Guía de Seguridad de las TIC
CCN-STIC 1023

Procedimiento de Empleo Seguro
Cisco Nexus 9000 Switch Series con modo ACI, APIC y software NX-OS-ACI



Noviembre 2026

Edita:

centro criptológico nacional

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 5
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 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
5.1 PRERREQUISITOS 10
5.2 INSTALACIÓN 10
5.2.1 CONFIGURACIÓN INICIAL DEL APIC 10
5.2.2 DESCUBRIMIENTO Y VALIDACIÓN DE LA TOPOLOGÍA DEL FABRIC 11
5.2.3 CONFIGURACIÓN INICIAL DE TENANTS 11
6 FASE DE CONFIGURACIÓN 12
6.1 MODO DE OPERACIÓN SEGURO 12
6.2 AUTENTICACIÓN 12
6.2.1 SERVIDORES DE AUTENTICACIÓN 13
6.3 ADMINISTRACIÓN DEL PRODUCTO 13
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 13
6.3.2 GESTIÓN IN-BAND DE LA ADMINISTRACIÓN 14
6.3.3 CONFIGURACIÓN DE ADMINISTRADORES (ROLES) 14
6.3.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 14
6.3.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 15
6.4 GESTIÓN DE CERTIFICADOS 15
6.5 SINCRONIZACIÓN 15
6.6 ACTUALIZACIONES 16
6.7 AUTO-CHEQUEOS 16
6.8 ALTA DISPONIBILIDAD 16
6.9 AUDITORÍA 17
6.9.1 REGISTRO DE EVENTOS 17
6.9.2 ALMACENAMIENTO LOCAL 17
6.9.3 ALMACENAMIENTO REMOTO 17
6.10 BACKUP 18
7 FUNCIONES DE SEGURIDAD 19
7.1 MODELO DE TENANTS, EPGS Y CONTRATOS 19
7.2 CONTROL DE FLUJO DE OPERACIÓN 19
7.3 OTRAS FUNCIONES DE FILTRADO 19
8 FASE DE OPERACIÓN 21
9 REFERENCIAS 22

10 ABREVIATURAS 23

ÍNDICE DE TABLAS

Tabla 1. Imágenes de software evaluadas 6
Tabla 2. Componentes del entorno de operación 8
Tabla 3. Modelos de hardware evaluados 9
Tabla 4. Servicios y puertos de administración 15

ÍNDICE DE FIGURAS

Figura 1: Diagrama del entorno de operación 8

1 INTRODUCCIÓN

Cisco Nexus 9000 Switch Series con modo ACI (Application Centric Infrastructure), APIC (Application Policy Infrastructure Controller) y software NX-OS-ACI conforman la solución de red definida por software (SDN) de Cisco para centros de datos. En la configuración evaluada, el producto opera en modo ACI.

El Cisco APIC actúa como controlador de gestión de seguridad centralizado y punto único de administración del fabric (el conjunto de switches y controladores interconectados bajo una gestión centralizada) ACI, proporcionando aplicación de políticas (tenants, EPGs y contratos), generación y monitorización de auditoría, y gestión de la configuración e imágenes del fabric. Es un appliance hardware con imagen software basada en Linux.

El APIC se despliega habitualmente en clúster, con un mínimo de tres controladores por motivos de escalabilidad y redundancia, aunque la configuración mínima soportada por el producto es de 1 nodo spine, 2 nodos leaf y 1 APIC. Cualquier controlador del clúster puede atender a cualquier usuario para cualquier operación.

El fabric ACI está compuesto por el APIC y los switches Cisco Nexus 9000 (modelos 9300, 9400 y 9500), configurados como nodos leaf o spine. El aprovisionamiento de los nodos se realiza de forma automática (zero-touch provisioning) mediante descubrimiento LLDP: cada APIC descubre en primer lugar el switch leaf al que está directamente conectado y, de forma escalonada, el resto de la topología (spines y leafs adicionales).

El administrador autorizado se conecta de forma segura a la CLI del APIC mediante SSHv2 y a la GUI web mediante HTTPS con TLS (v1.2 y v1.3). La API REST del APIC, aunque existe como interfaz programática interna empleada por la propia GUI y CLI, no es utilizada directamente por el administrador autorizado para gestionar el producto en la configuración evaluada.

El presente Procedimiento de Empleo Seguro (PES) desarrolla, para el producto Cisco Nexus 9000 Switch Series con modo ACI, APIC y NX-OS-ACI, las condiciones de entrega, instalación, configuración, operación y administración segura necesarias para su despliegue conforme al Esquema Nacional de Seguridad (ENS), categoría Alta. Este documento complementa la Taxonomía de productos STIC **Anexo D.11: Redes Definidas por Software (SDN) [REF1]** y la **guía del fabricante Common Criteria Administrator Guidance [REF2]**, sin sustituirlas.

Este PES incorpora, además, las correcciones de configuración por defecto identificadas durante la evaluación de seguridad del producto, necesarias para alcanzar la conformidad con el nivel ENS Alto. Estas correcciones, relativas a la versión de TLS, los algoritmos SSH y el tamaño de clave de los certificados, se detallan en el apartado 6.1 de este documento.

El producto protege sus activos (información y canales de administración, funcionalidad y datos de configuración/auditoría, actualizaciones del producto y flujos de tráfico cursados a través del fabric) frente a las amenazas de falta de responsabilidad sobre las acciones administrativas, tráfico malicioso, fallo de los mecanismos de seguridad, acceso no autorizado y reenvío indebido de datos de usuario. El correcto seguimiento de este PES es la medida principal para mitigar dichas amenazas en el entorno operacional.

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Cisco Nexus 9000 Switch Series con modo ACI, APIC y software NX-OS-ACI, en su versión evaluada: software Cisco NX-OS System Software-ACI 16.1(1f) para los switches del fabric y APIC 6.1(1f) para el controlador.

El alcance de este PES se corresponde con el alcance evaluado del producto (TOE): el clúster de controladores APIC junto con los switches Cisco Nexus 9000 en modo ACI (nodos leaf y spine) que conforman el fabric, incluyendo sus interfaces de administración local (consola serie) y remota (CLI mediante SSHv2 y GUI web mediante HTTPS).

