GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 816

Seguridad en Redes Inalámbricas

Julio 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

NIPO: 785-17-067-8

Fecha de Edición: julio de 2017
ISDEFE ha participado en la realización y modificación del presente documento y sus anexos, que ha sido financiado por Ministerio de Hacienda y Función Pública.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Una Red Inalámbrica consiste en un grupo de dispositivos "sin cable" (también llamados "dispositivos inalámbricos" o "dispositivos wireless") que se comunican entre sí a través de ondas electromagnéticas y sin necesidad, por lo tanto, de cableado.

Las Redes de Área Local Inalámbricas, normalmente se implementan como una extensión de la Red de Área Local cableada de la organización (LAN), para proporcionar movilidad a los usuarios, que no tendrán que estar en un puesto concreto como requiere una conexión física a la red.

El uso de redes inalámbricas está cada vez más extendido por las múltiples ventajas que ofrecen. Entre ellas, el ahorro de costes que supone no tener que realizar un cableado entre los nodos de la red, como en las redes cableadas tradicionales. Otra de las ventajas es permitir la movilidad es la no necesidad de estar en un sitio o puesto concreto para poder conectarse a los recursos de la organización.

Hoy en día, todos los dispositivos (ordenadores, teléfonos inteligentes, *smart TV*, etc.) incorporan la capacidad de conexiones inalámbricas de forma nativa.

Siendo evidentes las ventajas que ofrece la tecnología inalámbrica (también llamada "tecnología wireless"), hay que tener muy en cuenta los riesgos adicionales que añaden a los ya existentes en las redes cableadas. Estos riesgos deben tratarse de forma específica, e implementar las medidas de seguridad apropiadas que garanticen la seguridad de las comunicaciones que se llevan a cabo a través de las redes inalámbricas.

2. OBJETO

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para la implementación del Esquema Nacional de Seguridad (CCN-STIC-800), siendo de aplicación para la Administración Pública y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.

El objeto del documento es proporcionar una guía de buenas prácticas que ayude a las organizaciones a mejorar la seguridad de sus redes inalámbricas. Para ello, se indicarán los requisitos específicos del ENS que deben tenerse en cuenta en la implantación y operación de redes inalámbricas.

Las pautas que se establecen son de carácter general, de forma que puedan resultar de aplicación a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. Por ello, es de esperar que cada organización las particularice para adaptarlas a su entorno singular.

3. ALCANCE

Esta guía se refiere a las Redes de Área Local inalámbricas (también llamadas WLAN, *Wireless Local Area Networks* o Redes Wi-Fi) basadas en el estándar IEEE 802.11. Quedan excluidas de esta guía otro tipo de redes inalámbricas, como las redes

inalámbricas de área metropolitana (WiMAX) basadas en el estándar IEEE 802.16, las redes inalámbricas personales (WPAN) basadas en el estándar IEEE 802.15, etc.

Los mecanismos y protocolos de seguridad de las redes inalámbricas que se van a tratar a lo largo de esta guía, no incluyen WEP (Wireless Equivalent Privacy) ni ninguna de sus variantes (WEP2, WEP Plus o WEP dinámico). WEP, creado como método para asegurar la privacidad del estándar original IEEE 802.11, tiene a día de hoy múltiples vulnerabilidades de seguridad descubiertas y ha sido superado por otros protocolos más seguros como WPA (Wi-Fi Protected Access) y WPA2 (Wi-Fi Protected Access). Se considera, por lo tanto, que WEP no debe ser utilizado a día de hoy en ningún caso, como protocolo de seguridad de una red inalámbrica.

Se han desarrollado numerosas tecnologías inalámbricas en los últimos años, y siguen desarrollándose nuevas actualmente. Por lo tanto, las recomendaciones realizadas en la presente guía quedan sometidas a una continua revisión dado el constante avance tecnológico, así como a la aprobación de nuevos estándares y la aparición de nuevas vulnerabilidades.

En esta guía no se referencia ninguna solución inalámbrica concreta de fabricantes. Se recomienda consultar otras guías y documentación con información detallada de la instalación, configuración y administración de redes inalámbricas basadas en equipos y soluciones concretas de fabricantes, a la hora de proceder a la selección de una solución inalámbrica.

4. REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)

4.1 Definición y Generalidades

Se puede definir de forma general una red inalámbrica, como aquella formada por dispositivos con capacidades inalámbricas que se comunican entre sí a través de ondas electromagnéticas y sin necesidad de cableado (wireless).

Existen muchos tipos de redes inalámbricas que difieren en arquitectura, tecnología, estándar de comunicación, etc. La presente guía se refiere en exclusiva a las Redes de Área Local Inalámbricas, también conocidas como WLAN (Wireless Local Area Network) o Redes Wi-Fi. Estas redes inalámbricas se basan en el estándar IEEE 802.11, y será a este tipo, al que se hará referencia a partir de ahora como redes inalámbricas.

Los componentes principales de una red inalámbrica son:

- Dispositivos cliente. Son los equipos de usuario que solicitan conexión a la red inalámbrica para realizar la trasferencia de datos de usuario. Pueden ser ordenadores portátiles, teléfonos inteligentes (*smartphones*), *Smart TV*, etc.
- Puntos de Acceso (*Access Points*, AP). Son dispositivos que forman parte de la infraestructura inalámbrica, y se encargan de conectar los dispositivos cliente entre sí, o con la infraestructura de red cableada de la organización. A partir de ahora se hará referencia a estos dispositivos como AP.

Existen dos topologías de red inalámbrica: modo Ad Hoc y modo Infraestructura. En el modo Ad Hoc no existen los AP y los dispositivos cliente se comunican entre sí directamente. Este tipo de redes inalámbricas no entran dentro del alcance de esta guía, que se referirá únicamente al modo Infraestructura, en la que se utilizan AP para conectar los dispositivos cliente entre sí o con el sistema de distribución de red.

Las siguientes figuras muestran un diagrama general de las redes inalámbricas en modo Ad Hoc y modo Infraestructura.

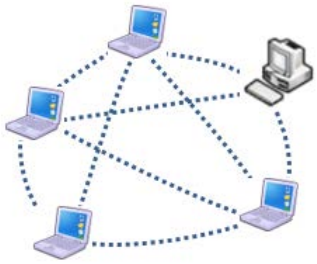

Figura 1. Diagrama de una red inalámbrica modo Ad Hoc.

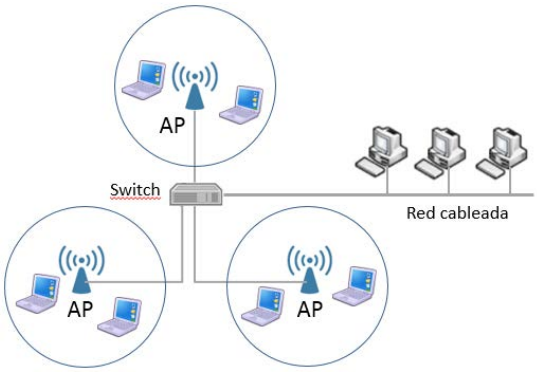

Figura 2. Diagrama de una red inalámbrica modo Infraestructura.

Los AP pueden ser de dos tipos: AP inteligentes y AP simples. Los primeros realizan de forma independiente todas las tareas de cifrado y gestión de los dispositivos cliente conectados a ellos. En el caso de los segundos, AP simples, el cifrado y la política de seguridad se procesan de forma centralizada en un controlador de la infraestructura inalámbrica. La ventaja de una gestión centralizada, es que no se deposita en cada uno de los AP las claves criptográficas.

Los riesgos de las redes inalámbricas son los mismos que afectan a las redes cableadas sumados a los riesgos específicos de un entorno inalámbrico. Existen multitud de fuentes de información donde se describen las amenazas y riesgos de las redes inalámbricas. En la siguiente lista se incluyen algunos de los más representativos.

- *Eavesdropping*. Cuando un individuo no autorizado utiliza alguna herramienta (normalmente antenas de gran alcance) para capturar de forma pasiva el tráfico

inalámbrico. Este tráfico le sirve para espiar información (en caso de que no vaya cifrada) y para detectar patrones de comportamiento.

- Denegación del Servicio (DoS). Cuando la infraestructura inalámbrica queda incapacitada para ofrecer el servicio. Por ejemplo, cuando un individuo no autorizado inyecta peticiones masivas de asociación a los AP dejándolos incapacitados para responder a las peticiones de los clientes legítimos.

- *Man-in-the-middle*. Cuando un individuo no autorizado se coloca en medio de la comunicación inalámbrica entre emisor y receptor, suplantando a una de las partes y haciendo creer a la otra que está hablando con el comunicante legítimo. El más conocido de estos ataques es el de *Rogue AP* (falso AP), que se produce cuando un individuo no autorizado logra suplantar a un AP legítimo con uno falso de las mismas características y mayor potencia de señal, haciendo que los clientes soliciten asociación en primer lugar al *Rogue AP*. A partir de aquí, se pueden ejecutar multitud de ataques posteriores (captura de credenciales, de tráfico, etc.).

- Ataques por fuerza bruta. Consisten en métodos para averiguar las claves criptográficas probando todas las combinaciones posibles. En caso de que la red inalámbrica no utilice algoritmos criptográficos y claves con la suficiente fortaleza, se pueden realizar este tipo de ataques ya que existen multitud de herramientas gratuitas que lo permiten.

- *MAC Spoofing*. Los AP pueden tener configurada una lista de direcciones MAC permitidas. Sin embargo, un individuo no autorizado puede suplantar una dirección MAC autorizada para lograr el acceso.

- Acceso de dispositivos no autorizados que están conectados al dispositivo cliente autorizado y que a través de él pueden lograr acceso a la red inalámbrica y por ende a la red cableada de la organización pudiendo introducir software dañino.

4.2 IEEE 802.11 - 802.11i

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura o modelo OSI (capa física y capa de enlace de datos), especificando sus normas de funcionamiento en una red de área local inalámbrica (WLAN).

Dentro del estándar IEEE 802.11, existen múltiples revisiones que representan una expansión o variación del estándar original. Estas revisiones se diferencian entre sí en aspectos como las bandas de frecuencia en las que operan (normalmente entre los 2,4 GHz y los 5 GHz), los métodos de codificación que utilizan, el ancho de banda que ofrecen, mejoras en rendimiento, mantenimiento, etc.

El protocolo que implementaba los mecanismos de seguridad especificados en el estándar original de IEEE 802.11, se denomina WEP (Wired Equivalent Privacy). Este protocolo ha sido declarado inseguro debido a las múltiples vulnerabilidades detectadas, y se considera por lo tanto inadecuado para redes inalámbricas que requieran un mínimo de seguridad.

A raíz de las vulnerabilidades de WEP, se desarrolló IEEE 802.11i, que es una enmienda al estándar original 802.11 y que añade nuevos y más robustos mecanismos de seguridad que contrarrestan las vulnerabilidades WEP.

Mientras se ratificaba la versión definitiva de IEEE 802.11i (junio 2004), y con el objetivo de solventar algunos de los problemas de seguridad de WEP sin necesidad de sustituir el hardware inalámbrico, se desarrolló un protocolo de seguridad que implementaba un subconjunto de las especificaciones 802.11i. Este protocolo fue aprobado por la Alianza Wi-Fi bajo el nombre de WPA (Wi-Fi Protected Access).

Posteriormente, una vez ratificado 802.11i, la Alianza Wi-Fi introdujo WPA2 (Wi-Fi Protected Access 2) que ya implementa el estándar IEEE 802.11i al completo. WPA2 no es compatible, en la mayoría de los casos, con en el hardware inalámbrico WEP, ya que este hardware no soporta la carga computacional que suponen las operaciones de cifrado del algoritmo AES, que es el algoritmo criptográfico central de WPA2.

WPA y WPA2 tienen dos modos de implementación: Personal, destinado al uso en redes personales pequeñas y *Enterprise*, destinado al uso en organizaciones. Ambas implementaciones difieren, principalmente, en los mecanismos de autenticación y distribución de claves. Personal utiliza el mecanismo de claves pre-compartidas PSK (Pre-shared Keys). Enterprise utiliza el mecanismo de autenticación 802.1X, con el empleo de un Servidor de Autenticación (AS), normalmente, RADIUS. En el Anexo D se indican más detalles sobre estos mecanismos de autenticación y distribución de claves.

IEEE 802.11i introduce el concepto de redes seguras RSN (Robust Security Networks), que son aquellas redes inalámbricas que solo permiten la creación de asociaciones de red seguras RSNA (Robust Security Network Associations).

Las RSNA son asociaciones lógicas establecidas entre los participantes de la comunicación 802.11i, que cuentan con un proceso automático de generación y distribución de claves criptográficas (llamado protocolo de negociación en 4 pasos, 4-Way Handshake).

Solo se puede garantizar una seguridad robusta cuando todos los dispositivos de la red emplean RSNA. Las redes que permiten la creación de asociaciones no RSNA y RSNA, son redes en transición a redes robustas (denominadas TSN, Transition Security Networks), y constituyen métodos temporales para proporcionar seguridad, mientras la organización migra su red a una RSN, basada en RSNA.

El establecimiento de una RSNA se realiza en 5 Fases, como se muestra en la siguiente figura.

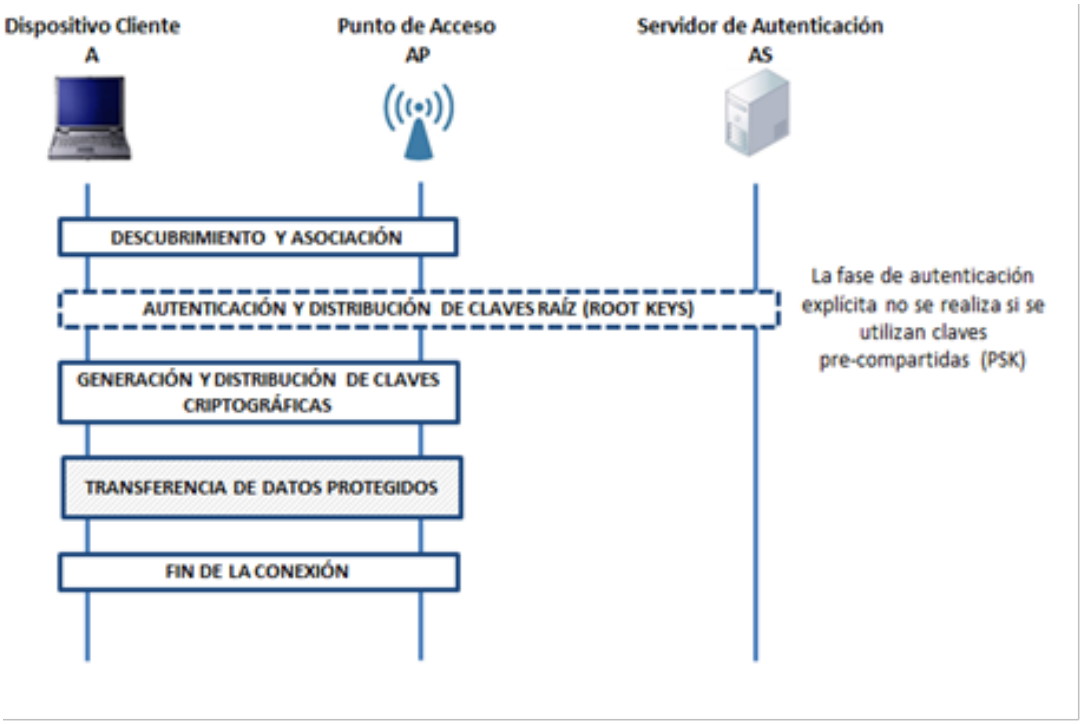

Figura 3. Fases en el establecimiento de una RSNA.

Fase 1. Descubrimiento y Asociación.

El dispositivo cliente solicita asociación al AP para conectarse a la red inalámbrica. En esta fase se negocia la *Suite* criptográfica y los tipos de autenticación.

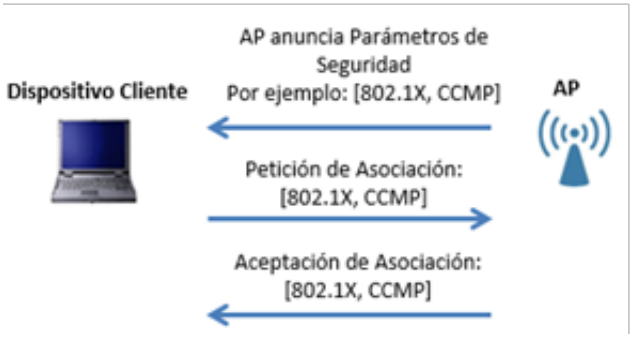

Figura 4. Fase Descubrimiento y asociación.

Fase 2. Autenticación y distribución de claves raíz.

Una vez que la asociación entre el dispositivo cliente y el AP se completa, se inicia la fase de autenticación y distribución de las claves raíz. Se realiza, por un lado, la autenticación mutua, cuyo objetivo es probar que el dispositivo cliente es legítimo y tiene autorización para conectarse a la red, y que la red a su vez, es también legítima y el usuario no se está conectando a una red falsa (por ejemplo, a un *rogue AP*). Por otro lado, se lleva a cabo la distribución de las claves raíz (*root keys*) que se utilizan para la

generación de todas las demás claves criptográficas de la comunicación (jerarquía de claves).

El proceso de autenticación se puede llevar a cabo de dos formas:

- A través del modelo de control de acceso basado en puerto definido en el estándar IEEE 802.1X y empleando el protocolo EAP (Extensible Authentication Protocol).
- A través del método de claves pre-compartidas PSK. En este caso no se realiza ningún proceso de autenticación explícito, ya que la mera posesión de una misma clave pre-compartida por parte del dispositivo cliente y el AP, sirve como prueba de autenticación.

La autenticación a través del modelo IEEE 802.1X, define tres entidades en el proceso: el suplicante (dispositivo cliente), el autenticador (AP) y el Servidor de Autenticación (AS). El proceso de autenticación se lleva a cabo entre el dispositivo cliente y el Servidor de Autenticación (AS). El AP únicamente realiza las funciones de encapsulado y transmisión de los mensajes entre uno y otro. Este proceso de autenticación se implementa a través del protocolo EAP, que en función del método empleado (método EAP) puede realizar la autenticación mediante diversos mecanismos: contraseñas estáticas, contraseñas dinámicas, certificados, etc. Se puede consultar más detalle sobre EAP y los métodos EAP en el Anexo D.

802.1X introduce el concepto de puertos controlados y puertos no controlados. El tráfico de autenticación EAP, fluye a través de los puertos no controlados. El resto del tráfico (no EAP) fluye por los puertos controlados, los cuales estarán bloqueados hasta que la autenticación finalice con éxito y, además, se haya generado y distribuido el material de claves criptográficas para la protección de la comunicación (siguiente fase). Se puede consultar más detalle sobre 802.1X en el Anexo D.

La siguiente figura representa los pasos generales del proceso de autenticación 802.1X/EAP. Se pueden usar varios protocolos entre el AP y el Servidor de Autenticación (AS), en este ejemplo se emplea RADIUS, que es uno de los más comunes.

