Guía de Seguridad de las TIC
CCN-STIC 1016

Procedimiento de Empleo Seguro
Cisco WLAN IOS-XE



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 11
5.1 INSTALACIÓN FÍSICA DEL WLC 11
5.2 CONFIGURACIÓN INICIAL DE INTERFACES EN CONTROLADOR FÍSICO 11
5.3 CONFIGURACIÓN INICIAL DEL DOMINIO REGULATORIO Y RADIO 12
5.4 CONFIGURACIÓN DE FECHA Y HORA 12
5.5 HABILITACIÓN DEL REGISTRO DE CAMBIOS DE CONFIGURACIÓN 12
5.6 INSTALACIÓN DE LOS AP 13
5.7 ALTA INICIAL DE PUNTOS DE ACCESO 13
5.8 AUTORIZACIÓN DE LOS AP 13
6 FASE DE CONFIGURACIÓN 14
6.1 MODO DE OPERACIÓN SEGURO 14
6.2 AUTENTICACIÓN 14
6.2.1 AUTENTICACIÓN DE ADMINISTRADORES 14
6.2.2 AUTENTICACIÓN DE CLIENTES INALÁMBRICOS 15
6.2.3 AUTENTICACIÓN ENTRE WLC Y SERVIDOR RADIUS 15
6.2.4 AUTENTICACIÓN ENTRE WLC Y AP 15
6.2.5 AUTENTICACIÓN CON SERVIDOR EST 15
6.2.6 AUTENTICACIÓN CON SERVIDOR SYSLOG 15
6.3 ADMINISTRACIÓN DEL PRODUCTO 16
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 16
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 17
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 18
6.4.1 INTERFACES DE GESTIÓN DEL CONTROLADOR 18
6.4.2 INTERFAZ DE GESTIÓN WIRELESS 18
6.4.3 DESHABILITACIÓN DEL ENVÍO DIRECTO DE SYSLOG DESDE AP 19
6.5 GESTIÓN DE CERTIFICADOS 19
6.5.1 GENERACIÓN DE CLAVES Y CSR PARA HTTPS 20
6.5.2 CERTIFICADOS PARA IPSEC 20
6.5.3 CERTIFICADOS PARA RADSEC 20
6.5.4 CERTIFICADOS LSC PARA AP MEDIANTE EST 21
6.6 SERVIDORES DE AUTENTICACIÓN 21
6.7 SINCRONIZACIÓN 22
6.8 ACTUALIZACIONES 22
6.9 AUTO-CHEQUEOS 23
6.10 AUDITORÍA 23
6.10.1 REGISTRO DE EVENTOS 23
6.10.2 ALMACENAMIENTO LOCAL 24

6.10.3 ALMACENAMIENTO REMOTO 24
6.11 BACKUP 24
7 FASE DE OPERACIÓN 25
8 REFERENCIAS 26
9 ABREVIATURAS 27

ÍNDICE DE TABLAS

Tabla 1: Componentes del entorno operacional 10

ÍNDICE DE FIGURAS

Figura 1: Diagrama de entorno operacional 9

1 INTRODUCCIÓN

Cisco WLAN IOS-XE 17.12.04 proporciona una plataforma de red inalámbrica corporativa basada en controladores Cisco Catalyst 9800 y puntos de acceso Catalyst. El producto combina ambos componentes para proporcionar acceso inalámbrico seguro a la red de la organización y administración centralizada de la infraestructura WLAN (Wireless Local Area Network).

El producto está formado por dos tipos de componentes principales. El controlador o Wireless LAN Controller (WLC) es responsable de la gestión centralizada de los puntos de acceso, de la configuración de las WLAN, de la autenticación de clientes inalámbricos mediante 802.1X y de la protección de los canales de administración y auditoría. Los Puntos de Acceso (AP) operan en el borde de la red, proporcionan conectividad radio en las bandas soportadas y ejecutan las funciones IEEE (Institute of Electrical and Electronics Engineers) 802.11 necesarias para la asociación, autenticación, cifrado y gestión de sesiones inalámbricas.

2 OBJETO Y ALCANCE

La presente guía se desarrolla para los controladores Cisco Catalyst 9800 y puntos de acceso Catalyst que corren el software IOS-XE 17.12.04.

El presente Procedimiento de Empleo Seguro (PES) contempla dos configuraciones de uso que se usarán a lo largo del documento:

a) **Configuración A: Controlador WLAN + AP.**

   En esta configuración, el WLC actúa como punto central de administración, autenticación, configuración WLAN, auditoría, gestión de certificados y control de los AP. Los AP se unen al WLC y quedan administrados desde este a través de un canal interno protegido. Este perfil es el que se corresponde directamente con la configuración distribuida descrita en la documentación Common Criteria.

b) **Configuración B: AP con capacidad de controlador integrado.**

   En esta configuración, el equipo AP incorpora o habilita funciones de controlador para su propia operación o para la gestión de otros AP. Para este caso, el PES aplica de forma acumulativa los controles definidos para el componente controlador y para el componente AP. Antes de considerar este perfil como equivalente al perfil evaluado, deberá verificarse expresamente que el modelo concreto, la imagen IOS-XE 17.12.04, las licencias y la documentación oficial del fabricante soportan FIPS (Federal Information Processing Standards) mode, CC (Common Criteria) mode, administración segura, auditoría, 802.1X/EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), RADsec (RADIUS over TLS), DTLS (Datagram Transport Layer Security) / CAPWAP (Control And Provisioning of Wireless Access Points) y gestión de certificados LSC (Locally Significant Certificates) / EST (Enrollment over Secure Transport).

El producto Cisco WLAN IOS-XE 17.12.04 ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [[REF1].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 0. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

Antes de desembalar el producto, revise el embalaje físico en el que se entregó. Compruebe que el embalaje exterior de cartón lleve impresos el logotipo y los motivos de Cisco Systems. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que el embalaje no haya sido abierto y vuelto a cerrar de forma evidente, examinando la cinta adhesiva que lo sella. Si parece que el embalaje ha sido vuelto a cerrar, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que la caja de cartón exterior lleve adherida una etiqueta blanca de Cisco Systems con código de barras, a prueba de manipulaciones y que indique si ha sido manipulada. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco). Esta etiqueta incluirá el número de producto de Cisco, el número de serie y otra información relativa al contenido de la caja.

