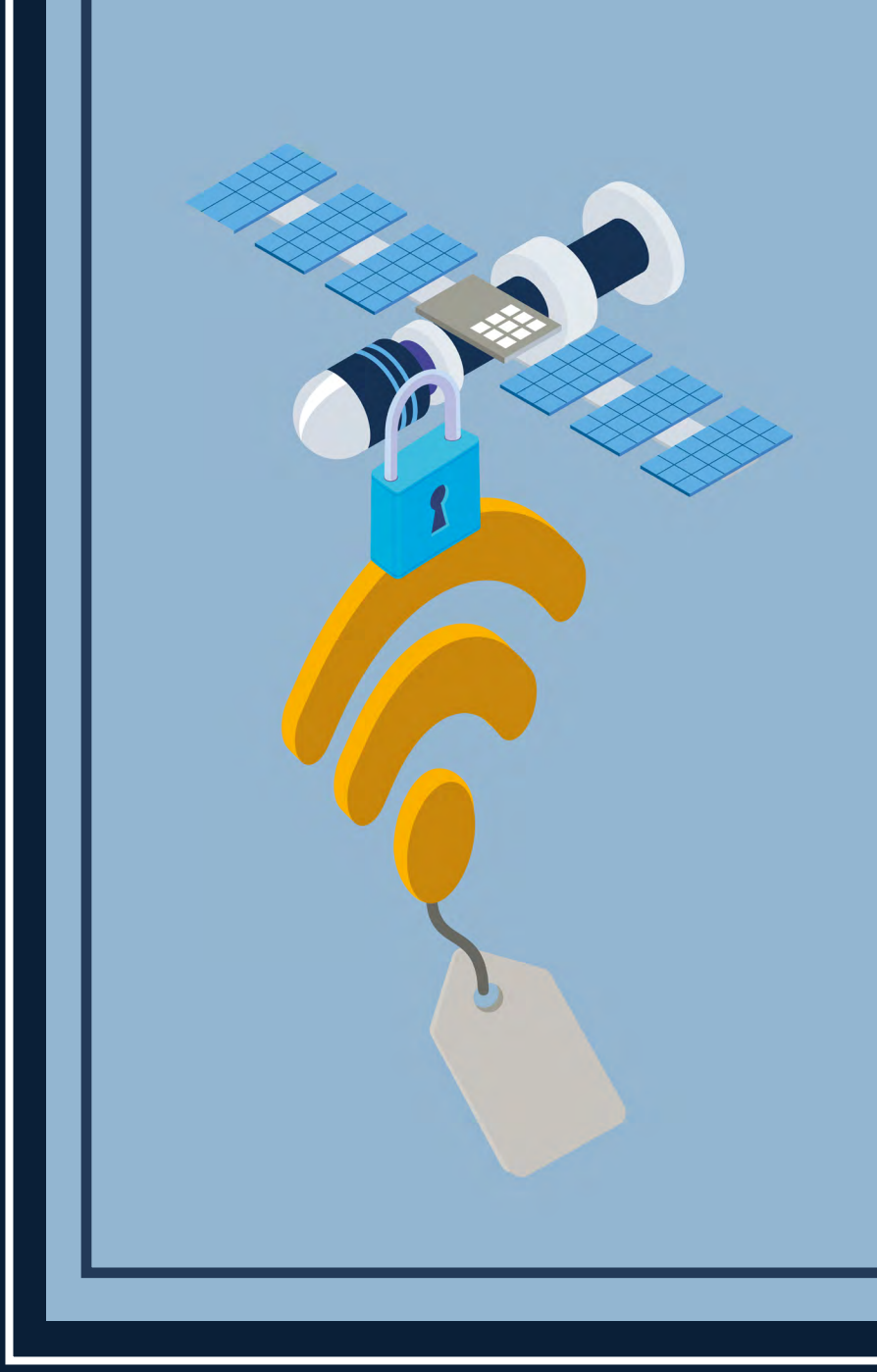
CCN-CERT

BP/11



Recomendaciones de seguridad en redes Wi-Fi corporativas

INFORME DE BUENAS PRÁCTICAS

JULIO **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP SEP - M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.08.13 23:06:50 +02'00'

Centro Criptológico Nacional, 2021

Fecha de edición: julio de 2021

Índice

1. Sobre CCN-CERT, CERT gubernamental nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción a las redes inalámbricas Wi-Fi

Una red inalámbrica se puede definir de forma general como aquella formada por dispositivos con capacidades de comunicarse entre sí a través de ondas electromagnéticas y sin necesidad de cableado (wireless).

Las redes inalámbricas se pueden clasificar en redes inalámbricas personales (WPAN), tales como las basadas en infrarrojos o bluetooth, redes inalámbricas de área local (WLAN), como IEEE 802.11 o HomeRF, y redes inalámbricas de área metropolitana o extendida (WMAN o WWAN): redes de diferentes generaciones como 2G/3G/4G/5G y estándares tecnológicos como CDMA y GSM, GPRS, UMTS, WiMAx (IEEE 802.16) o LTE.

Existen muchos tipos de redes inalámbricas que difieren en características como su tecnología, el estándar de comunicación, su arquitectura, etc. La presente guía se centra en exclusiva sobre las Redes WLAN o Redes Wi-Fi. Estas redes inalámbricas se basan en el estándar IEEE 802.11 y los productos son certificados por la Wi-Fi Alliance para asegurar la interoperabilidad.

Los componentes principales de una red inalámbrica Wi-Fi son:

- **Dispositivos cliente.** Son los equipos de usuario que solicitan conexión a la red inalámbrica para realizar la trasferencia de datos de usuario (ordenadores portátiles, teléfonos inteligentes, 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.

Una red inalámbrica se puede definir de forma general como aquella formada por dispositivos con capacidades de comunicarse entre sí a través de ondas electromagnéticas y sin necesidad de cableado (wireless)

Existen tres topologías comunes a la hora de hablar de redes inalámbricas Wi-Fi: ad-hoc, infraestructura y de malla.

1. En la **topología ad-hoc**, cada nodo forma parte de una red en la que todos los integrantes tienen la misma función y son libres de asociarse a cualquier nodo.

2. En la **topología infraestructura** existe un nodo central (AP), que sirve de enlace para todos los clientes. Este nodo servirá habitualmente para encaminar el tráfico hacia una red convencional o hacia otras redes distintas, convirtiendo tramas en formato 802.11 al formato nativo del sistema de distribución (normalmente 802.3 Ethernet). Para poder establecer la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP o sus repetidores y conocer los parámetros de la red.

3. La **topología de malla** mezcla las dos anteriores (mesh). En esta topología, un equipo actúa como AP y a su vez crea una red punto a punto, en la que cualquier cliente puede conectarse y comunicarse con un equipo que no esté en su rango de cobertura, ya que la conectividad se expande como una malla.

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 WLAN. La capa física ha ido evolucionando mediante la publicación de ampliaciones y modificaciones del estándar 802.11. Cada evolución de la capa física recibe el nombre del grupo de trabajo encargado de la evolución por ejemplo 11b, 11a, 11g, 11n, 11ac, 11ax, 11be… Para simplificar la identificación de las evoluciones tecnológicas, la Wi-Fi Alliance asigna identificadores numéricos correlativos para cada capa física siendo “Wi-Fi 4” el equivalente a 802.11n, “Wi-Fi 5” a 802.11ac, “Wi-Fi 6” a 802.11ax y todavía sin confirmar “Wi-Fi 7” a 802.11be.

Respecto a los mecanismos de seguridad, el protocolo que se implementaba 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 el IEEE 802.11i como una enmienda al estándar original 802.11 con mecanismos de seguridad más robustos para contrarrestar los problemas de WEP.

El protocolo que se implementaba en el estándar original de IEEE 802.11, denominado WEP ha sido declarado inseguro debido a las múltiples vulnerabilidades detectadas

Mientras se ratificaba la versión definitiva de IEEE 802.11i, 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 (pre-RSN y TKIP). Este protocolo fue aprobado por la Wi-Fi Alliance bajo el nombre de **WPA** (Wi-Fi Protected Access).

Posteriormente, una vez ratificado 802.11i, la Wi-Fi Alliance introdujo WPA2 (Wi-Fi Protected Access 2) que ya certificaba el soporte completo del estándar IEEE 802.11i (RSN y AES). **WPA2** no es compatible, en la mayoría de los casos, con en el hardware inalámbrico diseñado inicialmente para WEP, ya que este hardware no soporta la carga computacional que suponen las operaciones de cifrado del algoritmo AES, que es el algoritmo criptográfico principal de WPA2.

A día de hoy, la mayoría del hardware Wi-Fi tiene soporte de WPA2. WPA (pre-RSN y TKIP) ha sido declarado inseguro y, al igual que WEP, no debe utilizarse en redes corporativas.

WPA y WPA2 tienen dos modos de implementación:

- **Personal (PSK)**, acceso mediante una única clave pre-compartida con todos los clientes.
- **Enterprise (802.1X)**, acceso mediante 802.1X con credenciales dedicadas para cada cliente.

Principalmente, ambas implementaciones difieren en los mecanismos de autenticación y distribución de claves. La Personal utiliza el mecanismo de claves pre-compartidas PSK (Pre-shared Keys) mientras que la Enterprise utiliza el mecanismo de autenticación 802.1X, con el empleo de un Servidor de Autenticación (AS), normalmente, protocolo RADIUS.

En la medida de lo posible todas las redes Wi-Fi deberían utiliza el modo Enterprise con 802.1X y el uso de PSK estaría justificado sólo cuando los clientes no tienen soporte de 802.1X.

En el caso de ser necesario utilizar una red con PSK se recomienda utilizar los mecanismos no estándar que ofrecen algunos fabricantes que permiten asignar una clave pre-compartida diferente para cada dispositivo cliente diferenciando por su dirección MAC.

Durante el 2017 y 2018 se publicaron ataques críticos en el 4-way handshake de WPA2 (KRACK Attacks). Dicho hecho provocó el anuncio por parte de la Wi-Fi Alliance de la especificación del protocolo WPA3 (WPA3-v2.0 publicada el 20/12/2019).

El protocolo **WPA3** tiene dos objetivos principales. El primer objetivo es certificar en los productos Wi-Fi la correcta aplicación de las contramedidas propuestas contra los denominados KRACK Attacks. El segundo objetivo es el de actualizar los mecanismos existentes para aumentar el nivel de seguridad y evitar técnicas de ataque conocidas.