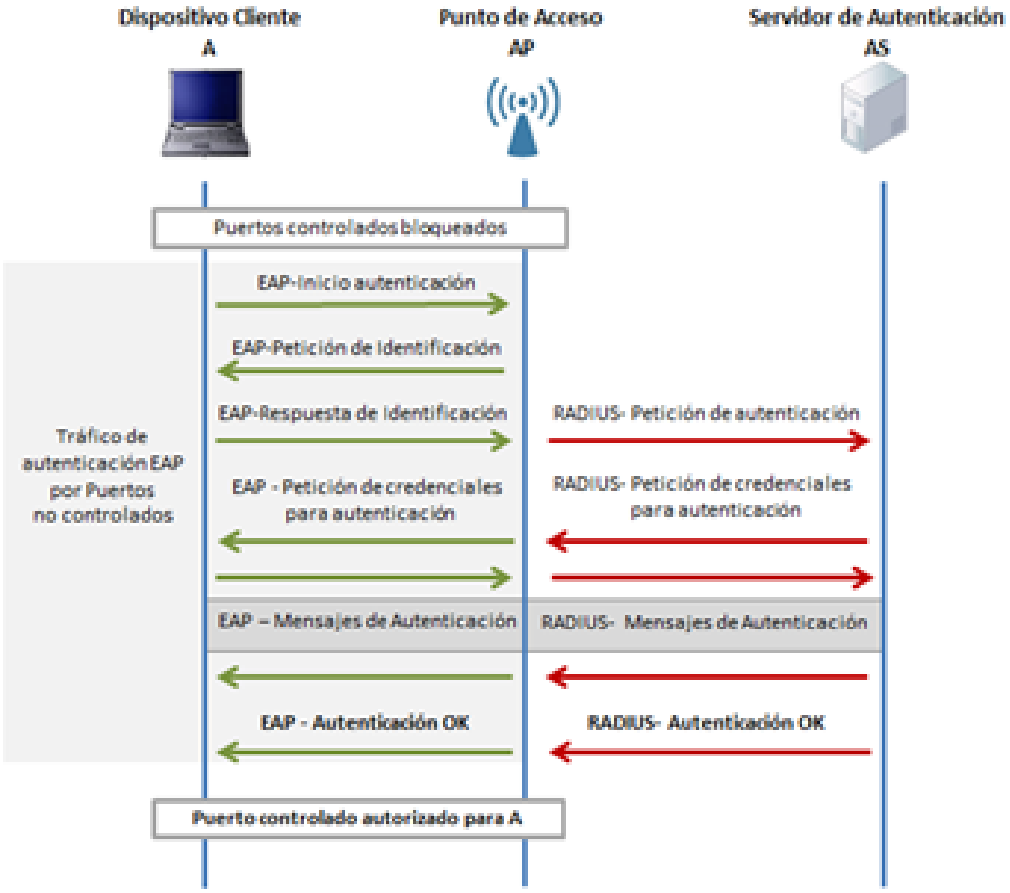

Figura 5. Fase Autenticación y distribución de claves raíz (root keys).

Durante este proceso de autenticación se genera y distribuye la clave raíz AAAK (Authentication, Authorization and Accounting Key), también llamada MSK (Master Session Key) al dispositivo cliente. Esta clave se deriva en el AS a partir de material de claves exportado por el método EAP empleado. El modo de llevar a cabo esta tarea no viene explícitamente indicado en IEEE 802.11i, y queda a disposición del tipo de implementación. Lo que sí indica el estándar es que el canal para la distribución de la MSK del AS al AP debe ser seguro y proporcionar protección de confidencialidad e integridad para evitar el compromiso de la clave.

Fase 3. Generación y distribución de las claves criptográficas.

Una vez finalizada la fase de autenticación, el dispositivo cliente y el AP disponen de las claves raíz (root keys) a partir de las cuales, a través del proceso de generación y distribución de claves, se obtiene el material de claves necesario para la protección de la comunicación.

Para ello, el proceso de generación y distribución de claves emplea dos tipos de negociación: la negociación en 4-etapas (4-way handshake) y la negociación de grupo (Group handshake). Ambas negociaciones utilizan mecanismos de cifrado y de protección de integridad para el material criptográfico distribuido.

Tras la finalización de esta fase, se considera completada la autenticación mutua, y los puertos controlados de 802.1X son desbloqueados definitivamente, permitiendo el tráfico de datos de usuario.

En el Anexo B se describen con detalle las jerarquías de clave y el proceso de generación y distribución de las mismas.

Fase 4. Transferencia de datos protegidos.

Esta es la fase de trasferencia de datos de usuario. La comunicación irá protegida a través de los algoritmos criptográficos de la suite criptográfica negociada y acordada en la primera fase de descubrimiento y asociación. Estos algoritmos harán uso de las claves criptográficas generadas y distribuidas en la fase anterior.

Hay dos suites criptográficas que se pueden emplear: TKIP y CCMP. En una RSNA es obligatorio el soporte de CCMP y opcional el de TKIP.

TKIP (Temporal Key Integrity Protocol) es una suite criptográfica creada para mejorar el protocolo de seguridad WEP sin necesidad de sustituir el hardware de los equipos inalámbricos (solo es necesaria una actualización del software o del firmware).

TKIP utiliza el algoritmo de cifrado RC4 y el mecanismo de integridad Michael MIC (Message Integrity Code). Ambos algoritmos tienen a día de hoy vulnerabilidades ampliamente conocidas, por lo que no se recomienda el uso de TKIP cuando los requisitos de seguridad son relevantes.

CCMP (Counter Mode with Cipher Block Chaining MAC Protocol). Es otra suite criptográfica también desarrollada para solventar los problemas de seguridad de WEP. Sin embargo, CCMP requiere la actualización del hardware inalámbrico debido a la elevada carga computacional del algoritmo de cifrado empleado (AES), y ofrece mayor nivel de protección.

CCMP es un mecanismo de encapsulación de datos basado en CCM (Counter Mode with CBC-MAC), que combina dos técnicas: CTR para la protección de confidencialidad y CBC-MAC para la protección de la integridad y autenticidad.

En el Anexo C se describen con detalle estas dos suites criptográficas.

Fase 5. Fin de la conexión.

La última fase será la de terminación de la conexión. En esta fase se borra la asociación entre el AP y el dispositivo cliente: el AP desautentica al dispositivo cliente, se eliminan todas las claves criptográficas empleadas en la conexión, y el puerto controlado 802.1X pasa de nuevo a estado bloqueado, de forma que ya no podrá pasar a través de él ningún tráfico de usuario.

4.3 Servicios de seguridad de la RSNA.

La siguiente figura muestra un resumen de los servicios de seguridad proporcionados por la RSNA en las distintas fases.

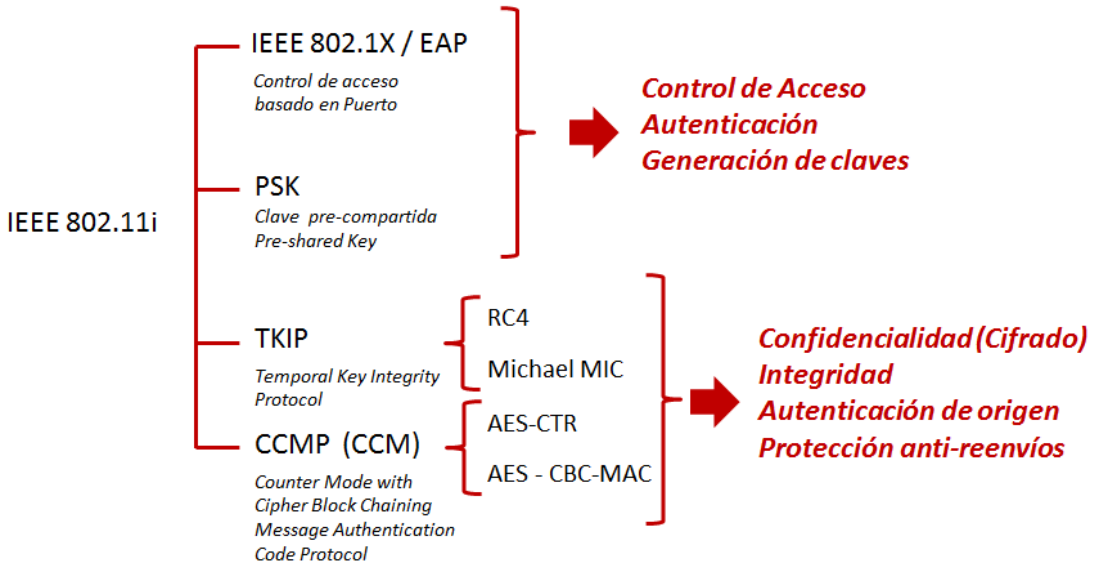

Figura 6. Servicios de seguridad proporcionados por una RSNA.

4.4 802.11w Protección de las tramas de gestión.

IEEE 802.11w (Protected Management Frames, PMF) fue publicado en 2009 como una adición a 802.11i, para dar cobertura de seguridad al tráfico de gestión de la conexión.

802.11w proporciona mecanismos de seguridad que logran extender la protección que se obtiene con 802.11i, de forma que no solo el tráfico de datos de usuario sea protegido, sino también las tramas de gestión intercambiadas durante la conexión.

Proporciona, por lo tanto, protección de confidencialidad, integridad, autenticidad de origen y protección anti-reenvíos para las tramas de gestión. Utiliza la misma suite criptográfica negociada para la protección de datos, TKIP o CCMP.

Las RSN 802.11i utilizarán un bit que representa la activación o no, de la capacidad de protección de las tramas de gestión.

5. MEDIDAS DE SEGURIDAD DEL ENS

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado a su vez por el Real Decreto 951/2015, de 23 de octubre (en adelante, ENS), es de aplicación por las Administraciones Públicas y tiene como objetivo asegurar el acceso, confidencialidad, integridad, autenticidad, trazabilidad, disponibilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos que gestionen el ejercicio de sus competencias.

Para el cumplimiento de los objetivos previstos en el ENS se definen y valoran los fundamentos que van a permitir categorizar sistemas y servicios. Esto supone que en función de la categoría deberán realizarse unas implementaciones de seguridad u otras, exigiéndose unos requisitos más restrictivos o menos.

La red inalámbrica desde el punto de vista del ENS debe considerarse como un sistema de información más, compuesto por elementos hardware y software y cuya misión y objetivo es dar acceso a recursos, información y servicios de la organización.

En este sentido, como sistema de información estará bajo el ámbito de aplicación del ENS, y le afectarán las medidas de seguridad especificadas en su Anexo II, que están condicionadas a la categoría del mismo (Artículo 43), la cual será calculada en base a la valoración del nivel de seguridad en cada dimensión (Anexo I).

Para determinar la categoría de la red inalámbrica como sistema de información dentro del ENS, habrá que tener en cuenta la criticidad de los recursos y servicios de la organización con los que se establece la comunicación a través de ella, y la criticidad de la información que fluye a través de sus conexiones.

Esta criticidad, desde el punto de vista del ENS, se mide atendiendo a una serie de criterios generales aplicables en cada una de las dimensiones de seguridad: integridad [I], confidencialidad [C], autenticidad [A], trazabilidad [T] y disponibilidad [D]. Estos criterios se encuentran definidos en la guía CCN-STIC-803 Esquema Nacional de Seguridad valoración de los sistemas.

Será la valoración de las consecuencias de un impacto negativo sobre la seguridad que afecte a las dimensiones de seguridad de estos servicios, recursos e información, lo que determinará la categoría de la red inalámbrica con sistema de información, pudiendo ser de categoría BÁSICA, MEDIA o ALTA.

Un ejemplo sencillo para ilustrar la forma de llevar a cabo esta valoración, con objeto de categorizar la red inalámbrica como sistema de información incluido en el ámbito de aplicación del ENS, es el que se describe a continuación.

Supongamos que la Administración A desea implementar, como mejora del servicio al ciudadano, una red inalámbrica en sus instalaciones, concretamente en las Salas de espera y en la Recepción. Esta red inalámbrica proporcionará un acceso gratuito de los ciudadanos a ciertos servicios públicos de información ofrecidos por la Administración.

En este ejemplo, los servicios y la información a la que se accede a través de la red inalámbrica son de carácter público, por lo que el nivel exigido de confidencialidad [C] en las comunicaciones, es BAJO. Sin embargo, la información proporcionada por la Administración debe ser auténtica y verídica, y en caso de ser objeto de manipulación por parte de individuos no autorizados, el perjuicio causado a la Administración podría ser grave, por lo que el nivel exigido de integridad [I] y autenticidad [A] es MEDIO. Respecto al nivel de disponibilidad [D] podría considerarse MEDIO, ya que, aunque no supone un perjuicio grave para los ciudadanos el no disponer de este acceso inalámbrico, el hecho de ofrecer un servicio que no se encuentra disponible sí puede dañar gravemente la imagen de la Administración. Finalmente, la trazabilidad [T] en este ejemplo es menos importante, ya que es un servicio público ofrecido a todos los

ciudadanos, por lo que se puede considerar esta dimensión de nivel BAJO. Con esto, la categoría de esta red inalámbrica a implantar por la Administración, sería MEDIA.

La valoración de la red inalámbrica como sistema de información es un proceso mucho más complejo que este, que únicamente sirve como ejemplo meramente ilustrativo, y para llevarlo a cabo la organización podrá apoyarse en las recomendaciones de la guía CCN-STIC-803 Esquema Nacional de Seguridad valoración de los sistemas.

Por lo tanto, considerando la red inalámbrica como sistema de información bajo el ámbito de aplicación del ENS, se verá afectada por todas las medidas de seguridad especificadas en el Real Decreto, en mayor o menor grado, dependiendo de la categorización.

El objeto de la presente guía es señalar los aspectos específicos y diferenciados de una red inalámbrica, que deben añadirse a la implementación "estándar" de las medidas de seguridad, de forma que la organización pueda contemplarlos a la hora de llevar a cabo la planificación, diseño e implantación de su red inalámbrica. Esta guía, por tanto, no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean específicas para una red inalámbrica y su implementación no se distinga de la que debería llevarse a cabo para cualquier otro sistema de información. Será en la guía CCN-STIC-804 Implantación de medidas ENS donde se podrá consultar el modo de implementación de estas medidas.

En el Anexo A se incluye una tabla resumen con los aspectos específicos de aplicación a una red inalámbrica, en función de la valoración de sus dimensiones de seguridad y de su categoría BÁSICA, MEDIA, ALTA. Se indica en la tabla la medida del ENS que corresponde a cada uno de los aspectos, y en qué apartado se detallan estas medidas, tanto en la presente guía, como en la guía CCN-STIC-804.

5.1 Medidas Organizativas [org]

Categoría Básica / Media / Alta

La red inalámbrica deberá incluirse en la Normativa, Procedimientos y Procesos de la organización.

5.1.1 Normativa [org.2]

Dentro de la Normativa **[org.2]**, deberá existir una Política de seguridad de la red inalámbrica, que junto con las decisiones que tome la organización para forzar su cumplimiento, será la base para todas las medidas de seguridad.

Dentro de esta Política deberán incluirse, al menos, los siguientes aspectos:

- Uso aceptable de la red inalámbrica. Aspectos relacionados con el uso apropiado e inapropiado de la red inalámbrica y las medidas disciplinarias correspondientes. Se indicará lo que se puede hacer a través de la red inalámbrica y a qué recursos se puede acceder. Se incluirán los requisitos de autenticación de

usuario para el acceso a la red inalámbrica, requisitos sobre los dispositivos cliente, requisitos específicos de la conexión, etc.

- Requisitos de seguridad de la infraestructura inalámbrica. Aspectos relativos a la asignación de roles y responsabilidades para la dirección, gestión y explotación de la red inalámbrica; tipo de información que podrá y que no podrá ser transmitida por la red inalámbrica; requisitos de seguridad física para los componentes de la infraestructura; configuración de seguridad de los elementos de la infraestructura; mecanismos de protección de la comunicación inalámbrica, incluyendo requisitos sobre cifrado, autenticación y gestión de claves criptográficas; etc.

- Requisitos de seguridad de los dispositivos cliente. Aspectos relacionados con las condiciones de uso permitido de los dispositivos clientes, es decir, cómo, cuándo y dónde se pueden utilizar para acceder a la red inalámbrica; tipos de dispositivos cliente autorizados; configuraciones de seguridad, etc.

- Evaluaciones de seguridad periódicas. Aspectos relacionados con el alcance y periodicidad de las auditorías de seguridad que revisan el estado global de la seguridad de la infraestructura inalámbrica.

5.1.2 Procedimientos [org.3]

También deberán existir los Procedimientos **[org.3]** correspondientes a la red inalámbrica, que serán acordes con los procedimientos relativos a la infraestructura general de la organización. Algunos de estos procedimientos son los siguientes.

- Operación y mantenimiento de la infraestructura inalámbrica. Se incluirán aspectos relativos a la actualización de parches, alta de nuevos dispositivos y usuarios, instalación y configuración de AP, actualización y gestión del inventario, etc.

- Gestión de eventos y registros de log. Se incluirán aspectos como la información a registrar, cuánto tiempo debe conservarse, cada cuánto tiempo debe revisarse, envío de copias de los eventos a servidores centralizados de gestión, etc.

- Gestión y respuesta a incidentes de seguridad en la red inalámbrica. Se analizará cómo los componentes de la infraestructura inalámbrica pueden verse afectados por los incidentes, para documentar las actividades que den respuesta a estos incidentes de forma efectiva y eficiente.

- Respuesta y actuación frente a pérdidas o robos de dispositivos inalámbricos.

- Monitorización de seguridad continua, que atienda a los ataques y las vulnerabilidades de la red inalámbrica.

- Auditorías periódicas de la infraestructura inalámbrica. Se definirá la periodicidad y alcance de las auditorías, cuyo objetivo será verificar que la red cumple con la política de seguridad de la organización.

5.1.3 Procesos de Autorización [org.4]

Finalmente, deberán elaborarse los Procesos de Autorización **[org.4]** necesarios para atender las necesidades de la red inalámbrica relativas a autorizaciones. Al menos los siguientes:

- Autorización de usuarios y dispositivos para el uso de la red inalámbrica.
- Autorización para el despliegue de nuevos componentes de la infraestructura inalámbrica (por ejemplo, AP).

5.2 Medidas Operacionales [op]

Categoría Básica / Media / Alta

5.2.1 Arquitectura de Seguridad [op.pl.2]

La Arquitectura de Seguridad **[op.pl.2]**, tal y como se indica en la guía CCN-STIC-804 (Apartado 4.1.2), esta medida es básicamente documental y descriptiva de cómo es la arquitectura de la red inalámbrica y su sistema de gestión.