Quedan fuera de alcance de este documento los componentes de red externos al fabric que forman parte del entorno operacional: el cortafuegos perimetral, los servidores de autenticación AAA externos (RADIUS/TACACS+, opcionales), el servidor PTP y el servidor syslog remoto (opcional). Dichos componentes deben ser desplegados y asegurados conforme a sus propios procedimientos de empleo seguro.

La API REST del APIC y el modo de operación NX-OS tradicional (sin ACI) quedan igualmente fuera del alcance de la evaluación de seguridad y, por tanto, de este PES, conforme a lo indicado en la **guía del fabricante [REF2]**.

El producto Cisco Nexus 9000 Switch Series con modo ACI, APIC y software NX-OS-ACI ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [**REF6**].

3 ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de los siguientes apartados:

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 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura conforme a ENS Alto.
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

Con el fin de garantizar que se recibe el producto correcto y que no ha sido manipulado durante la entrega, se deben realizar las siguientes comprobaciones, conforme a lo indicado en la **guía del fabricante [REF2]**:

a) Antes de desembalar el equipo, inspeccionar el embalaje físico y verificar que el cartón exterior está impreso con el logotipo y los motivos de Cisco Systems.

b) Verificar que el embalaje no ha sido abierto y vuelto a sellar, examinando la cinta de sellado del paquete.

c) Verificar que la caja presenta una etiqueta blanca con código de barras, resistente e indicadora de manipulación (tamper-resistant/tamper-evident), con el número de producto y de serie de Cisco.

d) Anotar el número de serie del equipo recogido en la documentación de envío y comprobar que coincide con el de la factura remitida por separado.

e) Verificar que la caja fue enviada efectivamente por el proveedor esperado (Cisco Systems o un distribuidor/partner autorizado), confirmando con dicho proveedor la empresa de mensajería y el número de albarán, por un canal distinto al de la propia entrega (teléfono, fax o sistema de seguimiento online).

f) Una vez desembalado el equipo, verificar que el número de serie del propio equipo coincide con el de la documentación de envío y la factura, y comprobar que el modelo recibido corresponde a alguno de los modelos de hardware evaluados (ver tabla del apartado 4.5).

g) Descargar la imagen de software evaluada exclusivamente desde `https://software.cisco.com`, y verificar que no ha sido manipulada comprobando su huella SHA512 frente a la publicada por Cisco, bien mediante una utilidad de hash externa, bien mediante el comando `show file <nombre_fichero> cksum` en el propio switch. Las imágenes evaluadas son las indicadas en la siguiente tabla; si el hash no coincide, no se debe instalar la imagen y se debe contactar con el Centro de Asistencia Técnica de Cisco (TAC).

Tabla 1. Imágenes de software evaluadas

Componente	Versión	Nombre de la imagen
Cisco Nexus 9000 Series ACI Mode Switch Software (64 bit)	16.1(1f)	aci-n9000-dk9.16.1.1f-cs_64.bin
Imagen APIC	6.1(1f)	aci-apic-dk9.6.1.1f.iso

h) Tras la instalación del hardware, seguir los requisitos previos de entorno (alimentación, refrigeración, espacio en rack) indicados en las guías de instalación de hardware del fabricante para cada modelo antes de proceder con la puesta en marcha.

4.2 ENTORNO DE INSTALACIÓN SEGURO

La **guía del fabricante [REF2]** define los siguientes objetivos de seguridad para el entorno operacional, que deben garantizarse antes de la puesta en producción del fabric:

- **OE.LOCATE:** los recursos de procesamiento del producto (controladores APIC y switches del fabric) deben ubicarse dentro de instalaciones de acceso controlado que impidan el acceso físico no autorizado.
- **OE.FIREWALL:** debe existir un cortafuegos en el entorno operacional, situado entre el fabric ACI y las redes externas, para proteger frente a tráfico malicioso o no autorizado.
- **OE.CONNECTION:** el entorno operacional debe proporcionar el soporte de red protegido necesario para evitar accesos no autorizados al producto.
- **OE.ADMIN:** los administradores autorizados deben estar formados y ser de confianza, y deben leer, comprender y seguir la guía del fabricante y este PES para instalar y operar el producto de forma segura.

Conforme a la configuración evaluada, el producto se administra mediante gestión in-band: se configura un EPG de gestión (mgmtInB) para que el tráfico de administración quede aislado del resto del tráfico de usuario mediante los mecanismos de tenants, EPGs y contratos descritos en el apartado 7, en lugar de emplear una red de gestión Out-of-Band física separada.

El acceso a las interfaces de administración (consola local, CLI SSHv2, GUI HTTPS) debe restringirse, mediante los mecanismos de control de acceso del entorno y del propio producto, a las estaciones de trabajo de los administradores autorizados.

4.3 REGISTRO Y LICENCIAS

El producto no requiere de un proceso de activación de licencias adicional para las funciones de seguridad evaluadas; el licenciamiento de Cisco ACI se gestiona conforme a los términos contractuales acordados con Cisco Systems, Inc.

Se debe conservar la documentación de licenciamiento y soporte contratada con el fabricante, ya que el acceso a actualizaciones de firmware y a los canales de soporte oficial (Cisco TAC) depende de disponer de un contrato de soporte en vigor.

4.4 CONSIDERACIONES PREVIAS

Antes de iniciar la instalación se debe verificar que el hardware adquirido es exactamente alguno de los modelos evaluados (ver tabla del apartado 4.5); el uso de hardware o software no evaluado invalida la configuración segura, conforme advierte expresamente la guía del fabricante [REF2].

Se debe definir previamente la topología del fabric (número de nodos spine, leaf y controladores APIC del clúster), el nombre del fabric, el identificador de POD, el rango del TEP pool de infraestructura y el identificador de VLAN de la red de infraestructura (Infra VLAN ID), ya que estos parámetros no pueden modificarse posteriormente sin reiniciar ("wipe") el fabric.

Se debe verificar que el identificador de VLAN de infraestructura elegido no se emplea en ningún otro punto de la red de la organización y que, si se emplea UCS en el entorno, no coincide con el rango reservado 3968-4047.

