GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT
centro criptológico nacional

CCN-CERT BP/11

Recomendaciones de seguridad en redes WiFi corporativas

Octubre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.10.29 08:39:59 +01'00'

Fecha de Edición: octubre de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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 a 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

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).

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 CDMA y GSM, GPRS, UMTS o redes IEEE 802.16 (WiMax).

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 WLAN o Redes WiFi. Estas redes inalámbricas se basan en el estándar IEEE 802.11.

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 (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.

Existen tres (3) topologías comunes a la hora de hablar de redes inalámbricas: ad-hoc, infraestructura y de malla.

- 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.
- 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.
- La **topología de malla** mezcla las dos anteriores. 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.

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, 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 WiFi bajo el nombre de WPA (WiFi Protected Access).

Posteriormente, una vez ratificado 802.11i, la Alianza WiFi introdujo **WPA2** (WiFi 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 principal de WPA2.

WPA y WPA2 tienen dos (2) 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. 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, RADIUS.

3. AMENAZAS Y RIESGOS EN REDES INALÁMBRIRCAS BASADAS EN EL ESTÁNDAR 802.11

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 WiFi. 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.

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

1. Puede obtenerse acceso a través de conexiones inalámbricas a otros entornos que, no siendo inalámbricos, estén conectados a estos.
2. La información que se transmite sin cables puede ser interceptada incluso a kilómetros de distancia, sin posibilidad de detectar esta captura.
3. Se pueden producir fácilmente ataques de denegación de servicio (DoS) contra este tipo de infraestructuras (inhibidores de señal, paquetes maliciosos, etc.).
4. Se puede inyectar tráfico en las redes inalámbricas a gran distancia (incluso kilómetros).
5. Se puede atacar a los clientes sin necesidad de una infraestructura centralizada, como podría ser un punto de acceso.
6. Se pueden desplegar equipos falsos (rogue AP) para obtener información. (redes sin cifrado o conociendo la clave del AP objetivo)
7. Una vez obtenido acceso a una red inalámbrica, se pueden realizar ataques de tipo “Man in the Middle”.
8. Se puede obtener información de conexión con tener acceso a un equipo legítimo y realizando un análisis forense del mismo.
9. Se puede obtener acceso a redes, utilizando las redes conectadas de terceros que no mantengan una política de seguridad adecuada.
10. Se pueden realizar ataques internos desplegando redes inalámbricas no autorizadas.
11. Se puede revelar información de la entidad propietaria en datos abiertos que son fácilmente capturables (SSID).

4. REDES WIFI CORPORATIVAS

Dentro de la arquitectura de una red WiFi corporativa, la más común es aquella compuesta por una sede principal, donde reside el núcleo de la red o centro de datos a través de la que se conectan los usuarios, además de por una serie de accesos remotos desde otras sedes de la misma organización o desde otros lugares a los que se hayan desplazado los usuarios. Esta arquitectura se representa en la siguiente figura.