Además de las consideraciones indicadas en la citada guía, los aspectos específicos de una red inalámbrica relacionados con la arquitectura de seguridad, que se deben tener en cuenta, son los siguientes:

- Cobertura de los puntos de acceso antes de ubicarlos físicamente, con objeto de minimizar la radiación de estos fuera del perímetro controlado por la organización. La ubicación física se deberá combinar con la configuración de las antenas de los AP para controlar la dirección y potencia de radiación y, por lo tanto, la cobertura final de la red inalámbrica.
- La red inalámbrica deberá ser modo infraestructura. No son recomendables las redes *Ad Hoc*. En la red tipo infraestructura, la configuración de seguridad se puede estandarizar y desplegar a los AP. En la red *Ad Hoc* los dispositivos cliente se conectan entre sí directamente y ejercen diversos roles de configuración más difíciles de controlar.

5.2.2 Autenticación [op.acc.5]

Dentro del diseño de la autenticación de una red inalámbrica, hay que determinar los aspectos que se definen a continuación. Indicar que estos aspectos se detallan en el apartado 4.2 y en el Anexo D de la presente guía.

a) Tipo de autenticación de la red inalámbrica. El estándar IEEE 802.11i (RSN) permite utilizar dos tipos de autenticación: basado en claves pre-compartidas (PSK) y basado en protocolo 802.1X/EAP.

b) Mecanismos de autenticación. Mecanismos empleados para la autenticación del servidor (AS) y para la autenticación del cliente (en caso de realizar autenticación mutua). En general, el servidor se autentica frente el cliente a través

de certificado, mientras que para la autenticación del cliente se podrán usar múltiples mecanismos (contraseñas, *tokens*, biometría, etc.) o una combinación de ellos.

c) Método EAP. EAP es el protocolo encargado del transporte, encapsulado y seguridad del proceso de autenticación. Existen diferentes métodos EAP con distintos mecanismos de autenticación y con distintas características de seguridad.

En la siguiente figura se muestra un diagrama que ilustra la selección de estos tres aspectos de autenticación que se describen más adelante.

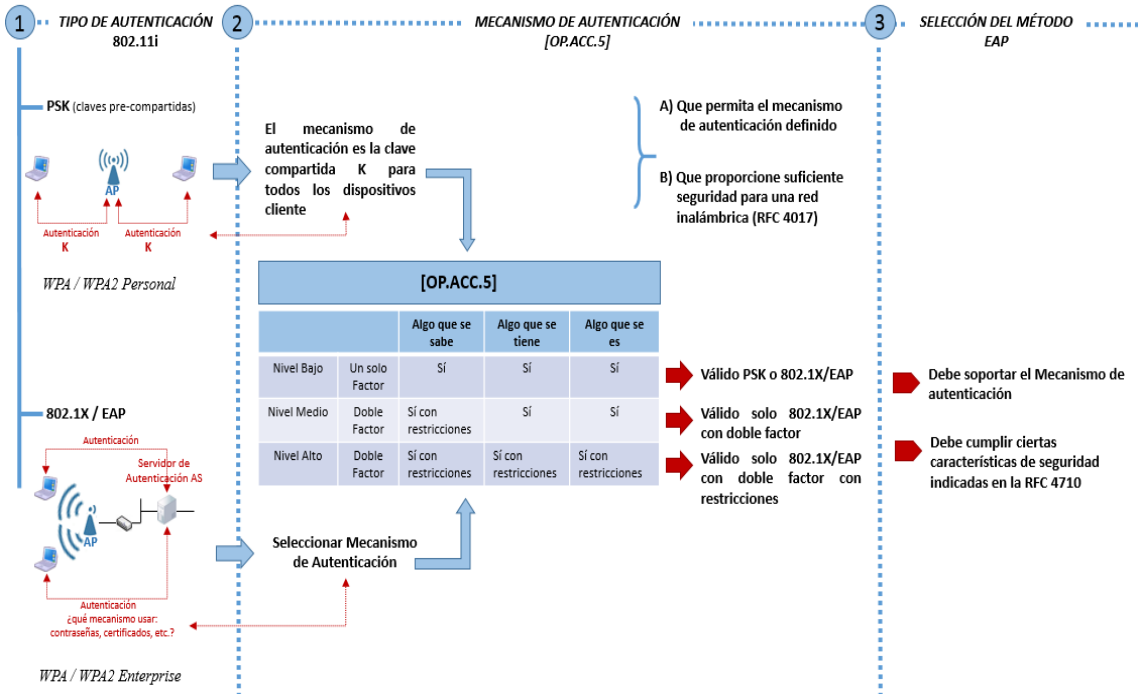

Figura 7. Aspectos de autenticación de la red inalámbrica.

Selección del Tipo de autenticación:

- Clave pre-compartida (PSK). Este método implica que solo existe una única clave para la conexión a la red inalámbrica. Esta clave es compartida por todos los equipos y todos los usuarios.

Este método tiene importantes defectos de seguridad, principalmente, la distribución y almacenamiento de la PSK, la falta de autenticación mutua efectiva, y la falta de trazabilidad.

No obstante, si el nivel de seguridad y las condiciones de la implementación lo permiten, es un método que no requiere infraestructura y es sencillo de implementar.

La autenticación por PSK solo será aceptable, por lo tanto, cuando las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen todas ellas un nivel Bajo.

Este tipo de autenticación es utilizado por WPA y WPA2 en sus implementaciones Personal.

- Basado en 802.1X/EAP. Este es un método de autenticación más seguro, ya que permite un proceso explícito de autenticación mutua, en el que cada cliente dispondrá de sus propias credenciales de acceso, proporcionando trazabilidad. Sin embargo, este método es más complejo y requiere de una infraestructura de servidor/es de Autenticación (AAA).

La autenticación basada en 802.1X/EAP será el tipo de autenticación requerido, cuando las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen cualquiera de ellas un nivel Medio o Alto.

Este tipo de autenticación es utilizado por WPA y WPA2 en sus versiones Enterprise.

Selección del Mecanismo de autenticación:

La medida de seguridad del ENS **[op.acc.5]** establece los requisitos sobre los mecanismos de autenticación en función del nivel de las dimensiones de seguridad: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T].

En el caso de que las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen todas ellas un nivel Bajo, podrá utilizarse la autenticación de un solo factor. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel mínimo de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta), y deberá existir y aplicarse una Política de contraseñas que indique, además de los requisitos de las contraseñas, el tiempo mínimo de renovación, los intentos máximos permitidos, etc.

En el caso de que alguna las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] o todas ellas, alcancen un nivel Medio y ninguna alcance nivel Alto, deberá utilizarse la autenticación de doble factor. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel Medio de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta), y deberá existir y aplicarse una Política de contraseñas con exigencias de nivel Medio sobre las mismas, su renovación, intentos máximos permitidos, etc.

En el caso de que alguna de las dimensiones [I C A T] alcance un nivel Alto, deberá utilizarse la autenticación de doble factor. Este factor podrá ser de cualquier tipo: contraseñas o claves concertadas, *tokens*, biometría, etc. En caso de uso de contraseñas o claves concertadas, estas deberán responder a un nivel Alto de fortaleza (frente a ataques de adivinación, diccionario y fuerza bruta), y deberá existir y aplicarse una Política de contraseñas exigencias de nivel Alto sobre las mismas, su renovación, intentos máximos permitidos, etc. En caso de uso de “algo que se tiene”,

deberán utilizarse elementos criptográficos hardware que hagan uso de Algoritmos acreditados por el Centro Criptológico Nacional (CCN).

Selección del Método EAP:

El método EAP debe seleccionarse, principalmente, en función de dos aspectos:

- Mecanismo de autenticación seleccionado (en el paso anterior), ya que éste deberá ser soportado por el método EAP.
- Características de seguridad requeridas por la red inalámbrica, ya que no todos los métodos EAP proporcionan las mismas características de seguridad (ver tabla 5 del Anexo D).

Podrá seleccionarse cualquier método EAP o ningún método EAP y realizar la autenticación empleando otros protocolos (como PAP, CHAP, MS-CHAP, etc.), solo cuando las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen todas ellas un nivel Bajo.

Deberá usarse un método EAP que proporcione, al menos, las características de seguridad indicadas como obligatorias en la RFC 4710 (ver tabla 5 del Anexo D), cuando alguna de las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] o todas ellas, alcancen un nivel Medio y ninguna alcance un nivel Alto.

Deberá usarse un método EAP que proporcione todas las características de seguridad indicadas como obligatorias y recomendables en la RFC 4710 (ver la tabla 5 del Anexo D) cuando alguna de las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] o todas ellas, alcancen un nivel Alto.

Se recomienda que la autenticación del Servidor de Autenticación (AS) frente al cliente, se realice a través de certificado, y que exista una configuración de seguridad apropiada el dispositivo cliente. Para ello, es recomendable que el cliente no admita certificados de cualquier CA (Autoridad de Certificación), sino sólo de aquella que se sabe que habrá emitido el certificado del servidor. También es recomendable que el cliente verifique que el nombre completo de dominio del servidor es el correcto. De este modo se reduce el riesgo de suplantación del servidor por partes ilegítimas.

En el Anexo A, se incluye una tabla resumen de los requisitos de autenticación para redes inalámbricas.

En el Anexo D se recoge un ejemplo de cómo configurar los aspectos de autenticación en una conexión a una red inalámbrica para un cliente Microsoft Windows 7 Enterprise.

5.2.3 Acceso Local para Administración de los AP [op.acc.6]

Nivel Medio / Alto [I C A T]

El acceso a la infraestructura inalámbrica desde la red cableada de la organización (acceso local) realizado con la finalidad de administración y gestión de los dispositivos, además de atender a las indicaciones realizadas en la guía CCN-STIC-804 (Apartado

4.2.6) sobre el acceso local **[op.acc.6]**, debe contemplar los siguientes aspectos específicos a la red inalámbrica:

En el caso de que las dimensiones de: integridad [I], confidencialidad [C], autenticidad [A] y trazabilidad [T] alcancen nivel Medio o Alto, el protocolo usado para la gestión de la infraestructura inalámbrica debe ser un protocolo de gestión seguro, como puede ser SSH, SSL/TLS o SNMPv3. Este será el único protocolo de gestión habilitado, debiendo de estar deshabilitado cualquier otro protocolo de gestión inseguro que tenga el AP entre sus funcionalidades como, por ejemplo, SNMPv1, SNMPv2, HTTP, etc. (ver Apartado 5.2.4 de Configuración de Seguridad).

Además, atendiendo al principio de segregación de tareas y roles indicado en la medida **[op.acc.3]**, el acceso local para administración del AP, solo estará disponible para los administradores autorizados a realizar estas funciones.

Los accesos, así como las actividades realizadas durante los mismos, deben quedar registrados (ver Apartado 5.2.6 **[op.exp.8]**).

El mecanismo de control de acceso para la administración de los dispositivos, dependerá del nivel exigido en las dimensiones de seguridad [I C A T] (ver Apartado 5.2.2 **[op.acc.5]**).

5.2.4 Configuración de Seguridad [op.exp.2]

Categoría Básica / Media / Alta

Deberá existir una Configuración de Seguridad definida y documentada, para los componentes de la infraestructura inalámbrica. Esta configuración deberá atender a los principios de mínima funcionalidad y seguridad por defecto.

5.2.4.1 Dispositivos cliente.

Es necesario realizar la distinción entre equipos corporativos y equipos externos.

Los equipos no corporativos o equipos externos, representan dispositivos cliente que no se encuentran bajo el control de la organización, perteneciendo generalmente a personal externo (“invitados”). Estos dispositivos no están sujetos a la política de seguridad de la información de la organización, por lo que, se debe poder identificar a los usuarios de manera unívoca y según el principio de mínima funcionalidad, se deberán restringir al máximo los permisos de acceso, debiendo solo acceder a los recursos estrictamente necesarios (en general, Internet y recursos de acceso público de la organización).

Los equipos corporativos serán aquellos dispositivos cliente que se encuentran bajo el control de la organización, y están, por lo tanto, sometidos a su política de seguridad.

Se recomienda la consulta de las guías CCN-STIC relacionadas con la implementación del ENS en equipos cliente (por ejemplo, 850 y 899 referidas a equipos cliente con sistema operativo Microsoft Windows).

La configuración de seguridad de los dispositivos corporativos, contemplará las medidas necesarias para el cumplimiento de la política de seguridad de la organización, como son, por ejemplo, el estado de actualización del antivirus, parches del sistema operativo, cortafuegos personales, etc.

Existirá, además, una configuración de seguridad específica que contemple las medidas de seguridad especificadas en la Política de seguridad de la red inalámbrica. Esta configuración de seguridad podrá invocarse solo cuando el dispositivo cliente se conecte a la red inalámbrica concreta.

Algunos de estos aspectos a tener en cuenta para el diseño de estas medidas específicas, son los siguientes:

- Acceso a la red. Cada dispositivo cliente solo debe poder acceder a los recursos o segmentos de red necesarios, y utilizando solo los protocolos indispensables.

  Es recomendable que los dispositivos no tengan configurada la conexión a la red inalámbrica de forma automática.

- Servicios de Red. Es recomendable deshabilitar todos los servicios de red que no sean necesarios.

Un aspecto importante a destacar, es el de las conexiones duales. Debe establecerse una política clara sobre el uso de estas conexiones, indicando claramente cuáles están autorizadas y cuáles prohibidas y bajo qué circunstancias.

Las conexiones duales implican la conexión simultánea del dispositivo cliente a dos o más redes, e introducen riesgos que deben ser evaluados. Un ejemplo es la conexión simultánea a la red inalámbrica y a la red cableada. Este tipo de conexión abre la posibilidad de que individuos no autorizados, consigan acceso al dispositivo cliente a través de la red inalámbrica, y desde ahí puedan lanzar ataques sobre la red cableada. Esta es por lo tanto un tipo de conexión dual que introduce un riesgo elevado. Sin embargo, una conexión a la red inalámbrica simultáneamente a una conexión bluetooth con el teclado, introduce un riesgo mucho menor.

Atendiendo al principio de mínima funcionalidad, por defecto no se deberían permitir las conexiones duales, y sólo se deben aceptar excepcionalmente y cuando lo permita la política de seguridad. Esto deberá reforzarse implementando los controles técnicos adecuados, que proporcionen la suficiente seguridad permitiendo a su vez la funcionalidad necesaria.

- Modo Ad Hoc. El modo Ad Hoc 802.11 habilitado, permite la conexión directa entre los dispositivos cliente sin necesidad de AP, por lo que abre la posibilidad a conexiones maliciosas por parte de individuos no autorizados. Es recomendable, por lo tanto, deshabilitar el modo Ad Hoc.

- Método EAP. Debe configurarse que únicamente se utilice el método EAP seleccionado en la arquitectura de autenticación, para evitar que se utilice ningún otro método EAP del que disponga el dispositivo cliente (Microsoft Windows, por ejemplo, dispone de varios métodos EAP de forma nativa).

- Cortafuegos personales. El despliegue de cortafuegos personales es adecuado cuando el dispositivo se conecta a la red inalámbrica, ya que ayuda a evitar que otros usuarios de la misma consigan acceso no autorizado al dispositivo.

5.2.4.2 Puntos de Acceso (AP) y configuración de la red inalámbrica.

Atendiendo al principio de mínima funcionalidad, deberán deshabilitarse todos los servicios y funciones del AP que no sean estrictamente necesarios.

Especialmente importantes en cuanto al riesgo que representan, son los interfaces de gestión no seguros de los que pueda disponer el AP, que deberán estar deshabilitados. Por ejemplo, agentes SNMP, interfaces de administración HTTP, etc.

En caso de que el uso de CCMP sea requisito (ver Apartado 5.4.1 [mp.com.2]), se deberán deshabilitar las funciones de seguridad que no deban usarse (WEP y TKIP) para prevenir su uso.

El AP deberá tener la funcionalidad de establecimiento de VPN (IPsec, TLS, SSH) para garantizar una comunicación segura con el Servidor de Autenticación (AS) si es necesario (ver Apartado 5.4.1 **[mp.com.2]**).

- Parámetros por defecto. No dejar parámetros con valores por defecto. Todos ellos deberán haber sido revisados y se les deberá haber asignado el valor apropiado.

  Debe revisarse el tipo de reinicio que puede llevarse a cabo en el AP. En algunos tipos de reinicio el dispositivo retorna a los valores de configuración por defecto, perdiendo la configuración de seguridad.

- Configuración del SSID. El SSID por defecto que tengan los AP, deberá cambiarse y configurarse de forma que no incluya ningún tipo de información útil, para un potencial atacante (nombre de la organización, situación de los puntos de acceso, etc.).

  Es una buena práctica que el AP oculte la emisión del SSID, de forma que un dispositivo solo pueda conectarse a la red inalámbrica si el SSID ha sido especificado explícitamente. Es una medida disuasoria, ya que no impide que un potencial atacante descubra el SSID con escáneres de red.

- Otra buena práctica es el uso de Listas de direcciones MAC, de forma que solo los dispositivos cuya dirección MAC se encuentre en la lista autorizada, podrán acceder a la red inalámbrica. Esta es también una medida disuasoria, ya que no impide que un potencial atacante pueda suplantar una de las direcciones MAC autorizadas sin mucha dificultad (MAC spoofing).

- Método EAP. Debe configurarse que únicamente se utilice el método EAP seleccionado en la arquitectura de seguridad, y evitar así que se utilice ningún otro método EAP del que disponga el dispositivo cliente.

- Horario operativo. Es recomendable inhabilitar los AP en horario no laborable cuando no vayan a ser utilizados por los usuarios legítimos, reduciendo así la posibilidad de ataques.

- Auditoría. Es recomendable que el AP disponga de la función de auditoría que permita realizar el registro de eventos y acciones de usuarios, y que además sea también capaz de reenviarlos a un servidor centralizado.

- Direccionamiento estático. Asignar direcciones IP estáticas a los dispositivos cliente, y no utilizar direcciones dinámicas asignadas por el DHCP, permite utilizar funcionalidades de filtrado por IP en otros elementos de seguridad de la red (como cortafuegos). Sin embargo, esto puede no ser viable en redes muy extensas debido a la carga administrativa que supone la gestión y asignación de IP y el número limitado de IP de las que puede disponer la administración.

- Tiempo de sesión limitado. Es recomendable que los AP tengan la funcionalidad de configurar un tiempo máximo de sesión. De esta forma, en el caso de que la conexión con un dispositivo cliente permanezca inactiva ese tiempo máximo de sesión, la asociación será disuelta por el AP y el cliente deberá re autenticarse.

5.2.4.3 Servidores de Autenticación (AS).

El Servidor de Autenticación (AS) deberá estar adecuadamente bastionado y protegido, con las medidas de seguridad apropiadas. Hay que tener en cuenta que, si el Servidor de Autenticación se ve comprometido, un individuo no autorizado podría conseguir acceso a la red sin necesidad de conexión física.

Se recomienda la consulta de las guías CCN-STIC relacionadas con la implementación del ENS en equipos servidor (por ejemplo, 870 y 851 referidas a equipos servidor con sistema operativo Microsoft Windows).

5.2.5 Gestión de la Configuración [op.exp.3]

Categoría Media / Alta

La infraestructura inalámbrica deberá tenerse en cuenta en el proceso de Gestión de la Configuración de la infraestructura de la organización, considerando, entre otras cosas, las necesidades de aprobar y documentar los cambios en la configuración de seguridad de la red inalámbrica, de realizar pruebas previas al despliegue de cualquier cambio, y las necesidades de copias de seguridad de configuraciones de seguridad previas.