Anote el número de serie del producto en la documentación de envío. El número de serie que aparece en la etiqueta blanca pegada en la caja exterior es el del dispositivo. Compruebe que el número de serie que figura en la documentación de envío coincide con el número de serie que aparece en la factura del equipo, enviada por separado. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

Compruebe que la caja haya sido enviada efectivamente por el proveedor previsto del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco). Para ello, puede confirmar con el proveedor que envió la caja a través de la empresa de mensajería que la entregó y que el número de albarán del envío coincide con el utilizado en la entrega. Compruebe también que los números de serie de los artículos enviados coinciden con los números de serie de los artículos entregados. Esta comprobación debe realizarse mediante algún medio que no haya participado en la entrega real del equipo, por ejemplo, por teléfono/fax u otro servicio de seguimiento en línea.

Una vez desembalado el producto, inspeccione la unidad. Compruebe que el número de serie que figura en la propia unidad coincide con el número de serie que aparece en la documentación de envío y en la factura. Si no es así, póngase en contacto con el proveedor del equipo (Cisco Systems o un distribuidor o socio autorizado de Cisco).

4.2 ENTORNO DE INSTALACIÓN SEGURO

Los componentes que formen parte del despliegue de Cisco WLAN IOS-XE 17.12.04 deberán instalarse en un entorno físicamente protegido, con acceso limitado exclusivamente a personal autorizado.

Esta protección aplica a los controladores físicos, a los servidores que alojen controladores virtuales, a los puntos de acceso ubicados en zonas no públicas cuando sea posible, a los servidores de autenticación, a los servidores de auditoría, a la infraestructura de certificación y a las estaciones de administración. La documentación de seguridad del

producto asume que el dispositivo se encuentra físicamente protegido y que el entorno impide ataques físicos que comprometan la operación o las interconexiones del producto.

En despliegues con Cisco Catalyst 9800 físico, el controlador se instalará en un CPD (Centro de Proceso de Datos), sala técnica o armario de comunicaciones con control de acceso físico, condiciones ambientales adecuadas, protección eléctrica y conectividad de red segregada. Las conexiones de consola, gestión fuera de banda, gestión wireless, uplinks, redundancia y alimentación deberán quedar documentadas y etiquetadas. Cualquier puerto físico no utilizado deberá permanecer desconectado o administrativamente deshabilitado cuando proceda.

Los puntos de acceso deberán instalarse siguiendo las guías hardware del modelo correspondiente y considerando previamente un estudio de cobertura radio. Antes de su instalación definitiva, el administrador deberá verificar que el modelo y dominio regulatorio son válidos para el país de operación, que la ubicación física reduce riesgos de manipulación no autorizada y que el cableado de red y alimentación PoE (Power over Ethernet) queda protegido frente a accesos no autorizados. La guía oficial indica expresamente que debe comprobarse la aprobación del modelo AP para el país de uso y recomienda realizar un site survey antes de instalar los AP.

El entorno de instalación seguro deberá incluir, como mínimo, los servicios externos necesarios para operar el producto de forma segura: servidor RADIUS/RADsec para autenticación de clientes mediante EAP-TLS, autoridad de certificación, servidor EST para provisión de certificados LSC, servidor syslog remoto protegido mediante IPsec (Internet Protocol Security), estación de administración y consola local. Estos componentes forman parte del entorno operacional requerido en la configuración evaluada del producto.

Para la configuración A: Controlador WLAN + AP, todos los AP deberán unirse al WLC a través de un canal interno protegido con DTLS/CAPWAP y deberán ser gestionados desde el controlador. Para la configuración B: AP con capacidad de controlador integrado, el equipo deberá ubicarse y protegerse como si fuese simultáneamente controlador y punto de acceso, aplicando las protecciones físicas, lógicas y administrativas correspondientes a ambos roles.

4.3 REGISTRO Y LICENCIAS

El registro de los equipos, la descarga de software y la gestión de licencias se realizará mediante los canales oficiales del fabricante. El administrador deberá utilizar una cuenta Cisco válida, como Cisco CCO o SMART account, para acceder a Cisco Software Central [REF2] y descargar las imágenes autorizadas para la plataforma correspondiente.

La versión validada de referencia para el presente PES es IOS-XE 17.12.04. Las imágenes identificadas en la documentación oficial para controladores son las siguientes: C9800-L-universalk9_wlc.17.12.04.SPA.bin, C9800-40-universalk9_wlc.17.12.04.SPA.bin, C9800-80-universalk9_wlc.17.12.04.SPA.bin y C9800-CL-universalk9.17.12.04.ova. El software de los AP se encuentra embebido en la imagen del WLC 17.12.04 y no se descarga ni instala por separado.

El administrador deberá verificar la versión software instalada mediante la consola o la interfaz de administración del controlador. La comprobación mínima será:

```
WLC# show version
WLC# show version | include Cisco IOS XE Software
```

Para los AP el comando será:

```
show ap image
```

El resultado deberá confirmar que la versión en ejecución corresponde a IOS-XE 17.12.04.

4.4 CONSIDERACIONES PREVIAS

La presente guía contiene todo lo necesario para la instalación y operación segura del producto, sin embargo, se puede consultar la documentación [REF3] para información adicional.

El administrador puede acceder a la CLI (Command Line Interface) conectando el puerto de consola RJ-45 o el puerto de consola USB (Universal Serial Bus) del producto a su PC o estación de trabajo y accediendo al producto a través de un programa de emulación de terminal. Configure la velocidad de transmisión y el formato de caracteres del PC o del terminal para que coincidan con las características predeterminadas del puerto de consola que se indican a continuación:

a) 9600 baud

b) 8 data bits

c) 1 stop bit

d) No parity

e) None (flow control)

Si se utiliza el puerto de consola USB, es posible que los ordenadores con Windows o Mac necesiten instalar un controlador USB la primera vez que se utilice.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El entorno de operación de Cisco WLAN IOS-XE 17.12.04 deberá disponer de los componentes externos necesarios para que el producto pueda operar de forma segura y conforme a la configuración descrita en la documentación de seguridad. El WLC proporciona la administración centralizada de la infraestructura inalámbrica, la gestión de los AP, la configuración de las WLAN, la autenticación de clientes mediante 802.1X, la integración con servicios externos de seguridad y el envío de auditoría. Los AP proporcionan el acceso radio a los clientes inalámbricos y quedan gestionados por el WLC una vez unidos al controlador, formando conjuntamente el sistema WLAN de acceso.