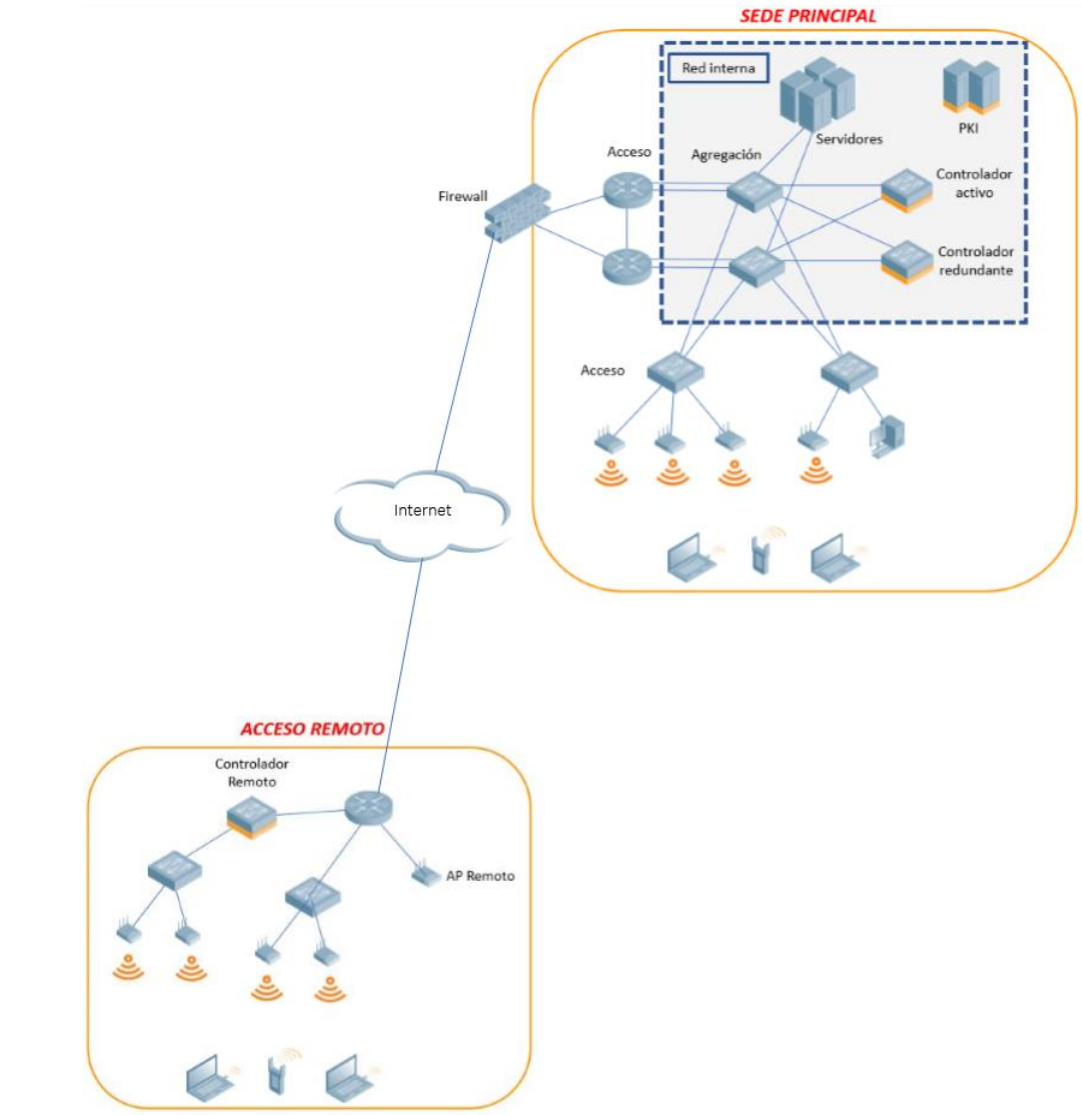

Figura 1.- Topología de una red corporativa

La sede principal corporativa está formada por:

- **Red de acceso**: es la que provee de conexión a los clientes, compuesta por:
  - Cortafuegos que controla el acceso del tráfico entrante y saliente de la red corporativa, filtrándolo en función de un conjunto de políticas de seguridad establecidas.

- Enrutadores de Acceso, que proveen de acceso a internet a los clientes.
- Puntos de Acceso WiFi, que permiten proveer de acceso a la red a los clientes WiFi.

- **Red interna**: es aquella en la que residen aquellos equipos sensibles a accesos no autorizados (área de acceso restringido), así como los equipos encargados de realizar las labores de agregación, permitiendo la incorporación de los tráficos entrantes y salientes (corporativo-Internet, Internet-corporativo). Los elementos que suelen encontrarse en esta zona de la red son:
  - Enrutadores de agregación, que permiten concentrar el tráfico de los clientes de la red interna.
  - Controladores de Puntos de Acceso, que gestionan de manera centralizada los Puntos de Acceso, servicios IP y políticas de seguridad de la red.
  - Servidores de acceso (AAA) como RADIUS o TACACS, de DHCP, proxys y bases de datos (LDAP, Directorio Activo), que permitirán suministrar todo tipo de información necesaria para responder a las solicitudes presentadas en la red.
  - Infraestructura de clave pública (PKI), encargada de generar y expedir certificados de identidad necesarios para la identificación de usuarios y sistemas, cifrado de datos digitales, firma de datos, garantía de no repudio y aseguramiento de las comunicaciones entre otros. Es un elemento imprescindible que, por seguridad, debe de estar aislado con el fin de que no se vea comprometida su disponibilidad, integridad y autenticidad.

