes.
- Beamforming: es una característica que permite al PA identificar en qué dirección es más eficiente radiar ondas. Esto permite focalizar más la radiación para disminuir áreas de cobertura fuera del PC.
- Autenticación RADIUS: Esta característica es necesaria para poder implementar servidores de autenticación RADIUS.
- Configuración remota: Dota al administrador de red de la capacidad de configurar el punto de acceso sin necesidad de estar físicamente en el punto de acceso.

FIREWALL WIDS/WIPS

	ASA 5505 / Security Plus	ASA 5510 / Security Plus	ASA 5512-X / Security Plus	ASA 5515-X
Velocidad de procesamiento	Hasta 150 Mbps	Hasta 300 Mbps	1 Gbps	1,2 Gbps
Sesiones simultáneas	10 000 /25 000	50 000 /130 000	100 000	250 000
Conexiones por segundo	4000	9000	10 000	15 000
Paquetes por segundo	85 000	190 000	450 000	500 000
Capacidad de procesamiento de redes VPN 3DES/AES5	100 Mbps	170 Mbps	200 Mbps	250 Mbps
Sesiones de usuario VPN de sitio a sitio y cliente IPsec IKEv1	25	250	250	250
Redes VLAN (enlaces troncales habilitados)	20	100	100	100
Switch Integrado (número de puertos)	8 (2 puertos POE)	5	6	6
Puertos Gigabit Ethernet	0	4	6	6
Precio	300 dólares	800 dólares	1600 dólares	1400 dólares

Características técnicas de los Firewall

Ponderaciones

Las ponderaciones asignadas a cada característica se deben a:

- Precio: se le asigna la ponderación más alta debido a que el ET dispone de recursos económicos reducidos. Asignar mayor valor a esta característica no implica una menor calidad ni seguridad, ya que todos los dispositivos han pasado los estándares de seguridad y calidad de la NSA.
- Velocidad: Especifica la velocidad a la que el modelo es capaz de procesar la información
- Paquetes por segundo: especifica el número de paquetes por segundo que atraviesan el firewall. Se considera igual de importante que la velocidad ya que ambas características expresan la rapidez de la información, ya sea de procesamiento o de emisión.
- Redes VLAN: esta característica especifica el número de redes virtuales lógicas (dentro de una misma red física) que el firewall admite. Se considera menos importante que las anteriores características debido a que la implementación de redes VLAN no es obligatoria, aunque sí dota de una gran flexibilidad de cara a futuras modificaciones de la red propuesta.

SERVIDOR DE AUTENTICACIÓN

	Aruba Clearpass Policy Manager	Cisco Integrated Services Engine
Formato	Hardware Software (como Virtual Appliance)	Software (Virtual Appliance)
Autenticación Pasiva	SI	NO
Estándares AAA	RADIUS TACACS PEAP EAP-TLS EAP-TTLS	RADIUS TACACS PEAP EAP-TLS EAP-TTLS
Active Directory	SI	SI
Compatibilidad con otros fabricantes	NO	SI
Precio	1000 dólares (hardware) 2100 dólares (software)	1750 dólares (software)

Características técnicas de los servidores de autenticación

Ponderaciones

Las ponderaciones asignadas a cada característica se deben a:

- Compatibilidad: se refiere a la interoperabilidad de un dispositivo con otro de la misma red. Se considera la característica más importante debido a que la compatibilidad entre dispositivos en una misma red debe ser plena.
- Precio: se considera el precio una característica importante debido al limitado presupuesto del ET. Asignar mayor valor a esta característica no implica una menor calidad ni seguridad, ya que todos los dispositivos han pasado los estándares de seguridad y calidad de la NSA.
- Formato: dentro de esta característica se encuentran servidores de autenticación instalados en dispositivos físico propios (hardware) y servidores que se pueden instalar dentro de otros dispositivos, por lo que vienen en forma de programa informático (software).

Bibliografía

[1] J. Salazar, *Redes Inalámbricas*. Techpedia, 2017.

[2] P. Brenner, "A Technical Tutorial on the IEEE 802.11 Standard," *BreezeCOM*, p. 24, 1997.

[3] C. C. Nacional, "Guía de Seguridad de las TIC Seguridad en Redes Inalámbricas," 2017.

[4] M. D. G. Waliullah, "Wireless LAN Security Threats & Vulnerabilities," *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 1, pp. 176–183, 2014.

[5] M. Rouse, "CIA Triad: confidentiality, integrity, and availability.," 2017. [Online]. Available: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[6] J. C. R, "ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Eva-," pp. 38781–38805, 2007.

[7] C. Systems and S. Jose, "Cisco WLAN 8.0 Common Criteria Security Target," pp. 1–58, 2016.

[8] I. Standard, "ISO/IEC 15408-1 Introduction and general model," 1999.

[9] I. Standard, "ISO/IEC 15408-2 Security functional requirements," 1999.

[10] I. Standard, "ISO/IEC 15408-3 Security assurance requiriments," 1999.

[11] Department of Defense, "Trusted computer system evaluation criteria," *Dep. Def.*, pp. 1–116, 1985.

[12] European Communities, *Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria*, no. June. 1991.

[13] E. Mate Bacic, "The Canadian trusted computer product evaluation criteria," in *[1990] Proceedings of the Sixth Annual Computer Security Applications Conference*, pp. 188–196.

[14] G. de E. Ministerio de la Presidencia, "Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica," *Boe 25 29/01/2010*, 2010.

[15] CCN-STIC, "Guía de Seguridad de las TIC CCN-STIC 804 ENS. Guía de implantación," pp. 1–100, 2017.

[16] SANS, "InfoSec Reading Room tu ho ll r igh," *Inf. Secur.*, 2002.

[17] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, "Guidelines for Media Sanitization," 2014.

[18] "CSfC Components List - NSA.gov." [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/components-list/. [Accessed: 25-Sep-2018].

[19] G. NSA, "CSfC Selections for VPN Gateways," 2018.

[20] G. NSA, "CSfC Selections for VPN Clients," 2018.

[21] G. NSA, “CSfC Selections for Authentication Server,” 2017.

[22] Cisco Systems, “Cisco 2900 Series Integrated Services Routers,” vol. 2, pp. 1–15, 2014.

[23] Cisco, “Cisco ASA 5505 Adaptive Security Appliance for Small Office or Branch Locations Data Sheet - Cisco,” pp. 1–5, 2016.

[24] CCN-STIC, “Guía de Seguridad de las TIC Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación,” 2017.

[25] C. C. Nacional, “SIN CLASIFICAR Taxonomía de referencia para productos de Seguridad TIC,” 2018.

[26] CNET, “Product reviews, how-tos, deals and the latest tech news - CNET,” 2018. [Online]. Available: https://www.cnet.com/. [Accessed: 10-Oct-2018].

[27] R. Acero, *Gestión de Riesgos*. Zaragoza: CUD, 2017.

[28] C. C. Nacional, “Guía de Seguridad de las TIC Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC,” 2017.