Se recomienda revisar, junto con el equipo de seguridad de la organización, la política de contraseñas, la política de retención de auditoría y el esquema de roles administrativos (RBAC) que se aplicará antes de iniciar la puesta en producción.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

A continuación, se muestra un diagrama del entorno de operación:

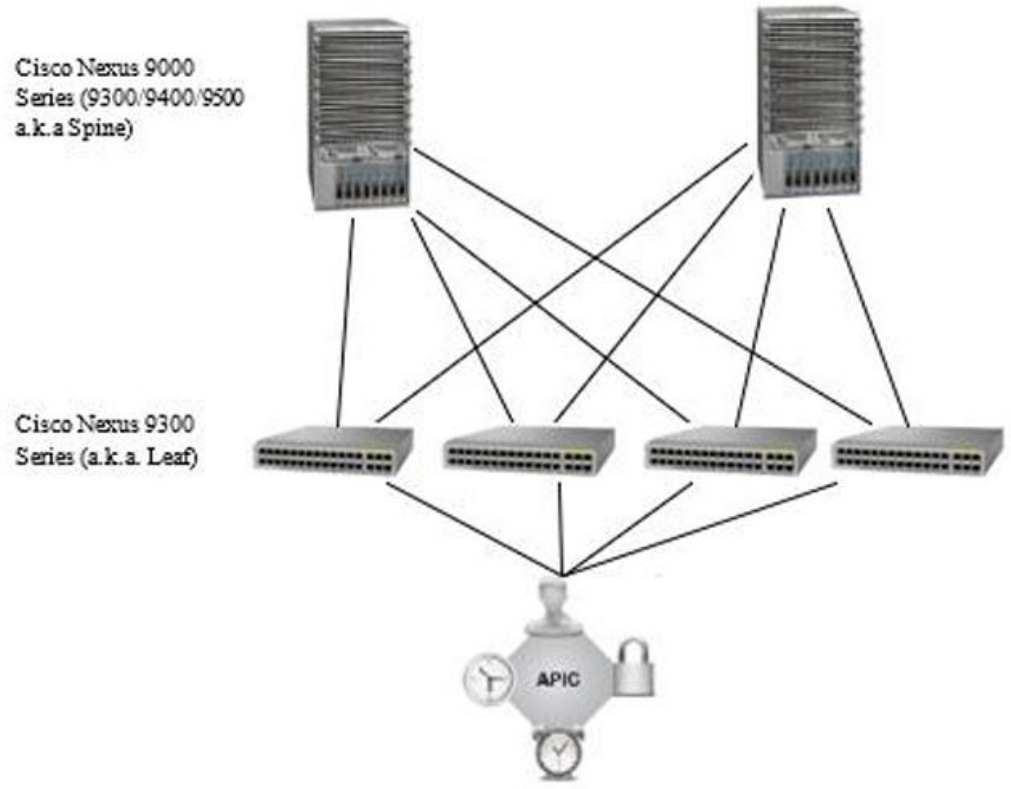


Figura 1: Diagrama del entorno de operación

Conforme a la Tabla 5 (Operational Environment Components) de la **guía del fabricante [REF2]**, el entorno de operación requiere los siguientes componentes:

Tabla 2. Componentes del entorno de operación

Componente	Requerido	Uso
Consola local	Sí	Consola de entorno TI conectada directamente al puerto serie del producto para su administración.
Cortafuegos	Sí	Situado entre el fabric ACI y la red externa.
Estación de gestión con cliente SSH	Sí	Empleada por el administrador para acceder a la CLI mediante SSHv2.

Componente	Requerido	Uso
Estación de gestión con navegador web	Sí	Empleada por el administrador para acceder a la GUI mediante HTTPS/TLS 1.2 o 1.3.
Servidor PTP	Sí	Sincronización horaria de todo el sitio; un switch spine (9400/9500) puede actuar como reloj maestro.
Servidor syslog	No	Recepción opcional de los mensajes syslog del producto.
Servidor RADIUS o TACACS+	No	Servidor AAA opcional del entorno operacional para autenticación de los administradores.

Adicionalmente, el fabric está compuesto por los siguientes elementos propios del producto:

a) APIC (Application Policy Infrastructure Controller): appliance hardware con imagen software basada en Linux, desplegado en clúster (mínimo 3 nodos recomendado).

b) Switches Cisco Nexus 9000 en modo ACI: switches leaf (modelos 9300) y spine (modelos 9400/9500) que conforman el fabric.

c) Módulos de línea, supervisores y módulos de fabric: componentes internos de los chassis modulares (9400/9500).

i) A continuación, se detallan los modelos de hardware y sus interfaces principales:

Tabla 3. Modelos de hardware evaluados

Modelo	Descripción	Interfaces
93108TC-FX	Switch fijo (leaf): 48 puertos 100M/1/10GBASE-T y 6 puertos QSFP28 40/100 Gbps; 4 núcleos CPU, 24 GB de memoria, 128 GB SSD.	1 RJ-45, 1 SFP+, 1 USB, 1 puerto serie RS-232
9504	Chassis modular (spine/leaf): 4 slots, hasta 4 tarjetas de línea, hasta 4 fuentes de alimentación, hasta 6 módulos de fabric, hasta 2 controladores de sistema y hasta 2 supervisores.	Según supervisor y módulos de E/S ACI instalados
Supervisor A/A+ (N9K-SUP-A/A+)	4 núcleos CPU, 16 GB de memoria, 64 GB SSD.	2 puertos USB, 1 puerto serie, 1 puerto Ethernet 10/100/1000 Mbps
N9K-X9736C-FX	Tarjeta de línea Ethernet 100 Gbps, 36 puertos.	36 puertos QSFP28
APIC-M4 / APIC-L4	Servidor APIC con CPU, disco y memoria de tamaño medio (hasta 1200 edge ports) o grande (más de 1200 edge ports).	2 puertos Ethernet 1/10 Gbps (LAN1/LAN2), 1 puerto de gestión Ethernet 1 Gbps, puerto serie RJ-45, 2 puertos USB 3.0

5 FASE DE INSTALACIÓN

En este apartado se describe cómo llevar a cabo la instalación segura de Cisco Nexus 9000 Switch Series con modo ACI, APIC y NX-OS-ACI, conforme al procedimiento descrito en la sección 3 de la **guía del fabricante [REF2]**.