Se recomienda estandarizar al máximo posible la Configuración de Seguridad de la infraestructura inalámbrica. Es recomendable, también, que esta configuración se pueda desplegar y mantener de forma automática en todos los dispositivos. Para ello se puede utilizar un software de gestión de configuración de la red inalámbrica, que disponga de estas capacidades de despliegue y mantenimiento, o se puede incorporar la infraestructura inalámbrica en el software de gestión de la configuración general de la organización, si este dispone de capacidades para gestionar la infraestructura inalámbrica. Esto aporta las siguientes ventajas:

- Proporciona una línea base de seguridad.

- Proporciona consistencia y uniformidad en la organización, de forma que la configuración de todos los componentes inalámbricos será homogénea en toda la organización.
- Facilita la formación y concienciación del usuario, al ser la configuración estándar.
- Reduce el tiempo y los recursos requeridos, no solo para desplegar la configuración de los dispositivos, sino también a la hora de planificar y ejecutar verificaciones y auditorías sobre la configuración y a la hora de realizar el mantenimiento.
- Permite detectar y corregir cambios no autorizados en la configuración de los dispositivos, y reaccionar de forma rápida a la detección de nuevas vulnerabilidades o incidentes recientes, que requieran de un cambio urgente en la configuración.

5.2.6 Registro de la actividad de los usuarios [op.exp.8]

Debe registrarse la actividad de los usuarios, en especial de los administradores, en la red inalámbrica. Como mínimo un registro detallado de los intentos de conexión exitosos y fallidos. Esto posibilita la trazabilidad de acciones y proporciona registros que podrán ser revisados en caso de que ocurra alguna actividad maliciosa.

Esta función debe estar habilitada en los AP y en los Servidores de Autenticación (AS) (ver Apartado 5.2.4 **[op.exp.2]**).

Debe registrarse la actividad de los administradores, en especial si realizan modificaciones a la configuración de seguridad.

Nivel Medio [T]

En caso de que la trazabilidad [T] tenga un nivel Medio, se realizará una revisión informal de los registros de actividad con objeto de identificar problemas de seguridad y tomar las acciones correctivas cuanto antes.

Nivel Alto [T]

En caso de que la trazabilidad [T] tenga un nivel Alto, los AP y los Servidores de Autenticación (AS) deben enviar los registros en tiempo real a un servidor centralizado para su almacenamiento, correlación y explotación automática. Además, deberán ser protegidos de forma que no puedan ser modificados ni eliminados por personal no autorizado. Esto ayuda a asegurar la integridad de los registros incluso si el AP o AS han sido comprometidos.

5.2.7 Monitorización [op.mon]

Categoría Básica

La monitorización de la seguridad es un aspecto fundamental en todas las redes y sistemas, pero aún adquiere mayor importancia en las redes inalámbricas, que están sujetas a las mismas amenazas y a otras específicas del entorno inalámbrico.

Debe llevarse a cabo una monitorización continua, que permita mantener un conocimiento constante del estado de la seguridad de la red inalámbrica, de forma que sea posible identificar y reaccionar de la forma más inmediata posible, a ataques, fallos en las configuraciones de seguridad, y cualquier otro problema en la seguridad de la red inalámbrica.

La monitorización de seguridad que se realice, debe atender al menos a estos dos aspectos:

a) Monitorización de los posibles ataques, tanto los específicos de redes inalámbricas, como aquellos que afectan a redes cableadas (ya que también afectan a redes inalámbricas). Se atenderá especialmente a los ataques activos, en los que un individuo no autorizado, no se limita a monitorizar el tráfico, sino que genera, altera o interrumpe las comunicaciones inalámbricas.

b) Monitorización de vulnerabilidades, a llevar a cabo sobre los componentes de la infraestructura inalámbrica, de la misma forma que se realice para la red cableada. Identificar y aplicar parches, verificar las configuraciones de seguridad y ajustarlas cuando sea necesario. Estas acciones deberían ser realizadas al menos con la misma frecuencia que se realicen en los componentes de la red cableada.

5.2.8 Detección de intrusión [op.mon.1].

Categoría Media / Alta

En caso de que la categoría sea Media o Alta, la monitorización de seguridad se llevará a cabo de forma automática a través de Sistemas de Detección de Intrusión Inalámbrica WIDS (Wireless Intrusion Detection Systems) y/o Sistemas de Prevención de Intrusión Inalámbricos WIPS (Wireless Intrusion Prevention Systems). Estos sistemas disponen de sensores que se despliegan en localizaciones determinadas dentro de las instalaciones de la organización. Los sensores realizan un barrido de frecuencias en las bandas y canales de la red inalámbrica, y seleccionan muestras del tráfico capturado, para analizarlo en busca de posibles ataques o vulnerabilidades. En el Anexo E se detalla el funcionamiento de estos sistemas.

El sistema WIDS o WIPS debe tener la misma cobertura que la red inalámbrica, para evitar que individuos no autorizados se instalen en zonas donde puedan eludir el sistema de detección.

Es recomendable que la monitorización de la infraestructura inalámbrica sea capaz de detectar, al menos, lo siguiente:

- Dispositivos inalámbricos no autorizados, incluyendo falsos AP (rogue AP) y dispositivos cliente.
- Dispositivos desconfigurados, o con una configuración de seguridad que no sea la estándar de la organización.
- Patrones de uso de la red inalámbrica anormales. Por ejemplo, un elevado número de dispositivos cliente utilizando un mismo AP, volumen de tráfico anormal

procedente de un dispositivo cliente, un elevado número de intentos fallidos de conexión a la red en un corto periodo de tiempo, etc.

- Escáneres activos que puedan estar generando tráfico ilícito a la red inalámbrica. Por ejemplo, las herramientas que individuos no autorizados utilizan para escanear redes inalámbricas realizadas en movimiento.
- Ataques DoS. Por ejemplo, registrando el número de eventos de terminación de conexiones en la red inalámbrica, y alertando cuando se supere un umbral, ya que eso puede significar un ataque DoS.
- Ataques de suplantación y *man-in-the-middle*. Por ejemplo, algunos WIDS pueden detectar cuando un dispositivo está tratando de suplantar la identidad de un cliente autorizado.

5.2.9 Auditorías de seguridad

La red inalámbrica deberá ser incluida en las Auditorías de seguridad periódicas que la organización realizará sobre sus sistemas e infraestructuras. De esta forma, podrá verificarse que la red inalámbrica cumple con las políticas y normativa de seguridad establecidas.

Las auditorías de la red inalámbrica deberán contemplar, al menos, los siguientes aspectos:

- Análisis de vulnerabilidades y medidas técnicas implantadas.
- Análisis del rango de cobertura y potencia de radiación de los AP.
- Análisis del estado de configuración de los AP.
- Análisis de los incidentes producidos y medidas correctoras aplicadas.

La periodicidad con la que deberán realizarse las auditorías la determina la organización. En el caso de la red inalámbrica, deberán tenerse en cuenta los siguientes factores:

- La localización de las instalaciones de la organización. En caso de que se encuentren cerca de áreas públicas concurridas y de fácil acceso, aumentará el riesgo de amenazas a la red inalámbrica.
- El nivel de seguridad de la información transmitida a través de la red inalámbrica.
- Cambios físicos en las instalaciones, que puedan afectar a la propagación y potencia de la señal inalámbrica.

5.3 Medidas de Protección [mp]

5.3.1 Protección de las Instalaciones e Infraestructuras [mp.if]

Los elementos de la infraestructura inalámbrica solo deben ser accesibles físicamente por personal autorizado.

Categoría Básica

Es especialmente importante restringir el acceso a los AP para evitar su manipulación (tampering), de forma que al menos estén fuera del alcance, como, por ejemplo, por encima del falso techo.

Adicionalmente, es recomendable también que el botón de *reset* de los AP se encuentre protegido, para evitar su pulsación de forma accidental o mal intencionada. Si la configuración de seguridad no es robusta, esto podría causar que el AP vuelva a su configuración de fábrica, deshabilitando todas las medidas de seguridad.

Categoría Media / Alta

En el caso de que sean los AP los que realizan las funciones de seguridad, como gestión del tráfico de autenticación, generación de claves criptográficas y cifrado, es recomendable que sean ubicados en CPD, salas de servidores, armarios o dependencias similares con controles de acceso físico apropiados. En caso de que sean otros los elementos que realizan estas funciones de seguridad (por ejemplo, *switches* de la red inalámbrica), serán éstos los que deberán protegerse físicamente de la forma anteriormente indicada.

5.3.2 Segregación de Redes [mp.com.4]

En el diseño de la seguridad de la red inalámbrica, debe tenerse en cuenta cómo esta red puede afectar a otras redes con las que tenga conexión (normalmente la red cableada de la organización), y a las que se puede acceder a través de ella.

Categoría Básica / Media

La red inalámbrica deberá estar segmentada en caso de que existan diferentes dominios de seguridad. Por ejemplo, segmentos de red distintos para el acceso de invitados (personal externo a la organización) y el acceso de personal interno.

Una práctica recomendable es segregar el tráfico de la red inalámbrica del tráfico de la red cableada a través de VLAN dedicadas. El uso de estas VLAN facilita la implementación de listas de control de accesos a la red, permitiendo identificar los protocolos y servicios autorizados a pasar desde la red inalámbrica a la red cableada.

Categoría Alta

La red inalámbrica deberá estar segmentada a través de un dispositivo lógico o físico asegurado y mantenido de la forma apropiada, para acotar el acceso a la información y la propagación de incidentes, tal y como se indica en el Apartado 5.4.4 de la CCN-STIC-804.

5.3.3 Formación [mp.per.4] y Concienciación [mp.per.3]

Categoría Básica / Media / Alta

La organización debe asegurarse de que todos los usuarios y el personal técnico que vaya a utilizar o a administrar la infraestructura inalámbrica dispone de la formación adecuada y es conocedor de las políticas y procedimientos.

Se debe concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad de la red inalámbrica alcance los niveles exigidos.

Tal y como se indica en la guía CCN-STIC-804, es necesario refrescar regularmente:

- La normativa de seguridad relativa al buen uso de la red inalámbrica.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento de reporte de incidencias de seguridad, seas reales o falsas alarmas.

Los administradores de la red inalámbrica deben ser plenamente conscientes de las amenazas y los riesgos de seguridad a los que se expone la red. Deben trabajar para asegurar el cumplimiento de la política de seguridad, y deben conocer perfectamente los procedimientos de configuración de seguridad de la infraestructura inalámbrica, los de gestión de incidentes de seguridad y otros procedimientos relativos a la red inalámbrica.

Es recomendable que los administradores estén al día sobre nuevas vulnerabilidades y ataques a la infraestructura inalámbrica, para lo cual pueden consultar multitud de fuentes que publican este tipo de información.

5.3.4 Borrado y destrucción [mp.si.5]

Los dispositivos inalámbricos almacenan información sensible relacionada con contraseñas, PSK, información de configuración, etc. Esta información puede ser utilizada por individuos no autorizados de forma muy provechosa para realizar ataques a la red inalámbrica.

Nivel Bajo [C]

En el caso de que la confidencialidad [C] alcance un nivel Bajo, los dispositivos inalámbricos que se vayan a reutilizar deberán ser objeto de borrado seguro. En el caso de los AP, habrá que eliminar como mínimo, la siguiente información:

- Claves PSK.
- Configuración de seguridad (hacer un *reset* a la configuración de fábrica).
- Registros de actividad y eventos.
- Cuentas de administración.

Nivel Medio / Alto [C]

En el caso de que la confidencialidad [C] alcance un nivel Medio o Alto, los dispositivos inalámbricos que se vayan a dar de baja, deben ser objeto de destrucción segura según se indica en el Apartado 5.5.5 de la guía CCN-STIC-804.

5.4 Criptografía

5.4.1 Protección de Confidencialidad, Autenticidad e Integridad [mp.com.2-3]

Como se indica en el apartado 4.2 y en el Anexo C, el estándar IEEE 802.11i (RSN) puede utilizar dos suites criptográficas para la protección de la comunicación inalámbrica: TKIP y CCMP.

TKIP es la suite que implementa WPA de forma obligatoria, y su algoritmo central es RC4. CCMP es la suite que implementa WPA2 de forma obligatoria y su algoritmo central es AES.

TKIP utiliza los algoritmos RC4 y Michael (como código de integridad de mensaje). Ambos algoritmos tienen vulnerabilidades de seguridad conocidas a día de hoy, por lo que TKIP no se considera adecuado para entornos con requisitos de seguridad elevados. Para estos entornos, CCMP es un mecanismo más seguro, pero requiere más recursos de computación.

Nivel Bajo [I C A]

En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan todas ellas un nivel Bajo, las medidas **[mp.com.2]** y **[mp.com.3]** no establecen ningún requisito sobre el cifrado de la comunicación inalámbrica.

Por lo tanto, se permite el uso de TKIP y, consecuentemente, de WPA. Esto favorece el uso de equipamiento antiguo que puede no soportar la carga computacional que supone el uso de CCMP (AES) con WPA2. Sin embargo, si el equipamiento inalámbrico lo permite y aunque no sea requisito exigido, se recomienda el uso de WPA2.

Nivel Medio [I C A]

En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan alguna de ellas nivel Medio y ninguna nivel Alto, las medidas [mp.com.2] y [mp.com.3] aplicadas a la red inalámbrica, establecen que la suite criptográfica usada para la protección de las comunicaciones, deberá emplear algoritmos acreditados por el Centro Criptológico Nacional (CCN).

Este requisito descarta el uso de TKIP, ya que RC4 (su algoritmo central), no pertenece a los algoritmos acreditados por el CCN según la guía CCN-STIC-807 – Criptografía de empleo en el ENS. Se requiere por lo tanto el uso de CCMP, cuyo algoritmo central es AES, que sí pertenece a la lista de algoritmos acreditados por el CCN. Los dispositivos inalámbricos deberán utilizar por lo tanto WPA2, ya que el uso de CCMP en WPA no es obligatorio y el dispositivo puede no implementarlo. Además, dentro de la configuración de seguridad del AP y del dispositivo cliente deberá inhabilitarse el uso de TKIP, para que en ningún momento (por precaución ante reinicios del equipo) se utilice esta suite criptográfica.

En el caso de equipamiento inalámbrico obsoleto que no pueda utilizar CCMP, y solo de forma temporal hasta que sea sustituido por la organización, se podrá utilizar TKIP si se utiliza una red privada virtual (VPN) para la protección de la comunicación. Esto exige que la organización disponga de infraestructura VPN (concentradores VPN).

La VPN se establecerá entre el dispositivo cliente (que deberá por lo tanto disponer de un software cliente de VPN) y el concentrador VPN que se encontrará en la red interna, y por lo tanto detrás del AP. La VPN deberá utilizar una suite criptográfica compuesta por algoritmos acreditados por el CCN.

Nivel Alto [I C A]

En caso de que las dimensiones de integridad [I], confidencialidad [C] y autenticidad [A] tengan alguna de ellas un nivel Alto, las medidas **[mp.com.2] y [mp.com.3]** aplicadas a la red inalámbrica, establecen que los dispositivos inalámbricos deberán utilizar WPA2 y además deberán ser productos certificados conforme a lo establecido en la medida **[op.pl.5].**

Siguiendo las indicaciones descritas en la medida operacional [op.pl.5], deberá utilizarse un dispositivo inalámbrico cuyas funcionalidades de seguridad y cuyo nivel, hayan sido evaluados conforme a normas europeas o internacionales, y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

En el Anexo A, se incluye una tabla resumen de los requisitos especificados por las medidas **[mp.com.2] y [mp.com.3]** para redes inalámbricas.

5.4.2 Protección de Claves Criptográficas [op.exp.11]

IEEE 802.11i (RSN) utiliza dos jerarquías de claves, una para la protección del tráfico unicast (clave Pairwise Master Key), y otra para la protección del tráfico multicast / broadcast (clave Group Master Key). En cada jerarquía se deriva la clave maestra (PSK o GMK) a partir de una clave raíz, que puede ser una clave pre-compartida, PSK, o una clave generada por el Servidor de Autenticación, MSK. De las claves maestras se derivan el resto de claves para la protección de la comunicación. En el Anexo B se pueden consultar los detalles sobre las jerarquías de claves criptográficas, así como el mecanismo de generación y distribución de las mismas.

Categoría Básica

En caso de que se utilicen claves pre-compartidas PSK, estas deberán generarse en medios aislados de los medios de explotación.

Se recomienda el uso de una PSK de al menos 12 caracteres, y generada de forma automática a través de algún dispositivo de generación de claves aleatorias PRNG (Pseudorandom Number Generator). La PSK deberá renovarse de forma periódica.

Categoría Media

El mecanismo de generación y distribución de claves que debe utilizarse es 802.11X/EAP. En la fase de autenticación y distribución de claves, la MSK (Master Session Key) es generada y distribuida entre el Servidor de Autenticación (AS) y el dispositivo cliente. Para la protección de esta distribución, se deberá utilizar CCMP (WPA2).

Se recomienda la configuración de un tiempo de vida máximo (*life time*) de las claves PMK (para tráfico *unicast*) y GMK (para tráfico *multicast*) no superior a 24 horas.

La distribución de la MSK del Servidor de Autenticación (AS) al AP deberá realizarse a través de un canal seguro, para lo que se requiere el uso de una VPN (Virtual Private Network). Se recomienda el uso de IPsec v3, o TLS 1.2.

Categoría Alta

Los dispositivos inalámbricos deberán usar WPA2 y además deberán ser productos certificados conforme a lo establecido en la medida **[op.pl.5]**.

Siguiendo las indicaciones descritas en la medida operacional [op.pl.5], deberá utilizarse un dispositivo inalámbrico cuyas funcionalidades de seguridad y cuyo nivel, hayan sido evaluados conforme a normas europeas o internacionales, y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

En el Anexo A, se incluye una tabla resumen de los requisitos especificados por la medida **[op.exp.11]** para la protección de claves criptográficas.

ANEXO A. RESUMEN DE REQUISITOS ENS PARA REDES INALÁMBRICAS

La siguiente tabla muestra un resumen de los Requisitos sobre los mecanismos criptográficos aplicados a redes inalámbricas, establecidos por las medidas **[mp.com.2] y [mp.com.3]** del ENS.

Niveles dimensiones de seguridad				Tipo de Autenticación	Mecanismo de Autenticación [op.acc.5]	Método EAP
I	A	C	T			
BAJO (Todas las dimensiones de nivel Bajo)				PSK *(WPA/WPA2 Personal)* 802.1X/EAP *(WPA/WPA2 Enterprise)*	Un solo factor de autenticación, de cualquier tipo: contraseñas o claves compartidas, *tokens*, certificados, biometría, etc. En el caso de uso de contraseñas o claves compartidas, deberán tener un nivel mínimo de Fortaleza y estar sujetas a una Política de renovación y gestión de contraseñas.	Cualquier método EAP o ningún método EAP (uso de otros protocolos de autenticación como PAP, CHAP, MS-CHAP, etc.)
MEDIO (Alguna de las dimensiones alcanza nivel Medio, o incluso todas ellas. Ninguna de nivel Alto).				802.1X/EAP *(WPA/WPA2 Enterprise)*	Doble factor de autenticación, de cualquier tipo: contraseñas o claves compartidas, *tokens*, certificados, biometría, etc. En el caso de uso de contraseñas o claves compartidas, deberán tener un nivel Medio de Fortaleza y estar sujetas a una Política de renovación y gestión de contraseñas con requisitos de nivel Medio.	Método EAP que proporcione, al menos, las características de seguridad indicadas como obligatorias en la RFC 4701, para una red inalámbrica.