Como ejemplo se puede observar el siguiente diagrama de un entorno mínimo:

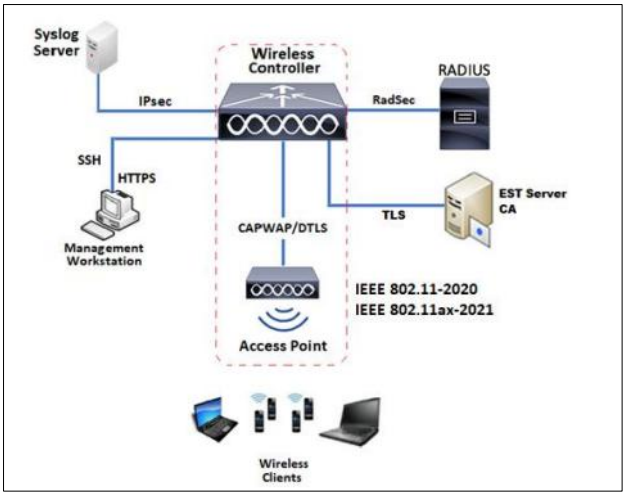


Figura 1: Diagrama de entorno operacional

La siguiente tabla recoge los componentes del entorno de operación que deberán estar presentes antes de la puesta en producción del producto.

Componente	Uso
Cliente Wireless	Permite a los usuarios establecer comunicaciones inalámbricas con la red privada de la organización a través del TOE.
Wireless LAN Controller (WLC)	Componente central de administración, autenticación, configuración WLAN, gestión de AP, auditoría, canales protegidos y políticas de seguridad.
Access Point (AP)	Proporciona acceso radio a los clientes WLAN y establece comunicaciones internas protegidas con el WLC mediante CAPWAP sobre DTLS.
Servidor RADIUS	Autentica los clientes inalámbricos mediante EAP-TLS.
Autoridad de certificación (CA)	Emite certificados válidos para el producto, servidores de autenticación, clientes inalámbricos y otros componentes. También proporciona al producto un mecanismo para comprobar el estado de revocación de certificados de pares, por ejemplo, mediante CRL.
Servidor EST	Autentica clientes EST y autoriza la emisión de certificados. Se emplea para el aprovisionamiento de certificados Locally Significant Certificates (LSC) utilizados por los AP en la configuración segura. Puede estar integrado en el propio servidor de CA o en un servidor dedicado.
Estación de administración	Equipo desde el que los administradores autorizados acceden al WLC mediante cliente SSH (Secure Shell) o navegador web con TLS. Debe ubicarse en una red de administración controlada y no en una WLAN de usuarios
Servidor Syslog	Recibe los registros de auditoría generados por el WLC y por los AP a través del WLC.

Tabla 1: Componentes del entorno operacional

En caso de usar la Configuración B de AP con capacidad de controlador integrado, el producto deberá tratarse como un componente que concentra las funciones de controlador y de punto de acceso. Por tanto, deberá integrarse con los mismos servicios externos: RADIUS, CA, EST, syslog y estación de administración.

5 FASE DE INSTALACIÓN

El presente PES únicamente desarrolla el procedimiento de instalación física. En el caso de la instalación virtual consultar la sección *5.3. Virtual Controller — Installation* de [REF3] sección] y la sección *1.7. Physical Scope of the TOE* de [REF4].

5.1 INSTALACIÓN FÍSICA DEL WLC

Para controladores físicos Cisco Catalyst 9800-L, 9800-40 o 9800-80, el administrador deberá seguir la guía de instalación hardware correspondiente al modelo concreto.

5.2 CONFIGURACIÓN INICIAL DE INTERFACES EN CONTROLADOR FÍSICO

En controladores físicos Cisco Catalyst 9800, se configurará inicialmente la interfaz de gestión fuera de banda, seguida de la interfaz de gestión wireless.

La interfaz GigabitEthernet1 se utilizará para gestión fuera de banda, salvo que el diseño de red aprobado establezca otra interfaz autorizada. Desde la CLI ejecutar los siguientes comandos:

```
WLC> enable
WLC# configure terminal
WLC(config)# interface GigabitEthernet1
WLC(config-if)# ip address <IP_GESTION_OOB> <MASCARA>
WLC(config-if)# no shutdown
WLC(config-if)# exit
WLC(config)# ip route <PREFIJO> <MASCARA> <NEXT_HOP>
```

La interfaz de gestión wireless deberá configurarse mediante VLAN (Virtual Local Area Network), SVI (Switched Virtual Interface) y asociación explícita al rol de gestión Wireless con los siguientes comandos:

```
WLC(config)# vlan <VLAN_WIRELESS_MGMT>
WLC(config-vlan)# name wireless_management
WLC(config-vlan)# exit
WLC(config)# interface vlan <VLAN_WIRELESS_MGMT>
WLC(config-if)# ip address <IP_WIRELESS_MGMT> <MASCARA>
WLC(config-if)# no shutdown
WLC(config-if)# exit
WLC(config)# wireless management interface <VLAN_WIRELESS_MGMT>
```

La interfaz física con conectividad hacia los AP deberá configurarse como trunk, permitiendo exclusivamente las VLAN necesarias conforme al diseño aprobado. Desde la CLI ejecutar los siguientes comandos:

```
WLC(config)# interface <INTERFAZ_HACIA_AP>
WLC(config-if)# switchport mode trunk
WLC(config-if)# switchport trunk allowed vlan <VLAN_WIRELESS_MGMT>
WLC(config-if)# shutdown
WLC(config-if)# no shutdown
```

5.3 CONFIGURACIÓN INICIAL DEL DOMINIO REGULATORIO Y RADIO

El administrador deberá configurar el país o dominio regulatorio aplicable al despliegue. Para ello usar los siguientes comandos desde la CLI, deshabitando primero radio y tras haber cambiado el país volviéndolo a habilitar con los siguientes comandos:

```
WLC(config)# ap dot11 6ghz shutdown
WLC(config)# ap dot11 5ghz shutdown
WLC(config)# ap dot11 24ghz shutdown
WLC(config)# ap country ES
WLC(config)# no ap dot11 24ghz shutdown
WLC(config)# no ap dot11 5ghz shutdown
WLC(config)# no ap dot11 6ghz shutdown
```

5.4 CONFIGURACIÓN DE FECHA Y HORA

Una vez finalizada la configuración inicial de interfaces y conectividad básica, el administrador deberá configurar la fecha, hora y zona horaria del controlador. La hora del sistema es necesaria para disponer de marcas temporales fiables en los registros de auditoría, validar certificados, aplicar temporizadores de sesión y soportar funciones criptográficas dependientes del tiempo. Nota: la configuración segura evaluada durante la certificación Common Criteria no contempla el uso de NTP (Network Time Protocol).