5.1 PRERREQUISITOS

Verificar que la topología física (cableado entre nodos leaf y spine, y conexión del/los servidor(es) APIC a los switches leaf/9300 o 9400) respeta las reglas de conexión soportadas por el fabric, y que todos los switches están físicamente conectados y encendidos en la configuración deseada antes de iniciar el registro de switches.

Tener preparada la imagen de software evaluada y verificada conforme al apartado 4.1.

Disponer de una consola y teclado conectados directamente al APIC para la configuración inicial.

El controlador APIC se entrega con una contraseña de BIOS por defecto ("password"); se debe cambiar esta contraseña por defecto durante el proceso de arranque inicial, siguiendo el procedimiento "Changing the BIOS Default Password" de la **guía del fabricante** [**REF2**].

Tener decidida la política de contraseñas fuertes (ver apartado 6.2) que se aplicará durante la configuración inicial del usuario administrador.

5.2 INSTALACIÓN

5.2.1 CONFIGURACIÓN INICIAL DEL APIC

Al arrancar por primera vez, la consola del APIC presenta un diálogo de configuración inicial. Los parámetros principales que se deben proporcionar son:

a) **Fabric Name:** nombre único del fabric, especialmente si existen varios fabrics ACI en la organización.

b) **Number of Controllers:** número de controladores APIC del clúster; se recomienda un mínimo de 3 para redundancia.

c) **Controller ID:** cada APIC debe configurarse en orden correlativo, empezando por el ID 1, durante el primer arranque.

d) **Controller Name:** nombre identificativo del controlador (por ejemplo, APIC_1).

e) **TEP Address Pool:** rango de direcciones para los Tunnel End Points (TEP), empleado para el tráfico VXLAN entre switches leaf y spine.

f) **VLAN ID for Infra Network:** identificador de VLAN para la red de infraestructura entre leaf y spine (por ejemplo, 3967); no debe coincidir con el rango reservado 3968-4047 si se emplea Cisco UCS en el entorno.

g) **Authorized Administrator User Configuration:** se debe responder "Y" (Sí) para habilitar la comprobación de contraseñas fuertes, conforme a la política descrita en el apartado 6.2.

A continuación, se muestra un extracto orientativo del diálogo de configuración inicial en consola:

```
Enter the fabric name [ACI Fabric1]:
Enter the fabric ID (1-128) [1]:
Enter the number of active controllers in the fabric (1-9) [3]:
Enter the POD ID (1-9) [1]:
Enter the controller ID (1-3) [1]:
Enter the controller name [apic1]:
Enter address pool for TEP addresses [10.0.0.0/16]:
Enter the VLAN ID for infra network (2-4094): 3967
Enter address pool for BD multicast addresses (GIPO)
[225.0.0.0/15]:
Enable strong passwords? [Y]:
Enter the password for admin:
Re-enter the password for admin:
```

Nota: los valores de TEP address pool, Infra VLAN ID y multicast address pool no pueden modificarse posteriormente sin reiniciar por completo ("wipe") el fabric; deben revisarse cuidadosamente antes de confirmar la configuración.

5.2.2 DESCUBRIMIENTO Y VALIDACIÓN DE LA TOPOLOGÍA DEL FABRIC

Cada APIC del clúster descubre en primer lugar el switch leaf al que está directamente conectado; a partir de ahí, descubre de forma escalonada los spines y el resto de leafs del fabric (descubrimiento en cascada). El administrador autorizado debe, no obstante, registrar/autorizar explícitamente cada switch en el APIC.

Para validar los nodos registrados mediante la GUI: acceder a `Fabric > Inventory > Fabric Membership` y consultar la pestaña *Registered Nodes*, donde se muestran los switches registrados junto con su ID de nodo y la dirección IP asignada.

Para validar la topología del fabric mediante la GUI: acceder a `Fabric > Inventory > Pod n` y consultar la pestaña *Topology*, donde se muestra un diagrama con todos los switches, instancias APIC y enlaces detectados. Se puede pasar el cursor sobre cada elemento para ver su estado de salud, y hacer doble clic para ver la conectividad a nivel de puerto.

5.2.3 CONFIGURACIÓN INICIAL DE TENANTS

Una vez configurados los nodos del fabric, el administrador autorizado emplea la pestaña Tenants de la GUI para la gestión de tenants. Un tenant es un contenedor lógico de políticas de aplicación que representa una unidad de aislamiento (organización, unidad de negocio o dominio), sin representar necesariamente una red privada. El fabric incluye por defecto el tenant "common" (políticas compartidas por todos los tenants), el tenant "infra" (preconfigurado para la infraestructura del fabric) y el tenant "mgmt" (preconfigurado para la conectividad in-band y out-of-band de los nodos del fabric).

Dentro de cada tenant se configuran, según proceda: contextos o redes privadas (VRF), dominios de difusión de nivel 2 (Bridge Domain), perfiles de aplicación (Application Profile) y grupos de endpoints (EPG), conforme al modelo descrito en el apartado 7 de este documento.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

La configuración por defecto del APIC **no cumple** con el nivel ENS Alto en tres aspectos. Es obligatorio aplicar las siguientes correcciones antes de poner el producto en explotación:

a) TLS 1.3 deshabilitado por defecto y presencia de cipher suites TLS 1.2 no conformes con ENS Alto. Corrección: acceder a `Fabric > Fabric Policies > Policies > Pod > Management Access > default > Web access` y activar TLS 1.3, deshabilitando las cipher suites no conformes.

b) Algoritmos SSH no conformes habilitados por defecto. Corrección: acceder a `Fabric > Fabric Policies > Policies > Pod > Management Access > default > Console Access` y seleccionar únicamente los cifrados SSH permitidos: AES-CTR-128, AES-CTR-256 y CHACHA20-POLY1305, conforme a la **guía CCN-STIC-807 [REF3]**.

c) Certificados por defecto con clave RSA de 2048 bits, no conforme con ENS Alto. Corrección: acceder a `Admin > AAA > Security` y crear un nuevo key ring con módulo RSA de 3072 o 4096 bits (o, alternativamente, un certificado ECDSA), aplicando dicho key ring a la interfaz de gestión web.