En la medida de lo posible todas las redes Wi-Fi deberían utiliza el modo Enterprise con 802.1X

Características principales de WPA3 y sus modos de funcionamiento

- **WPA3-Personal-SAE**
  - Modo WPA3-Personal-*Only*
    - Uso obligatorio de Management Frame Protection (MFP) 802.11w
    - Uso obligatorio de Simultaneous Authentication of Equals (SAE)
  - Modo WPA3-Personal-*Transition*
    - MFP-802.11w opcional para un cliente WPA2-Personal
    - PSK para los clientes WPA2-Personal y SAE para los WPA3-Personal
- **WPA3-Enterprise-802.1X**
  - Modo WPA3-Enterprise-*Only*
    - Uso obligatorio de MFP-802.11w
  - Modo WPA3-Enterprise-*Transition*
    - Uso opcional de MFP-802.11w para los clientes WPA2-Enterprise
  - Modo WPA3-Enterprise-*192-bit*
    - Uso obligatorio de MFP-802.11w
    - Cifrado del tráfico de usuario con AES-GCM de 256 bits
    - Conjunto de cifrado restringido (*cipher suites*) en el canal EAP:
      - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - ECDHE y ECDSA usando curva elíptica P-384
      - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - ECDHE usando curva elíptica P-384
        - RSA >= 3072 bits
      - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - DHE y RSA >= 3072 bits

Sobre WPA3 se han publicado nuevas vulnerabilidades y ataques que obligan a replantear si es necesario realizar modificaciones sobre el protocolo (Dragonblood que afecta a Dragonfly de SAE y EAP-pwd). También si han publicado vulnerabilidades que afectan a chips de clientes y puntos de acceso permitiendo el descifrado de las tramas en buffer al ser enviadas con TK=0 tras producirse una desasociación (vulnerabilidad Kr00K publicada en Febrero de 2020).

Las tecnologías inalámbricas están en constante cambio y evolución. Es muy importante que los administradores se mantengan actualizados y apliquen las contramedidas necesarias ante las vulnerabilidades y amenazas publicadas. También es importante conocer las evoluciones del estándar y contemplarlas cuando sea necesaria una renovación tecnológica.

3. Riesgos y amenazas en redes Wi-Fi

Las redes inalámbricas están expuestas a la mayoría de los riesgos que tienen las redes cableadas y, además, se añaden los introducidos por la tecnología Wi-Fi.

Para controlar estos riesgos, aquellas organizaciones que requieran del uso de este tipo de redes deben adoptar salvaguardas que permitan reducir al mínimo la probabilidad de impacto, tanto en infraestructuras existentes como en aquellas de nuevo despliegue.

Además, como en cualquier tecnología, es imprescindible un continuo seguimiento de las nuevas vulnerabilidades que puedan aparecer en el futuro y afectar a la organización.

Siempre que sea posible se recomienda el uso de un acceso cableado y deshabilitar las interfaces inalámbricas.

Siempre que sea posible se recomienda el uso de un acceso cableado y deshabilitar las interfaces inalámbricas

A continuación, se muestran las principales amenazas que afectan a redes inalámbricas:

- Por una vulnerabilidad no conocida, el equipo podría verse comprometido por tener habilitada la interfaz inalámbrica sin necesidad de contacto físico por parte del atacante.
- Puede obtenerse acceso a través de conexiones inalámbricas a otros entornos que, no siendo inalámbricos, estén conectados a estos.
- La información que se transmite sin cables puede ser interceptada incluso a kilómetros de distancia, sin posibilidad de detectar esta captura.
- Se pueden producir fácilmente ataques de denegación de servicio (DoS) contra este tipo de infraestructuras (inhibidores de señal, paquetes maliciosos, etc.)
- Se puede inyectar tráfico en las redes inalámbricas a gran distancia (incluso kilómetros).
- Mediante redes sin cifrado o conociendo la infraestructura, se pueden desplegar equipos falsos (rogue AP) realizando una suplantando para obtener información (por ejemplo suplantando el servidor Radius para robar credenciales corporativas usuario/contraseña si no se utilizan certificados con EAP-TLS).
- Una vez obtenido acceso a una red inalámbrica, se pueden realizar ataques de tipo “Man in the Middle”.
- Se puede obtener información de conexión con tener acceso a un equipo legítimo y realizando un análisis forense del mismo.
- Se puede obtener acceso a redes, utilizando las redes conectadas de terceros que no mantengan una política de seguridad adecuada.
- Se pueden realizar ataques internos desplegando redes inalámbricas no autorizadas.
- Se puede revelar información de la entidad propietaria y los dispositivos cliente en datos abiertos que se pueden capturar fácilmente (SSID y direcciones MAC).

Una vez obtenido acceso a una red inalámbrica, se pueden realizar ataques de tipo “Man in the Middle”

4. Redes Wi-Fi corporativas

El servicio de Wi-FI de una corporación se compone principalmente por dos bloques estructurales:

- Los dispositivos de usuario que actúan como cliente final.
- La arquitectura física de acceso y los servicios complementarios.

Esta guía contempla el acceso al servicio Wi-Fi de dispositivos y usuarios ambos corporativos. Se presupone que los dispositivos han sido homologados y configurados para soportar un control de acceso basado en 802.1X utilizando el método EAP-TLS. Mediante un despliegue inicial, los dispositivos han sido configurados y provisionados con un certificado de cliente para identificar dispositivo y usuario.

Los administradores del servicio Wi-Fi deberán configurar y utilizar los diferentes mecanismos y soluciones existentes para asegurar los pilares básicos del control de acceso a una red:

- Autenticar usuarios y dispositivos.
- Autorizar aplicando las políticas acordes al rol usuario/dispositivo.
- Verificar de forma continua la salud y el comportamiento del dispositivo.
- Asegurar las comunicaciones mediante capas de cifrado (Wi-Fi y VPN).
- Registrar las acciones realizadas para su análisis y monitorización (*Accounting*).

Los administradores del servicio Wi-Fi deberán configurar y utilizar los diferentes mecanismos y soluciones existentes para asegurar los pilares básicos del control de acceso a una red

4.1 Arquitectura del servicio Wi-Fi

En los siguientes apartados analizaremos las características principales respecto a la definición de arquitectura lógica, arquitectura física y segregación de la red.

Para definir la arquitectura tanto física como lógica de una red Wi-Fi corporativa es difícil generalizar unas recomendaciones ya que para su diseño no afecta únicamente las necesidades y características propias de la corporación sino que también afecta el producto de fabricante elegido como solución de servicio Wi-Fi.

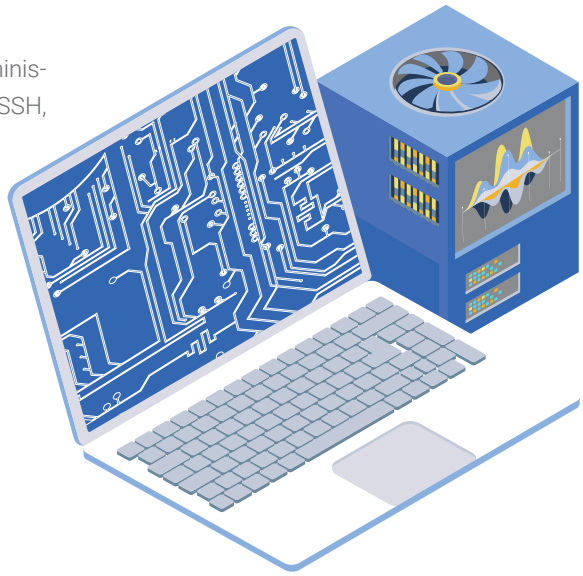
4.1.1 Arquitectura lógica y física

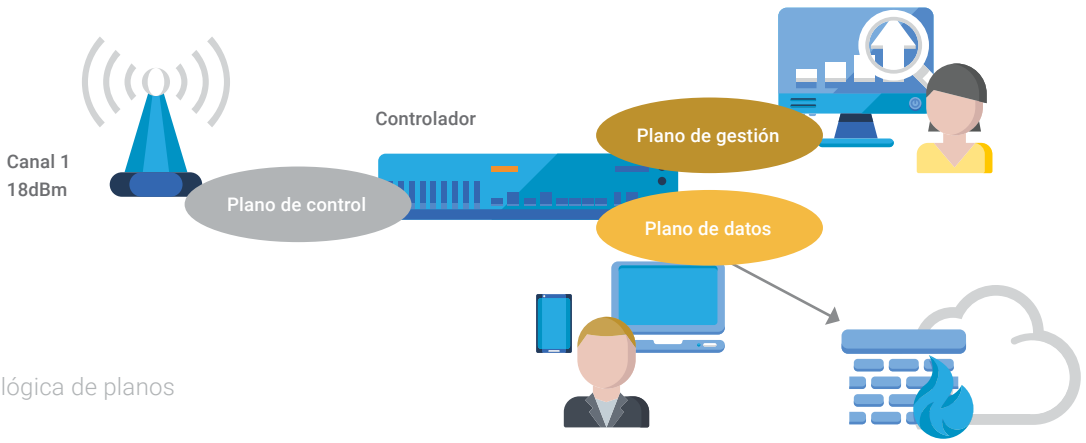
Al hablar de arquitectura lógica de una red Wi-Fi corporativa se pueden definir tres planos funcionales (*planes o layer*) representados en la **Figura 1**:

1. **Plano de Datos** (*Data o Forwarding Plane*): El encargado de mover los paquetes de datos de los usuarios en diferentes sentidos: usuario-red, red-usuario y usuario-usuario.

2. **Plano de Control** (*Control Plane*): Donde residen los diferentes protocolos, procesos y funciones del servicio Wi-Fi: encaminamiento de paquetes, protección de bucles, asignación automática de canales y potencias, etc.

3. **Plano de Gestión** (*Management Plane*): El que permite al administrador configurar y monitorizar el servicio Wi-Fi: GUI-Web, CLI-SSH, SNMP, syslog, etc.