Las conexiones remotas pueden establecerse a través de un Punto de Acceso remoto, un Punto de Acceso conectado a un Controlador remoto, el propio enrutador de acceso a internet de un usuario desplazado, etc.

4.1 SEGREGACIÓN DE REDES

Para un correcto agrupamiento y aislamiento de los distintos equipos que componen una red WiFi corporativa, se propone la creación de las siguientes redes virtuales (VLAN) en la arquitectura:

- Red de acceso: crear distintas VLAN por departamento, disponibilidad física o nivel de seguridad.
- Red interna, crear:
  - Red de Acceso a Internet: permitirá proveer a la red corporativa de acceso a internet a través de un enrutador de acceso.
  - Red de Gestión: servirá para realizar las tareas de administración y configuración de todos los sistemas conectados a la misma.
  - Red de Datos: permitirá intercambiar las peticiones RADIUS entre los clientes WiFi y los datos sobre el estado del dispositivo conectado a la red WiFi.

- Redes de transición de los usuarios: son redes que sólo se definirán en el Controlador de Puntos de Acceso con el objetivo de implementar el modelo de seguridad. Estas son:
  - Red de Validación: red en la que se establecerá al cliente una vez que éste haya concluido satisfactoriamente el proceso de autenticación WiFi 802.1X (nivel 1 del modelo de seguridad que se verá a posteriori) y hasta que se conozca si cumple o no con los requisitos de estado de salud del dispositivo.
  - Red de Cuarentena: red a la que se deriva a aquellos clientes que no cumplen con los requisitos de seguridad definidos del estado del dispositivo, comprobación del estado del dispositivo y donde existirán una serie de procedimientos de remediación definidos por la política corporativa que permitan corregir el estado del mismo.
  - Red de Estado Saludable: red a la que se conectan aquellos clientes que además de autenticarse satisfactoriamente en la red WiFi, cuentan con dispositivos que cumplen con los requisitos de estado de salud de la misma. Es desde esta red desde la cual los clientes tienen permiso para establecer un túnel VPN/IPsec (nivel 3 del modelo de seguridad que se verá a posteriori). En esta red existirá un servidor de direcciones IP que permita aportar una nueva dirección IP a través de la que se transmita y reciba tráfico encapsulado.
  - Red Túnel: es la red a través de la que se encapsula el tráfico mediante un túnel VPN/IPsec. Queda fuera del ámbito de la guía 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 donde se realice la instalación.

5. MODELO DE SEGURIDAD

En este apartado se pretende mostrar el modelo de seguridad basado en una arquitectura de tres capas o niveles que se recomienda implementar para configurar una red WiFi corporativa segura.

5.1 NIVEL 1: AUTENTICACIÓN WPA2-ENTREPRISE CON EAP-TLS

Se recomienda emplear como método de autenticación de usuarios en el acceso a la red WiFi, WPA2-Enterprise con EAP-TLS, ya que emplea el protocolo IEEE 802.1x para el intercambio de certificados entre cliente y servidor, realizándose una doble verificación (el cliente comprueba que el servidor contra el que se está autenticando es el adecuado y el servidor que ese cliente está autorizado a acceder a la red). Además, se aconseja el uso de servidores RADIUS como servidores de autenticación.

Con esto, sólo se permite el acceso a la red WiFi presentando un certificado de identidad en el proceso de autenticación.

Para la implementación de este nivel será necesario contar con una infraestructura que permita generar los certificados de cliente y servidor (PKI), así como de bases de datos para

almacenar esas credenciales como, por ejemplo, un LDAP, un Directorio Activo o cualquier otra base de datos.