Una vez aplicadas, el producto emplea los conjuntos de cifrados conformes con ENS Alto.

Los certificados empleados deben ser de tipo RSA (3072 o 4096 bits) o ECDSA.

Adicionalmente, conforme a la funcionalidad excluida de la **configuración evaluada [REF2]**, Telnet y SNMP deben permanecer deshabilitados: Telnet transmite las credenciales en texto claro (deshabilitado por defecto, no debe reactivarse) y SNMP podría permitir a un tercero no autorizado acceder al dispositivo de red. Ambos servicios están recogidos como funcionalidad excluida en la **guía del fabricante** [**REF2**], Tabla 6 "Excluded Functionality".

6.2 AUTENTICACIÓN

Todos los administradores autorizados deben ser identificados y autenticados antes de acceder al APIC, tanto por CLI (SSHv2) como por GUI web (HTTPS/TLS). Cada administrador debe disponer de un nombre de usuario y contraseña únicos.

Se debe habilitar el bloqueo de cuenta tras un número configurado de intentos fallidos de inicio de sesión, accediendo a `Admin > AAA > Security > Default Settings` y activando la opción *"Lockout User after multiple login attempts"*.

Se debe configurar el cierre de sesión por inactividad, en el mismo apartado `Admin > AAA > Security > Default Settings`, mediante el parámetro *"Web/Console(SSH/Telnet) Session Idle Timeout (s)"*, con un valor entre 60 y 65525 segundos. Se recomienda emplear el menor valor operativamente viable.

Por defecto, el producto comprueba la fortaleza de las contraseñas, impidiendo elegir contraseñas débiles. La contraseña debe tener al menos 12 caracteres e incluir caracteres alfabéticos en mayúsculas y minúsculas, y caracteres numéricos conforme al nivel ENS Alto; puede incluir caracteres especiales del teclado estadounidense, con la excepción de que no puede comenzar por comillas (" o '), barras verticales (|) ni el símbolo mayor que (>). Se

recomienda además evitar secuencias de caracteres consecutivos o repetidos, palabras de diccionario y nombres propios.

Las contraseñas de los administradores no se almacenan en claro; el producto únicamente conserva el hash de la contraseña, cifrado mediante AES-256 a partir de una passphrase de 16 a 32 caracteres que no puede ser recuperada ni leída por ningún usuario ni administrador.

Además de la autenticación local (empleada por defecto), el producto admite servidores de autenticación externos RADIUS y TACACS+, que deben desplegarse en la red interna (de confianza) del entorno operacional.

Se debe configurar un banner de aviso que se muestre antes de la solicitud de usuario y contraseña, tanto en CLI como en GUI, accediendo a `System > System Settings > System Alias and Banners` y completando los campos *Controller CLI Banner*, *Switch CLI Banner* y, si se desea un banner en la GUI, marcando *"Show Prelogin Banner"* e indicando la URL del contenido a mostrar.

6.2.1 SERVIDORES DE AUTENTICACIÓN

Cuando se empleen servidores RADIUS o TACACS+ externos (componente opcional del entorno operacional), su configuración se realiza conforme a la **guía del fabricante [REF2]**. Dichos servidores deben ubicarse en la red interna de confianza.

Se recomienda emplear los servidores de autenticación externos como mecanismo centralizado de gestión de identidades de los administradores, reservando las cuentas locales del APIC para escenarios de contingencia.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El producto dispone de las siguientes interfaces de administración:

a) Consola local: acceso directo mediante el puerto serie del APIC o del switch.

b) CLI remota: acceso mediante SSHv2, habilitado y configurado por defecto durante la configuración inicial. El servidor Telnet permanece deshabilitado por defecto y no debe reactivarse.

c) GUI web: acceso remoto mediante navegador, empleando HTTPS con TLS 1.2 o 1.3 (una vez aplicada la corrección del apartado 6.1). El producto soporta, como mínimo, Chrome 59, Firefox 54 e Internet Explorer 11. El acceso se realiza mediante la URL https://<dirección_IP_de_gestión>; HTTPS está habilitado por defecto y la redirección HTTP a HTTPS está deshabilitada por defecto.

Para configurar SSHv2 en el puerto de gestión del APIC se pueden emplear comandos como los siguientes:

```
apic1# configure
apic1(config)# switch 101
apic1(config-switch)# interface inband-mgmt0
apic1(config-switch-if)# ip address 10.13.1.1/24 gateway
10.13.1.254
```

```
apic1(config-switch-if)# exit
apic1(config-switch)# exit
```

La API REST del APIC, aunque protegida mediante HTTPS/TLS, no se emplea directamente por el administrador autorizado para gestionar el producto en la configuración evaluada; es utilizada internamente por la propia GUI y CLI.

6.3.2 GESTIÓN IN-BAND DE LA ADMINISTRACIÓN

En la configuración evaluada, el APIC se administra mediante gestión in-band (no out-of-band). Se debe configurar un grupo de endpoints de gestión in-band (mgmtInB) dentro del tenant "mgmt", de forma que únicamente se permita el acceso de gestión in-band dentro del fabric, separado del tráfico de datos de usuario mediante un contrato (vzBrCP) específico. Como buena práctica adicional, se recomienda emplear una red o VLAN de gestión dedicada, independiente de la política concreta de gestión in-band aquí descrita.

A título de ejemplo, la asignación de una VLAN para la gestión in-band del APIC mediante CLI incluye la creación de un dominio VLAN de gestión in-band y su asociación a los puertos de leaf correspondientes:

```
apic1(config)# vlan-domain inband-mgmt
apic1(config-vlan)# vlan 10
apic1(config-vlan)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# exit
```

Esta configuración debe realizarse antes de asignar las direcciones estáticas de APIC, leafs y spines, para garantizar que las políticas de flujo de tráfico se aplican correctamente desde el primer momento.

6.3.3 CONFIGURACIÓN DE ADMINISTRADORES (ROLES)

El producto mantiene un rol de Administrador Autorizado (Authorized Administrator) para administrar el producto local y remotamente. Durante la instalación se crea el usuario administrador inicial con todos los permisos necesarios; pueden crearse administradores autorizados adicionales, cada uno con nombre de usuario y contraseña propios.