[Figura 1]
Arquitectura lógica de planos funcionales

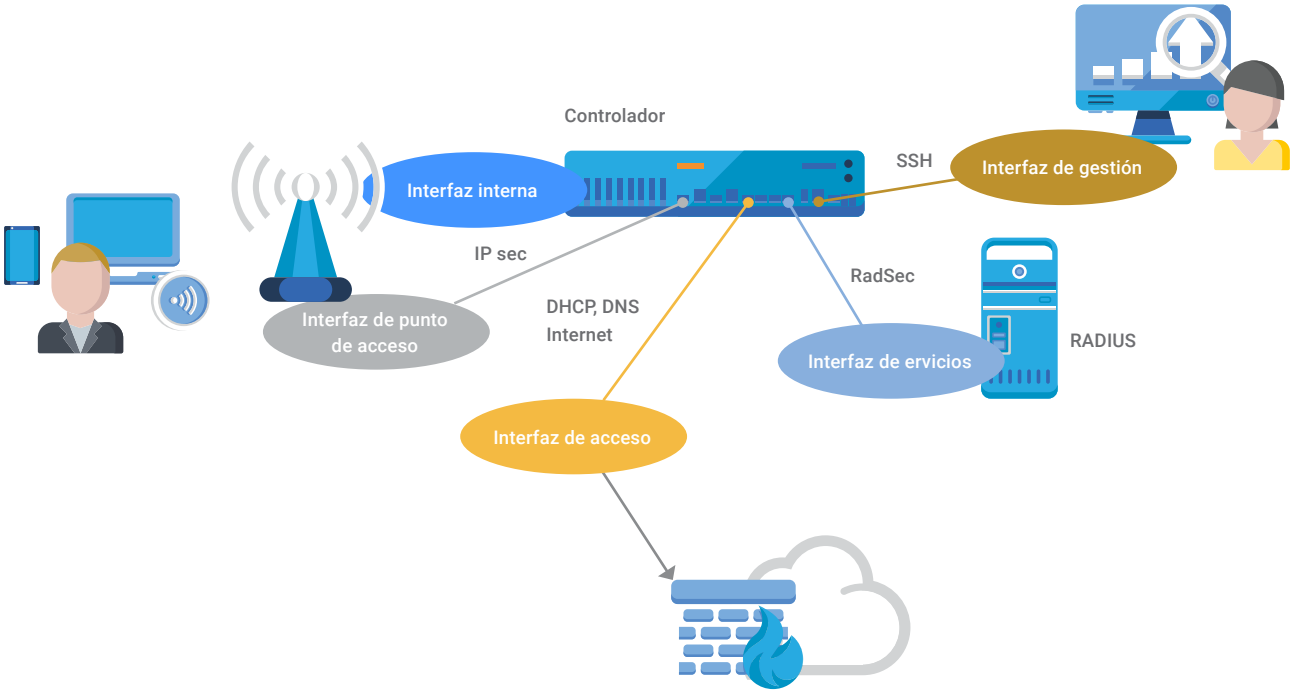
Para securizar una red Wi-Fi es importante conocer dónde se ubica cada uno de los planos lógicos y cómo se comunican los diferentes elementos que forman parte del servicio. Cada producto y solución de fabricante tiene su propia definición de arquitectura y es tarea del administrador conocer las características propias para realizar una correcta configuración.

Por ejemplo, nos podemos encontrar con soluciones totalmente centralizadas basadas en un controlador y los denominados puntos de acceso ligeros. Los puntos de acceso establecen un túnel IPsec contra el controlador siendo éste el encargado de gestionar todas las tareas definidas en el plano de datos, control y gestión.

La **Figura 2** representa como el controlador puede tener interfaces físicas dedicadas para el tráfico de gestión (GUI-Web, CLI-SSH, SNMP, syslog, etc.) y disponer de otras interfaces físicas independientes para el plano de datos segregando el tráfico de los usuarios en diferentes VLANs.

El controlador podría actuar como un equipo de nivel 2 conmutando el tráfico de usuarios Wi-Fi hacia la red de acceso o bien podría asumir tareas de nivel 3 realizando enrutamiento del tráfico entre las diferentes redes de usuario. En ambos casos podría realizar funciones de Firewall o incluso realizar identificación de aplicaciones, filtrado y categorización de URLs, análisis IDS/IPS, análisis de malware, etc.

Para securizar una red Wi-Fi es importante conocer dónde se ubica cada uno de los planos lógicos y cómo se comunican los diferentes elementos que forman parte del servicio



[Figura 2]
Arquitectura de interfaces físicas

El controlador también asume otras tareas del plano de control como la orquestación en la asignación de canales y potencias. En función de la solución de fabricante, ciertas tareas del plano de control podrían delegarse a un servidor o servicio cloud fuera del controlador.

Hay soluciones basadas en controlador que descentralizan algún plano lógico. Por ejemplo, un administrador puede tomar la decisión de ceder el plano de datos al punto de acceso sin ser necesario concentrar el tráfico en el controlador. En este caso, el tráfico de usuario será vertido a la propia interfaz de la antena, segregando en diferentes VLANs de usuario y manteniendo el túnel IPsec hacia el controlador para mantener centralizado el plano de gestión y control.

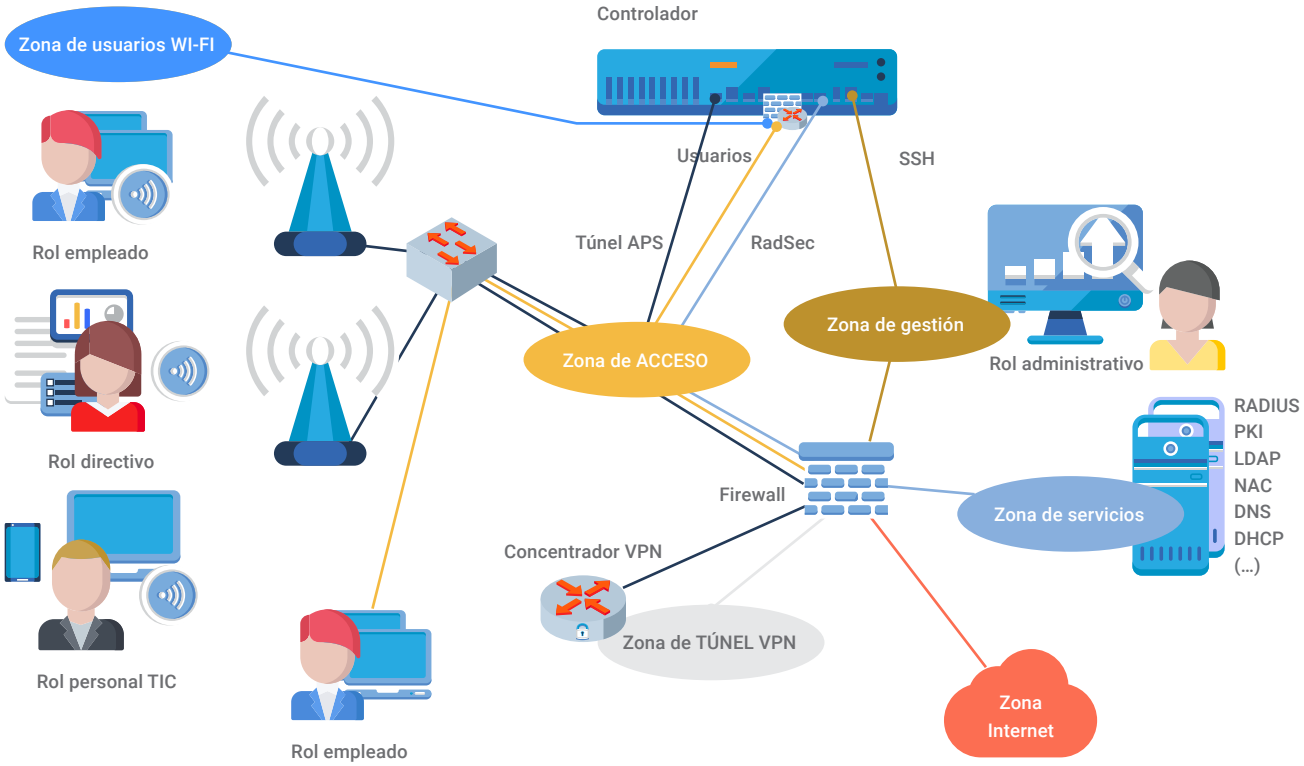
También podemos encontrar soluciones totalmente descentralizadas comúnmente denominadas sin controlador o "controller-less". El plano de datos es cedido a cada punto de acceso y el plano de control puede ser de tipo mallado en el cual todos los puntos de acceso interactúan como iguales o bien del tipo master en el cual un punto de acceso asume el rol de administrador del plano de control. Respecto al plano de gestión puede ser asumido igualmente por algún punto de acceso master o centralizarse virtualmente en un servicio cloud.

4.1.2 Segregación de zonas, redes y roles

Para un correcto agrupamiento y aislamiento de los distintos equipos que componen una red Wi-Fi corporativa, se recomienda maximizar la segregación. Sería ideal aplicar un modelo zero trust que aplique políticas de seguridad en toda comunicación que se produzca entre cualquier elementos de la red, bien sean clientes como servidores.

Para simplificar el ejemplo se propone la creación zonas, redes virtuales (VLAN) y roles en la arquitectura lógica que se representan en la **Figura 3**.

- **Zona de acceso:** conjunto de redes configuradas en los conmutadores de acceso:
  - **Red para puntos de acceso:** red dedicada a la comunicación entre puntos de acceso y controlador los cuales establecen un túnel IPsec.
  - **Red de usuarios:** crear distintas VLANs por departamento, disponibilidad física, nivel de seguridad o rol/perfil de usuario.
  - **Red para acceso a servicios:** red dedicada para el acceso a servicios como pueden ser las peticiones RADIUS del controlador.
- **Zona de túnel VPN:** cuando un usuario establece un túnel VPN con el concentrador de túneles corporativo se define una red de confianza protegida extremo a extremo. Queda fuera del ámbito de la guía recomendar cuáles son las redes a las que se tiene acceso a través del túnel ya que variará en función de los intereses y políticas de la corporación.
- **Zona de acceso a Internet:** permitirá proveer a la red corporativa de acceso a Internet a través de un firewall que protege todas las comunicaciones entre zonas.
- **Zona de gestión:** servirá para realizar las tareas de administración y configuración de todos los sistemas conectados a la misma.



[Figura 3]
Segregación de zonas, redes y roles

- **Zona de servicios:** donde se ubican los servidores corporativos. Se recomienda realizar micro-segmentación y aplicar seguridad a cualquier comunicación que se produzca entre los distintos elementos tanto clientes como servidores.

- **Redes de usuarios de controlador:** son redes que sólo se definirán en el controlador de puntos de acceso con el objetivo de proteger las comunicaciones con la red acceso.

Si se decide que el controlador actuará como un equipo de nivel 3 (realizando tareas de enrutamiento) se pueden definir dos zonas en el controlador para los usuarios: zona de redes de usuario Wi-Fi y zona de redes de acceso corporativo.

Una vez finalizada la autenticación del dispositivo de usuario, dentro del controlador, se aplica el concepto de rol de autorización para cada sesión. El rol afecta al tráfico de usuario y los intercambios de sesiones con la red de acceso corporativa.

La aplicación de un rol puede forzar un cambio de red de usuario asignando una nueva VLAN o puede indicar que no se cambie de VLAN, para no afectar a la configuración IP del cliente, pero que se modifiquen las reglas de filtrado de red

Se pueden definir los siguientes roles:

- **Rol de validación:**

  Se aplicará al cliente que haya concluido satisfactoriamente el proceso de autenticación 802.1X (fase 2 del modelo de seguridad que se verá posteriormente). El cliente permanecerá con este rol mientras se analiza si cumple con los requisitos de estado de salud del dispositivo y otros atributos de autorización. Se permitirán los accesos estrictamente necesarios para poder obtener configuración IP y recibir o realizar conexiones contra los servicios de la solución de agente NAC.

- **Rol de cuarentena:**

  Se aplicará a aquellos clientes que no cumplan con los requisitos de seguridad. Puede ser debido a un informe negativo del agente NAC respecto al estado del dispositivo o por indicación de algún otro atributo de autorización. Si es posible una remediación, la política del rol permitirá el acceso a los recursos necesarios para solucionar el problema.