La configuración de fecha y hora se realizará desde modo privilegiado y modo de configuración global:

```
WLC> enable
WLC# configure terminal
```

Se configurará la zona horaria aplicable al entorno de operación. Para despliegues en España peninsular se podrá utilizar CET con desplazamiento UTC+1, adaptando el valor si la política corporativa exige otra referencia horaria:

```
WLC(config)# clock timezone CET 1 0
```

Si se requiere horario de verano, se configurará el ajuste correspondiente. Para España peninsular puede configurarse el cambio recurrente entre horario de verano e invierno según la política de la organización:

```
WLC(config)# clock summer-time CEST recurring last Sun Mar 02:00
last Sun Oct 03:00
```

El calendario del sistema se deberá marcar como válido para que el dispositivo considere autorizada la hora configurada:

```
WLC(config)# clock calendar-valid
```

Tras salir del modo de configuración, el administrador ajustará la hora manualmente con el siguiente comando:

```
WLC(config)# end
WLC# clock set <hh:mm:ss> <dia> <mes> <año>
```

5.5 HABILITACIÓN DEL REGISTRO DE CAMBIOS DE CONFIGURACIÓN

El WLC deberá registrar los cambios realizados sobre la configuración. Para ello se habilitará el registro de eventos con el siguiente comando:

```
WLC(config)# logging on
```

Para ver la configuración detallada de auditoría consultar la sección *6.10 AUDITORÍA* de la presente guía.

5.6 INSTALACIÓN DE LOS AP

Antes de instalar los AP, el administrador deberá leer y aplicar las guías de instalación hardware o getting started guide del modelo concreto. También deberá revisar la información regulatoria, advertencias de seguridad y restricciones de instalación aplicables al país y al dominio regulatorio del AP.

5.7 ALTA INICIAL DE PUNTOS DE ACCESO

Los AP deberán descubrir el controlador y unirse inicialmente al mismo. Esta alta inicial permite verificar la conectividad CAPWAP, identificar los AP autorizados y obtener el número de serie que será necesario posteriormente para la autorización de AP mediante número de serie.

En esta fase inicial, el AP podrá utilizar un certificado instalado de fábrica MIC o un certificado autofirmado SSC (Self-Signed Certificate), según el tipo de controlador utilizado. En la configuración segura final, los AP deberán utilizar certificados LSC aprovisionados mediante EST.

Tras completar el descubrimiento y permitir la unión inicial del AP, el administrador verificará desde el WLC que el AP se ha unido correctamente con el siguiente comando:

```
WLC# show ap summary
```

Para más información, consultar la sección 5.27 DTLS - CAPWAP de la guía [REF3].

5.8 AUTORIZACIÓN DE LOS AP

Antes de activar FIPS mode y CC mode deberán haberse identificado los números de serie de los AP autorizados. La configuración segura requiere que el administrador autorice explícitamente los AP que pueden unirse, utilizando el número de serie del AP. El número de serie se puede obtener con el siguiente comando:

```
WLC> enable
WLC# show ap config general
```

Posteriormente, se procederá a activar la autorización de AP por número de serie. Esta medida impide que puntos de acceso no autorizados se unan al controlador y formen parte del sistema WLAN. Para ellos se deberán usar los siguientes comandos:

```
WLC# configure terminal
WLC(config)# ap auth-list authorize-serialNum
```

A continuación, se añadirá el número de serie de cada AP autorizado. El valor utilizado deberá corresponder al número de serie correcto del AP, preferentemente el Top Assembly Serial Number cuando aplique:

```
WLC(config)# username <AP_SERIAL_NUMBER> serial-number
```

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

El modo de operación seguro de Cisco WLAN IOS-XE 17.12.04 requiere que el producto opere con el modo FIPS y modo Common Criteria habilitados. Para ello es necesario seguir los siguientes pasos:

Primero, el administrador deberá configurar una clave de autorización FIPS con una longitud de 32 caracteres. Esta clave deberá ser definida por el administrador de acuerdo con la política de gestión de credenciales de la organización:

```
WLC# configure terminal
WLC(config)# fips authorization-key <clave_32_caracteres>
WLC(config)# end
```

Tras configurar la clave FIPS, el controlador deberá reiniciarse para que el modo FIPS quede habilitado con el siguiente comando:

```
WLC# reload
```

Después del reinicio, el administrador deberá comprobar que FIPS mode se encuentra activo con el siguiente comando:

```
WLC# show fips status
```

Una vez verificado FIPS mode, el administrador deberá activar Common Criteria mode mediante los siguientes comandos:

```
WLC(config)# wireless wlancc
WLC(config)# end
```

Después se reiniciará el controlador de nuevo con el comando:

```
WLC# reload
```

6.2 AUTENTICACIÓN

Cisco WLAN IOS-XE 17.12.04 utiliza distintos mecanismos de autenticación en función del tipo de entidad que interactúa con el producto. En la configuración segura se distinguen tres ámbitos: autenticación de administradores, autenticación de clientes inalámbricos y autenticación entre componentes del TOE o con servicios externos. La documentación de seguridad identifica autenticación local para administradores, 802.1X/EAP-TLS para clientes WLAN y certificados X.509v3 para canales como TLS, DTLS e IPsec.

6.2.1 AUTENTICACIÓN DE ADMINISTRADORES

El WLC deberá utilizar el modelo AAA (Authentication, Authorization and Accounting) para controlar el acceso administrativo con los siguientes comandos:

```
WLC(config)# aaa new-model
WLC(config)# aaa authentication login default local
WLC(config)# aaa authorization exec default local
WLC(config)# aaa authorization credential-download default local
WLC(config)# ip http authentication aaa
```

Las cuentas administrativas serán locales al WLC, nominales y asociadas a privilegios de administración. La política concreta de usuarios, contraseñas se desarrolla en la sección *6.3.2 CONFIGURACIÓN DE ADMINISTRADORES* de la presente guía.

6.2.2 AUTENTICACIÓN DE CLIENTES INALÁMBRICOS

Los clientes inalámbricos deberán autenticarse mediante IEEE 802.1X, actuando el producto como autenticador y un servidor RADIUS externo como servidor de autenticación.

El método de autenticación recomendado para clientes WLAN es EAP-TLS, utilizando certificados X.509v3 emitidos por la PKI (Public Key Infrastructure) de la organización. Se deberá hacer uso de RADIUS para autenticar clientes inalámbricos mediante EAP-TLS y FreeRADIUS 3.0.x o superior para RADsec. Para configurar el modelo AAA se usarán los siguientes comandos:

```
WLC(config)# aaa group server radius <grupo_radius>
WLC(config-sg-radius)# server name <servidor_radius>
WLC(config-sg-radius)# exit
WLC(config)# aaa authentication dot1x default group <grupo_radius>
```

6.2.3 AUTENTICACIÓN ENTRE WLC Y SERVIDOR RADIUS

La comunicación entre el WLC y el servidor RADIUS deberá protegerse mediante RADsec, usando certificados X.509v3. El WLC deberá validar el certificado del servidor RADIUS mediante la cadena de confianza configurada y un identificador de referencia, por ejemplo, SAN DNS (Subject Alternative Name Domain Name System) o SAN IP.