El cliente presentará como credenciales de autenticación un certificado de identidad, instalado en su máquina, que llegará al servidor RADIUS a través del Controlador. El servidor RADIUS verificará si ese cliente se encuentra autorizado para acceder a la red, comprobando en el almacén de credenciales que ese usuario existe y que la Autoridad de Certificación que ha expedido ese certificado es válida. En el caso de que sí esté autorizado, el servidor RADIUS enviará su certificado de servidor al cliente para que este lo coteje con el que tiene instalado como certificado de servidor RADIUS y, en el caso de que ambos coincidan, se realiza el proceso de autenticación y se establece la conexión.

Si el certificado de identidad presentado por el cliente no se encuentra en la base de datos de credenciales conectada al servidor RADIUS o el certificado que envía el servidor RADIUS es distinto del que tienen instalado el cliente como certificado de servidor, no se produce el proceso de autenticación de la red por lo que se rechaza la conexión pidiéndose que se introduzcan las credenciales de acceso de nuevo.

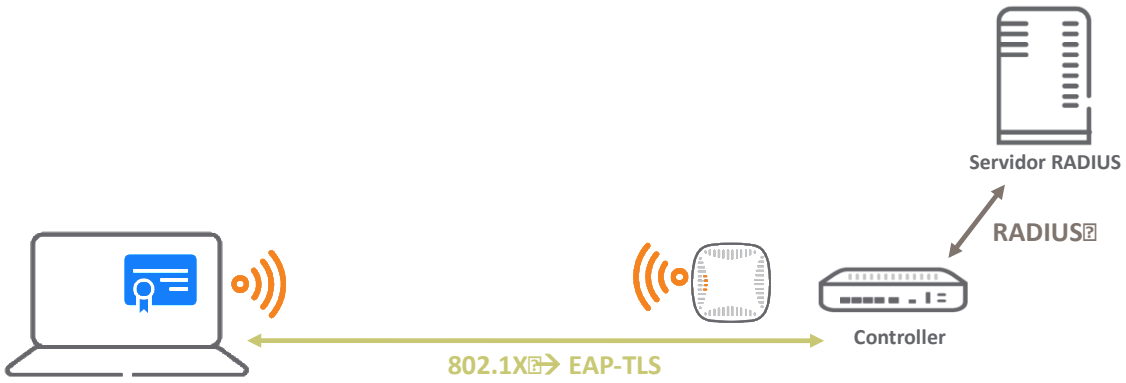

Figura 2.- Autenticación del cliente a la red WiFi

Un cliente WiFi no sólo se autenticará contra la red en el caso de que acceda a la misma por primera vez, sino que también lo hará cuando se produzca un cambio entre los distintos niveles del modelo de seguridad además de realizarse una autenticación periódica al menos una vez al día para verificar que se cumple este primer requisito de seguridad. Es recomendable habilitar esta autenticación periódica por el riesgo de seguridad que puede presentar un sistema conectado a la red durante largos periodos de tiempo sin que éste se autentique.

5.2 NIVEL 2: COMPROBACIÓN DEL ESTADO DEL DISPOSITIVO

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.

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).
- Sistemas de protección como Antivirus instalado y en ejecución, con instalación de 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 de estado que permita verificar el estado del equipo conectado. 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.

Cada vez que el cliente se autentique en la red y hasta que no se conozca si el dispositivo cumple o no con los requisitos, éste permanece en una red de espera.