- **Rol de estado saludable:**

  Se aplicará a aquellos clientes que cumplan con los requisitos de seguridad establecidos. Este rol permitirá a los clientes crear un túnel VPN (fase 4 del modelo de seguridad que se verá a continuación). Al establecer el túnel VPN se tendrá acceso a la red túnel donde existirá un servidor de direcciones IP que permita aportar una nueva dirección IP a través de la que se transmita y reciba tráfico encapsulado.

- **Rol de estado saludable con perfil:**

  Es posible que sea necesario aplicar políticas diferentes en función del perfil de usuario en cuyo caso se podría crear un rol específico para cada perfil (por ejemplo empleados, directivos, personal técnico, estudiantes, profesores, etc.)

5. Modelo de seguridad

En este apartado se mostrará el modelo de seguridad basado en cuatro fases a configurar e implementar en una red Wi-Fi corporativa segura. El modelo se aplica a dispositivos corporativos y a usuarios también corporativos.

Se recomienda emplear un único SSID corporativo **802.1X-Enterprise** que utilice como método de autenticación **EAP-TLS** con certificados de servidor y cliente. Una vez autenticado y autorizado el cliente, se cifrará el canal inalámbrico con **AES**. Seguidamente se realizará un análisis continuo del estado de salud del dispositivo con un **agente NAC** y/o se monitorizará el comportamiento del dispositivo mediante técnicas de ***fingerprinting***. El resultado del análisis del estado de salud modificará el nivel de autorización si fuese necesario. Finalmente para asegurar un cifrado extremo a extremo se establecerá un **túnel VPN cifrado**.

- **Fase 0:**
  Configuración del servicio corporativo y despliegue de los clientes.
- **Fase 1:**
  Asociación y autenticación por dirección MAC.
- **Fase 2:**
  Autenticación y autorización 802.1X con EAP-TLS.
- **Fase 3:**
  Acceso a la red y comprobación continua de la salud del dispositivo.
- **Fase 4:**
  Establecimiento de un túnel VPN cifrado.

> **El modelo se aplica a dispositivos corporativos y a usuarios también corporativos**

5.1 Fase 0: configuración y despliegue

Antes de iniciar las fases propias del acceso, es necesario configurar la solución del servicio Wi-Fi por parte del administrador y realizar el despliegue de configuración de los dispositivos cliente para acceder correctamente al servicio Wi-Fi.

5.1.1 Configuración del modo Enterprise

La especificación de WPA3-v2.0 da la opción de configurar diferentes modos WPA3-Enterprise. La **Figura 4** representa la toma de decisión del modo WPA3-Enterprise a configurar: Only, Transition o 192-bits. Los modos estarán condicionados a las características soportadas por los diferentes elementos de la solución Wi-Fi:

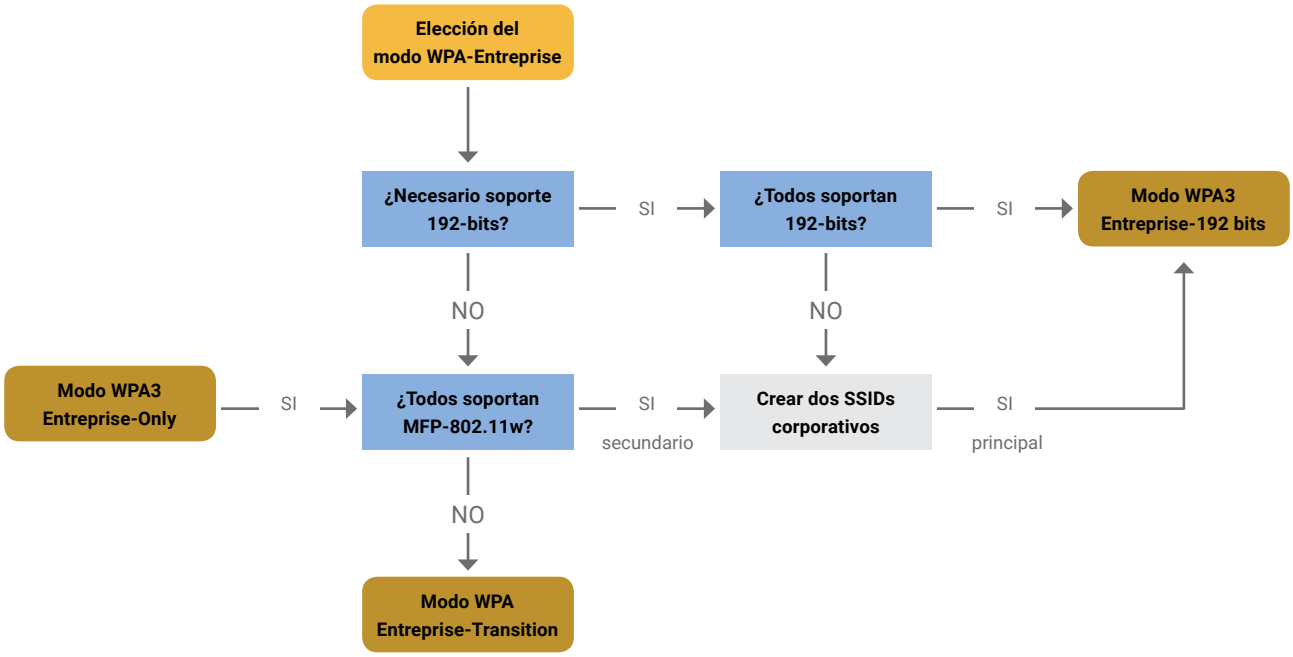
- **MFP-802.11w:** en dispositivos cliente y puntos de acceso.
- ***Cipher suites* robustas:** en suplicante del cliente y servidor de autenticación.
- **Cifrado AES-256-GCM:** en dispositivos cliente y puntos de acceso.

En la medida de lo posible, se recomienda utilizar un único SSID para dar acceso a la red Wi-Fi corporativa (por ejemplo "corp_1X"). En el momento de escribir estas recomendaciones, el nivel máximo de seguridad lo ofrece el modo WPA3-Enterprise-192-bits (MFP-802.11w obligatorio, conjuntos de cifrado robustos y cifrado de tráfico AES-256-GCM).

Si todos los dispositivos y elementos de la infraestructura Wi-Fi soportan el modo WPA3-Enterprise-192-bits se recomienda su uso en el SSID corporativo.

Pero siendo WPA3 una especificación muy reciente, es posible que no todos los dispositivos soporten el modo 192-bits. Si el soporte por parte de los clientes es parcial, será necesario definir un segundo SSID

Si todos los dispositivos y elementos de la infraestructura Wi-Fi soportan el modo WPA3-Enterprise-192-bits se recomienda su uso en el SSID corporativo



[Figura 4]
Elección del modo WPA3-Enterprise

corporativo para dar acceso a los dispositivos no compatibles (por ejemplo "corp_1X_2") con el objetivo de mantener el máximo nivel de seguridad 192-bits en el SSID principal.

En los SSIDs que no se configure el modo 192-bits, se recomienda permitir al menos de forma opcional todas las características que son un requisito en el modo 192-bits: uso de las *cipher suites* robustas, cifrado AES-256-GCM y MFP-802.11w.

Cuando todos los dispositivos soportan WPA3-Enterprise pero solo algunos soportan 192-bits se podría configurar el primer SSID en modo WPA3-Enterprise-192-bits y el segundo SSID en modo WPA3-Enterprise-Only haciendo obligatorio el uso de MFP-802.11w.

En el caso de ser necesario dar servicio a dispositivos WPA2-Enterprise no compatibles con MFP-802.11w, el segundo SSID deberá configurarse en modo WPA3-Enterprise-Transition haciendo opcional el uso de MFP-802.11w para los dispositivos WPA2-Enterprise.

Si se decide no configurar el modo 192-bits, se podría optar por configurar un único SSID corporativo en modo WPA3-Enterprise-Only, si todos los dispositivos soportan MFP-802.11w, o por el contrario WPA3-Enterprise-Transition si algún dispositivo no soporta MFP-802.11w.

Se podría dar el caso en el que la infraestructura Wi-Fi no soporte WPA3 y la única alternativa sea configurar un SSID con WPA2-Enterprise en

cuyo caso se recomienda permitir los niveles máximos de seguridad soportados al menos de forma opcional: MFP-802.11w, cifrado AES-256-GCM y soporte de *cipher suites* robustas en el servidor de autenticación.

Se recomienda definir un plan de migración de todos los dispositivos no compatibles con WPA3-Enterprise para aumentar los mecanismos de seguridad y aplicar las contramedidas ante vulnerabilidades publicadas.

5.1.2 Configuración del servicio Wi-Fi

Supondremos que la infraestructura Wi-Fi anunciará un SSID corporativo principal en modo WPA3-Enterprise-192-bits denominado "corp_1X" y un segundo SSID en modo WPA3-Enterprise-Transition denominado "corp_1X_2" para dar servicio a los dispositivos que no soportan todos los requisitos del modo de seguridad 192-bits.

Los puntos de acceso anunciaran los dos servicios y los dispositivos mediante un despliegue serán provisionados de configuración indicando, entre otros parámetros, el SSID que les corresponde. Todos los mecanismos de seguridad del modo 192-bits serán ofrecidos de forma opcional en el SSID en modo WPA3-Enterprise-Transition.

Para realizar la autenticación, se establecerá entre el cliente suplicante y el servidor de autenticación un canal EAP que irá sobre los protocolos 802.1X y RADIUS (tramo usuario-controlador y tramo controlador-servidor respectivamente). La comunicación RADIUS entre controlador y servidor de autenticación estará protegida mediante el protocolo RadSec (basado en TLS). El canal EAP encapsulará el método EAP-TLS para realizar una autenticación basada en certificados.

Para utilizar el **método EAP-TLS**, será necesario contar con una infraestructura PKI que permita generar y gestionar los certificados de cliente y servidor. También serán necesarios servicios complementarios como bases de datos para almacenar atributos de autorización (un LDAP, un directorio activo o cualquier otra base de datos).

Se generará un certificado digital para el servidor de autenticación firmado por una CA sobre la que los clientes tendrán confianza y del certificado verificarán el hostname del servidor.

El servidor de autenticación tendrá confianza en la CA que firme los certificados de los clientes y verificará su estado de revocación (por ejemplo con el protocolo OCSP: *Online Certificate Status Protocol*).

5.1.3 Despliegue de configuración de clientes

Los clientes dispondrán de un certificado digital que estará firmado por una CA sobre la que el servidor de autenticación tendrá confianza. Es recomendable que en el certificado de cliente se incluyan atributos que identifiquen tanto al usuario como a su dispositivo.

El servidor de autenticación utilizará ciertos atributos del certificado durante el proceso de autorización para tomar la decisión del rol o política que debe aplicar a la sesión que se ha autenticado (por ejemplo CN, SAN o el email).

Se definirá un protocolo o mecanismo de configuración de los dispositivos clientes preferentemente automatizado.

Es importante que el cliente no pueda modificar los parámetros de configuración ya que podría desactivar comprobaciones básicas que permitiría el acceso a un servicio Wi-Fi suplantado (por ejemplo si se desactiva la verificación del hostname y CA-root que firma el certificado del servidor de autenticación).