Para más información consultar la sección 5.26 TLS – RADsec de [REF3] y la sección *6.6 SERVIDORES DE AUTENTICACIÓN* de la presente guía.

6.2.4 AUTENTICACIÓN ENTRE WLC Y AP

La autenticación entre WLC y AP se realiza mediante certificados X.509v3 y un canal interno protegido CAPWAP sobre DTLS. En la configuración segura, los AP deberán utilizar certificados LSC obtenidos mediante EST.

6.2.5 AUTENTICACIÓN CON SERVIDOR EST

El servidor EST se utiliza para el aprovisionamiento de certificados LSC a los AP. La comunicación entre el WLC y el servidor EST deberá realizarse mediante TLS 1.2 con autenticación mutua basada en certificados X.509v3.

El WLC deberá validar el certificado del servidor EST, incluyendo cadena de confianza, usos extendidos de clave y el identificador del servidor en SAN DNS o SAN IP. Si el certificado no es válido o no se puede verificar la revocación cuando sea requerida, la conexión no deberá establecerse.

6.2.6 AUTENTICACIÓN CON SERVIDOR SYSLOG

El envío de registros de auditoría al servidor syslog remoto deberá protegerse mediante IPsec/IKEv2 (Internet Key Exchange).

La autenticación del peer IPsec se realizará preferentemente mediante certificados X.509v3, usando RSA (Rivest-Shamir-Adleman) o ECDSA (Elliptic Curve Digital Signature Algorithm). La autenticación mediante certificados se configurará siguiendo el procedimiento IPsec descrito en la sección *6.5.2 Certificados para IPsec* del presente PES y en la sección 5.25 IPsec de la guía [REF3].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración local del WLC se realizará mediante consola local. En controladores físicos, el acceso se realizará por puerto de consola RJ-45 o USB. En controladores virtuales 9800-CL, se realizará mediante la consola de la máquina virtual en VMware ESXi.

La administración remota se realizará únicamente mediante:

a) SSHv2 para acceso remoto CLI.

b) HTTPS sobre TLS 1.2 para acceso WebGUI (Graphical User Interface).

No se permitirá administración remota desde clientes inalámbricos.

No deberán utilizarse protocolos inseguros para administración o transferencia de configuración. En particular los siguientes:

a) Telnet

b) SSHv1

c) HTTP

d) TLS 1.0 o TLS 1.1

e) FTP

f) IKEv1

Para desactivar tales protocolos inseguros se usarán los siguientes comandos:

```
WLC(config)# ip ssh version 2
WLC(config)# line vty 0 4
WLC(config-line)# transport input ssh
WLC(config-line)# exec-timeout 5
WLC(config-line)# exit
WLC(config)# line vty 5 15
WLC(config-line)# transport input ssh
WLC(config-line)# exec-timeout 5
WLC(config-line)# exit
WLC(config)# no ip http server
WLC(config)# ip http secure-server
WLC(config)# ip http tls-version TLSv1.2
```

Para configurar de manera segura SSHv2 se usarán los siguientes comandos:

```
WLC(config)# ip domain name <dominio>
WLC(config)# crypto key generate rsa label SSH-KEY modulus 3072
WLC(config)# ip ssh rsa keypair-name SSH-KEY
WLC(config)# ip ssh version 2
WLC(config)# ip ssh server algorithm kex ecdh-sha2-nistp256 ecdh-
sha2-nistp384
```

```
WLC(config)# ip ssh server algorithm encryption aes256-gcm@openssh.com aes128-gcm@openssh.com
WLC(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
WLC(config)# ip ssh server algorithm mac hmac-sha2-256
WLC(config)# ip ssh rekey time 60
WLC(config)# ip ssh rekey volume 1000000
```

La administración WebGUI deberá usar HTTPS con TLS 1.2 y certificado X.509v3 emitido por la PKI de la organización.

Se generará una clave ECDSA P-256 o RSA 3072 para HTTPS. Este PES recomienda ECDSA P-256 o superior cuando sea compatible con la infraestructura PKI:

```
WLC(config)# crypto key generate ec keysize 256 exportable label HTTPS-KEY
```

Se habilitará HTTPS, TLS 1.2 y ciphersuites seguras y timeout:

```
WLC(config)# ip http secure-server
WLC(config)# ip http tls-version TLSv1.2
WLC(config)# ip http secure-ciphersuite ecdhe-ecdsa-aes-gcm-sha2
WLC(config)# ip http secure-ecdhe-curve secp256r1
WLC(config)# ip http secure-trustpoint <trustpoint_https>
WLC(config)# ip http session-idle-timeout 300
```

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

La administración segura se realizará mediante cuentas locales en el WLC. El rol principal es el de Security Administrator el cual puede administrar el producto local y remotamente. Este rol cuenta con privilegio 15, el máximo.

La creación de usuarios administrativos locales se realizará mediante el comando username, asignando privilegio, política Common Criteria y contraseña protegida mediante SHA-256 (Secure Hash Algorithm).

```
WLC(config)# username <usuario_admin> privilege 15 common-criteria-policy <politica_cc> algorithm-type sha256 secret <password>
```

6.3.2.1 POLÍTICA SEGURA DE CONTRASEÑAS

Se configurará una política de contraseñas mediante *aaa common-criteria policy* y se aplicará a todas las cuentas administrativas locales con los siguientes comandos:

```
WLC(config)# aaa common-criteria policy CC
WLC(config-cc-policy)# min-length 12
WLC(config-cc-policy)# lifetime day 60
WLC(config-cc-policy)# exit
```

La política mínima del será:

a) Longitud mínima:12 caracteres.

b) Composición: Mayúsculas, minúsculas, números y símbolos. Usar los cuatro grupos si es posible, mínimo tres.

c) Historial: Al menos 5 contraseñas anteriores si el producto o el AAA externo lo soporta.

d) Caducidad: 60 días.

e) Tiempo mínimo antes de cambio: 10 días si el producto o el AAA externo lo soporta.

f) Almacenamiento: Hash SHA-256 mediante algorithm-type sha256.