ALTO (Alguna de las dimensiones alcanza nivel Alto, o incluso todas ellas).	802.1X/EAP *(WPA/WPA2 Enterprise)*	Doble factor de autenticación, de cualquier tipo: contraseñas o claves compartidas, *tokens*, certificados, biometría, etc. En el caso de uso de contraseñas o claves compartidas, deberán tener un nivel Medio de Fortaleza y estar sujetas a una Política de renovación y gestión de contraseñas con requisitos de nivel Medio. En el caso de uso de "algo que se tiene" deberán usarse elementos criptográficos hardware que utilicen algoritmos acreditados por el CCN.	Método EAP que proporcione, al menos, las características de seguridad indicadas como obligatorias y las indicadas como recomendables en la RFC 4701, para una red inalámbrica.

Tabla 1. Requisitos autenticación para redes inalámbricas.

La siguiente tabla muestra un resumen de los Requisitos sobre los mecanismos criptográficos aplicados a redes inalámbricas, establecidos por las medidas **[mp.com.2] y [mp.com.3]** del ENS.

Niveles dimensiones de seguridad			Mecanismos Criptográficos
I	A	C	
BAJO (Todas las dimensiones de nivel Bajo)			Dispositivos WPA (TKIP, RC4) Dispositivos WPA2 (CCMP, AES)
MEDIO (Alguna de las dimensiones alcanza nivel Medio, o incluso todas ellas. Ninguna de nivel Alto).			Dispositivos *WPA2* (CCMP, AES) Excepción*:* En caso de equipamiento inalámbrico antiguo no actualizable a WPA2, se permitirá el uso de WPA (TKIP) cuando se cumplan las siguientes condiciones: • Solo de forma temporal hasta su sustitución. • Cuando se implemente una VPN entre el cliente inalámbrico y la red interna cableada de la organización. • La VPN deberá usar algoritmos criptográficos acreditados por el CCN.

ALTO (Alguna de las dimensiones alcanza nivel Alto, o incluso todas ellas).	Dispositivos *WPA2* (CCMP, AES) Dispositivos Certificados [op.pl.5]

Tabla 2. Requisitos sobre Mecanismos criptográficos.

La siguiente tabla muestra un resumen de los Requisitos sobre la protección de claves criptográficas aplicados a redes inalámbricas, establecidos por la medida **[op.exp.11]** del ENS.

Categoría	Mecanismos Criptográficos
BÁSICA	Se permite el uso de PSK. Recomendado PSK de 12 caracteres mínimo y generada vía un dispositivo PRNG.
MEDIA	Generación y distribución de claves 802.1X/EAP CCMP para protección de distribución de claves VPN entre el AP y el AS (preferiblemente IPsec v3 o TLS 1.2)
ALTA	Dispositivos certificados [op.pl.5]

Tabla 3. Requisitos de Protección de claves criptográficas.

La siguiente tabla muestra un resumen los Requisitos aplicados a redes inalámbricas, establecidos por otras medidas del ENS indicadas en el Apartado 5 de la presente guía.

ID	RQ[1] RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
1	RQ	**Política de Seguridad**. Al menos: - Uso aceptable de la red inalámbrica - Requisitos de seguridad de la infraestructura inalámbrica	Normativa de Seguridad	[org.2]	X	X	X	CCN-STIC-816. Apdo. 5.1 CCN-STIC-804. Apdo. 3.2

[1] "RQ" representa un Requisito (requerido por el ENS). "RM" representa una Recomendación, es decir, no requerido explícitamente por el ENS, pero recomendable su implementación.

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
		- Requisitos de seguridad de los dispositivos cliente - Evaluaciones de seguridad periódicas						
2	RQ	**Procesos y Procedimientos**. Al menos: - Autorización de usuarios y dispositivos - Autorización de despliegue de nuevos componentes - Operación y mantenimiento - Gestión de eventos y registros de log - Gestión y respuesta a incidentes - Actuación frente a pérdida o robo de dispositivos inalámbricos - Monitorización de seguridad continua - Auditorías de seguridad periódicas	Procedimientos de Seguridad Proceso de Autorización	[org.3] [org.4]	X	X	X	CCN-STIC-816. Apdo. 5.1 CCN-STIC-804. Apdo. 3.3 y 3.4
3	RQ	Realizar un análisis de cobertura y potencia de radiación de los AP para seleccionar su ubicación, minimizando la radiación fuera del perímetro controlado.	Arquitectura de Seguridad	[op.pl.2]	X	X	X	CCN-STIC-816 Apdo. 5.2.1 CCN-STIC-804 Apdo. 4.1.2
4	RQ	Red inalámbrica tipo Infraestructura. No se recomienda Ad Hoc.	Arquitectura de Seguridad	[op.pl.2]	X	X	X	CCN-STIC-816 Apdo. 5.2.1 CCN-STIC-804 Apdo. 4.1.2

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
5	RM	Autenticación del Servidor de Autenticación (AS) frente al dispositivo cliente, a través de certificado. Además el cliente solo deberá aceptar certificados de un Servidor de Autenticación (AS) concreto (identificado con su nombre completo de dominio) y solo de la CA que firma el certificado del servidor.	Autenticación	[op.acc.5]		X	X	CCN-STIC-816 Apdo. 5.2.2
6	RQ	El método EAP empleado para autenticación debe cumplir los requisitos de seguridad para redes inalámbricas indicados en la RFC 4017.	Autenticación	[op.acc.5]		X	X	CCN-STIC-816 Apdo. 5.2.2
7	RM	Es recomendable que el método EAP sea uno de los incluidos en el programa de certificación WPA2.	Autenticación	[op.acc.5]		X	X	CCN-STIC-816 Apdo. 5.2.2
8	RQ	Las conexiones para Administración de los AP desde la red cableada interna de la organización deberán contar con mecanismos de protección (por ejemplo, SSH, TLS o SNMPv3).	Acceso Local	[op.acc.6]		X [ICAT]	X [ICAT]	CCN-STIC-816 Apdo. 5.2.3 CCN-STIC-804 Apdo. 4.2.6
9	RQ	Los AP deberán tener deshabilitados los interfaces de gestión inseguros.	Acceso Local Configuración de Seguridad	[op.acc.6] [op.exp.2]		X [ICAT]	X [ICAT]	CCN-STIC-816 Apdo. 5.2.3 y 5.2.4 CCN-STIC-804 Apdo. 4.2.6

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
10	RQ	**Configuración de Seguridad. Dispositivos cliente**. - Acceso restringido a la red inalámbrica, solo a los recursos estrictamente necesarios - No tener habilitada la conexión automática a la red inalámbrica - Solo habilitados los protocolos y servicios necesarios - Modo Ad Hoc deshabilitado - Solo habilitado método EAP definido para autenticación	Configuración de Seguridad	[op.exp.2]	X	X	X	CCN-STIC-816 Apdo. 5.2.4 CCN-STIC-804 Apdo. 4.3.2 CCN-STIC relacionadas con la implementación del ENS en equipos cliente.
11	RQ	**Configuración de Seguridad. AP.** - Deshabilitados servicios y funciones no necesarias (mínima funcionalidad) - Solo habilitados los protocolos y servicios necesarios - Solo habilitado método EAP definido para autenticación - No dejar parámetros por defecto - SSID no debe proporcionar información útil - Disponer de Función de auditoría:	Configuración de Seguridad	[op.exp.2]	X	X	X	CCN-STIC-816 Apdo. 5.2.4 CCN-STIC-804 Apdo. 4.3.2

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
		registro de eventos y acciones de usuarios y administradores						
12	RM	**Configuración de Seguridad. AP.** - Ocultar emisión del SSID. - Utilizar listado de direcciones MAC - Inhabilitar AP en horarios no operativos - Direccionamiento estático - Configurar tiempo de sesión limitado	Configuración de Seguridad	[op.exp.2]	X	X	X	CCN-STIC-816 Apdo. 5.2.4 CCN-STIC-804 Apdo. 4.3.2
13	RQ	**Configuración de Seguridad. AP.** - Tener deshabilitadas las funciones de seguridad distintas de CCMP (WEP, TKIP) - Disponer de funciones para establecimiento de VPN con el AS	Configuración de Seguridad	[op.exp.2]		X	X	CCN-STIC-816 Apdo. 5.2.4 CCN-STIC-804 Apdo. 4.3.2
14	RQ	**Configuración de Seguridad. Servidor de Autenticación (AS).** - Bastionado y protegido adecuadamente	Configuración de Seguridad	[op.exp.2]		X	X	CCN-STIC-816 Apdo. 5.2.4 CCN-STIC-804 Apdo. 4.3.2 CCN-STIC relacionadas con implementación del ENS en equipos servidor.
15	RM	Configuración de seguridad estándar y herramienta de despliegue automático de la configuración.	Gestión de la Configuración	[op.exp.3]		X	X	CCN-STIC-816 Apdo. 5.2.5 CCN-STIC-804 Apdo. 4.3.3

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
16	RQ	AP y Servidores de Autenticación (AS) deben registrar las conexiones exitosas y fallidas de los usuarios y administradores.	Registro de la actividad de los usuarios	[op.exp.8]	X [T]	X [T	X [T]	CCN-STIC-816 Apdo. 5.2.6 CCN-STIC-804 Apdo. 4.3.8
17	RQ	AP y AS deben enviar los registros de actividad a un servidor centralizado.	Registro de la actividad de los usuarios	[op.exp.8]			X [T]	CCN-STIC-816 Apdo. 5.2.6 CCN-STIC-804 Apdo. 4.3.8
18	RQ	Monitorización continua de la red inalámbrica: monitorización de ataques y de vulnerabilidades.	Monitorización	[op.mon]	X	X	X	CCN-STIC-816 Apdo. 5.2.7 CCN-STIC-804 Apdo. 4.6
19	RQ	Monitorización de seguridad automática a través de Sistemas de detección y prevención de intrusiones (WIDPS).	Monitorización	[op.mon.1]		X	X	CCN-STIC-816 Apdo. 5.2.7 CCN-STIC-804 Apdo. 4.6.1
20	RQ	Realizar Auditorías de Seguridad periódicas de la red inalámbrica.	Auditorías de Seguridad	[op.mon]	X	X	X	CCN-STIC-816 Apdo. 5.2.8 CCN-STIC-802 - Auditorías en el ENS
21	RQ	Acceso restringido a los elementos de la infraestructura de la red inalámbrica.	Protección Física	[mp.if]	X	X	X	CCN-STIC-816 Apdo. 5.3.1 CCN-STIC-804 Apdo. 5.1
22	RM	AP fuera del alcance y protección del botón de *reset*.	Protección Física	[mp.if]	X	X	X	CCN-STIC-816 Apdo. 5.3.1 CCN-STIC-804 Apdo. 5.1
23	RQ	Protección de los AP en CPD, Cuartos de Servidores, Armarios o similar.	Protección Física	[mp.if]		X	X	CCN-STIC-816 Apdo. 5.3.1 CCN-STIC-804 Apdo. 5.1
24	RQ	Segmentar la red inalámbrica en caso de que existan varios dominios de seguridad.	Segregación de Redes	[mp.com.4]	X	X	X	CCN-STIC-816 Apdo. 5.3.2 CCN-STIC-804 Apdo. 5.4.4

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
25	RM	Separar el tráfico de la red inalámbrica, de la cableada de la organización a través de VLAN dedicadas.	Segregación de Redes	[mp.com.4]	X	X	X	CCN-STIC-816 Apdo. 5.3.2 CCN-STIC-804 Apdo. 5.4.4
26	RQ	Segmentar la red inalámbrica para acotar el acceso a la información y la propagación de incidentes de seguridad.	Segregación de Redes	[mp.com.4]			X	CCN-STIC-816 Apdo. 5.3.2 CCN-STIC-804 Apdo. 5.4.4
27	RQ	Los usuarios y el personal técnico relacionados con la infraestructura inalámbrica dispondrán de la formación adecuada y será conocedor de las políticas y procedimientos.	Formación	[mp.per.4]	X	X	X	CCN-STIC-816 Apdo. 5.3.3 CCN-STIC-804 Apdo. 5.2.4
28	RQ	Concienciación regular al personal acerca de su papel y responsabilidad respecto a la red inalámbrica.	Concienciación	[mp.per.3]	X	X	X	CCN-STIC-816 Apdo. 5.3.3 CCN-STIC-804 Apdo. 5.2.3
29	RQ	Los Administradores de la red inalámbrica deberán estar correctamente formados y al día de las amenazas y vulnerabilidades.	Formación	[mp.per.4]	X	X	X	CCN-STIC-816 Apdo. 5.3.3 CCN-STIC-804 Apdo. 5.2.4
30	RQ	En caso de que se vayan a reutilizar los AP, realizar borrado seguro de la información sensible contenida en ellos, al menos, claves PSK, Configuración de seguridad, registros de actividad y eventos, cuentas de administración.	Borrado y destrucción	[mp.si.5]	X [C]	X [C	X [C	CCN-STIC-816 Apdo. 5.3.4 CCN-STIC-804 Apdo. 5.5.5

ID	RQ1 RM	Requisito o Recomendación de Seguridad	Medida de Seguridad ENS		Categoría			Apartados de CCN-STIC-816 y otras guías
			Descripción	Código	B	M	A	
31	RQ	En caso de que se vayan a dar de baja los AP, realizar una destrucción segura de los mismos.	Borrado y destrucción	[mp.si.5]			X [C	CCN-STIC-816 Apdo. 5.3.4 CCN-STIC-804 Apdo. 5.5.5

ANEXO B. JERARQUÍA Y DISTRIBUCIÓN DE CLAVES 802.11i

IEEE 802.11i utiliza dos jerarquías de claves para las RSNA:

- La jerarquía de claves emparejadas PKH (Pairwise Key Hierarchy), diseñada para la protección del tráfico *unicast*.
- La jerarquía de claves de grupo GKH (Group Key Hierarchy), diseñada para la protección del tráfico *multicast y broadcast*.

Pairwise Key Hierarchy (PKH). Esta jerarquía de claves, está compuesta por varias claves que van derivando unas de otras:

- Claves raíz (*root keys*) a partir de las cuales genera el resto de claves y que deben estar instaladas en los dispositivos participantes en la comunicación.
- PMK - Clave maestra emparejada (Pairwise Master Key), derivada de las claves raíz.
- PTK – Clave transitoria emparejada (Pairwise Transient Key), derivada de la PMK y otras variables.
- Claves finales, derivadas de la PTK, y usadas para proporcionar los servicios de seguridad a la comunicación.

La siguiente figura muestra un esquema de estas claves y cómo van derivando unas de otras.

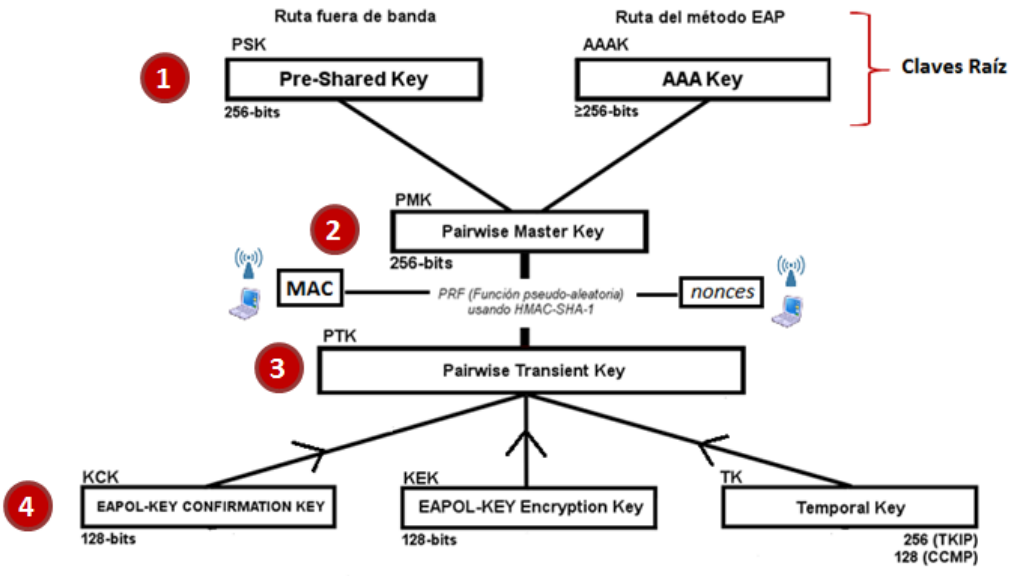

Figura 8. Jerarquía de claves emparejadas PKH (Pairwise Key Hierarchy)

Paso 1 - Las claves raíz (*root keys*), que sirven de material de claves básico para generar todas las demás claves requeridas en los protocolos de protección de confidencialidad e integridad, pueden ser:

- Clave pre-compartida PSK (Pre-Shared Key). Una clave pre-compartida, PSK, es una clave estática distribuida al Servidor de Autenticación (AS) y al dispositivo cliente, a través de un método fuera de banda (*out-of-band*), como pueden ser mecanismos de clave pública automatizados o métodos manuales, como dispositivos USB. Si alguna clave PSK se viese comprometida, se deberían distribuir de nuevo mediante estas mismas técnicas. La distribución de claves PSK en redes grandes podría no ser factible. Su longitud de clave es de 256 bits.
- Clave AAAK (Authentication, Authorization and Accounting Key), también llamada MSK (Master Session Key). Es una clave derivada de los métodos EAP, distribuida entre el Servidor de Autenticación (AS) y el dispositivo cliente (suplicante) y distribuida del AS al AP (autenticador) a través de un canal seguro.

Paso 2 - La clave raíz, PSK o AAAK, distribuida a los dispositivos, se emplea para generar la clave maestra PMK (Pairwise Master Key).

Paso 3 - La clave maestra PMK, se emplea a su vez, junto con las direcciones MAC del dispositivo cliente y del AP, y valores *nonces* generados por ambos, para derivar mediante funciones pseudo-aleatorias, la clave transitoria PTK (Pairwise Transient Key).

Paso 4 - Finalmente, la clave transitoria PTK se compone de las siguientes tres claves:

- EAPOL-KCK (EAP Over LAN Key Confirmation Key). Se emplea para proporcionar servicios de integridad y autenticidad a las tramas de control intercambiadas entre el dispositivo cliente y el AP, durante la configuración de la RSN. También se emplea como prueba de posesión de la clave maestra PMK.
- EAPOL-KEK (EAP Over LAN Key Encryption Key). Se emplea para proporcionar confidencialidad en el intercambio del material de claves y otros datos, durante el establecimiento de la RSNA.
- TK (*Temporal Key*). Se emplea para proporcionar protección al tráfico de usuario. La longitud de TK es de 128 bits en CCMP y 256 bits en TKIP.