La especificación de WPA3-v2.0 contempla la posibilidad de deshabilitar la opción que permite en el cliente añadir una excepción de confianza respecto al certificado de servidor de autenticación cuando falla la validación del mismo (TOD: *Trust Override Disable, UOSC: User Override of Server Certificate*). Para clientes que han sido configurados en despliegue se recomienda indicar el OID TOD-STRICT: "1.3.6.1.4.1.40808.1.3.1" en el certificado del servidor de autenticación para evitar interacción y excepciones en caso de fallo de de validación.

Un ejemplo de los parámetros a configurar en los clientes:

[Figura 5] Despliegue y configuración del cliente

	Cliente WPA3-Enterprise-192-bits	Cliente WPA3-Enterprise-Transition
SSID corporativo	“corp_1X”	“corp_1X_2”
MFP-802.11w	Obligatorio	Opcional
Cifrado	AES-256-GCM	AES-128-CCMP Opcional: AES-256-GCM
Credenciales	Clave privada de cliente y Certificado cliente (firmado por CA-root-cliente)	
Datos del servidor Radius a verificar obligatoriamente	Certificado CA-root-servidor hostname (por ejemplo: ”radius.corp.es”)	

5.2 Fase 1: asociación y autenticación MAC

Una vez configurado el servicio Wi-Fi y desplegados los clientes, se inician las fases propias del acceso al servicio Wi-Fi.

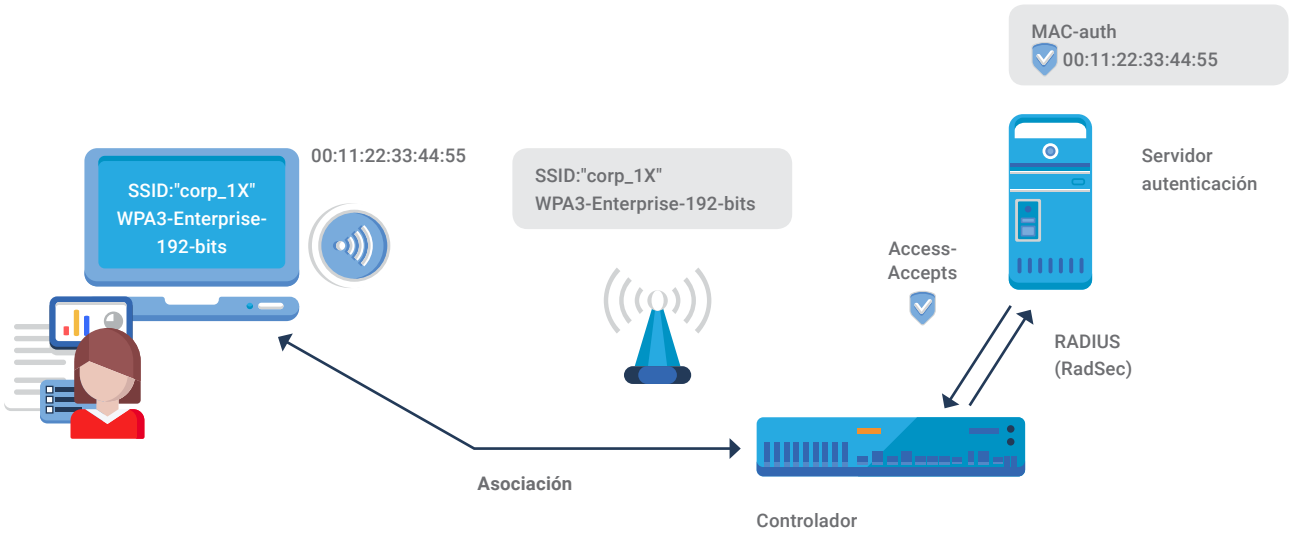
En la primera fase, el cliente no dispone de ningún mecanismo que le permita tener confianza en la infraestructura que le ofrece el servicio Wi-Fi. La única información que se valida es el nombre del SSID de los anuncios *beacon*. Al recibir un anuncio de servicio se inicia la asociación.

El cliente podría utilizar mecanismos no estandarizados para la detección de servicios maliciosos como la coherencia de geolocalización, un *fingerprinting* de las características anunciadas en los *beacons* y las direcciones BSSID de los puntos de acceso. Todos los datos de la trama *beacon*, que incluye el SSID y las direcciones MAC, son fácilmente suplantables y nunca se deben utilizar como único sistema de autenticación.

Durante la asociación, representada en la **Figura 6**, se recomienda que la infraestructura corporativa realice una primera autenticación basada en la dirección MAC del cliente inalámbrico, aunque sabemos que es un atributo que se puede suplantar fácilmente.

Respecto a la autenticación MAC, se pueden combinar dos tipos de políticas: las basadas en listas blancas o en listas negras. Una lista blanca puede contener todas las direcciones MAC de los clientes corporativos configurados durante el despliegue. Una lista negra puede contener todas las direcciones MAC consideradas maliciosas.

Una vez configurado el servicio Wi-Fi y desplegados los clientes, se inician las fases propias del acceso al servicio Wi-Fi



[Figura 6]
Asociación y autenticación MAC

Por dar un ejemplo, se podría dar acceso a la fase 2 (802.1X) a todas las direcciones MAC que aparezcan en una lista blanca, bloqueando la asociación a cualquier dirección MAC desconocida o que esté registrada en la lista negra.

Otro ejemplo, se podría omitir la lista blanca y permitir por defecto cualquier dirección MAC que no esté incluida en una lista negra.

Una autenticación basada en dirección MAC nos permite realizar un bloqueo y protección de acceso al servidor de autenticación. Por ejemplo, al detectar un intento DoS contra 802.1X podríamos incluir en la lista negra a todas las direcciones MAC participantes bloqueando permanentemente o durante un tiempo definido como mecanismo de contención.

5.3 Fase 2: autenticación y autorización 802.1x con EAP-TLS

Si el cliente supera con éxito la asociación y autenticación MAC, la infraestructura le solicitará que utilice el protocolo 802.1X para establecer una comunicación EAP con el servidor de autenticación (**paso 1 y 2** de la **Figura 7**). El método que se utilizará en el canal EAP es EAP-TLS.

El servidor de autenticación tras comprobar el identificador de identidad del cliente, enviará su certificado **(paso 3)** para que el cliente pueda verificar el hostname y decidir si confía en la CA que firma el certificado **(paso 4)**, según la configuración realizada durante el despliegue de los clientes.

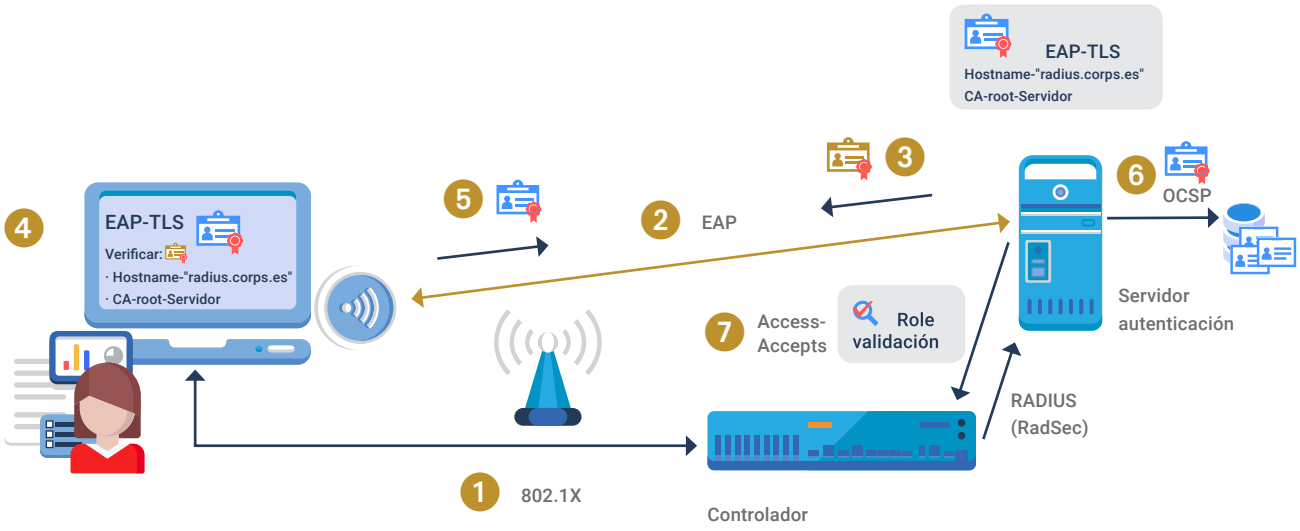
Si todo es correcto, el cliente enviará su certificado al servidor de autenticación **(paso 5)**. El servidor verificará los atributos del certificado del cliente y consultará su validez mediante los recursos de la CA de confianza que firma el certificado del cliente , por ejemplo OCSP **(paso 6)**.

Si el servidor concluye que la autenticación es correcta proseguirá con la autorización del dispositivo cliente.

Para la autorización, el servidor recopilará una serie de atributos de diferentes fuentes y junto con los datos obtenidos en el proceso de autenticación se determinará el rol resultante que se debe aplicar a la sesión del dispositivo cliente.

Los atributos de autorización pueden ser estáticos como los datos personales del usuario, o dinámicos como los informes de estado de salud del dispositivo, la ubicación física, el comportamiento en la red aplicando firmas basadas en patrones, etc.

Si el cliente supera con éxito la asociación y autenticación MAC, la infraestructura le solicitará que utilice el protocolo 802.1X para establecer una comunicación EAP con el servidor de autenticación



[Figura 7]
Autenticación mediante EAP-TLS

El rol resultante puede contener configuraciones como la VLAN, los filtros de firewall a aplicar, el control de ancho de banda o cualquier otro parámetro que permita aplicar la infraestructura de red. Si el servidor determina que no tiene suficientes datos para decidir sobre la salud del dispositivo, podrá aplicar un "rol de validación" para ofrecer los servicios mínimos necesarios para recibir un informe de estado de salud del dispositivo (paso 7).

Al finalizar el proceso de autenticación y autorización:

- El cliente podrá calcular la PMK (Pairwise Master Key).
- El servidor de autenticación utilizará el canal RADIUS para enviar al controlador o punto de acceso todos los atributos necesarios de autorización y cálculo de la PMK.

Acto seguido se realizará el *4-way-handshake* entre punto de acceso y cliente para verificar la confianza mutua derivando de la PMK las claves de cifrado para el tráfico en el tramo inalámbrico (PTK y GTK).

Mientras que el dispositivo cliente permanezca asociado al servicio Wi-Fi, se mantendrá activo el canal EAP para realizar re-autenticaciones con el servidor y regeneración de las claves criptográficas según los intervalos definidos.

5.4 Fase 3: acceso a la red y estado de salud del dispositivo

Una vez superada la autenticación, aplicados los atributos de autorización y finalizado el 4-way handshake, el cliente tiene acceso a la red de datos (**paso 1** de la **Figura 8**). Los atributos de autorización definirán la política de acceso y los servicios permitidos **(paso 2)**.