6.3.2.2 INTENTOS FALLIDOS Y BLOQUEO

El WLC deberá bloquear intentos de fuerza bruta contra cuentas administrativas. Se establece un máximo de tres intentos fallidos y un bloqueo de cinco minutos.

```
WLC(config)# aaa authentication rejected 3 in 300 ban 300
```

Para más información consultar las secciones 5.16 a 5.21 de [REF3].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

La configuración de interfaces, puertos y servicios deberá limitar la superficie de exposición del controlador y de los puntos de acceso. Solo deberán habilitarse las interfaces, VLAN, puertos y servicios necesarios para la operación segura del producto. Para más información consultar las secciones 5.4, 5.5, 5.24, 5.25, 5.26, 5.27, 6.6 y 6.7 de [REF3].

6.4.1 INTERFACES DE GESTIÓN DEL CONTROLADOR

El controlador WLC deberá disponer, como mínimo, de una interfaz de gestión fuera de banda y una interfaz de gestión wireless. La interfaz GigabitEthernet1 se utiliza para gestión fuera de banda, GigabitEthernet2 para gestión wireless y una tercera interfaz puede utilizarse para alta disponibilidad.

La interfaz de gestión fuera de banda deberá configurarse con dirección IP, máscara y estado activo:

```
WLC(config)# interface GigabitEthernet1
WLC(config-if)# description Gestion fuera de banda - Administracion WLC
WLC(config-if)# ip address <IP_GESTION_OOB> <MASCARA>
WLC(config-if)# no shutdown
WLC(config-if)# exit
```

También deberá configurarse la ruta necesaria para que el controlador sea accesible únicamente desde las redes de administración autorizadas:

```
WLC(config)# ip route <PREFIJO> <MASCARA> <NEXT_HOP>
```

6.4.2 INTERFAZ DE GESTIÓN WIRELESS

La interfaz de gestión wireless deberá configurarse mediante VLAN y SVI. Esta interfaz será utilizada para funciones wireless y comunicación con los AP.

```
WLC(config)# vlan <VLAN_WIRELESS_MGMT>
WLC(config-vlan)# name wireless_management
WLC(config-vlan)# exit

WLC(config)# interface vlan <VLAN_WIRELESS_MGMT>
WLC(config-if)# description Gestion Wireless - AP Join
WLC(config-if)# ip address <IP_WIRELESS_MGMT> <MASCARA>
WLC(config-if)# no shutdown
WLC(config-if)# exit
```

```
WLC(config)# wireless management interface <VLAN_WIRELESS_MGMT>
```

Las interfaces físicas o virtuales que conecten con la red de AP deberán configurarse como trunk únicamente con las VLAN necesarias. No deberán permitirse VLAN no utilizadas ni redes ajenas al diseño aprobado.

```
WLC(config)# interface <INTERFAZ_HACIA_AP>
WLC(config-if)# description Trunk hacia red de AP
WLC(config-if)# switchport mode trunk
WLC(config-if)#       switchport       trunk       allowed       vlan
<VLAN_WIRELESS_MGMT>,<VLAN_CLIENTES>
WLC(config-if)# shutdown
WLC(config-if)# no shutdown
```

6.4.3 DESHABILITACIÓN DEL ENVÍO DIRECTO DE SYSLOG DESDE AP

Para la configuración evaluada (Configuración A), debe deshabilitarse la transmisión de mensajes Syslog desde AP hacia hosts externos ya que estos son enviados al WLC, donde se centraliza su almacenamiento y su posterior envío al servidor syslog remoto. Esto se puede hacer de manera sencilla, desde la WebGUI accediendo a Configuration > Tags and Profiles > AP Join > Management y estableciendo el host Syslog del AP a 127.0.0.1.

6.5 GESTIÓN DE CERTIFICADOS

El producto utiliza certificados X.509v3 para proteger y autenticar diversos canales: administración HTTPS, IPsec para syslog remoto, RADsec para RADIUS, TLS con EST y DTLS/CAPWAP entre WLC y AP.

El WLC deberá disponer de trustpoints para las autoridades de certificación raíz e intermedias necesarias. Los certificados CA deberán importarse en formato PEM (Privacy Enhanced Mail) y validarse antes de utilizarse como anclas de confianza. Como ejemplo genérico para importar una CA raíz:

```
WLC(config)# crypto pki trustpoint <TP_ROOT_CA>
WLC(ca-trustpoint)# enrollment terminal pem
WLC(ca-trustpoint)# chain-validation stop
WLC(ca-trustpoint)# revocation-check none
WLC(ca-trustpoint)# exit
WLC(config)# crypto pki authenticate <TP_ROOT_CA>
```

Hay que tener en cuenta que durante los pasos concretos de enrolamiento inicial es posible usar *revocation-check none*; no obstante, para operación segura de canales externos se configurará comprobación de revocación mediante CRL (Certificate Revocation List) siempre que sea aplicable y esté soportado por el servicio con el siguiente comando:

```
WLC(ca-trustpoint)# revocation-check crl
```

La validación mediante CRL requiere que los certificados incluyan los correspondientes puntos de distribución CRL y que dichos repositorios sean accesibles desde el entorno operacional. Según la configuración Common Criteria evaluada del producto, la validación de revocación mediante Online Certificate Status Protocol (OCSP) no está soportada.

6.5.1 GENERACIÓN DE CLAVES Y CSR PARA HTTPS

Para HTTPS se generará una clave ECDSA P-256 o RSA 3072. Este PES recomienda ECDSA P-256 o superior cuando sea compatible con la PKI corporativa.

```
WLC(config)# crypto key generate ec keysize 256 exportable label
HTTPS-KEY
WLC(config)# crypto key generate rsa general modulus 3072 label
HTTPS-KEY
```

A continuación, se configurará el trustpoint, se generará la solicitud CSR (Certificate Signing Request) y se importará el certificado firmado:

```
WLC(config)# crypto pki trustpoint <TP_HTTPS>
WLC(ca-trustpoint)# enrollment terminal pem
WLC(ca-trustpoint)#      subject-name      C=ES,      ST=<provincia>,
L=<localidad>, O=<organizacion>, OU=<unidad>, CN=<fqdn_wlc>
WLC(ca-trustpoint)# eckeypair HTTPS-KEY
WLC(ca-trustpoint)# revocation-check none
WLC(ca-trustpoint)# exit
WLC(config)# crypto pki enroll <TP_HTTPS>
WLC(config)# crypto pki import <TP_HTTPS> certificate
```