Group Key Hierarchy (GKH). Esta jerarquía de claves, está compuesta por varias claves que van derivando unas de otras:

- Clave maestra de grupo GMK (Group Master Key), que es una clave auxiliar generada por el Servidor de Autenticación (AS), para derivar el resto de claves a partir de ella.
- Clave temporal de grupo GTK (Group Temporal Key), derivada de la GMK. La implementación exacta de la GTK no está definida y puede variar mucho de un fabricante a otro. La clave GTK es de 256 bits para TKIP y 128 para CCMP.

La siguiente figura muestra un esquema de las claves GKH.

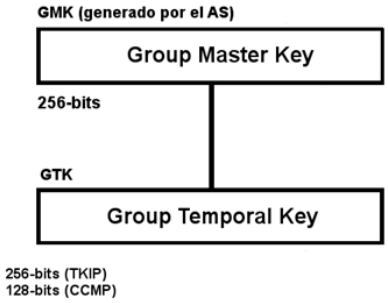

Figura 9. Jerarquía de claves de Grupo GKH (Group Key Hierarchy)

La generación de estas claves criptográficas se realiza a través del proceso de generación y distribución de claves, que representa la última etapa en la autenticación mutua entre el dispositivo cliente y el AP.

Este proceso tiene lugar tras la fase de autenticación, y una vez que el dispositivo cliente y el AP disponen de las claves raíz (*root keys*) instaladas, a partir de las cuales obtienen la PMK.

Los objetivos del proceso de generación y distribución de claves serán los siguientes:

- Verificar la existencia de la misma PMK (Pairwise Master Key) en el dispositivo cliente y en el AP.
- Asegurar que las claves a generar son nuevas.
- Derivar las claves temporales (TK) que se emplearán para la protección del tráfico *unicast* de usuario.
- Derivar las claves temporales (GTK) que se emplearán para la protección del tráfico *multicast / broadcast*.

En función de la jerarquía de claves a generar, son dos procesos lo que se emplean: proceso de negociación en 4-etapas (4-Way Handshake) para la PKH y proceso de negociación de grupo (Group Handshake) para la GKH. En ambos procesos se protege la integridad y confidencialidad de los mensajes intercambiados a través de algoritmos criptográficos.

El proceso de negociación en 4-etapas se implementa mediante el intercambio de cuatro mensajes. Al finalizar el intercambio, se habrá probado que tanto el dispositivo cliente, como el AP, disponen de la misma PMK (Pairwise Master Key) sin necesidad de descubrirla, y, además, se habrá derivado la PTK (Pairwise Temporal Key) de la que se obtienen las claves criptográficas para la protección del tráfico de usuario.

En caso de que se deba soportar tráfico *multicast o broadcast*, a continuación del proceso de 4-etapas, el AP enviará una GTK nueva a cada dispositivo cliente. Esta GTK irá cifrada y con protección de integridad.

ANEXO C. SUITES CRIPTOGRÁFICAS 802.11i

La suite criptográfica será el conjunto de algoritmos a utilizar para la protección de la confidencialidad (cifrado), integridad y autenticidad de los datos.

802.11i define dos suites criptográficas: TKIP y CCMP.

TKIP (Temporal Key Integrity Protocol). TKIP fue diseñado para proporcionar un mayor nivel de seguridad que la que WEP proporcionaba, sin necesidad de sustituir el equipamiento hardware inalámbrico, y siendo solo necesario realizar una actualización del software o del firmware de los dispositivos.

El encapsulado realizado por TKIP proporciona funcionalidades adicionales al protocolo WEP, y no requiere la instalación de hardware adicional, por lo que se considera un protocolo adecuado para construir sistemas en transición (TSN). Los principales servicios de seguridad que proporciona esta suite son los siguientes:

- Protección de la confidencialidad, empleando el algoritmo RC4. Esta solución presenta algunas vulnerabilidades que no la hace óptima para los requisitos más altos de seguridad.
- Protección de la integridad, empleando el algoritmo de resumen de mensaje de Michael, por el que se crea un código MIC (Message Integrity Code).
- Prevención anti-reenvío a través de técnicas de secuenciado de tramas. Cada trama cuenta con un contador de secuencia TSC (TKIP Sequence Counter), que proporciona protección contra ataques de reenvío. Las tramas que no llegan en orden son desechadas.
- Empleo de una nueva clave de cifrado para cada cierto número de tramas.
- Implementación de otras contramedidas cuando el dispositivo cliente o el AP, detectan un error en el MIC, ya que es un fuerte indicador de un ataque activo. Estas contramedidas son las siguientes:
  - Registro de eventos de seguridad.
  - Limitación de fallos de MIC. Si se detectan varios fallos en un intervalo de tiempo concreto, se rechazan durante un periodo de tiempo nuevas asociaciones.
  - Cambio de la PTK (Pairwise Transient Key) y GTK (Group Temporal Key). Las claves temporales son eliminadas y deben ser reinicializadas.
  - Bloqueo de puertos IEEE 802.1X.

Durante el proceso de desencapsulado se realizan varias comprobaciones en las tramas. Si el TSC indica que hay una violación en el secuenciado de la trama, se descarta. Además, el MIC se recalcula con los datos recibidos y se compara con el incorporado en el paquete y, si no coinciden, la trama se descarta y se invocan las contramedidas TKIP.

Indicar que actualmente, tanto el algoritmo de cifrado RC4, como el mecanismo de integridad MIC, presentan vulnerabilidades ampliamente conocidas, por lo que no se recomienda el uso de TKIP.

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)

CCMP fue diseñado para ofrecer el máximo nivel de protección. Sin embargo, el consumo computacional que exige el algoritmo central de CCMP (AES), hace que esta suite no sea compatible con el hardware inalámbrico WEP, siendo necesaria la sustitución del mismo.

CCMP es un mecanismo de encapsulación de datos basado en CCM[2] (Counter Mode with CBC-MAC), que combina dos técnicas: CTR para la protección de confidencialidad y CBC-MAC para la protección de la integridad y autenticidad.

CTR y CBC son dos modos de operación de cifradores de bloque. Los cifradores de bloque son algoritmos de cifrado solo válidos para cifrar y descifrar bloques de un tamaño fijo de bits. Los modos de operación son algoritmos que describen cómo aplicar repetidamente el cifrado de bloque, para cifrar de forma segura cantidades de datos superiores a un bloque.

El cifrador de bloque que utiliza CCM es AES y con un tamaño de clave y de bloque de 128 bits.

El modo de operación CTR (Counter Mode) para cifradores de bloque, hace que estos operen como si fuesen cifradores de cadena. La función de cifrado se aplica a un grupo de bloques de entrada, denominados contadores (counters), produciendo una secuencia de bloques de salida que se combinan mediante XOR con el texto plano para producir el texto cifrado. Cada contador empleado en la secuencia de cifrado bajo la misma clave, debe ser distinto del resto. Estos contadores pueden estar combinados o concatenados con un vector de inicialización o *nonce*.

CTR por sí solo no protege la integridad del mensaje, cumpliendo únicamente con un propósito de protección de confidencialidad. Para proteger la integridad es necesario proporcionar un MAC junto al texto cifrado.

La siguiente figura muestra el esquema del cifrado CTR.

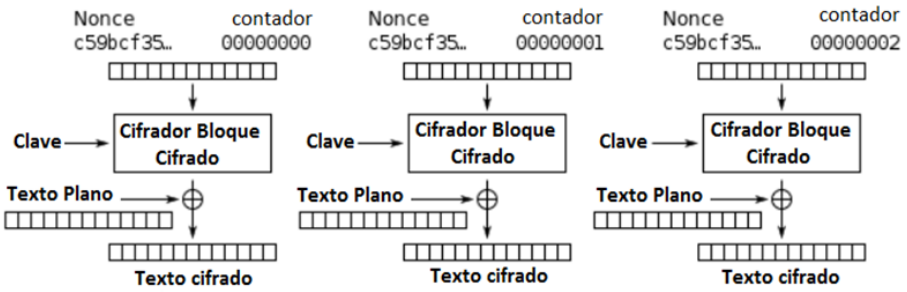

Figura 10. Cifrado CTR.

2 CCM está definido en la RFC 3610 *Counter with CBC-MAC (CCM)*

CBC-MAC (Cipher Block Chaining Message Authentication Code) es una técnica que permite obtener un MAC a partir de un cifrado en bloques, donde cada bloque en texto plano se mezcla empleando una función XOR, con el bloque de texto cifrado que le precede. Para calcular el CBC-MAC de un mensaje m, este se divide en bloques (m1, m2,… mx) y se cifra en modo CBC con vector de inicialización cero.

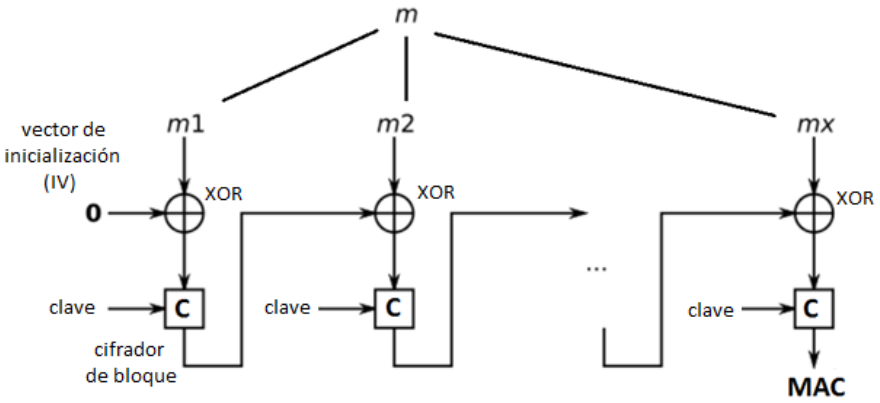

Figura 11. Cifrado CBC-MAC.

Las dos técnicas utilizadas en CCM (CTR y CBC-MAC) se aplican siguiendo lo que se llama autentica y entonces, cifra, es decir, primero se computa CBC-MAC sobre el mensaje para obtener el valor X y posteriormente, el mensaje y el valor X se cifran con el modo CTR. Para ambas técnicas se puede utilizar la misma clave.

ANEXO D. AUTENTICACIÓN 802.1X / EAP

El estándar IEEE 802.1X (protocolo de control de acceso basado en puerto) es una solución de seguridad ratificada por el IEEE en junio de 2001, que permite autenticar a un usuario que solicite acceder a la red. Fue desarrollado originalmente para redes LAN cableadas con objeto de evitar el uso no autorizado en entornos abiertos, de modo que solo los terminales autorizados pudieran acceder a los recursos de la red. Posteriormente, esta idea se adaptó para poder extender su uso a redes inalámbricas.

802.1X proporciona los medios necesarios para bloquear el acceso de los usuarios hasta que la autenticación sea exitosa, controlando así el acceso a los recursos de la red inalámbrica. Es un entorno basado en mecanismos de autentificación, autorización y distribución de claves, y además incorpora controles de acceso para los usuarios que se asocien a la red.

Como se ha indicado en apartados anteriores, 802.1X define varios términos relacionados con la autenticación: suplicante (dispositivo cliente que solicita la autenticación), autenticador (AP) y Servidor de Autenticación (AS). El Servidor de Autenticación (AS) determina, a partir de las credenciales proporcionadas por el suplicante, si éste está autorizado a acceder a los servicios proporcionados por el autenticador. Otra de las funciones principales del AS es la de generar e intercambiar las claves criptográficas con el dispositivo cliente, y distribuirlas de forma segura al AP. La figura siguiente, muestra las dos funciones del Servidor de Autenticación.

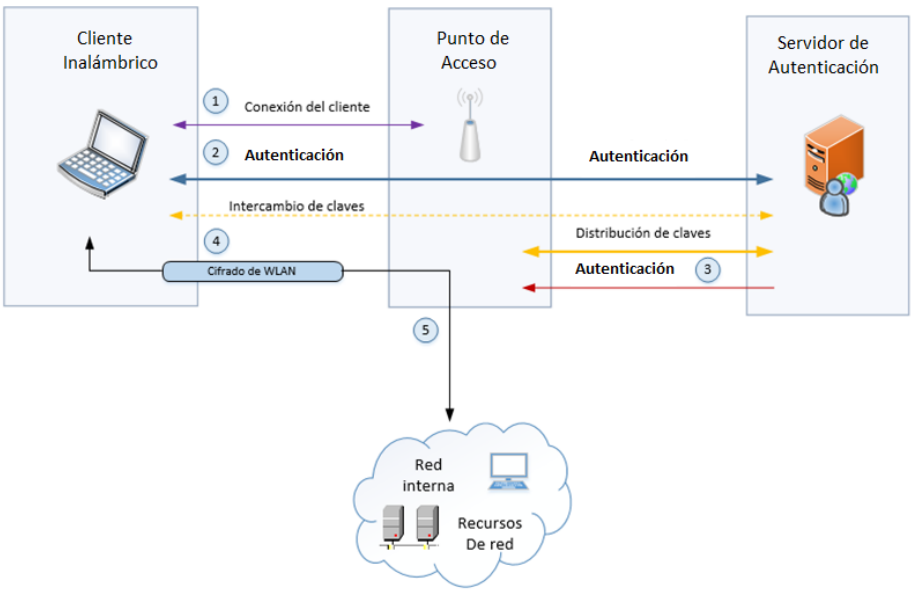

Figura 12. Función de autenticación y de distribución de claves del AS.

El protocolo EAP (Extensible Authentication Protocol)[3] se emplea durante la fase de autenticación de 802.11i. EAP proporciona el marco de autenticación para las RSN 802.11i que utilizan el protocolo de control de acceso basado en puerto IEEE 802.1X.

3 EAP se define en la RFC 3748 "Extensible Authentication Protocol (EAP)"

EAP no es un protocolo de autenticación, sino un protocolo encargado del transporte, encapsulado y seguridad del proceso de autenticación. Existen diferentes "métodos EAP" en función de los mecanismos de autenticación que se desee utilizar: autenticación basada en contraseñas, certificados digitales, *tokens*, etc. También soportan una combinación de mecanismos de autenticación (por ejemplo, un certificado y una contraseña).

EAP se utiliza también para implementar el proceso de generación, acuerdo y distribución de claves criptográficas entre el dispositivo cliente y el Servidor de Autenticación (AS). Estas claves serán utilizadas por la suite criptográfica, para la protección de la comunicación en la RSN. Este material criptográfico puede ser derivado de mutuo acuerdo entre el dispositivo cliente y el AS, o puede ser generado por el AS y distribuido al dispositivo cliente. El AS posteriormente deberá distribuirlo por un canal seguro al AP.

Existen multitud de métodos EAP, que lo hacen muy versátil para cualquier tipo de implementación. IEEE 802.11i no especifica ningún método EAP particular para la RSN. Lo que sí define son una serie de suposiciones y requisitos básicos que debe cumplir el método EAP empleado, para permitir que el modelo de seguridad de IEEE 802.11i se mantenga. Si el método EAP y el mecanismo de autenticación empleado son débiles, se pueden debilitar seriamente las protecciones de seguridad de la RSN.

Cada método EAP tiene sus propias características de seguridad, de modo que algunos métodos tendrán características que otros no tengan. No todos los métodos proporcionan la protección necesaria para una red inalámbrica. La RFC 4017[4] identifica las características de seguridad obligatorias, las recomendables y las opcionales para redes inalámbricas.

La siguiente tabla recoge un resumen de las principales características de seguridad[5]:

Característica de Seguridad	Nivel Requerido	Descripción
Generación y distribución de claves criptográficas	Obligatorio	Es requisito imprescindible que el método EAP pueda generar y distribuir el material de claves criptográficas a emplear, posteriormente, por la suite criptográfica para la protección del tráfico de datos 802.11i.
Fortaleza de clave	Obligatorio	El material de claves generado debe tener una fortaleza mínima: al menos 128 bits de longitud efectiva de clave, y debe generarse una MSK (Master Session Key) y una EMSK (Extended Master Session Key) de al menos 512 bits.

4 RFC 4017 "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs".

5 Para conocer los requisitos de seguridad completos, deben consultarse las RFC 4017 y RFC 3748.

Característica de Seguridad	Nivel Requerido	Descripción
Autenticación Mutua	Obligatorio	El método EAP debe proporcionar la autenticación mutua entre el dispositivo cliente y el AS en el mismo intercambio.
Compartición de parámetros de estado	Obligatorio	Es imprescindible que el AS y el dispositivo cliente compartan ciertos parámetros de estado, asociados con el método EAP: número de versión del método, credenciales proporcionadas y aceptadas y cualquier otro atributo propio del método, que haya sido negociado entre ambos.
Resistencia frente ataques de diccionario	Obligatorio	En caso de que el método EAP se base en contraseña, deberá proporcionar resistencia contra ataques de diccionario. Es decir, no permitirá a un individuo no autorizado capturar tráfico EAP, y utilizar un diccionario de contraseñas comunes para adivinar la contraseña.
Resistencia frente ataques *man-in-the-middle* ("hombre en el medio")	Obligatorio	El método EAP deberá ser resistente a ataques *man-in-the-middle*. Es decir, un individuo no autorizado no podrá emplear un dispositivo para suplantar al AP en la comunicación con el dispositivo cliente, ni viceversa.
Negociación de la suite criptográfica EAP	Recomendable	Es recomendable que el método EAP pueda negociar el uso de la suite criptográfica a emplear en el intercambio de mensajes EAP.
Fragmentación de paquetes	Recomendable	Es recomendable que el método EAP permita la fragmentación de paquetes, para poder manejar mensajes de mayor tamaño que la MTU (Máxima Unidad de Transmisión) EAP.
Confidencialidad	Opcional	La confidencialidad se refiere al cifrado de los mensajes EAP, incluidas las peticiones y respuestas, los indicadores de éxito o fallo y las identidades de usuario EAP.
Reconexión rápida	Opcional	Se refiere a la capacidad de un método EAP para actualizar una asociación de seguridad previamente establecida, usando menos mensajes de los necesarios para crear la asociación inicial.

Tabla 5. Características de seguridad de los métodos EAP para redes inalámbricas.

Los métodos EAP actualmente existentes, salvo aquellos que son propiedad de fabricantes, se encuentran en el Registro de IANA[6].

La selección del método EAP más apropiado para una red inalámbrica puede resultar una tarea compleja. Dependerá de los mecanismos de autenticación que se vayan a emplear, los cuales deberán ser soportados por el método EAP, y de las características de seguridad que requiera la red inalámbrica, ya que como se ha comentado anteriormente, no todos los métodos proporcionan las mismas características de seguridad.

Dado que los métodos EAP deben ser capaces de generar y distribuir el material de claves criptográficas (característica obligatoria), y esto representa un proceso complejo, es recomendable el uso de tecnologías maduras en este aspecto. Esto limita mucho las posibilidades de elección entre los métodos EAP. Actualmente[7], solo cumplen este requisito los métodos basados en TLS.