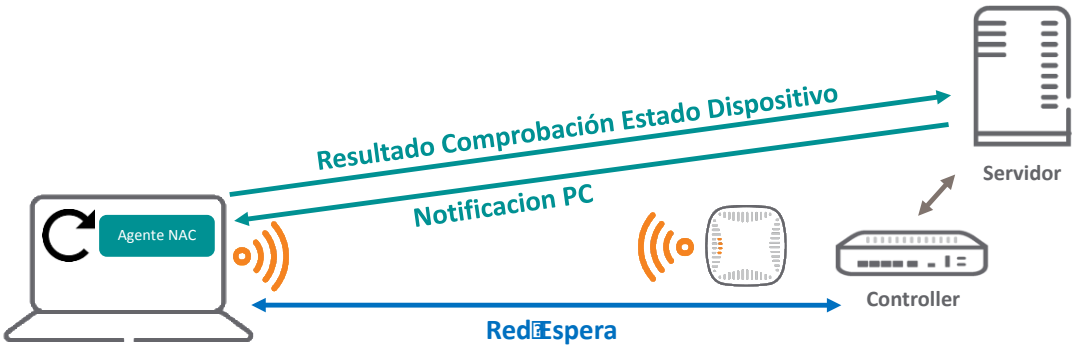

Figura 3.- Comprobación del estado del dispositivo a través del agente NAC

Si el cliente cumple con los requisitos especificados anteriormente, el servidor notificará al cliente de un cambio en su estado y se le trasladará a una red de estado en el que se ha verificado su nivel de seguridad.

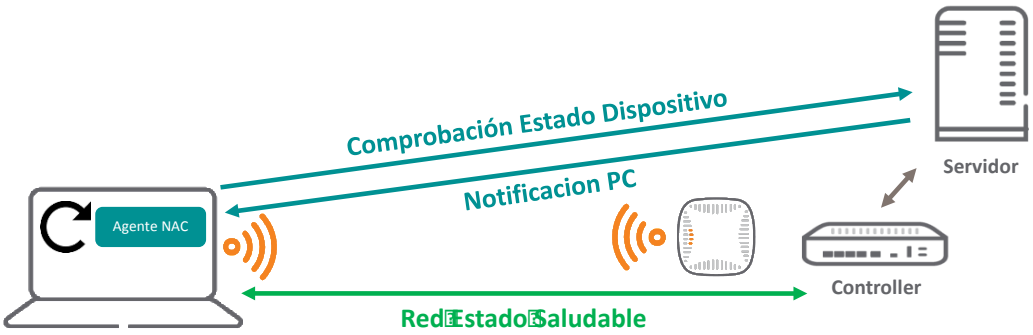

Figura 4.- Estado del dispositivo verificada su seguridad

Por el contrario, si el cliente no cumple con los requisitos especificados, el cliente será notificado de que su estado ha pasado a ser “cuarentena” y será trasladado a una red de cuarentena donde existan procedimientos de remediación que permitan cambiar su estado.

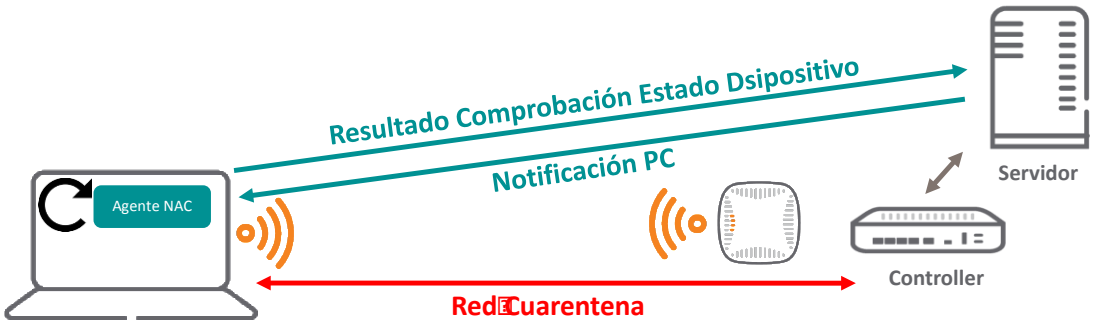

Figura 5.- Estado del dispositivo en cuarentena

5.3 NIVEL 3: ESTABLECIMIENTO DE TÚNEL CIFRADOS (VPN/IPSEC)

El establecimiento de túneles cifrados (VPN/IPsec) permitirá proteger la información en tránsito a través de mecanismos robustos de cifrado y autenticación. En el proceso de establecimiento del túnel, es necesario que se negocien una serie de parámetros de seguridad a través del protocolo IKE, entre los que se encuentra la suite criptográfica.

Se recomienda hacer uso de los siguientes algoritmos.