6.5.2 CERTIFICADOS PARA IPSEC

Para IPsec, consultar la guía [REF3] donde se describe la generación de claves, creación de trustpoints, CSR, importación de certificado y configuración de validación mediante CRL en la sección 5.25 IPsec, apartados Generate a Crypto Key Pair for IPsec y Create Trustpoints for IPsec. Como ejemplo para la generación de claves se pueden usar los siguientes comandos:

```
WLC(config)# crypto key generate ec keysize 256 exportable label
IPSEC-KEY
WLC(config)# crypto key generate rsa general modulus 3072 label
IPSEC-KEY
```

6.5.3 CERTIFICADOS PARA RADSEC

Para RADsec, consultar la guía [REF3] donde describe la generación de una clave RSA, trustpoints de cliente y servidor, CSR, importación de certificados y validación del identificador del servidor RADIUS en la sección 5.26 TLS – RADsec. Como ejemplo para la generación de claves se pueden usar el siguiente comando:

```
WLC(config)# crypto key generate rsa general modulus 3072 label TLS-
RADSEC-KEY
```

Hay que tener en cuenta que la configuración RADsec requiere trustpoint de cliente y trustpoint de servidor que puede ser configurado con los siguientes comandos:

```
WLC(config-radius-server)# tls trustpoint client <TP_RADSEC_CLIENT>
WLC(config-radius-server)# tls trustpoint server <TP_RADSEC_SERVER>
WLC(config-radius-server)#   tls   match-server-identity   hostname
<fqdn_radius>
```

6.5.4 CERTIFICADOS LSC PARA AP MEDIANTE EST

Los certificados LSC de AP se aprovisionan usando EST. Consultar la guía [REF3] en las secciones 5.31 Configure Locally Significant Certificates (LSC) Using EST - ECC Certificates y 5.32 Enable LSC Provisioning for AP donde se describe este proceso. Se utilizarán claves ECC (Elliptic Curve Cryptography) para EST y CAPWAP/DTLS, por ejemplo con los siguientes comandos:

```
WLC(config)# crypto key generate ec keysize 384 exportable label
CAPWAP-SERVER-ECC
WLC(config)# crypto key generate ec keysize 256 exportable label
EST-TLS-CLIENT-ECC
```

Después de configurar trustpoints y perfil de enrolamiento EST, se habilitará el aprovisionamiento LSC:

```
WLC(config)# ap lsc-provision trustpoint <TP_CAPWAP_CA>
WLC(config)# ap lsc-provision
WLC(config)# wireless management trustpoint <TP_CAPWAP_CA>
```

La verificación se realizará comprobando que el AP utiliza LSC:

```
WLC# show ap config general | include Cert|Cisco AP Name
```

6.6 SERVIDORES DE AUTENTICACIÓN

Cisco WLAN IOS-XE 17.12 utiliza servidores externos de autenticación para validar clientes inalámbricos mediante 802.1X/EAP-TLS. El servidor externo previsto en la configuración segura es RADIUS, protegido mediante RADsec.

Una vez configurados los certificados y trustpoints, se definirá el servidor RADIUS con TLS con los siguientes comandos:

```
WLC(config)# radius server <NOMBRE_RADIUS>
WLC(config-radius-server)# address ipv4 <IP_RADIUS>
WLC(config-radius-server)# key 0 <secreto_radius>
WLC(config-radius-server)# tls port 2083
WLC(config-radius-server)# tls trustpoint client <TP_CLIENTE_RADSEC>
WLC(config-radius-server)#       tls       trustpoint       server
<TP_SERVIDOR_RADSEC>
WLC(config-radius-server)#   tls   match-server-identity   hostname
<FQDN_RADIUS>
WLC(config-radius-server)# exit
```

Aunque el comando incluye una clave/secreto RADIUS, la autenticación principal del canal RADsec se realizará mediante certificados X.509v3. La clave RADIUS deberá protegerse y no deberá considerarse sustituto de los certificados.

La verificación del estado del servidor RADsec se realizará con:

```
WLC# show aaa servers
```

Para una información más detallada sobre la configuración consultar la sección 5.26 TLS – RADsec de [REF3].

6.7 SINCRONIZACIÓN

La sincronización temporal es necesaria para disponer de marcas de tiempo fiables en los eventos de auditoría, validar certificados, aplicar temporizadores de sesión, controlar bloqueos de autenticación y gestionar lifetimes de protocolos criptográficos. Nota: la configuración segura evaluada durante la certificación Common Criteria no contempla el uso de NTP (Network Time Protocol). Para este producto se utilizará la configuración manual de fecha, hora, zona horaria y horario de verano con los siguientes comandos:

```
WLC(config)# clock timezone CET 1 0
```

Si se requiere horario de verano, se configurará el ajuste correspondiente. Para España peninsular puede configurarse el cambio recurrente entre horario de verano e invierno según la política de la organización:

```
WLC(config)# clock summer-time CEST recurring last Sun Mar 02:00
last Sun Oct 03:00
```

El calendario del sistema se deberá marcar como válido para que el dispositivo considere autorizada la hora configurada:

```
WLC(config)# clock calendar-valid
```

Tras salir del modo de configuración, el administrador ajustará la hora manualmente con el siguiente comando:

```
WLC(config)# end
WLC# clock set <hh:mm:ss> <dia> <mes> <año>
```

6.8 ACTUALIZACIONES

Las actualizaciones de firmware, software e imágenes del producto deberán realizarse únicamente mediante imágenes oficiales obtenidas desde Cisco Software Central [REF2], utilizando una cuenta Cisco autorizada, por ejemplo, Cisco CCO o SMART account.

La imagen descargada deberá colocarse en un servidor accesible desde el WLC y se deberá usar SFTP (Secure File Transfer Protocol) para la transferencia.

Antes de realizar cualquier actualización, el administrador deberá verificar la versión actualmente instalada:

```
WLC# show version
```

Para instalar la imagen se usará el siguiente comando:

```
WLC# install add file
sftp://<usuario>@<servidor>/<ruta>/<imagen.bin> activate commit
```

Tras completarse el proceso y reiniciarse el sistema cuando corresponda, el administrador deberá verificar que la nueva versión se encuentra activa de nuevo con el comando:

```
WLC# show version
```

Los AP reciben la imagen desde el WLC tras el reinicio o proceso de actualización. Después del arranque del AP, este descargará su nueva imagen desde el WLC y realizará una verificación de firma digital antes de ejecutarla.

Para más información consultar la sección 6.27. Update WLC and AP Software de [REF3].

6.9 AUTO-CHEQUEOS

Cisco WLAN IOS-XE 17.12 ejecuta auto-chequeos de seguridad para verificar la integridad del software y el correcto funcionamiento de los módulos criptográficos. Estos auto-chequeos se ejecutan durante el arranque de los componentes del producto y, en el caso del WLC, también pueden ejecutarse bajo demanda por el administrador autorizado.