TLS (Transport Layer Security)[8] es un protocolo de autenticación que proporciona la autenticación de servidor frente el cliente o la autenticación mutua entre servidor y cliente, así como la negociación segura de la suite criptográfica y el intercambio de material de claves entre las partes. TLS ha sido establecido como protocolo de autenticación a utilizar con EAP, existiendo varios métodos EAP basados en TLS.

Todos los métodos EAP basados en TLS soportan, además, los requisitos obligatorios para redes inalámbricas indicados en la RFC 4017 (ver tabla 5 del Anexo D). Respecto a los requisitos recomendables y opcionales, en general también los cumplen, aunque en algunos casos depende de la implementación del método.

Los cuatro métodos más extendidos basados en TLS son: EAP-TLS, EAP-TTLS, PEAP y EAP-FAST.

- **EAP-TLS**[9] se considera uno de los métodos más seguros para las redes inalámbricas y está ampliamente soportado por los fabricantes de dispositivos inalámbricos. Utiliza certificados X.509 como mecanismo de autenticación de cliente y servidor, de ahí su fortaleza de autenticación. Si, además, las claves privadas asociadas al certificado son almacenadas en una tarjeta o dispositivo hardware, la seguridad se verá incrementada. Sin embargo, el hecho de tener que desplegar una PKI y certificados en todos los dispositivos cliente, complica la operación y mantenimiento.
- **EAP-TTLS** (Tunneled TLS)[10] es un método que se basa en el uso de TLS, pero no requiere certificados X.509 para la autenticación del cliente, solo es necesario para la autenticación del servidor. Una vez que el Servidor de Autenticación se

6 IANA Extensible Authentication Protocol Registry: http://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml#eap-numbers-4
7 Dado el constante avance tecnológico, será necesario considerar que los métodos EAP van actualizándose y saliendo nuevos métodos.
8 TLS 1.2 se define en la RFC 5246.
9 EAP-TLS se define en la RFC 5216 "The EAP-TLS Authentication Protocol".
10 La RFC 5281 proporciona información sobre EAP-TTLSv0.

ha autenticado en el cliente (validando el certificado), se establece entre el AS y el dispositivo cliente una conexión segura (túnel). A través de este túnel se realizará la autenticación de cliente pudiendo utilizarse cualquier mecanismo o incluso varios: contraseñas, *tokens*, etc. ya que esta información de autenticación irá protegida.

- **PEAP** (Protected Extensible Authentication Protocol) es un método muy similar a EAP-TTLS. Tampoco requiere certificados para autenticación del cliente, solo para el servidor. Igualmente establece un canal de comunicación protegido para las transacciones de autenticación de cliente en el servidor. Dado que son muy similares, es probable que uno de los dos métodos (PEAP y EAP-TTLS) desaparezca, pero no se puede intuir cuál de ellos será, ya que actualmente están apoyados por unos y otros fabricantes.
- **EAP-FAST** es otro método EAP basado en TLS, creado por Cisco. Lo que lo diferencia de otros métodos basados en TLS, es que establece el canal seguro de comunicación utilizando lo que se llama PAC (Protected Access Credential), que es un mecanismo de clave pre-compartida PSK y no requiere por lo tanto el uso de certificados en el servidor y en el cliente. El problema de este método es el establecimiento de la PAC inicial, que o bien se hace a través de certificados, con lo que este método pierde la ventaja frente a EAP-TTLS o PEAP, o se hace a través de canales no seguros. Actualmente solo Cisco soporta este método.

ANEXO E. DETECCIÓN DE INTRUSIÓN (SISTEMAS WIDPS)

Los Sistemas de Detección de Intrusiones (IDS), son aplicaciones capaces de detectar los accesos no autorizados a una red o a un equipo informático. Los Sistemas de Prevención de Intrusiones (IPS), además de detectar, son capaces de tomar acciones para evitar estos accesos no autorizados.

Estos sistemas, tienen su versión para la detección de intrusiones en redes inalámbricas, y se denominan WIDS (Wireless IDS) o WIPS (Wireless IPS). Están compuestos por los siguientes elementos:

- Sensores: dispositivos que monitorizan y capturan la actividad de la red.
- Servidores de Administración: equipos que analizan la información enviada por los sensores.
- Servidores de Base de Datos: equipos que almacenan los eventos generados por los servidores de administración, tras su análisis.
- Consola: interfaz de gestión y control del sistema.

En la siguiente figura se muestra una arquitectura típica de WIDS / WIPS.

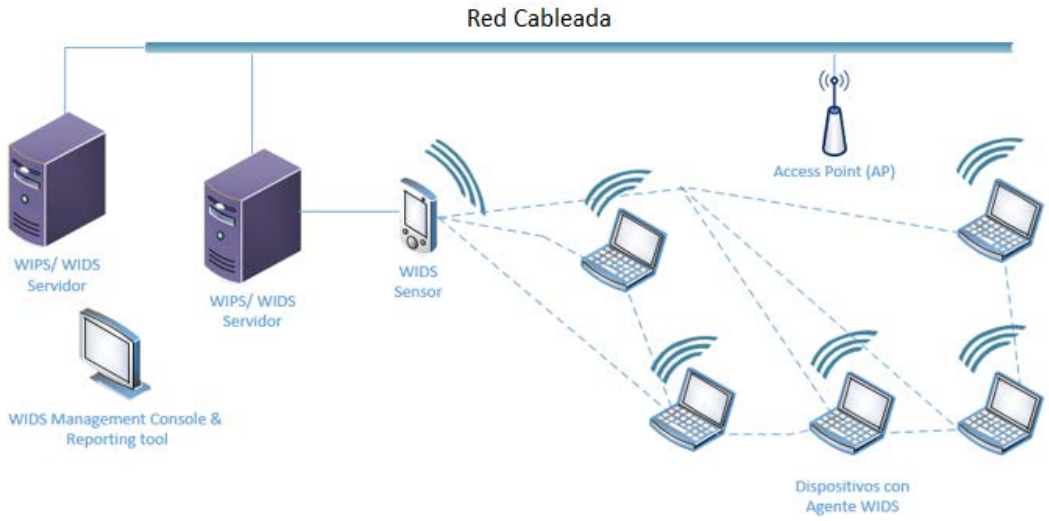

Figura 13. Arquitectura de un Sistema WIDS / WIPS.

Los sensores de los WIDS / WIPS pueden ser de varios tipos:

- Dedicados: son dispositivos independientes y dedicados únicamente a esta función de sensor. Algunos sensores pueden analizar el tráfico, y otros únicamente lo capturan y envían al Servidor de Administración para su análisis. Los sensores están conectados a la red cableada y pueden ser fijos o móviles. Los sensores fijos se instalan en una localización fija donde puedan disponer de alimentación, conexión a la red cableada, etc. Los sensores móviles están diseñados para ser portables y poder usarse en distintas localizaciones o incluso en movimiento.

- No dedicados: el sensor no es un dispositivo, sino una función integrada en otros dispositivos de la red inalámbrica, como AP o conmutadores.
- Sensores software en dispositivo cliente: son unidades software que se instalan en los dispositivos cliente y tienen la función de detectar ataques en su rango de frecuencias, o vulnerabilidades dentro de los dispositivos cliente y enviar esta información a los Servidores de Administración. Estos sensores software pueden utilizarse también para reforzar las políticas de seguridad en los dispositivos clientes.

Algunas de las funciones de los WIPS / WIDS son las siguientes:

- Permitir detectar y alertar la presencia de dispositivos inalámbricos no autorizados: clientes y AP (rogue AP).
- Operar en base a políticas de seguridad establecidas.
- Relacionar paquetes capturados para comparar y verificar su origen. Pueden verificar la dirección MAC del dispositivo para comprobar si se encuentra en listas autorizadas y alertar a un administrador ante discrepancias.
- Para evitar la falsificación de direcciones MAC (MAC spoofing), algunos WIPS de alto nivel son capaces de analizar las firmas únicas de radiofrecuencia que los dispositivos inalámbricos generan, y bloquear las desconocidas.
- Detectar el estado de conexión de todos los clientes.
- Detectar comunicaciones Ad Hoc no permitidas entre los clientes.
- Detectar ataques de denegación de servicio (DoS) en el proceso de autenticación.
- Detectar ataques de suplantación y *man-in-the-middle* (“hombre en el medio”).
- Administración, gestión y monitorización remota de los sensores.
- Detectar dispositivos inalámbricos con una configuración incorrecta (distinta de la configuración de seguridad).
- Detectar patrones de tráfico no habituales y sospechosos.

El sistema WIDS / WIPS debe tener la misma cobertura que la red inalámbrica, para evitar que individuos no autorizados se instalen en zonas donde puedan eludir el sistema de detección.

El sistema WIDS debe tener visibilidad completa de la red inalámbrica. Revisará todos los canales posibles del espectro de frecuencias (incluyendo los 200 canales extendidos) y también los canales de espectro de móviles, asegurando que no haya puntos ciegos en los que dispositivos falsos o que generan interferencias, se puedan estar ocultando.

ANEXO F. CONFIGURACIÓN DE UN CLIENTE MICROSOFT WINDOWS

En este Anexo se recoge un ejemplo de cómo configurar una conexión a red inalámbrica para un cliente Microsoft Windows 7 Enterprise. En el ejemplo se muestra la selección de las distintas opciones de seguridad de la conexión, tanto de autenticación, como de cifrado.

Las posibilidades de selección se recogen en el árbol de opciones mostrado en la siguiente figura:

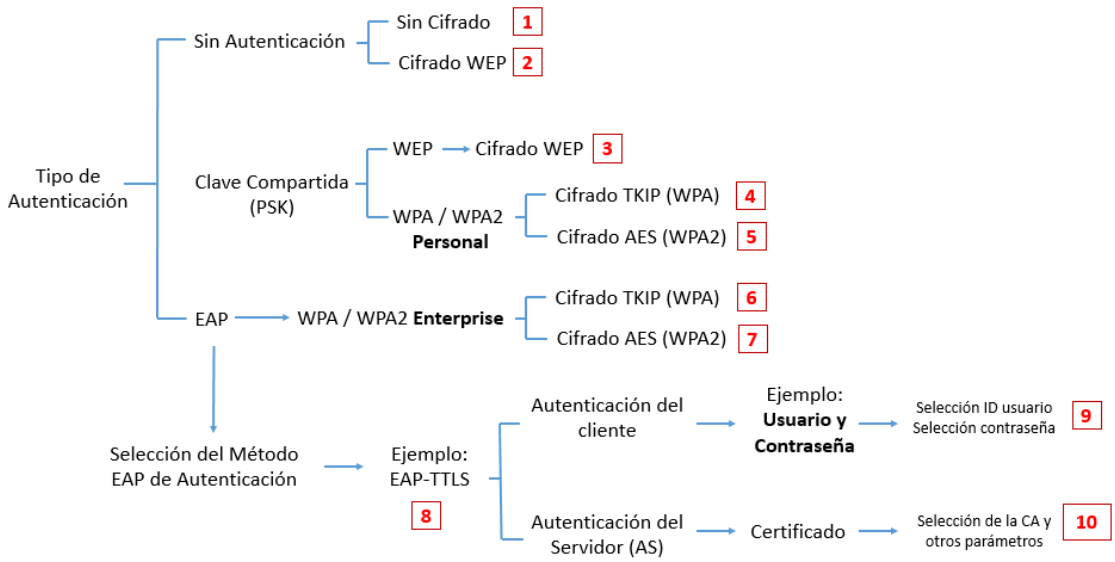

Figura 14. Árbol de opciones de configuración de conexión inalámbrica en cliente Windows.

Como indica en el Apartado 5.2.2 relativo a la autenticación, el primer paso es la selección del tipo de autenticación. El cliente Windows permite seleccionar "Sin autenticación" (opciones 1 y 2 de las figuras), pero para implementar 802.11i debemos seleccionar uno de sus dos tipos de autenticación:

- **Por clave compartida (PSK)**, lo cual nos lleva a la implementación "Personal" de WPA y WPA2 (opciones 4 y 5 de las figuras).
- **A través de protocolo 802.1X / EAP**, lo cual nos lleva a la implementación "Enterprise" de WPA y WPA2 (opciones 6 y 7 de las figuras).

Se escogerá también el algoritmo de cifrado. IEEE 802.11i proporciona dos algoritmos de cifrado:

- **TKIP**, implementado de forma obligatoria en WPA y de forma opcional en WPA2 (opciones 4 y 6 de las figuras).
- **AES**, implementado de forma obligatoria en WPA2 y de forma opcional en WPA (opciones 5 y 7 de las figuras).

En las siguientes figuras se muestran las pantallas de configuración de la conexión de red y las ventanas de selección de las opciones (1 a 7) anteriormente descritas.

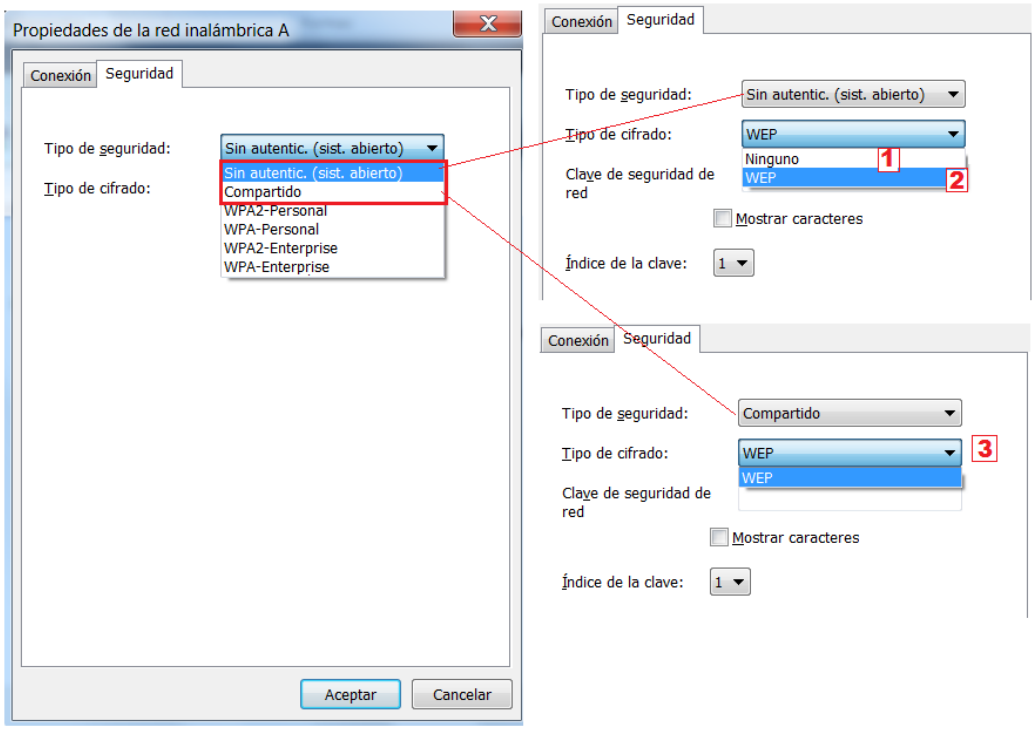

Figura 15. Configuración de la conexión inalámbrica en cliente Windows (I).

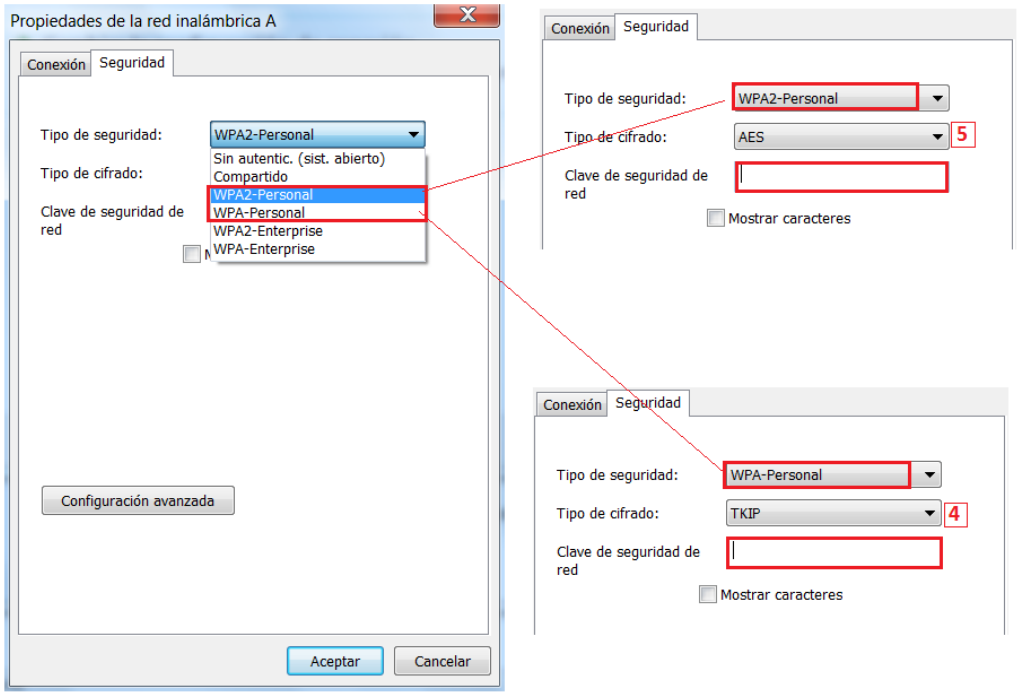

Figura 16. Configuración de la conexión inalámbrica en cliente Windows (II).