El producto permite crear roles administrativos adicionales basados en control de acceso por roles (RBAC), como por ejemplo el rol "Tenant-admin", cuyo acceso queda restringido al tenant al que está asociado. La creación de roles adicionales no afecta al flujo de tráfico; únicamente distribuye las funciones de administración entre varios administradores en lugar de uno solo. La descripción completa de los roles disponibles se encuentra en el apartado "User Roles" de la **guía del fabricante** [**REF2**], que remite al procedimiento "Role-Based Access Control".

Se debe gestionar a los usuarios administradores conforme al principio de mínimo privilegio, concediendo acceso únicamente a los usuarios necesarios en cada momento y revisando periódicamente los permisos asignados y las cuentas inactivas.

6.3.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Se debe restringir el acceso a las interfaces de gestión (consola, CLI, GUI) a los rangos de direcciones IP de las estaciones de trabajo de gestión autorizadas, mediante contratos aplicados

al EPG de gestión in-band, a nivel de fabric; adicionalmente, se recomienda restringir dicho acceso también a nivel del cortafuegos perimetral del entorno operacional.

Se deben mantener deshabilitados los servicios de gestión no empleados en la configuración evaluada: Telnet y SNMP, por tratarse de servicios inseguros no permitidos en el nivel ENS Alto, conforme a la funcionalidad excluida indicada en el apartado 6.1.

Los servicios y puertos de administración habitualmente empleados son los siguientes:

Tabla 4. Servicios y puertos de administración

Servicio	Puerto / Protocolo	Uso
GUI web	TCP/443 (HTTPS)	Administración remota mediante navegador
CLI	TCP/22 (SSHv2)	Administración remota por línea de comandos
Syslog remoto	Según configuración (recomendado sobre VRF de gestión)	Envío opcional de eventos y registros de auditoría
PTP	Protocolo PTP (IEEE 1588)	Sincronización horaria de todo el fabric
RADIUS / TACACS+	Según configuración del servidor AAA	Autenticación y autorización de administradores externos (opcional)

6.3.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

Todas las comunicaciones administrativas deben emplear HTTPS con TLS 1.2 o TLS 1.3 (GUI) o SSHv2 (CLI), conforme a lo descrito en el apartado 6.1. Los conjuntos de cifrado permitidos deben restringirse a los indicados en dicho apartado y en la **guía CCN-STIC-807 [REF3].**

Las comunicaciones hacia el servidor syslog remoto, en caso de emplearse, deben protegerse mediante la instancia de enrutamiento y reenvío virtual (VRF) de gestión, que proporciona una transmisión protegida. La configuración concreta se describe en el apartado "Secure Installation and Configuration" de la **guía del fabricante** [**REF2**].

6.4 GESTIÓN DE CERTIFICADOS

Se debe crear un key ring propio con certificado RSA de 3072 o 4096 bits (o ECDSA) desde `Admin > AAA > Security`, sustituyendo el certificado por defecto (RSA-2048) empleado por la interfaz de gestión web, conforme a lo indicado en el apartado 6.1.

Se recomienda sustituir el certificado autofirmado por un certificado emitido por una autoridad de certificación (CA) reconocida por la organización, y planificar su renovación periódica antes de la fecha de caducidad.

6.5 SINCRONIZACIÓN

En la configuración evaluada, la sincronización horaria del fabric se realiza mediante el protocolo PTP (Precision Time Protocol, IEEE 1588), y no mediante NTP. Los relojes se organizan en una jerarquía maestro-miembro; durante la configuración de PTP no se identifica un reloj maestro externo, sino que uno de los switches spine (9400/9500) se elige automáticamente como reloj

maestro (grandmaster), al que se sincroniza el resto del fabric. La configuración de PTP se describe en el apartado "Clock Management" de la **guía del fabricante** [**REF2**].

Para habilitar PTP mediante la GUI: acceder a `System > System Settings > PTP and Latency Measurement` y seleccionar *Enabled*.

Para establecer la hora local puede emplearse el comando `clock set <HH:MM:SS> <día> <mes>` en la CLI. La correcta sincronización horaria es imprescindible para la correlación y el sellado temporal de los registros de auditoría.

6.6 ACTUALIZACIONES

Las actualizaciones de firmware del APIC y de los switches del fabric deben obtenerse exclusivamente desde https://software.cisco.com, verificando su huella SHA512 antes de su instalación, del mismo modo que se describe en el apartado 4.1 para la entrega segura del producto.

Se recomienda establecer un procedimiento periódico de revisión y aplicación de actualizaciones de seguridad publicadas por el fabricante, priorizando aquellas que corrijan vulnerabilidades de severidad alta o crítica, y validar la actualización en preproducción cuando sea posible antes de aplicarla en el fabric de producción.

6.7 AUTO-CHEQUEOS

Durante el arranque inicial y en cada reinicio, el producto ejecuta una batería de auto-chequeos (self-tests) para verificar su correcto funcionamiento. Todos los puertos permanecen bloqueados, sin reenviar tráfico, mientras se ejecutan estos chequeos; el sistema únicamente pasa a estado operativo, habilitando el reenvío de tráfico, cuando todos los componentes de todos los chequeos superan la prueba.

El producto emplea un test de respuesta conocida (Known-Answer Test, KAT) para cada función criptográfica aprobada (cifrado, descifrado, autenticación y generación de números aleatorios), comparando el resultado obtenido con un resultado de referencia previamente conocido.

Además de los auto-chequeos de arranque, el producto ejecuta chequeos condicionales cada vez que se invoca la función asociada: un test de consistencia de pares (pair-wise consistency test) al generar un par de claves pública/privada, y un test continuo del generador de números aleatorios (continuous random number generator test) cada vez que se genera un número aleatorio.

Si alguno de los auto-chequeos falla, el producto transita a un estado de error, deteniendo toda transmisión de datos y mostrando información de estado indicando el fallo; en dicho estado se eliminan las claves criptográficas. Ante un fallo persistente, se debe generar un volcado de núcleo (mediante el comando "system cores") y contactar con el Centro de Asistencia Técnica de Cisco (TAC).