Una vez superada la autenticación, aplicados los atributos de autorización y finalizado el 4-way handshake, el cliente tiene acceso a la red de datos

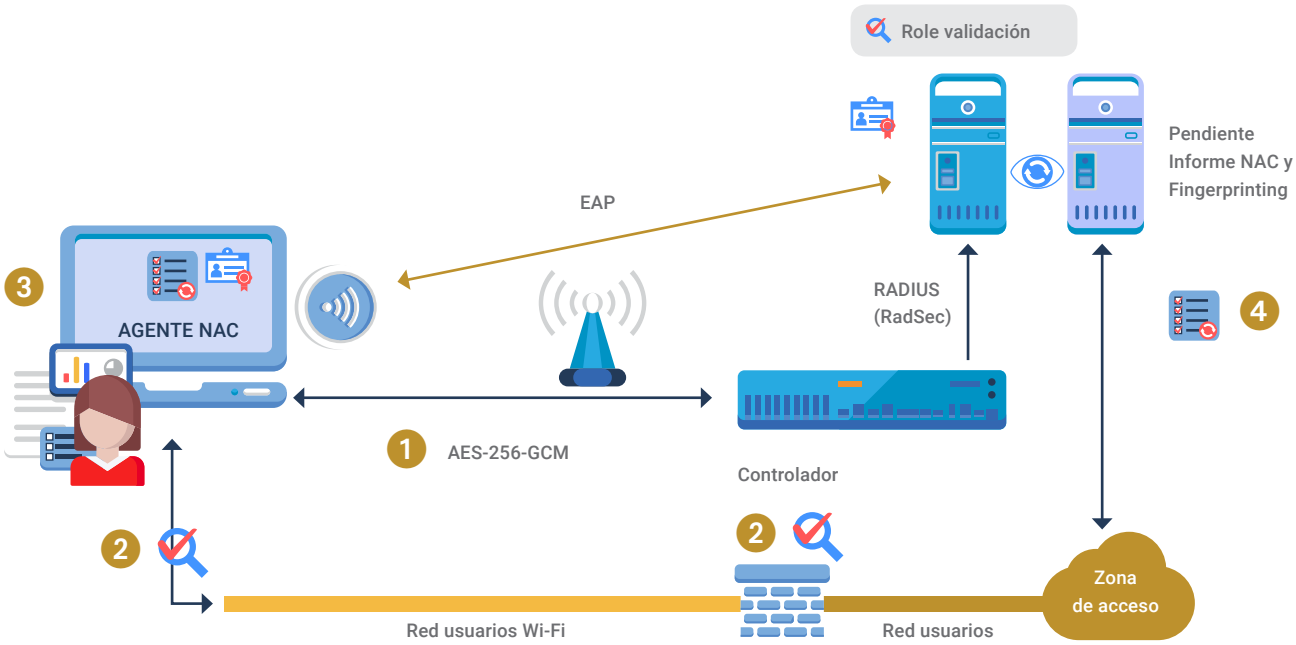
El primer servicio básico que se ofrece al cliente es el de DHCP que le permitirá configurar la interfaz IP (dirección IP, máscara de subred, ruta por defecto, servidor DNS y otros parámetros corporativos). El uso de DHCP por parte del cliente será obligatorio evitando las configuraciones manuales. Para simplificar los procesos de registro y auditoría la asignación de IP será estática por dispositivo vinculando cada dirección IP a una dirección MAC.

Para simplificar la gestión de políticas de seguridad se recomienda el uso de nombres de usuario, grupos o roles como alternativa al uso de direcciones IP. Se recomienda registrar el mapeo entre dirección IP y nombre de usuario para permitir su referencia en las políticas y registros de acceso.

Todas las comunicaciones directas entre clientes serán bloqueadas para evitar la propagación de infecciones. En caso de ser necesaria la comunicación directa entre clientes se deben estudiar posibles alternativas para ofrecer el mismo servicio o habilitar soluciones tipo proxy.

Todas las comunicaciones de red serán analizadas y protegidas por equipos de seguridad (firewall, IDS/IPS, URL-filtering, análisis de malware, netflow, etc.)

Las herramientas de análisis de red permiten generar atributos dinámicos que se utilizarán en el proceso de autorización para determinar el rol del usuario. Se puede hacer fingerprinting o perfilado analizando las peticiones DHCP, el user-agent de las peticiones http, las aplicaciones identificadas por el firewall, los patrones de sesiones netflow, etc.



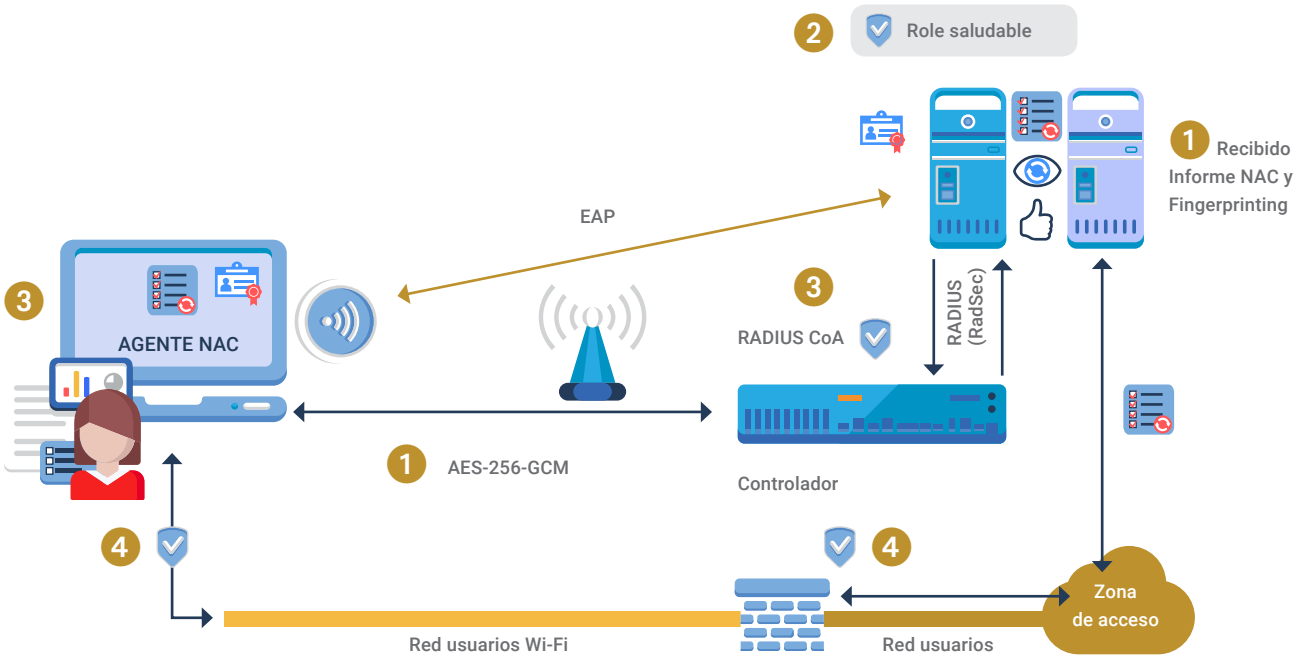
[Figura 8]
Comprobación del estado del dispositivo a través del agente NAC

Para realizar un mejor análisis y perfilado, se recomienda emplear un programa, agente o sistema (agente NAC) instalado en el equipo del usuario que vaya a acceder a la red que permita verificar que el terminal con el que se va a acceder cuenta con unos requisitos mínimos de seguridad **(paso 3)**.

Estos requisitos mínimos recomendados son:

- Que el sistema operativo del equipo cliente esté actualizado con versiones no anteriores a dos meses (o lo que determine la política de seguridad de la organización).
- Que el equipo disponga de un sistema de protección como antivirus o solución EDR instalado y en ejecución, con actualizaciones no anteriores a dos meses (o lo determinado por el análisis de riesgos que se haya hecho).

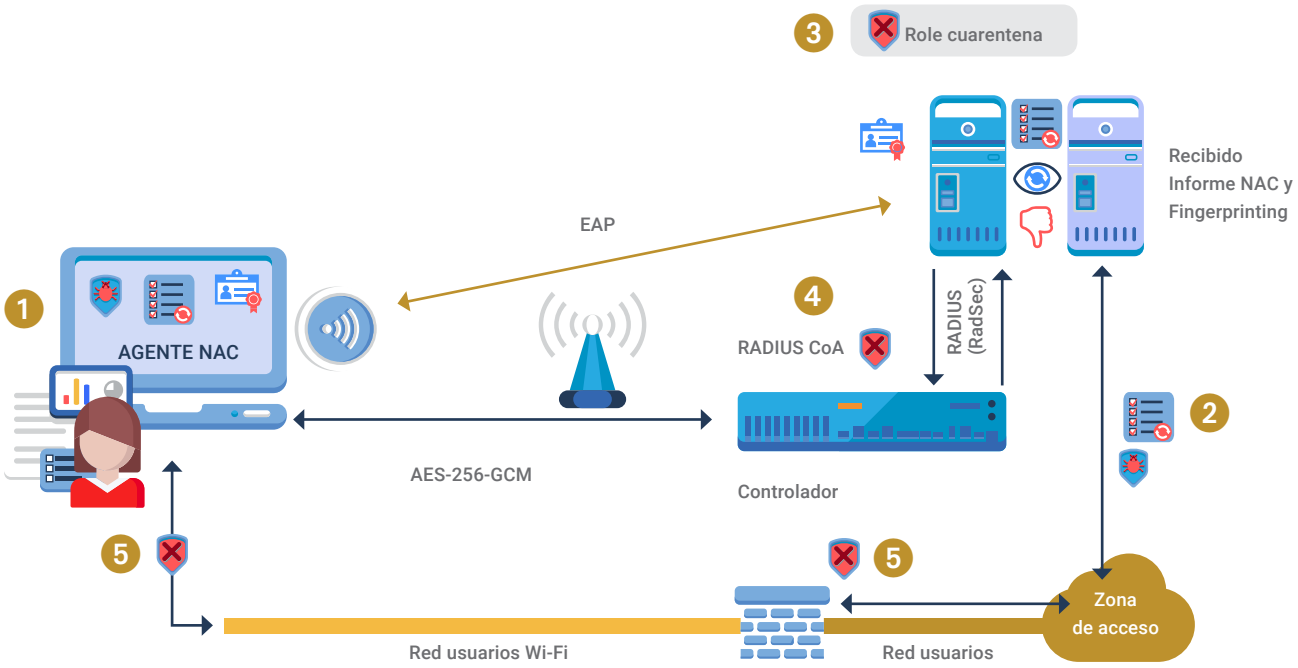
El agente NAC enviará el estado del dispositivo a un servidor NAC que permita verificar la salud del equipo conectado **(paso 4)**. Este agente se ejecutará de manera periódica (se recomienda hacerlo cada 30 segundos), permitiendo conocer si ha cambiado el estado del dispositivo con lo que se pueden definir y aplicar distintas políticas de acceso a la red en función del cumplimento de los requisitos de acceso a la misma.