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 6.- Algoritmos criptográficos recomendados

El establecimiento del túnel VPN/IPsec sólo se permitirá si el cliente se encuentra en la "Red de Estado Saludable", es decir, una vez que se ha autenticado en la red WiFi y que se ha verificado que el equipo a través del que se conecta cumple con los requisitos mínimos de seguridad especificados. Para el establecimiento del túnel será necesario contar con un software que permita levantar túneles VPN/IPsec (cliente VPN).

Una vez que el túnel esté en funcionamiento, el cliente contará con dos conexiones distintas, la conexión mediante la "Red de Estado Saludable" y la conexión de la Red Túnel. Todo el tráfico intercambiado por el cliente viajará a través del túnel.

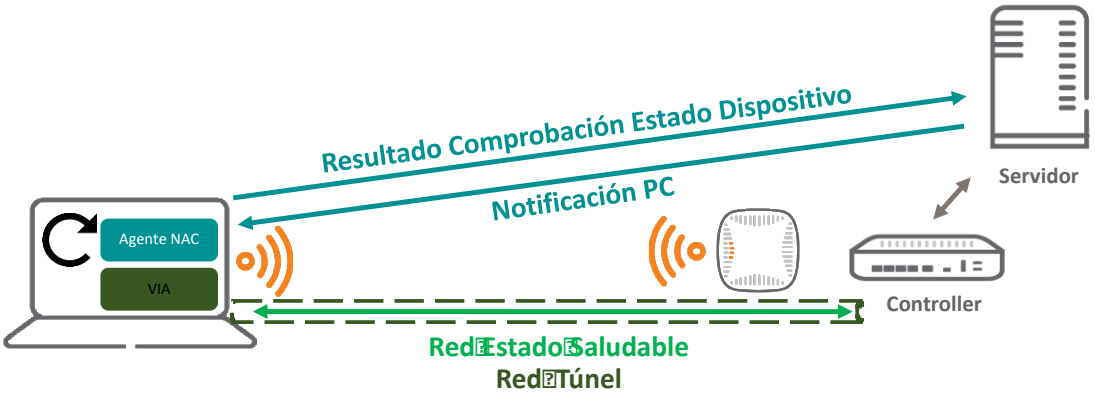

Figura 7.- Levantamiento del túnel VPN/IPsec

6. APLICACIÓN DEL MODELO DE SEGURIDAD

El cliente se verá trasladado de un nivel a otro en función del cumplimiento de los distintos requisitos especificados en cada uno de ellos. Para cada nivel, se definen unos roles de usuario en los que se especifican entre otros, las redes a las que estarán conectados esos clientes, políticas de acceso a los distintos servicios, permisos para establecer túneles VPN/IPsec, etc.

El cliente podrá subir de nivel si cumple con los requisitos exigidos o bajar si en algún momento de la conexión deja de cumplirlos.

6.1 NIVEL 1: AUTENTICACIÓN WPA-ENTERPRISE CON EAP-TLS

Para que el cliente alcance este nivel, será necesario que las credenciales de acceso presentadas a través del certificado de identidad de usuario instaladas en el equipo cliente se encuentren en el almacén de credenciales que se consulte, así como que la Autoridad de Certificación que haya expedido dicho certificado sea válida.

Además, el certificado de servidor que tiene instalado el cliente tiene que ser el mismo que el Servidor de autenticación presente al cliente durante el proceso de autenticación.

Una vez que el cliente supere el proceso de autenticación satisfactoriamente, se le asignará un "Rol_Validacion" en el que permanecerá hasta conocer el estado de salud del dispositivo con el que se ha conectado. Este "Rol_Validacion" permitirá:

- Que se le asigne como identificador de VLAN el correspondiente a la "Red de Validación".
- Que se sean aplicadas las siguientes políticas de cortafuegos:
  - Permiso para ejecutar el servicio de DHCP y así adquirir una dirección IP de la "Red de Validación".
  - Permisos necesarios de conexión del agente NAC de comprobación del estado de seguridad del equipo.
  - Prohibición del resto de conexiones.