6.8 ALTA DISPONIBILIDAD

El APIC se debe desplegar en clúster, con un mínimo recomendado de tres controladores, para garantizar la disponibilidad y redundancia de la gestión del fabric. Cada APIC mantiene un vector de dispositivos (Appliance Vector, AV) que asocia cada identificador de APIC con su dirección IP y su identificador único (UUID); este vector se descubre y propaga mediante LLDP mientras cada switch reinicia, hasta que todos los switches y controladores APIC comparten el mismo AV.

El producto ofrece un modo de mantenimiento denominado *Graceful Insertion and Removal (GIR)*, que permite aislar un switch de la red con mínima interrupción del servicio para realizar tareas de depuración en tiempo real. Durante la retirada elegante (graceful removal), todos los protocolos externos se detienen de forma ordenada excepto el protocolo de fabric (IS-IS), y el switch deja de atraer tráfico de los spines; al finalizar la depuración, se debe recomisionar el switch para devolverlo al modo normal de operación.

El producto permite revertir una configuración a un estado anterior conocido como correcto mediante la función *"Atomic Replace"*: si el modo de importación se configura como `atomic` y el tipo de importación como `replace`, la configuración importada sobrescribe la configuración existente, eliminando cualquier elemento no presente en el fichero importado.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

El producto genera y registra mensajes de sistema en la consola y en fichero de log por defecto. Los parámetros de registro por defecto son: registro en consola habilitado a nivel de severidad 2, registro en monitor habilitado a nivel 5, registro en fichero habilitado a nivel 5, registro de módulo habilitado a nivel 5, y registro en servidor syslog remoto deshabilitado.

Cada evento se almacena en uno de tres registros (logs) según su naturaleza: el registro de auditoría (audit log), que contiene eventos iniciados por el usuario como inicios/cierres de sesión o cambios de configuración; el registro de estado de salud (health score log); y el registro de eventos (event log), con eventos generados por el propio sistema como transiciones de estado de enlaces.

Se debe configurar la política de retención de registros estableciendo el tamaño máximo (Maximum Size), con un rango permitido de 1.000 a 500.000 registros (valor por defecto: 100.000), y la ventana de purga (Purge Window Size), con un rango de 100 a 1.000 registros por lote (valor por defecto: 250), sabiendo que la purga se ejecuta periódicamente cada 30 segundos.

6.9.2 ALMACENAMIENTO LOCAL

Los registros se almacenan localmente en un fichero circular que se sobrescribe (purga) al alcanzar su capacidad máxima. Para consultar los registros mediante la GUI: acceder a `Admin > AAA > Authentication`, pestaña *History*, y dentro de ella las subpestañas *Event Records* (registro de eventos) y *Audit Logs* (registro de auditoría); se puede pulsar sobre cualquier entrada para ver el detalle del evento.

El producto permite al administrador autorizado eliminar los registros de auditoría almacenados (no existe interfaz para modificarlos), mediante el comando `clear logging` (y, para el buffer NVRAM, `clear logging nvram`). Esta acción debe reservarse a tareas de mantenimiento autorizadas y quedar debidamente justificada.

6.9.3 ALMACENAMIENTO REMOTO

Se recomienda configurar el envío de mensajes de log a un servidor syslog remoto ubicado en la red interna de confianza (componente opcional del entorno operacional), empleando preferiblemente la instancia de enrutamiento y reenvío virtual (VRF) de gestión, que proporciona una transmisión protegida (no se ha verificado en la evaluación el uso de TLS para

esta comunicación). Ver el procedimiento "Configuring Syslog Servers" de LA **guía del fabricante** [**REF2**].

Se debe verificar que el servidor remoto recibe correctamente los registros tras completar la configuración, y de forma periódica durante la fase de operación.

6.10 BACKUP

Se recomienda establecer una política de copia de seguridad periódica de la configuración del fabric, almacenando las copias en una ubicación segura y protegida, distinta del propio clúster APIC, conforme a la política de continuidad de la organización. La guía del fabricante no detalla un procedimiento específico de backup más allá de la exportación/importación de configuración empleada por la función Atomic Replace; se recomienda consultar la documentación de administración del fabricante para el procedimiento de copia de seguridad completo vigente en la versión desplegada.

Antes de aplicar cambios significativos de configuración (actualizaciones de firmware, cambios masivos de políticas), se recomienda generar una copia de seguridad puntual adicional que permita una restauración rápida en caso de ser necesario.

7 FUNCIONES DE SEGURIDAD

Además de la configuración administrativa descrita en los apartados anteriores, el producto ofrece un conjunto de funciones de seguridad de red que deben configurarse conforme a la política de tráfico de la organización:

7.1 MODELO DE TENANTS, EPGS Y CONTRATOS

Existen los siguientes modelos de tenants, EPGs y contratos:

a) Tenant (fvTenant): contenedor lógico de políticas de aplicación que permite al administrador ejercer el control de flujo basado en dominios; representa una unidad de aislamiento a nivel de política, no una red privada.

b) Grupo de endpoints (EPG): objeto lógico con nombre que agrupa endpoints con requisitos de política comunes (seguridad, movilidad de máquina virtual, QoS, servicios de nivel 4 a 7). El fabric distingue, entre otros, EPGs de aplicación (fvAEPg), EPGs de red externa de nivel 2 (l2extInstP) y de nivel 3 (l3extInstP), y EPGs de gestión out-of-band (mgmtOoB) o in-band (mgmtInB).

c) Contratos (vzBrCP): las EPGs solo pueden comunicarse entre sí conforme a las reglas definidas en un contrato, que especifica los protocolos y puertos permitidos. Si no existe contrato, la comunicación entre EPGs distintas está deshabilitada por defecto (modelo de lista blanca); la comunicación dentro de una misma EPG está siempre implícitamente permitida.

7.2 CONTROL DE FLUJO DE OPERACIÓN

El producto permite denegar el flujo de información tanto para tráfico IP como no IP: para tráfico IP (broadcast, multicast desconocido o unicast desconocido de nivel 2), el tráfico se deniega salvo que esté identificado como de confianza mediante una combinación EPG-a-EPG en lista blanca; si los atributos de seguridad no coinciden con un contrato administrado (RACL o VACL), o si el tráfico no se asocia a un VRF configurado, el flujo se deniega.