En caso de que alguna prueba fallase, el sistema muestra información en consola, bloquea el reenvío de tráfico y el componente afectado se reinicia automáticamente.

El administrador autorizado puede ejecutar los self-tests criptográficos en el WLC después de que la imagen haya cargado correctamente mediante el siguiente comando:

```
WLC# test crypto self-test
```

6.10 AUDITORÍA

El WLC almacena localmente los eventos de auditoría y envía en tiempo real los eventos a un servidor syslog externo mediante un canal protegido con IPsec. Los AP transmiten sus eventos al WLC, donde se almacenan junto con los eventos del controlador.

6.10.1 REGISTRO DE EVENTOS

Cisco WLAN IOS-XE 17.12 genera eventos de auditoría para accesos administrativos, cambios de configuración, generación o eliminación de claves, reinicio de servicios, fallos de autenticación, fallos de establecimiento de SSH/HTTPS/TLS/DTLS/IPsec, cambios de hora, actualizaciones, self-tests, asociación de clientes WLAN, eventos 802.1X y estado de canales protegidos.

Para configurar el registro de eventos desde los eventos necesario se usarán los siguientes comandos:

```
WLC(config)# logging on
WLC(config)# archive
WLC(config-archive)# log config
WLC(config-archive-log-cfg)# logging enable
WLC(config-archive-log-cfg)# hidekeys
WLC(config-archive-log-cfg)# logging size <1-1000>
WLC(config-archive-log-cfg)# notify syslog
WLC(config-archive-log-cfg)# end
WLC(config)# logging buffer 150000000
WLC(config)# login on-failure log
WLC(config)# login on-success log
WLC(config)# service timestamps log datetime year
WLC(config)# logging trap debugging
WLC(config)# ip ssh logging events
WLC(config)# crypto logging session
WLC(config)# crypto logging ikev2
WLC(config)# wireless client syslog-detailed
```

Para información más detallada consultar las secciones 5.7 a 5.15 de [REF3].

6.10.2 ALMACENAMIENTO LOCAL

El WLC almacena registros de auditoría localmente. La configuración evaluada requiere un buffer local de 150000000 bytes, el cual se puede configurar mediante el comando:

```
WLC(config)# logging buffer 150000000
```

Cuando el espacio local se llena, el WLC sobrescribe los eventos más antiguos para admitir eventos nuevos.

Los logs podrán consultarse mediante el siguiente comando:

```
WLC# show logging
```

6.10.3 ALMACENAMIENTO REMOTO

El WLC deberá transmitir los eventos de auditoría a un servidor syslog remoto. En la configuración evaluada, este envío debe protegerse mediante IPsec. La configuración de IPsec para proteger syslog remoto puede consultarse en la sección 5.25 IPsec de [REF3],.

Una vez completada la configuración de IPsec, se definirá el servidor syslog remoto mediante los siguientes comandos:

```
WLC(config)# logging host <ip_syslog>
WLC(config)# logging trap debugging
```

Para generar los eventos de auditoría requeridos por la configuración evaluada deberán verificarse que los comandos referenciados en la sección 6.10.1 REGISTRO DE EVENTOS del presente PES han sido habilitados.

Asimismo, para generar determinados eventos criptográficos requeridos por la configuración CC deberán habilitarse los siguientes comandos de depuración tras cada reinicio del producto:

```
WLC# debug crypto pki validation
WLC# debug crypto pki transaction
WLC# debug crypto pki api
WLC# debug crypto pki messages
WLC# debug crypto isakmp
WLC# debug crypto ipsec
WLC# debug crypto ikev2
WLC# debug crypto engine
WLC# debug logging system error
WLC# debug ssl openssl errors
```

6.11 BACKUP

Se deberán realizar backups periódicos de la configuración y de los elementos necesarios para recuperar el servicio WLAN de forma segura. Los backups deberán almacenarse en repositorios protegidos, preferentemente mediante protocolos seguros como SFTP, y deberán cifrarse o protegerse conforme a la política de la organización. Para realizar el backup se podrá utilizar los siguientes comandos:

```
WLC#                        copy                        running-config
sftp://<usuario>@<servidor>/<ruta>/running-config-wlc.txt
WLC#                        copy                        startup-config
sftp://<usuario>@<servidor>/<ruta>/startup-config-wlc.txt
```

7 FASE DE OPERACIÓN

Durante la fase de operación del producto, el administrador debe llevar a cabo las siguientes tareas de mantenimiento:

- Mantenimiento del control de acceso al producto.
- Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado.
- Seguir las alertas de seguridad de Cisco ([REF5]) y, si es necesario, aplicar un parche (*Minor Release* o *Maintenance Release*).
- Mantenimiento de los registros de auditoría, incluyendo su revisión periódica para detectar eventos de seguridad, accesos no autorizados, errores de operación y cambios de configuración. Estos registros estarán protegidos contra borrados y modificaciones no autorizados, y solamente el personal de seguridad autorizado podrá acceder a ellos.

8 REFERENCIAS

[REF1] CPSTIC
(https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic)

[REF2] Cisco Software Central
(https://software.cisco.com)

[REF3] Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Common Criteria Configuration Guide Version: 1.0 Date: May 6, 2025 (https://www.commoncriteriaportal.org/files/epfiles/st_vid11456-st.pdf)

[REF4] Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target Version: 1.2 Date: April 6, 2025 (https://www.niap-ccevs.org/api/file/get_public_file/?file_id=34773)

[REF5] Cisco Security Advisories
(https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&keyword=catalyst&sort=-day_sir#~Vulnerabilities)

9 ABREVIATURAS

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
CA	Certification Authority
CAPWAP	Control And Provisioning of Wireless Access Points
CC	Common Criteria
CLI	Command Line Interface
CPD	Centro de Proceso de Datos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNS	Domain Name System
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
LSC	Locally Significant Certificate
MAC	Media Access Control
MIC	Manufacturer Installed Certificate
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OVA	Open Virtual Appliance
PEM	Privacy Enhanced Mail
PES	Procedimiento de Empleo Seguro
PID	Product Identifier
PKI	Public Key Infrastructure

PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
RADsec	RADIUS over TLS
RSA	Rivest-Shamir-Adleman
SAN	Subject Alternative Name
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SSC	Self-Signed Certificate
SSH	Secure Shell
SVI	Switched Virtual Interface
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WLC	Wireless LAN Controller
WLAN	Wireless Local Area Network