6.2 NIVEL 2: COMPROBACIÓN DEL ESTADO DEL DISPOSITIVO

En este nivel se examina al equipo cliente conectado, que previamente ha superado el proceso de autenticación descrito en el nivel 1, a través de la ejecución del agente NAC. Si el cliente cumple con los requisitos de estado de salud del dispositivo especificado, adquiere el "Rol_EstadoSaludable" y si no los cumple el "Rol_Cuarentena". El "Rol_EstadoSaludable" posibilita:

- Que se le asigne como identificador de VLAN el correspondiente a "Red de Estado Saludable".
- Que se le apliquen las siguientes políticas de cortafuegos:
  - Permiso para ejecutar el servicio de DHCP y así adquirir una dirección IP de la "Red de Estado Saludable".
  - Permisos necesarios de conexión del agente NAC.
  - Permiso para conectarse al servidor de direcciones IP que permita al cliente obtener una nueva dirección IP y establecer el túnel VPN/IPsec.
  - Prohibición del resto de conexiones.

El "Rol_Cuarentena" permite:

- Que se le asigne como identificador de VLAN el correspondiente a la "Red de Cuarentena".
- Que se le apliquen las siguientes políticas de cortafuegos:
  - Permiso para ejecutar el servicio de DHCP y así adquirir una dirección IP de la "Red de Validación".
  - Permisos de conexión del agente NAC.
  - Permiso para conectarse con los servidores o equipos que permitan salir del estado de cuarentena. Variará en función de la política de cada corporación.
  - Prohibición del resto de conexiones.

6.3 ESTABLECIMIENTO DE TÚNEL VPN/IPSEC

Una vez que el cliente tiene asociado el "Rol_EstadoSaludable", obtendrá permisos para levantar el túnel VPN/IPsec a través del cliente VPN. Para ello será necesario que en el equipo cliente se encuentren instalados el certificado de curva elíptica de usuario, el certificado de curva elíptica de Autoridad de Certificación y el perfil de autenticación de VPN.

El cliente levantará el túnel VPN/IPsec utilizando el certificado de cliente de curva elíptica. Para ello, adquiere el "Rol_VPN/IPsec" mediante el cual se permite:

- Asignar el perfil de conexión correspondiente al "Perfil Conexion-VPN" para implementar el nivel 3 de seguridad.

- Que se le apliquen las siguientes políticas de cortafuegos:
  - Permiso para ejecutar el servicio de DHCP y así adquirir una dirección IP de la "Red de Túnel".
  - Permisos de conexión necesarios para el agente NAC.
  - Permiso para permitir la conexión con las redes o equipos a través del túnel VPN.
  - Prohibición del resto de conexiones.

6.4 RESUMEN DE POLÍTICAS DE FILTRADO

En la siguiente tabla se resumen las políticas de cortafuegos asociadas a los roles de usuario definidos para el caso de uso.

	Servidor DHCP	Red Datos	Red Gestión	Red Estado Saludable	Resto redes
Rol_Validación	Red Validación	Agente NAC	deny	deny	deny
Rol_Cuarentena	Red Cuarentena	Agente NAC	deny	deny	deny
Rol_EstadoSaludable	Red Estado Saludable	Agente NAC	deny	Intercambios IPsec	deny
Rol_VPN/Ipsec	Red Túnel	OnGuard	deny	deny	deny

Figura 8.- Resumen de las políticas de filtrado de roles de usuario

A los clientes WiFi en los roles de Validación, Cuarentena, Estado Saludable y de VPN/IPsec sólo se les permitirá acceder a los servicios del agente NAC necesarios para que lleguen las peticiones y respuestas del agente instalado en los clientes. Los puertos típicos empleados son los siguientes:

Descripción	Servicio	Protocolo	Puerto
Protocolo de Autenticación RADIUS	RADIUS	UDP	1812
Protocolo de Contabilidad RADIUS	RADIUS	UDP	1813
Cambio de Autorización en RADIUS	RFC 3576	UDP	3799
Protocolo seguro de transferencia de hipertexto	HTTPS	TCP	443
Agente NAC OnGuard <-> ClearPass Policy Manager	Control Channel	TCP	6658

Figura 9.- Puertos de Acceso a Servidor NAC

A los clientes WiFi en el "Rol_EstadoSaludable" hay que permitirles además la conectividad con los servicios que les permitan establecer el túnel VPN. Esto es posible a través de los siguientes puertos:

Descripción	Servicio	Protocolo	Puerto
NAT transversal	IPsec/NAT-T	UDP	4500
Internet Key Exchange	IKE	UDP	500

Figura 10.- Puertos de Acceso al servicio de VPN/IPsec

7. 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.