Para tráfico no IP, si los atributos de seguridad no coinciden con un contrato administrado (RACL, PACL o VACL) mediante lista blanca EPG-a-EPG, el flujo se deniega. El control se aplica tanto a tráfico IPv4 como IPv6.

El producto aplica valores por defecto restrictivos: los flujos de tráfico solo se permiten una vez que las políticas de control de flujo de información han sido configuradas y aplicadas explícitamente por el administrador autorizado. Ver el apartado “Information Flow Policies” de la **guía del fabricante** [**REF2**].

El producto soporta la aplicación de políticas en el primer punto de contacto del endpoint con la red, lo que facilita un enfoque de micro-segmentación (Zero Trust), pudiendo reservar recursos físicos dedicados en exclusiva a un EPG.

7.3 OTRAS FUNCIONES DE FILTRADO

Limitación de ancho de banda por puerto lógico mediante políticas de plano de datos (Data Plane Policing, DPP), aplicadas a nivel de EPG en cada switch leaf donde dicho EPG está desplegado.

Filtrado por defecto de BPDU en los puertos de acceso de los switches, mediante el comando "bpdu-filter".

Filtrado de tráfico DHCP (cliente y servidor) y de mensajes ICMPv6 Router Advertisement (tipo 134) mediante las funcionalidades First-Hop Security (FHS).

Filtrado del tráfico de control dirigido a la CPU mediante Control Plane Policing (CoPP), configurado como lista de permisos (whitelist).

Se recomienda definir la política de tenants, EPGs y contratos junto con el equipo responsable de la arquitectura de red de la organización, documentando los flujos de tráfico permitidos antes de desplegar el fabric en producción.

8 FASE DE OPERACIÓN

Durante la fase de operación se recomienda llevar a cabo, de forma periódica, las siguientes tareas:

a) Revisar los registros de auditoría y de eventos del producto (Admin > AAA > Authentication > History), prestando especial atención a los intentos de acceso fallidos y a los bloqueos de cuenta.

b) Comprobar el estado de las alarmas (faults) del fabric y corregir cualquier comportamiento anómalo detectado, incluyendo intentos de conexión de switches no autorizados.

c) Revisar los permisos de los administradores conforme al principio de mínimo privilegio, deshabilitando cuentas inactivas y validando que la asignación de roles (RBAC) sigue siendo adecuada.

d) Verificar la correcta llegada de los registros al servidor syslog remoto, en caso de estar configurado.

e) Comprobar la disponibilidad de nuevas actualizaciones de firmware publicadas por Cisco y planificar su aplicación, verificando siempre la huella SHA512 antes de instalarlas.

f) Verificar que la política de copias de seguridad se ejecuta correctamente y que las copias se conservan en un lugar seguro.

g) Revisar el estado del clúster APIC (disponibilidad de todos los controladores, coherencia del Appliance Vector) y el estado de la sincronización PTP, incluyendo qué spine actúa como reloj maestro.

h) Revisar periódicamente la vigencia de los certificados configurados y planificar su renovación antes de la caducidad.

i) Revisar los tenants, EPGs y contratos configurados, comprobando que siguen respondiendo a los flujos de tráfico de negocio autorizados y retirando aquellos que hayan quedado obsoletos.

j) Comprobar que ningún administrador ha dejado un switch en modo de mantenimiento (GIR) de forma prolongada sin justificación operativa.

k) Verificar que los servicios excluidos de la configuración evaluada (Telnet, SNMP) permanecen deshabilitados tras cualquier cambio de configuración o actualización de firmware.

9 REFERENCIAS

REF1 Taxonomía de productos STIC Anexo D.11: Redes Definidas por Software (SDN). CCN-STIC-140. Abril 2026.
https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6014-guia-140-anexo-d11-rfs-sdn/file.html

REF2 Cisco Nexus 9000 Switch Series with ACI mode, APIC and NX-OS software-ACI. Common Criteria Administrator Guidance. Versión 1.0. Abril, 2025
https://www.cisco.com/c/dam/en_us/solutions/industries/government/security_certification/pdfs/nexus-9000-switch-aci-mode-apic-agd.pdf

REF3 CCN-STIC-807. Criptología de empleo en el Esquema Nacional de Seguridad. Mayo 2022.
https://www.ccn-cert.cni.es/ca/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

REF4 CCN-STIC-2001. Definición de la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.
https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/2000-organismo-de-certificacion/4549-ccn-stic-2001-definicion-de-la-certificacion-nacional-esencial-de-seguridad-lince/file.html

REF5 CCN-STIC-2002. Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.
https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/2000-organismo-de-certificacion/4557-ccn-stic-2002-metodologia-de-evaluacion-para-la-certificacion-nacional-esencial-de-seguridad-lince/file.html

REF6 CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

10 ABREVIATURAS

ACI	Application Centric Infrastructure
AES	Advanced Encryption Standard
APIC	Application Policy Infrastructure Controller
AV	Appliance Vector
BPDU	Bridge Protocol Data Unit
CCN	Centro Criptológico Nacional
CLI	Command Line Interface
CoPP	Control Plane Policing
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
DPP	Data Plane Policing
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
EPG	End-Point Group
FHS	First-Hop Security
FIPS	Federal Information Processing Standards
GIR	Graceful Insertion and Removal
GUI	Graphical User Interface
HTTPS	Secure Hyper Text Transfer Protocol
KAT	Known-Answer Test
LLDP	Link Layer Discovery Protocol
MO	Managed Object
NX-OS	Cisco Nexus Operating System
PES	Procedimiento de Empleo Seguro
PTP	Precision Time Protocol
RACL	Router Access Control List
RADIUS	Remote Authentication Dial-In User Service
RBAC	Control de Acceso Basado en Roles
RSA	Rivest-Shamir-Adleman
SDN	Software-Defined Networking
SSH	Secure Shell
TAC	Technical Assistance Center

TACACS+	Terminal Access Controller Access-Control System Plus
TEP	Tunnel Endpoint
TLS	Transport Layer Security
TOE	Target of Evaluation
UUID	Universally Unique Identifier
VACL	VLAN Access Control List
VRF	Virtual Routing and Forwarding
VXLAN	Virtual Extensible LAN