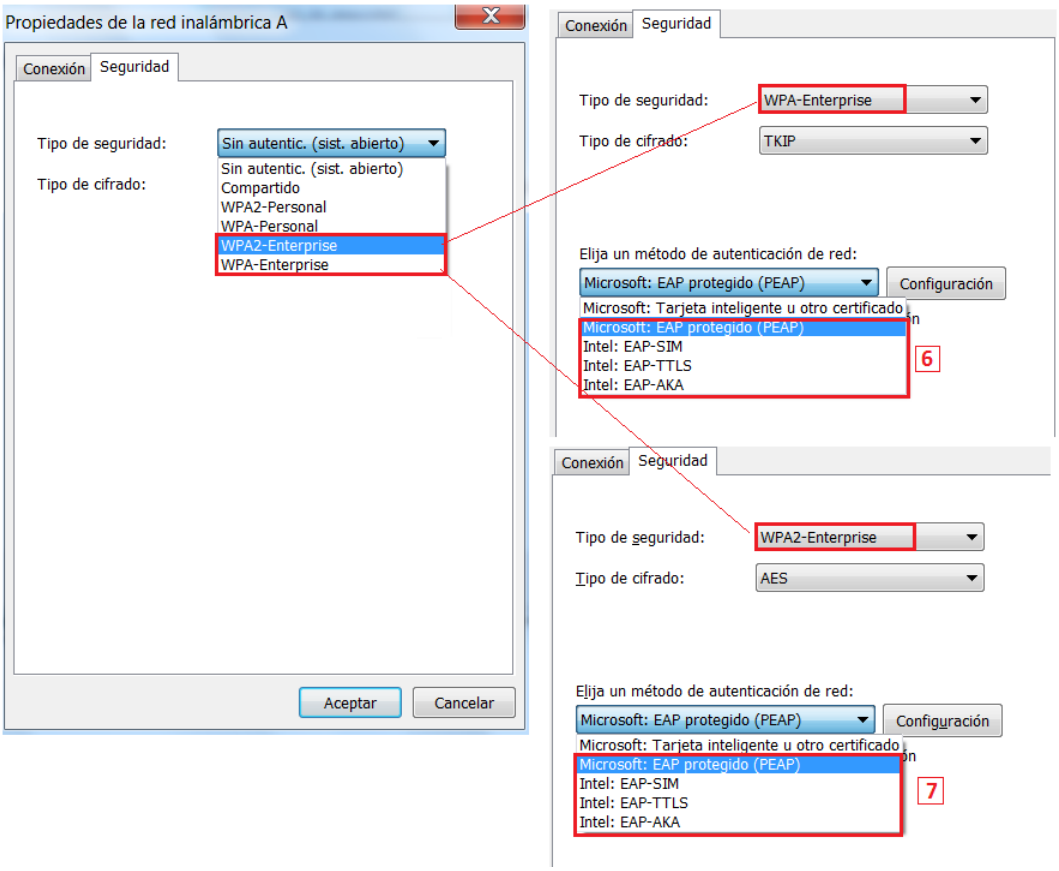

Figura 17. Configuración de la conexión inalámbrica en cliente Windows (III).

Al seleccionar como Tipo de autenticación 802.1X/EAP, el siguiente paso consiste en escoger el método EAP de autenticación. Como se indica en el Apartado 5.2.2 y en el Anexo D, la selección de este método depende: (a) del mecanismo de autenticación de cliente y servidor que se vaya a emplear (contraseñas, certificado, etc.), el cual deberá ser soportado por el método EAP, y (b) de las características de seguridad requeridas para la red inalámbrica, ya que unos métodos proporcionan unas características de seguridad que otros no proporcionan (ver tabla 5 del Anexo D).

En el ejemplo mostrado en las figuras se ha seleccionado el método EAP-TTLS. Este método implica que sólo el Servidor de Autenticación (AS) requiere certificado para la autenticación con el cliente. Respecto al mecanismo de autenticación del cliente, se ha seleccionado credenciales de usuario / contraseña, implementado a través del protocolo MS-CHAP-v211.

11 MS-CHAP (*Microsoft Challenge Handshake Protocol*) es la versión de Microsoft del protocolo de autenticación por contraseñas basado en el proceso de "desafío mutuo" (*challenge / response*). Básicamente implica que el Servidor de Autenticación (AS) envía al cliente un "desafío" (*challenge*), compuesto por un identificador de sesión y una secuencia arbitraria. El cliente envía una "respuesta" que contiene el ID de usuario, junto con un *Hash* del "desafío", el identificador de sesión y la contraseña. Finalmente, el Servidor de Autenticación (AS) verifica que la respuesta es correcta y que coincide con la contraseña que tiene almacenada del cliente.
MS-CHAP-v2 se define en la RFC 2759.

En la siguiente figura se muestran las pantallas de configuración de la conexión de red y las ventanas de selección de estas opciones (8 a 10).

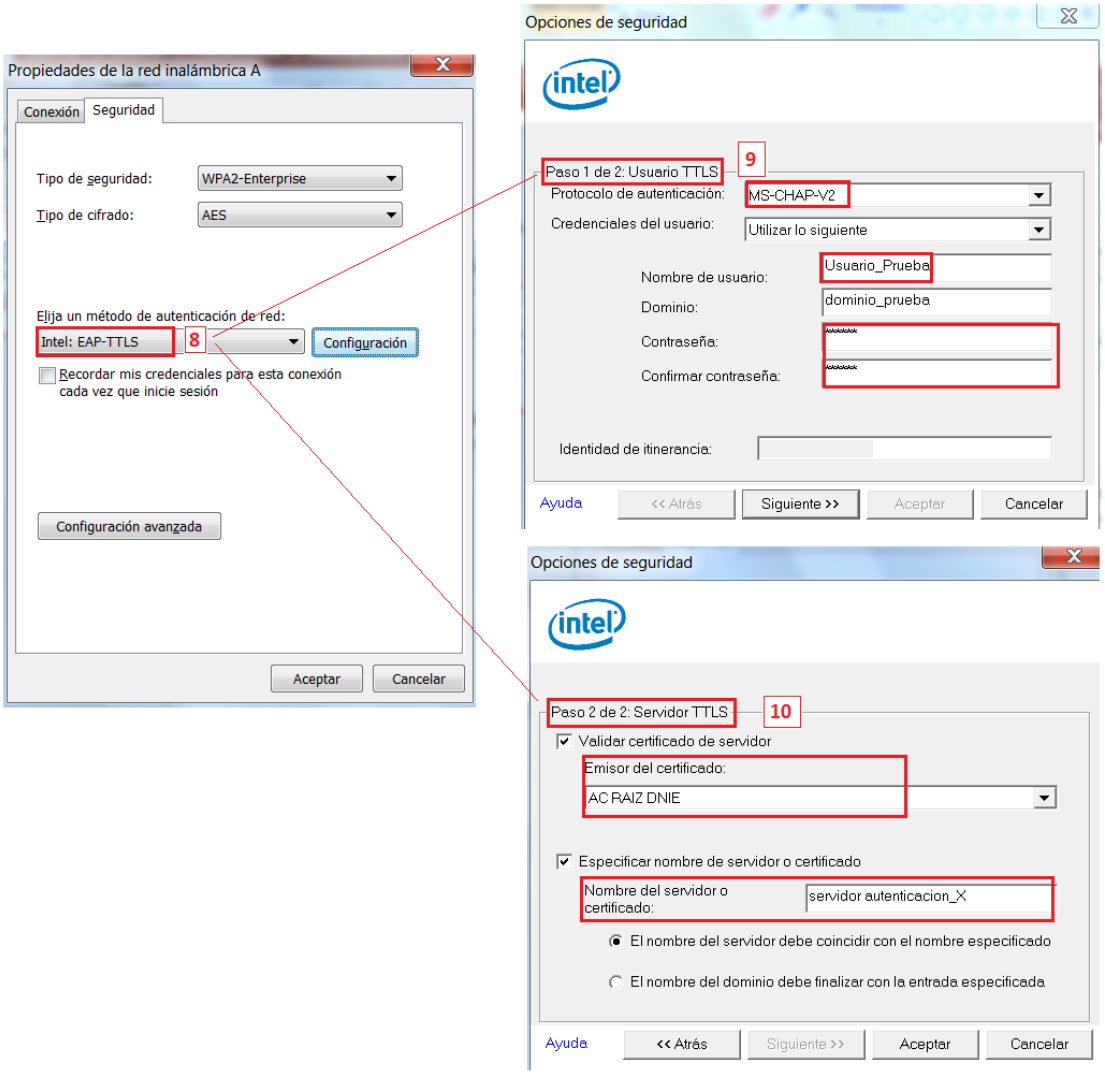

Figura 18. Configuración de la conexión inalámbrica en cliente Windows (IV).

Se puede observar en la figura anterior, que en la configuración de los parámetros de autenticación del servidor (AS), permite seleccionar:

- La Autoridad de Certificación (CA) emisora del certificado que se considerará válida. Se ofrece la versión "cualquier CA de confianza". En la tabla 4 del Anexo A, la RM5 indica que es recomendable seleccionar la CA concreta emisora del certificado del Servidor, para evitar falsificaciones de certificados emitidos por otra CA que pueda estar reconocida en el cliente.
- El nombre del Servidor de Autenticación (AS). En la RM5 también se indica que es recomendable especificar el nombre completo de dominio del servidor, para sólo aceptar certificados procedentes de ese servidor concreto, y evitar falsificaciones.

ANEXO G. GLOSARIO DE TÉRMINOS

AAA (Authentication Authorization and Accounting). Familia de protocolos que realizan tres funciones: Autenticación (prueba de identidad de una entidad a otra), Autorización (concesión de privilegios de acceso a la entidad autenticada) y Contabilización (seguimiento del consumo de recursos por parte de la entidad autenticada y autorizada). Los protocolos AAA más conocidos son RADIUS y TACACS.

AS (Authentication Server). Servidor que proporciona un servicio de autenticación de entidades que se conectan a la red o a un recurso corporativo.

AP (Access Point). El Punto de Acceso inalámbrico es un dispositivo inalámbrico (wireless) encargado de proporcionar el servicio de conexión a la red, a los dispositivos cliente inalámbricos.

Autenticación. Es el acto de confirmar que algo (o alguien) es quien dice ser. Para ello la parte que debe verificar la identidad, solicita ciertas evidencias a la parte que debe probar su identidad. La verificación de que estas evidencias son correctas proporciona la autenticación. Cuando los dos participantes en una comunicación se autentican el uno frente al otro, se llama autenticación mutua.

Autenticación de origen (*Data Origin Authentication*). Propiedad que permite al receptor verificar que el mensaje no ha sido alterado en el tránsito (integridad de datos) y que ha sido originado del emisor legítimo (autenticidad).

Autenticidad. Propiedad o característica que garantiza la fuente de la que proceden los datos.

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). Protocolo de seguridad usado por IEEE 802.11i (WPA2). CCMP está basado en modos de operación del cifrador de bloque AES. Combina dos técnicas: CTR para la protección de confidencialidad y CBC-MAC para la protección de la integridad y autenticidad.

Cifrador de bloque. Es un algoritmo solo válido para cifrar y descifrar bloques de bits de tamaño fijo.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

DHCP (Dynamic Host Configuration Protocol). Protocolo de configuración dinámica de Host (DHCP), es un protocolo cliente-servidor que proporciona de forma automática a un host (cliente) una dirección IP dinámica y otros parámetros de configuración de red como, por ejemplo, la puerta de enlace predeterminada y la máscara de subred.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Dominios de seguridad. Conjunto de usuarios y sistemas sujetos a requisitos de seguridad comunes. Unos ejemplos de dominios de seguridad serían: Dominio de Uso Público, Dominio Difusión limitada, Dominio Confidencial.

EAP (Extensible Authentication Protocol). Protocolo que se emplea durante la fase de autenticación para las RSN 802.11i que utilizan el protocolo de control de acceso basado en puerto IEEE 802.1X. EAP no es un protocolo de autenticación, sino un protocolo encargado del transporte, encapsulado y seguridad del proceso de autenticación.

GMK (Group Master Key). Clave maestra que se derivada en la jerarquía de claves Group Key Hierarchy (GKH) a partir de las claves raíz (*root keys*) de las que disponen los dispositivos inalámbricos. A partir de la GMK se derivan las demás claves criptográficas usadas para la protección y cifrado de tráfico *multicast / broadcast*.

Integridad. Propiedad o característica consistente en que el archivo de información no ha sido alterado de manera no autorizada.

MAC (Message Authentication Code). Información utilizada para autenticar un mensaje, es decir, para confirmar que el mensaje provenía del remitente declarado (su autenticidad) y no ha sido cambiado en tránsito (su integridad).

Modo de operación de cifrador de bloque. Es un algoritmo describe cómo aplicar repetidamente la operación de cifrado de bloque para cifrar de forma segura cantidades de datos mayores que un bloque.

MSK (Master Session Key) o **AAAK** (Authentication, Authorization and Accounting Key*)*. Clave maestra generada por los métodos EAP y distribuida entre el Servidor de Autenticación (AS) y el dispositivo cliente. A partir de la MSK, se genera la PMK (Pairwise Master Key) de la que se deriva todo el material de claves.

Multicast y Broadcast. Envío de información a varios receptores (multicast) o a todos los receptores de la red (broadcast). En el caso de redes 802.11, los mecanismos de protección de la comunicación entre los dispositivos cliente y el AP, utilizan la jerarquía de claves de grupo GKH (Group Key Hierarchy).

Nonces. Es un valor arbitrario de un solo uso, utilizado en criptografía. Normalmente es un número aleatorio o pseudo-aleatorio que se utiliza en los protocolos de autenticación, para evitar el empleo de paquetes antiguos de la comunicación en ataques de reenvío (*replay attacks*). También se utilizan como vectores de inicialización (IV) en funciones hash criptográficas.

OSI *(*Open Systems Interconnection). Modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization).

PKI (Public Key Infraestructure). Una Infraestructura de clave pública es una Infraestructura hardware y software, que junto con políticas y procedimientos de seguridad ofrece servicios de seguridad, como autenticación, cifrado y no repudio de transacciones. Está formada por una serie de componentes, entre ellos la Autoridad de Certificación (CA) encargada de emitir y revocar certificados, y la Autoridad de Registro (RA) encargada de verificar el enlace entre la clave pública, el certificado y la identidad del titular. PKI proporciona la infraestructura para el uso de certificados que podrán a su vez utilizarse para autenticación, firma y cifrado.

PMK (Pairwise Master Key). Clave maestra que se derivada en la jerarquía de claves Pairwise Key Hierarchy (PKH) a partir de las claves raíz (*root keys*) de las que disponen los dispositivos inalámbricos. A partir de la PMK se derivan las demás claves criptográficas usadas para la protección y cifrado de tráfico *unicast*.

PSK (Pre-shared Key). La clave pre-compartida, es una clave secreta conocida y compartida entre el AP y los dispositivos cliente, necesaria para la autenticación y acceso a la red inalámbrica. Se distribuye previamente a través de un canal fuera de banda (*out-of-band*).

RSN (Robust Security Networks). Concepto introducido por IEEE 802.11i con el que se denomina a las redes seguras, que son aquellas redes inalámbricas que solo permiten la creación de asociaciones de red seguras RSNA (*Robust Security Network Associations*).

RSNA *(*Robust Security Associations). Son asociaciones lógicas establecidas entre los participantes de la comunicación 802.11i, que cuentan con un proceso automático de generación y distribución de claves criptográficas (llamado protocolo de negociación en 4 pasos, *4-Way Handshake*).

SSH *(*Secure Shell*)*. Protocolo de nivel de aplicación que permite acceder de forma remota, a servidores y otros equipos de forma segura.

SSID (Service Set Identifier). Es un identificador de 32 octetos (habitualmente una cadena legible de caracteres) que identifica la red inalámbrica, y que va incluido en todos los paquetes de datos intercambiados en esa red. Los dispositivos inalámbricos deben conocer el SSID para conectarse a la red inalámbrica.

SSL/TLS (Secure Socket Layer/Transport Layer Security). Protocolo que proporcionan servicios de seguridad a las comunicaciones a través de Internet. Impide que ciertas actividades maliciosas tengan éxito, como escuchas (*eavesdropping*), manipulación (*tampering*) o falsificación de mensajes.

Suite Criptográfica. Conjunto de algoritmos criptográficos y sus parámetros, mediante los que se proporcionan los servicios de seguridad para la protección de las comunicaciones (cifrado, integridad, autenticidad, autenticación, etc.).

TCP/IP *(*Transmission Control Protocol/Internet Protocol*).* Conjunto de protocolos de red que respaldan a Internet y que hacen posible la transferencia de datos entre redes de ordenadores.

TKIP (Temporal Key Integrity Protocol). Protocolo de seguridad usado por IEEE 802.11. Fue diseñado por el grupo de trabajo IEEE 802.11i junto con la Alianza Wi-Fi como solución intermedia para reemplazar WEP sin necesidad de cambiar el equipamiento inalámbrico existente. TKIP utiliza los mismos mecanismos de cifrado que WEP (algoritmo de cifrado RC4) pero proporciona mayor nivel de seguridad utilizando una clave de 128 bits, y cambiando las claves cada cierto número de paquetes.

Unicast. Envío de información entre un único emisor y un único receptor. En el caso de redes 802.11, implica una asociación única entre el dispositivo cliente y el AP, y el uso de la jerarquía de claves emparejadas PKH (Pairwise Key Hierarchy).

Usuarios Remotos. Aquellos usuarios que por necesidades laborales requieren el acceso remoto a los recursos internos de la organización, empleando la infraestructura de un tercero como soporte de comunicaciones (generalmente Internet).

VLAN (Virtual Local Area Network). Método para crear redes lógicas independientes, dentro de una misma red física. Reduce los dominios de difusión (*broadcast*) y permite realizar la segmentación de la red física en tramos independientes y establecer reglas de comunicación entre ellos.

WEP (Wired Equivalent Privacy). Protocolo de seguridad original de las redes inalámbricas 802.11, del que se han detectado múltiples vulnerabilidades.

WIDPS (Wireless Intrusion Detection and Prevention System). Un sistema de detección y prevención de intrusiones inalámbrico es un dispositivo, o un software, que monitoriza la red inalámbrica en busca de actividad maliciosa o violaciones de la política de seguridad, y es capaz de tomar acciones para evitar estos accesos no autorizados.

Wi-Fi. Es una marca de la Alianza Wi-Fi "Wi-Fi Alliance" y hace referencia al mecanismo de conexión de dispositivos inalámbricos.

Wireless. El término significa literalmente "sin cables" y se refiere a tecnologías, dispositivos o redes que no utilizan un medio físico cableado para establecer la comunicación, sino que esta se realiza a través de ondas electromagnéticas.

WPA (Wi-*Fi Protected Access*). Protocolo de seguridad de redes inalámbricas 802.11, creado para solventar las deficiencias encontradas en WEP, sin necesidad de sustituir el equipamiento inalámbrico. Implementa un subconjunto de las especificaciones 802.11i.

WPA2 (Wi-Fi Protected Access 2). Protocolo de seguridad de las redes inalámbricas 802.11i. WPA2 no es compatible, en la mayoría de los casos, con en el hardware inalámbrico WEP, ya que este hardware no soporta la carga computacional que suponen las operaciones de cifrado del algoritmo AES, que es el algoritmo criptográfico central de WPA2.

ANEXO H. REFERENCIAS

- 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.
- Guía CCN-STIC-808 - Verificación del cumplimiento de las medidas en el ENS. Sept. 2011.
- Guía CCN-STIC-807 - Criptografía de empleo en el Esquema Nacional de Seguridad abril 2015.
- CCN-STIC-406: Guía de Seguridad de las TIC. Seguridad en Redes inalámbricas basadas en el estándar 802.11. Dic 2006.
- CCN-STIC-804: Guía de Implantación Esquema Nacional de Seguridad. Marzo 2013.
- SP800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. National Institute of Standards and Technology (NIST). Feb 2007.
- SP800-153: Guidelines for Securing Wireless Local Area Networks (WLAN). National Institute of Standards and Technology (NIST). Feb 2012.
- SP800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks. National Institute of Standards and Technology (NIST). Jul 2008.
- Wi-Fi Alliance [http://www.wi-fi.org/]
- RFC 3748 “Extensible Authentication Protocol (EAP)” https://tools.ietf.org/html/rfc3748
- RFC 4017 “Extensible Authentication Protocol (EAP) Method Requirements for Wireless LAN” https://tools.ietf.org/html/rfc4017