7.1 CONSIDERACIONES INCIALES

- Realice 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 de los mismos, 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.
- **Analizar el equipamiento a adquirir**, comprobando la capacidad para soportar los protocolos requeridos y la publicación de actualizaciones por parte del fabricante. Instalación de equipos redundantes de aquellos equipos que en caso de fallo, error o ataque no permitan un funcionamiento normal de la red. Realice un inventario de dispositivos que se deberán revisar 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), definiendo la ubicación de los puntos de acceso procurando 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 tiene 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. Realice comprobaciones periódicas del cumplimiento de las políticas de seguridad.
- **Formar** a los usuarios en el uso de esta tecnología y los riesgos asociados a su utilización.

7.2 ACTUALIZACIONES Y COPIAS DE SEGURIDAD

- 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.

7.3 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 bloquea el equipo y se solicita 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. Almacene las credenciales cifradas. Utilice canales seguros para transferir información entre equipos como certificados, agentes, software, etc. Instale los certificados de autenticación WiFi 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 niveles de seguridad** del modelo definido anteriormente para la conexión de los clientes usuarios vía WiFi.
- Emplee el acceso WiFi a través del protocolo **IEEE 802.1X con 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 o TACACS con el fin de prevenir ataques internos.

7.4 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.
- Tener 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**.
- Prohíba o deshabilite todas aquellas configuraciones que empleen **IPv6** si no lo va a emplear en su red.
- Habilite el modo **FIPS** si dispone de el 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 WiFi en caso de disponer de el mismo.

7.5 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 WiFi.
- **Limite los puertos** que han de estar abiertos en los equipos de red a los servicios que estos estén empleando.

- 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.

7.6 CONTROL DE USO DE RECURSOS DEL SISTEMA

Un punto importante a tener en cuenta es el uso de memoria de los equipos que se estén empleando en el despliegue ya que, si no se tiene espacio suficiente en disco, no se podrán almacenar datos que resultan significativos a nivel de seguridad. Algunos ejemplos de ello son los ficheros de logs, ficheros de monitorización, ficheros de copias de seguridad, informes de auditorías, ficheros con almacenamiento de cuentas expiradas, etc.

Para prevenir la falta de espacio, existen funcionalidades que indican que, si se alcanza un porcentaje de disco vacío, se realizará una limpieza de datos ya existentes para, de esa manera, liberar espacio.

7.7 OTRAS RECOMENDACIONES

- Realice un **análisis periódico de vulnerabilidades** y valorar 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.

8. 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 WiFi en un entorno corporativo.

	Decálogo Básico de Seguridad
1	Realice el análisis y gestión de riesgos asociados antes de la implementación de la red WiFi. Analizar 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. Mantener todos los equipos actualizados, copias de seguridad y procedimientos de recuperación probados.
3	Crear una red de gestión exclusiva, que sólo transporte tráfico de gestión y administración, en la que emplear protocolos seguros.
4	Genere las credenciales personales, usuario/contraseña y certificado. Cree distintos roles de usuarios para una mejor aplicación de la política de seguridad.
5	Utilice sistemas de autenticación centralizada como servidores RADIUS o TACACS.
6	Realice una asignación de direcciones IP fija para cada cliente en cada una de las distintas redes.
7	Configure los tres (3) niveles de seguridad mediante protocolo IEEE 802.1X con EAP-TLS e IPSEC 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.

9. REFERENCIAS

- CCN-STIC-406 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 http://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/600-guias-de-otros-entornos/2701-ccn-stic-647b-configuracio-segura-de-equipos-de-red-aruba-para-entornos-wifi/file.html
- CCN-STIC-816-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