[Figura 9]
Dispositivo en estado saludable

Los informes de estado del agente NAC y los atributos de análisis se pondrán a disposición del servidor de autenticación para que pueda tomar la decisión del rol que debe aplicarse a la sesión de un dispositivo.

Inicialmente tras la autenticación, el servidor de autenticación puede aplicar el **"rol de validación"** hasta recibir el informe de estado de salud. Si el informe es saludable, mediante un Radius CoA, se cambiará al **"rol de estado saludable"** (Figura 9).



[Figura 10]
Dispositivo en estado cuarentena

Si por el contrario el informe indicara que no cumple con los requisitos de seguridad cambiará al **"rol de cuarentena"** restringiendo el acceso a únicamente los servicios mínimos necesarios para solucionar los problemas detectados **(Figura 10)**.

También se podrá modificar la autorización de clientes que han sido considerados como saludables a cuarentena si se detecta un cambio de estado.

Por ejemplo, un cambio en el *fingerprinting* de tipo de dispositivo o sistema operativo al analizar el user-agent o DHCP, algún patrón de tráfico sospechoso o uso de alguna aplicación no permitida al analizar netflow o la identificación de aplicaciones del firewall, el acceso a alguna URL maliciosa, la descarga de algún malware, etc.

5.5 Fase 4: establecer el túnel VPN cifrado

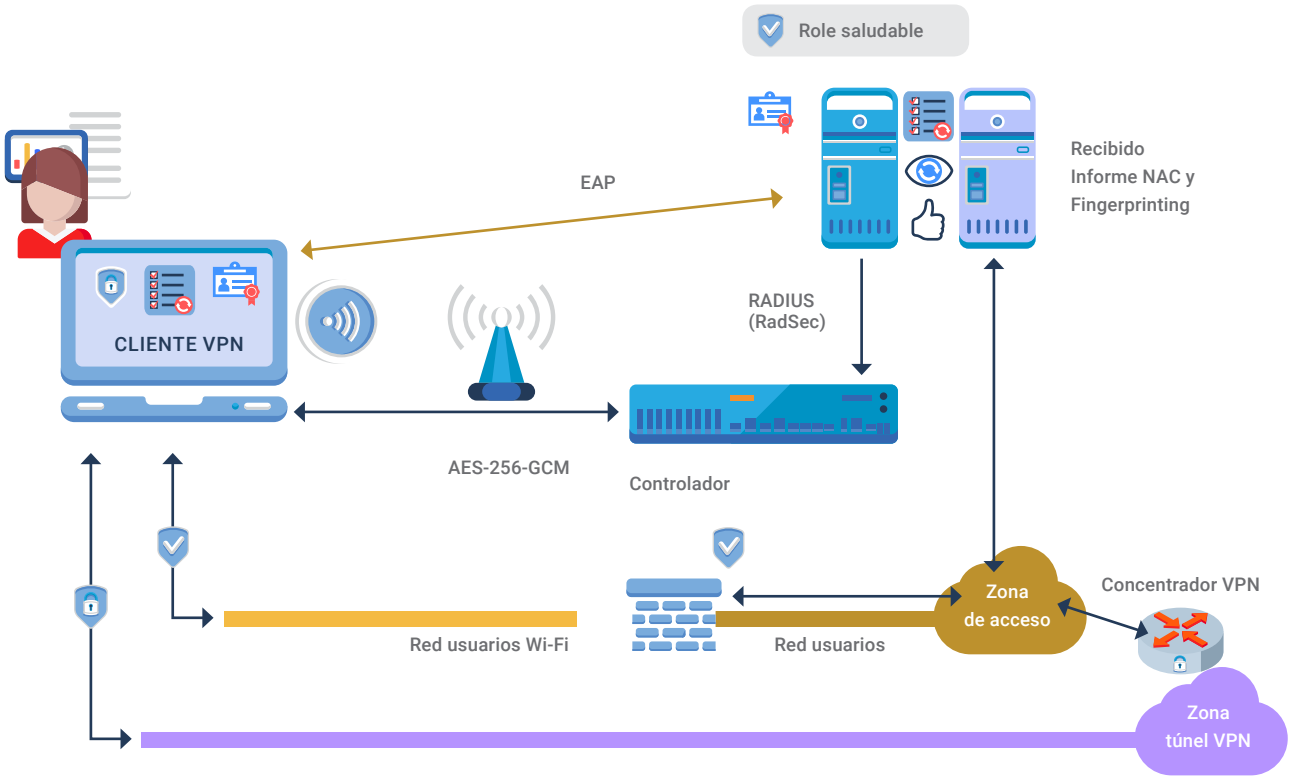
El cifrado inalámbrico se complementará con el establecimiento de un túnel VPN cifrado con el concentrador VPN corporativo. Así se extiende el cifrado desde el cliente hasta una zona de confianza corporativa siendo protegida la información en tránsito a través de mecanismos robustos de cifrado y autenticación.

Se recomienda consultar las guías específicas respecto a soluciones de túneles VPN para determinar la solución que cubra las necesidades de la corporación. De forma general se debe utilizar el nivel máximo de seguridad soportado por el producto y los clientes VPN.

Se puede tomar como referencia las siguientes suites criptográficas:

[Figura 11] Algoritmos criptográficos recomendados

ALGORITMO	MEDIO	ALTO
Cifrado Advanced Standard (AES)	128 bits	256 bits
Firma Digital Elliptic Curve Digital Signature Algorithm (ECDSA)	256 bit curve	384 bit curve
Intercambio de claves Elliptic Curve Diffie-Hellman (ECDH)	256 bit curve	384 bit curve
Hashing Secure Hash Algorithm (SHA)	SHA-256	SHA-384



[Figura 12]
Establecer el túnel VPN

En función de la solución implantada y de su integración con la solución Wi-Fi, el proceso de asociación, autenticación, verificación de estado y establecimiento de túnel VPN podrá realizar con un único agente o aplicación.

Por el contrario nos podemos encontrar con soluciones no integradas en las que por una parte tenemos el suplicante encargado de la asociación y autenticación, por otra un agente NAC encargado del informe de estado y finalmente un cliente VPN encargado de establecer el túnel cifrado.

Sea cual sea la solución, el túnel VPN se debe establecer lo antes posible justo después de tener acceso a la red para securizar todas las comunicaciones. Pero sería comprensible tomar la decisión de no permitir el establecimiento del túnel VPN hasta que el dispositivo obtenga el rol de estado saludable.

Una vez que el túnel esté en funcionamiento, el cliente contará con dos conexiones distintas, la conexión mediante la "Red de usuarios Wi-Fi" y la conexión de la "Red túnel VPN". Ésta última será la interfaz por defecto de todo el tráfico del cliente.

La "Red de usuarios Wi-Fi" con un cifrado AES-GCM-256 desde el cliente hasta el punto de entrega del plano de datos del controlador, transportará la encapsulación cifrada de la "Red túnel VPN". Al salir del controlador la "Red túnel VPN" será encapsulada y atravesará cualquier infraestructura existente hasta llegar al concentrador VPN que proporciona un canal autenticado y cifrado desde el dispositivo del cliente hasta el propio concentrador VPN.

Pese al doble cifrado de la "Red de usuarios Wi-FI" y "Red túnel VPN", se establecerán sesiones seguras a nivel de aplicación con protocolos que cifren el canal desde el cliente hasta el servidor de aplicaciones (por ejemplo https y TLS). Y sobre ese canal de aplicación se protegerá la información enviada para que sea accesible solo por los usuarios o destinatarios autorizados (por ejemplo cifrando los correos electrónicos o los ficheros con la clave pública del destinatario autorizado bien sea PGP o de certificado).

Las diferentes capas de cifrado protegen las comunicaciones ante vulnerabilidades como Kr00k ya que si un atacante logra descifrar tramas Wi-Fi lo único que conseguirá es ver tramas cifradas por el túnel VPN.

Pese al doble cifrado de la "Red de usuarios Wi-FI" y "Red túnel VPN", se establecerán sesiones seguras a nivel de aplicación con protocolos que cifren el canal desde el cliente hasta el servidor de aplicaciones

6. Recomendaciones de seguridad

En este apartado se recogen una serie de recomendaciones de seguridad que se deben tener en cuenta a la hora de desplegar la red. En apartados anteriores ya se han indicado algunas de ellas.

Para ampliar la información aquí descrita, se pueden consultar las guías indicadas en el apartado de referencias.

6.1 Consideraciones iniciales

- Realizar el **análisis y gestión de riesgos** antes de comenzar con el despliegue de la red que incluya la disponibilidad de los sistemas y servicios, la integridad de los datos y las transacciones, el nivel de confidencialidad, la autenticidad de los datos intercambiados y la trazabilidad de estos intercambios sobre el equipamiento que se va a utilizar, las conexiones que se van a establecer entre ellos y quién y cómo va a operarlos.

- **Plantear el acceso por cable.** Un acceso con cable siempre tendrá una menor exposición ante amenazas. No se puede descartar el compromiso del dispositivo por tener habilitada la interfaz inalámbrica explotando alguna vulnerabilidad no conocida con el agravio de tener éxito sin ser necesario el contacto físico y desde mucha distancia.

- **Analizar el equipamiento a adquirir.** Comprobar la capacidad para soportar los protocolos requeridos y la publicación de actualizaciones por parte del fabricante. Aplicar redundancia sobre los equipos que en caso de fallo, error o ataque no permitan un funcionamiento normal del servicio. Realizar un inventario de dispositivos y revisarlo periódicamente.

- **Asegurar el acceso físico** a las dependencias de la organización, especialmente a las áreas donde se encuentren desplegados equipos.

- **Realizar un análisis del alcance de la radiación** de los puntos de acceso (este análisis se debe contemplar en los análisis de seguridad periódicos). Definir la ubicación de los puntos de acceso y procurar mantenerlos alejados del exterior del perímetro de la organización.

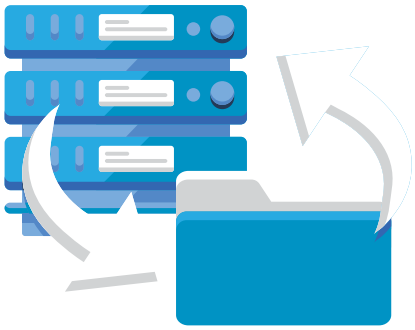
- Elaborar una serie de **políticas de seguridad** que definan quiénes tienen acceso físico a los equipos de red, quiénes tienen acceso para administrarlos y qué procedimientos deben ejecutarse en caso de intrusión. Esta política también debe especificar qué métodos emplear para recuperar el funcionamiento habitual de los dispositivos en caso de fallos, errores, intrusiones, etc. Hay que realizar comprobaciones periódicas del cumplimiento de las políticas de seguridad.

- Para evitar el acceso malicioso a la red cableada de los puntos de acceso, autenticar y autorizar el acceso cableado de los puntos de acceso mediante **802.1X con EAP-TLS** en los conmutadores de acceso.

- **Formar** a los usuarios en el uso de esta tecnología y los riesgos asociados a su utilización.

6.2 Consideraciones iniciales

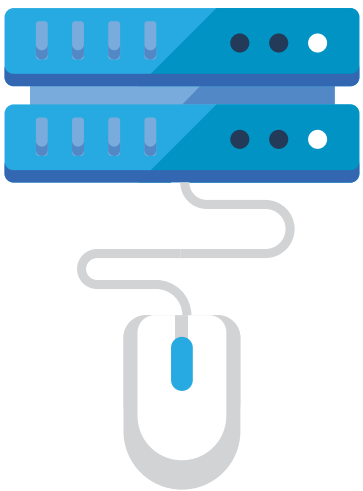
- Mantenga sus **equipos actualizados** a la última versión. Descargue las actualizaciones a través de los proveedores oficiales de los fabricantes en tanto se ofrezca dicho servicio mediante un protocolo seguro de comunicación.
- Realice **copias de seguridad** periódicamente, almacenándolas en equipos distintos a aquellos que se están copiando.
- Establezca mecanismos que definan **procedimientos de recuperación** de la información, así como mecanismos de pruebas de su correcto funcionamiento antes de su puesta en marcha.
- Transfiera ficheros a través de la opción de subida local (local file) o **SCP**. Deshabilite el uso de FTP y TFTP.



6.3 Métodos y condiciones de acceso

- Cree una **red dedicada de gestión** que sólo transporte tráfico de gestión y administración.
- Utilice **como métodos de acceso a los equipos seguros** como el acceso mediante interfaz de comandos (CLI), interfaz web (Web GUI) o SSH (puerto 22 TCP) con listas de acceso. Solicite siempre credenciales de usuario para acceder a los equipos, cualquiera que sea el método que se emplee.

- Establezca procedimientos seguros que permitan llevar un **control sobre el establecimiento y cambio de credenciales de acceso** (ya sea usuario-contraseña o certificado).
- Defina un tiempo máximo de inactividad ***(session timeout)*** a partir del cual se bloquee el equipo y se solicite volver a introducir las credenciales de acceso del usuario.
- Genere las **credenciales tipo usuario-contraseña y certificados de manera individual** y conforme a la política de contraseñas que corresponda ya que se facilita el proceso de trazabilidad del usuario. Utilice canales seguros para transferir información entre equipos como certificados, agentes, software, etc. Instale los certificados de autenticación Wi-Fi de manera que no sean exportables o borrables.
- Bloquee todos aquellos accesos que no desee a los sistemas, ya sea mediante **cortafuegos** o configurando restricciones de acceso en los propios equipos.
- Configure los **tres mecanismos de seguridad** del modelo definido anteriormente para la conexión de los clientes usuarios vía Wi-Fi (802.1X, agente NAC y túnel VPN cifrado).
- Emplee el acceso Wi-Fi a través del protocolo **IEEE 802.1X con el método EAP-TLS**. Deshabilite la opción de uso de TLSv1.0 y TLSv1.1.
- Configure el **agente NAC** de tal forma que cada 30 segundos realice una comprobación sobre el estado de salud del dispositivo.
- Utilice **IKEv2** para el establecimiento de túneles IPsec.
- Utilice **sistemas de autenticación centralizada** como servidores RADIUS y proteja los canales de comunicación con protocolos seguros como RadSec.



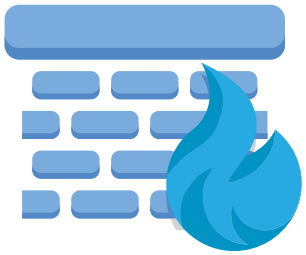
6.4 Configuración de servicios en el equipo

- Elimine toda **la información que viene configurada por defecto** de aquellos servicios de los que vaya a hacer uso.
- Emplee, en la medida de lo posible, un **servidor DHCP** ajeno al controlador de puntos de acceso. Además, se recomienda configurar la asignación fija de direcciones IP para cada cliente y que no se obtenga una dirección IP hasta que el usuario éste autenticado.
- Tenga todos los dispositivos sincronizados en tiempo mediante **NTP** y habilitando la autenticación.
- Utilice servidores externos del tipo **SNMP** y ***syslog*** que permitan recoger datos específicos sobre los equipos y las transacciones producidas en la red. Utilice **SNMPv3** puesto que incluye mejoras de seguridad de autenticación y envío de datos cifrados con respecto a SNMPv1 y SNMPv2.
- Habilite solo **protocolos seguros** en el controlador de puntos de acceso.
- Evite ataques de denegación de servicio a través del establecimiento de controles de **broadcast y multicast**.
- Prohíba o deshabilite todas aquellas configuraciones que empleen **IPv6** si no lo va a emplear en su red.
- Habilite el modo **FIPS** si dispone del mismo.
- Emplee **listas de acceso** para configurar los servicios habilitados para cada equipo o dispositivo cliente.
- Habilite el sistema de detección de intrusiones inalámbrico **(Wireless IDS)** del controlador Wi-Fi en caso de disponer del mismo.

Deshabilite todas aquellas configuraciones que empleen IPv6 si no lo va a emplear en su red

6.5 Políticas de usuario y reglas de cortafuegos

- Establezca **roles de usuarios** que permitan realizar un acceso jerárquico (con distintos permisos) a los servicios definidos.
- Limite el tráfico entre los usuarios conectados a la red: prohibición de comunicación peer-to-peer a través de la prevención de **tráfico entre usuarios**, limitación en el acceso a puertos, etc.
- Establezca listas de acceso **(ACL)** de direcciones IP válidas sólo para clientes Wi-Fi.
- **Limite los puertos** que han de estar abiertos en los equipos de red a los servicios que estos estén empleando y preferentemente realice una identificación y **filtrado de aplicaciones** independientemente del puerto de protocolo utilizado.
- Incluya mecanismos que eviten o mitiguen tanto ***ARP Spoofing*** como ***IP Spoofing*** con el fin de evitar ataques del tipo *Man-In-The-Middle* y de clonación/suplantación de direcciones IP.
- Establezca un control de defensa a través de la configuración de una serie de reglas del **cortafuegos** del controlador.



6.6 Eventos y monitorización del sistema

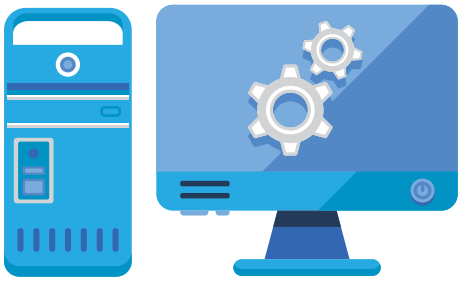
Un punto importante a tener en cuenta es la recopilación de eventos y la monitorización de los recursos del sistema para detectar posibles anomalías que podrían llegar a afectar al servicio.

Algunos ejemplos de indicadores a monitorizar son la CPU, la memoria RAM, el espacio de almacenamiento disponible, los procesos activos, el tráfico cursado por las interfaces físicas, las sesiones establecidas, el número de usuarios asociados y autenticados, el tiempo de respuesta de servicios como Radius, DHCP y DNS, los registros de autenticación y asociación, la temperatura del equipo, etc.

Los recursos pueden ser monitorizados mediante SNMPv3 o protocolos propietarios de la solución del fabricante. Hoy en día es común poder consultar el estado de los equipos utilizando consultar web mediante API-REST. También es común el uso de mecanismos como syslog para exportar los eventos del sistema a una consola central.

Es muy recomendable contar un una herramienta tipo SIEM con capacidades de realizar correlación sobre los datos monitorizados y los eventos de sistema recopilados. Incluso se puede llegar a realizar análisis basado en el comportamiento de dispositivo y usuario (UEBA).

Además de monitorizar y realizar correlación, todas la métricas y eventos son necesarios para llevar a cabo una investigación forense dado el caso de producirse un incidente. En importante definir una política de almacenamiento y tratamiento histórico de eventos para poder acceder a los datos en caso de ser requeridos por un incidente de seguridad.



6.7 Otras recomendaciones

- Realice un **análisis periódico de vulnerabilidades** y valore otras configuraciones que mejoren la seguridad de su red.
- **Monitorice el tráfico de la red** y realice una búsqueda periódica de anomalías.
- Implemente sistemas de **Detección de Intrusiones (IDS)** para la detección de posibles anomalías que generen alarmas.

7. Decálogo básico de seguridad

Este decálogo de buenas prácticas pretende sentar las bases sobre las medidas de seguridad a tener en cuenta cuando se instala una red Wi-Fi en un entorno corporativo.

1. **Plantee la eliminación de cualquier acceso inalámbrico priorizando los acceso cableados. Realice el análisis y gestión de riesgos asociados antes de la implementación de la red Wi-Fi. Analice el equipamiento necesario a adquirir, planificando la cobertura radio necesaria y definiendo la política de seguridad que aplica.**
2. **Realice un inventario de dispositivos haciendo una revisión periódica de este y de las posibles vulnerabilidades. Mantenga todos los equipos actualizados, copias de seguridad y procedimientos de recuperación probados.**
3. **Cree una red de gestión exclusiva, que sólo transporte tráfico de gestión y administración, en la que emplee protocolos seguros.**
4. **Genere certificados con datos de usuario y dispositivo. Cree distintos roles de usuarios para una mejor aplicación de la política de seguridad.**
5. **Utilice sistemas de autenticación centralizada como servidores RADIUS utilizando canales seguros como RadSec.**
6. **Realice una asignación mediante DHCP de dirección IP fija para cada cliente/dispositivo en cada una de las distintas redes.**
7. **Configure los clientes para utilizar 802.1X-EAP-TLS, agente NAC y túnel VPN cifrado según lo recomendado.**
8. **Limite el acceso físico a los equipos así como el acceso lógico en función de los roles definidos y desactive el servicio cuando no se estén utilizando.**
9. **Implemente sistemas de Detección de Intrusiones (IDS) para la detección de posibles anomalías que generen alarmas.**
10. **Monitorice el tráfico de la red y realice una búsqueda periódica de anomalías.**

8. Referencias

CCN-STIC-406 Seguridad en redes inalámbricas:	http://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/71-ccn-stic-406-seguridad-en-redes-inalambricas/file.html
CCN-STIC-647b Configuración segura de equips de red Aruba para entornos Wi-Fi:	http://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/600-guias-de-otros-entornos/2701-ccn-stic-647b-configuracion-segura-de-equipos-de-red-aruba-para-entornos-wifi/file.html
CCN-STIC-816 Seguridad en redes inalámbricas en el ENS:	http://www.ccn-cert.cni.es/pdf/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html
CCN-STIC-836 Seguridad en VPN en el marco del ENS:	https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html
WPA3-v2.0 Especificación publicada el 20/12/2019:	https://www.wi-fi.org/file/wpa3-specification

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional