Guía de Seguridad de las TIC
CCN-STIC 1015

Procedimiento de Empleo Seguro
Cisco Routers IOS-XR 7.11



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 3
2 OBJETO Y ALCANCE 3
2.1 SOFTWARE 3
3 ORGANIZACIÓN DEL DOCUMENTO 4
4 FASE PREVIA A LA INSTALACIÓN 5
4.1 ENTREGA SEGURA DEL PRODUCTO 5
4.2 ENTORNO DE INSTALACIÓN SEGURO 5
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 7
5 FASE DE INSTALACIÓN 8
5.1 MANEJO DE LOS COMANDOS DE CISCO 8
6 FASE DE CONFIGURACIÓN 9
6.1 MODO DE OPERACIÓN SEGURO 9
6.1.1 HABILITACIÓN DEL MODO DE OPERACIÓN SEGURO (FIPS) 9
6.2 AUTENTICACIÓN 9
6.3 ADMINISTRACIÓN DEL PRODUCTO 10
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 10
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 12
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 12
6.5 GESTIÓN DE CERTIFICADOS 13
6.6 SERVIDORES DE AUTENTICACIÓN 13
6.7 SINCRONIZACIÓN 13
6.8 ACTUALIZACIONES 14
6.9 AUTO-CHEQUEOS 14
6.10 ALTA DISPONIBILIDAD 14
6.11 AUDITORÍA 14
6.11.1 REGISTRO DE EVENTOS 14
6.11.2 ALMACENAMIENTO LOCAL 14
6.11.3 ALMACENAMIENTO REMOTO 15
6.12 BACKUP 15
7 FASE DE OPERACIÓN 16
8 REFERENCIAS 17
9 ABREVIATURAS 19

ÍNDICE DE TABLAS

Tabla 1: Componentes Entorno de Operación 7
Tabla 2: Modo de comandos 8

ÍNDICE DE FIGURAS

Figura 1: Versiones de Software 3
Figura 2: Verificación del hash 5

1 INTRODUCCIÓN

Los routers Cisco que corren el software IOS-XR 7.11 están diseñados para operar como equipos de *routing* seguro. Por tanto, permiten la interconexión de redes mediante la gestión de tráfico entre distintos segmentos de red y la aplicación de políticas de encaminamiento y control.

El sistema soporta múltiples mecanismos de comunicación definidos en la pila de red, incluyendo protocolos de transporte y servicios asociados, así como funcionalidades criptográficas para proteger las comunicaciones.

Los distintos componentes hardware y software trabajan conjuntamente para establecer canales seguros para la administración, protección del tráfico y operación continua del dispositivo.

La plataforma puede interactuar con componentes externos de administración y operación, incluyendo estaciones de gestión remota mediante SSHv2, consola local, servidores de auditoría (syslog), autoridades de certificación y dispositivos pares MACsec.

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación segura de los routers Cisco ejecutando Cisco IOS-XR 7.11.

El producto **Cisco Aggregation Services Router 9000 (ASR9K) IOS-XR 7.11** 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]. **Se debe consultar el Catálogo para determinar la versión y modelos cualificados en cada momento.**

2.1 SOFTWARE

El router lleva un Software Cisco IOS-XR cuya versión tiene la siguiente nomenclatura:

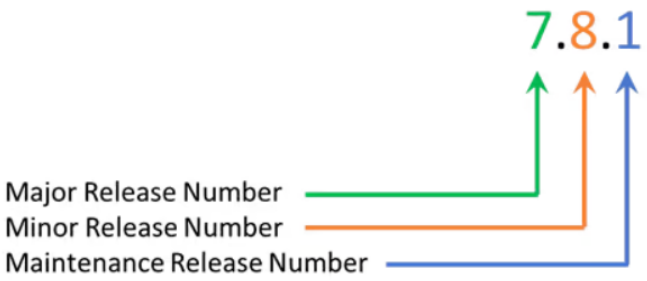


Figura 1: Versiones de Software

Más información sobre la estrategia de versionado de IOS-XR se encuentra en la guía de Cisco: IOS-XR [

REF2

].

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

La entrega al cliente debe garantizar tanto la integridad física del equipamiento como la autenticidad del software instalado, de forma que se prevenga cualquier manipulación durante la cadena de suministro.

Durante la recepción del producto, se recomienda verificar el estado físico del embalaje, asegurando que no existan daños visibles, aperturas no autorizadas o alteraciones en los sellos y elementos de protección suministrados por el fabricante.

Asimismo, debe comprobarse que los modelos hardware recibidos coinciden con los equipos cualificados.

En relación con el software, el producto se entrega con uno instalado. No obstante, puede que no sea la versión del software recomendada, en cuyo caso el producto deberá actualizarse. El software Cisco IOS-XR 7.11 está disponible en el Software Center de Cisco [REF3].

El administrador debe descargar la imagen únicamente desde el sitio autorizado de Cisco, buscando el modelo correspondiente, y verificar antes de la instalación la integridad y autenticidad del binario mediante el hash publicado por el fabricante, calculado con el algoritmo SHA-512, tal y como exige el mecanismo de verificación de actualizaciones del producto. Cualquier discrepancia entre el hash calculado localmente y el hash publicado debe implicar el rechazo de la imagen y la notificación al fabricante.

Adicionalmente, el uso de SHA-512 como mecanismo de verificación de integridad está alineado con los algoritmos hash autorizados por el CCN para mecanismos criptográficos de empleo en el ENS.

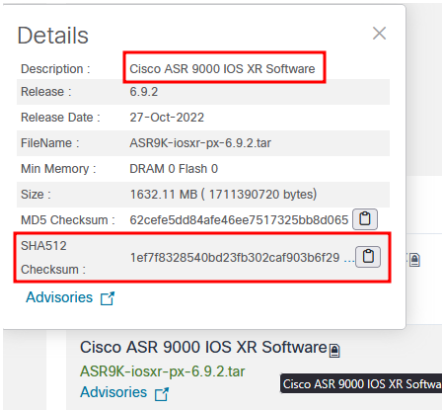


Figura 2: Verificación del hash

4.2 ENTORNO DE INSTALACIÓN SEGURO

El producto deberá instalarse en un Centro de Procesamiento de Datos (CPD) con medidas de seguridad física. El acceso a dichas instalaciones deberá estar limitado a un conjunto de personas que posean una autorización expresa.

4.3 REGISTRO Y LICENCIAS

El sistema de licenciamiento utilizado por Cisco IOS-XR es *Smart Licensing.* Para la gestión de licencias, la organización debe disponer de una cuenta asociada a los servicios de licenciamiento de Cisco. Existen tres opciones de despliegue de Smart Licensing:

- **Despliegue directo**, donde el dispositivo se comunica directamente con los servicios de licenciamiento de Cisco.
- **Despliegue on-premises**, utilizando una infraestructura de licenciamiento gestionada localmente por la organización.
- **Despliegue offline**, destinado a entornos sin conectividad hacia los servicios de Cisco.

El administrador deberá seleccionar la modalidad más adecuada en función de los requisitos operativos y de conectividad de la organización.

La información detallada sobre los mecanismos de licenciamiento y las modalidades de despliegue soportadas puede consultarse en la documentación oficial de Cisco [REF4].

4.4 CONSIDERACIONES PREVIAS

Antes de proceder con la instalación y configuración segura del producto, es necesario considerar los requisitos de hardware del dispositivo, dado que el entorno evaluado está basado en plataformas específicas de la familia Cisco ASR 9000.

El producto está compuesto por chasis modulares o standalone, procesadores de ruta (Route Processors) y tarjetas de línea, incluyendo modelos concretos como ASR-9006, ASR-9010, ASR-9906 o ASR-9912, junto con procesadores Intel Xeon y memoria RAM en rangos típicos de 16 a 48 GB según modelo. Estas características físicas son fundamentales para garantizar la correcta operación y las capacidades de seguridad evaluadas del sistema.

Adicionalmente, el producto requiere la existencia de una infraestructura de entorno (IT environment) correctamente desplegada antes de su configuración. En particular, se deben disponer elementos externos como un servidor de auditoría (syslog), una estación de gestión con cliente SSH, una autoridad de certificación (CA) y una consola local, que forman parte del entorno necesario para operar el sistema de forma segura.

Desde el punto de vista de red y comunicaciones, es imprescindible que el entorno permita el uso de canales seguros, dado que toda la gestión del dispositivo se realiza a través de SSHv2 para administración remota y TLS para el envío de logs al servidor syslog. Por tanto, deben habilitarse previamente las configuraciones de red necesarias (conectividad IP, resolución de nombres, sincronización horaria, etc.) y garantizar que los dispositivos de seguridad perimetral (firewalls) no bloqueen estos protocolos.

Asimismo, antes de la configuración del sistema, se deben establecer adecuadamente los mecanismos de autenticación y control de acceso**.** El producto requiere que todos los administradores estén autenticados antes de acceder a cualquier funcionalidad de gestión, pudiendo utilizar bases de datos locales o servidores externos (AAA).

Es necesario tener en cuenta que el producto debe configurarse conforme a las guías de configuración segura proporcionadas por el fabricante, las cuales forman parte del entorno evaluado. Estas guías establecen los parámetros necesarios para habilitar funcionalidades de seguridad como auditoría, criptografía, gestión de usuarios o actualización de software. No seguir estas configuraciones puede implicar que el sistema no opere dentro del entorno evaluado ni bajo las garantías de seguridad previstas.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

A continuación, se listan los principales componentes que forman parte del entorno de operación de Cisco ASR 9000 en su configuración evaluada. Estos elementos son necesarios para garantizar el correcto funcionamiento y las capacidades de seguridad del sistema.

COMPONENTE	DESCRIPCIÓN
Management Workstation with SSH Client	Estación de trabajo de gestión utilizada por los administradores para acceder al dispositivo a través de conexiones seguras SSH.
Local Console	Consola local conectada directamente al dispositivo, empleada para tareas de administración y configuración inicial.
MACsec Peer	Dispositivo externo compatible con MACsec utilizado para establecer comunicaciones cifradas a nivel de enlace (Layer 2) con el equipo evaluado.
Audit (Syslog) Server	Servidor de registro externo encargado de almacenar los eventos de auditoría generados por el producto, utilizando canales seguros (TLS).
Certificate Authority (CA)	Autoridad de certificación utilizada para emitir y validar certificados digitales empleados en la autenticación y establecimiento de canales seguros.

Tabla 1: Componentes Entorno de Operación

5 FASE DE INSTALACIÓN

La instalación física del producto se debe realizar según las instrucciones de las guías de Cisco: *Hardware Installation Guide* [REF5].

El software IOS XR 7.11 se puede encontrar preinstalado en el dispositivo, y si la versión no coincide con la recomendada, puede obtenerse mediante descarga desde el portal de Cisco [REF3], requiriendo credenciales de acceso.

5.1 MANEJO DE LOS COMANDOS DE CISCO

Cisco IOS-XR se basa en una arquitectura de *feature packages*, por lo que determinadas funcionalidades de seguridad requieren la instalación de paquetes software específicos.

Antes de proceder con la configuración del producto, es necesario informarse sobre el formato de los comandos, haciendo uso de las guías de cisco [REF6] y [REF8].

Modo del comando	Descripción
Modo de ejecución de la máquina virtual XR	Ejecute comandos en la máquina virtual XR para visualizar el estado operativo del enrutador. Ejemplo: `RP/0/RP0/CPU0:router#`

Configuración global de la máquina virtual XR	Realizar configuraciones de seguridad, enrutamiento y otras funciones de XR en la máquina virtual XR.
	Ejemplo:
	`RP/0/RP0/CPU0:router#configure`
	`RP/0/RP0/CPU0:router(config)#`

Modo de ejecución de la máquina virtual de administrador del sistema	Ejecute comandos en la máquina virtual de administración del sistema para visualizar y supervisar el estado operativo del hardware del enrutador. Desde este modo, se puede reiniciar el chasis o los módulos de hardware individuales.
	Ejemplo:
	`RP/0/RP0/CPU0:router#admin`
	`sysadmin-vm:0_RP0#`

Modo de configuración de la máquina virtual de administrador del sistema	Ejecute comandos de configuración en la máquina virtual de administración del sistema para gestionar y operar los módulos de hardware de todo el chasis.
	Ejemplo:
	`RP/0/RP0/CPU0:router#admin`
	`sysadmin-vm:0_RP0#config`
	`sysadmin-vm:0_RP0(config)#`

Tabla 2: Modo de comandos

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para utilizar el producto en un modo de operación seguro, se deberá seguir la guía *"Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance"* [REF7], complementada por la *"System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x"* [REF8].

Siguiendo las guías mencionadas se podrán configurar correctamente las interfaces y funcionalidades de seguridad del Cisco ASR 9000, asegurando un entorno protegido y conforme con los requisitos establecidos en la evaluación *Common Criteria*.

6.1.1 HABILITACIÓN DEL MODO DE OPERACIÓN SEGURO (FIPS)

Cuando el entorno requiera el uso del modo FIPS, es necesario disponer del paquete: *ASR9K-x64-iosxr-px-k9-7.11.1.tar*. Tras seguir los pasos descritos en la sección 6.3.1.1 CANAL SSH.

Posterior mente se deben ejecutar los siguientes pasos:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto fips-mode
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router# show logging
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router# reload location all
```

Tras habilitar FIPS, es necesario reiniciar el sistema para que el dispositivo opere en dicho modo. El procedimiento se encuentra descrito en la sección 3.2.5 de la guia "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance"* [REF7].

6.2 AUTENTICACIÓN

El producto implementa distintos mecanismos de autenticación:

- **Autenticación mediante usuario y contraseña (credenciales):** este mecanismo constituye el método principal de autenticación. Para la creación y gestión de cuentas administrativas puede consultarse el apartado correspondiente de administración de usuarios [REF7].
- **Autenticación mediante claves criptográficas (SSH keys)**. El producto permite asociar claves públicas a usuarios administrativos, verificando la correspondencia entre la clave presentada durante el proceso de autenticación y la previamente registrada en el sistema, ver el apartado 6.3.1.1 CANAL SSH. En caso de discrepancia, el acceso es rechazado. Este mecanismo proporciona una alternativa a la autenticación basada exclusivamente en contraseña.
- **Autenticación basada en certificados digitales (X.509):** especialmente en comunicaciones con servicios externos como servidores de logs.
- **Autenticación frente a servidores externos (AAA)**. El producto dispone de funcionalidades AAA para la gestión de usuarios, grupos, autorización y control de privilegios. Asimismo, el producto contempla la integración con servidores de autenticación externos mediante los mecanismos AAA soportados por IOS-XR [REF9].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

Cisco ASR 9000 permite administración tanto local, mediante la consola del sistema IOS-XR, como remota, mediante SSHv2.

En relación a la configuración segura de protocolos de administración esta información se describe en la guía de usuario del producto [REF7], en los siguientes apartados:

- *Steps to Configure SSH Server on the Router*
- *Remote Administration Protocols*
- *X.509 Certificates*
- *Logging to Syslog Server via TLS*

No se permite el uso de protocolos inseguros, por lo que siguiendo la guía anterior se debe garantizar que ninguno de los siguientes se encuentra en uso:

- Telnet: el producto lo mantiene deshabilitado por defecto y no debe habilitarse.
- SSHv1: Se deberá habilitar exclusivamente SSHv2 siguiendo el procedimiento descrito en la sección *Steps to Configure SSH Server on the Router*, anteriormente referenciada.
- TLS inferior a 1.2: Los servicios que utilicen TLS deberán configurarse con TLS 1.2 o superior, según la sección *Logging to Syslog Server via TLS*, anteriormente referenciada.
- FTP: no se recomienda su uso para la transferencia de ficheros.
- HTTP: no se recomienda su uso para tareas de administración. Se deberá utilizar HTTPS cuando la funcionalidad esté disponible.
- IKEv1: no se recomienda su uso. En caso de emplear VPN IPsec se deberá utilizar IKEv2.

Además, el producto tiene la capacidad de configurar los algoritmos y funciones criptográficas para cumplir con las especificaciones de la **guía CCN-STIC-807**. Para ello, se deberá seguir la guía *"Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance"* [REF7], complementada por la *"System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x"* **[**REF4**]**.

6.3.1.1 CANAL SSH

Debe configurarse el servicio SSH. Para asegurar un uso seguro de este, se deben llevar a cabo las siguientes configuraciones, de tal forma que el producto emplee:

- SSH versión 2.
- El grupo 16 de DH para intercambio de clave.
- Claves RSA de 3072 bits.
- Los algoritmos de AES-128-CBC y AES-256-CBC
- Las funciones SHA2-256, SHA2-512.

Las claves criptográficas RSA, serán utilizadas por el servidor SSH para identificarse ante los clientes remotos y establecer canales de comunicación protegidos.

Para aplicar dichas configuraciones se ejecutarán los comandos indicados en la sección *3.3 Network Protocols and Cryptographic Settings* de la guia *"Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance"* [REF7].

Una vez generadas las claves, se habilita el servicio SSHv2 en el dispositivo con los siguientes comandos:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server v2
RP/0/RSP0/CPU0:router(config)# commit
```

Durante el primer arranque se solicita la creación de las credenciales administrativas del sistema. A continuación, debe configurarse la interfaz de gestión del equipo.

El primer paso consiste en acceder al modo de configuración global:

```
RP/0/RSP0/CPU0:router# configure
```

Posteriormente se selecciona la interfaz de gestión que será utilizada para la administración del dispositivo:

```
RP/0/RSP0/CPU0:router(config)# interface MgmtEth 0/RP0/CPU0/0
```

Una vez seleccionada la interfaz, debe asignarse una dirección IP y una máscara de red adecuadas al entorno donde será desplegado el producto:

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address <direccion-ip>/<prefijo>
```

Con la dirección configurada, la interfaz debe habilitarse para permitir el intercambio de tráfico de gestión:

```
RP/0/RSP0/CPU0:router(config-if)# no shutdown
```

Después de activar la interfaz se abandona el modo de configuración de interfaz:

```
RP/0/RSP0/CPU0:router(config-if)# exit
```

Para permitir la comunicación con estaciones de gestión ubicadas fuera de la red local, debe configurarse una ruta por defecto hacia la puerta de enlace correspondiente:

```
RP/0/RSP0/CPU0:router(config)# router static address-family ipv4 unicast 0.0.0.0/0 <gateway>
```

Una vez definidos los parámetros de gestión necesarios, los cambios deben almacenarse en la configuración activa mediante:

```
RP/0/RSP0/CPU0:router(config)# commit
```

Los detalles completos de este procedimiento pueden consultarse en la guía *"System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x"* [REF8].

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Cisco ASR 9000 permite la configuración de usuarios administrativos mediante el sistema AAA (*Authentication, Authorization and Accounting*), incluyendo la definición de roles, grupos de usuarios, privilegios asociados, política de contraseñas y parámetros de sesión.

Los detalles necesarios para seguir las configuraciones a aplicar a continuación se encuentran en el documento "*System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*" **[**REF4**]**, debiendo el administrador consultar las guías indicadas para su implementación:

- **Configuración de los roles de administración:** consultar el capítulo "Configuring AAA Services", secciones "*User*" y "*User Groups, and Task Groups*".

- **Configuración de la Política segura de contraseñas**: consultar el capítulo "*Configuring AAA Services"*. La configuración a establecer deberá cumplir con los siguientes requisitos mínimos:
  - Longitud mínima de la contraseña: doce (12) caracteres.
  - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales.
  - Número de contraseñas anteriores que no se permite utilizar: cinco (5).
  - Tiempo de validez en días de las contraseñas tras el cual expiran: dos meses (60 días).
  - Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.
- **Configuración de los parámetros de sesión:** consultar las secciones "*Session Termination"* y "*User Lockout"*. La configuración debe cumplir con los siguientes requisitos mínimos:
  - Tiempo de inactividad de las sesiones: cinco (5) minutos.
  - Número de intentos fallidos de inicio de sesión: tres (3) intentos.
  - Tiempo de bloqueo tras los intentos fallidos: cinco (5) minutos.
- **Configuración del mensaje de aviso y consentimiento en el inicio de sesión**: consultar la sección "*login Banners*".

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Cisco ASR 9000 permite la configuración segura de interfaces, puertos y servicios de red mediante la definición de parámetros de interfaz, habilitando o deshabilitando servicios y control del tráfico asociado.

Para la configuración de estos aspectos, el administrador deberá consultar la documentación del fabricante:

- "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*" **[**REF7**]**.
- "*System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers*" [REF9].

En estas secciones se describe cómo configurar direcciones IP, habilitar o deshabilitar interfaces y restringir los servicios disponibles en el sistema.

6.5 GESTIÓN DE CERTIFICADOS

Cisco ASR 9000 incorpora funcionalidades criptográficas que permiten el uso de algoritmos y funciones hash para la protección de las comunicaciones y la gestión de certificados digitales. Estos mecanismos están implementados mediante librerías criptográficas del sistema operativo IOS-XR y son configurables por el administrador.

Para la configuración de los algoritmos criptográficos, el administrador deberá consultar la siguiente documentación:

- "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*" **[**REF7**]**.
- "*System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*" **[**REF4**]**.

El producto permite el uso de algoritmos que cumplen con las especificaciones de la guía **CCN-STIC-807**:

- RSA con claves de, al menos, 3072 bits de longitud (configurable en la generación de claves criptográficas).
- ECDSA con curvas P-256 o superior, utilizado en mecanismos criptográficos soportados por el sistema.
- DSA con claves de longitud configurable, permitiendo valores iguales o superiores a 3072 bits según configuración.
- Funciones hash SHA-256 o superior, empleadas en mecanismos de integridad y autenticación.

6.6 SERVIDORES DE AUTENTICACIÓN

Cisco ASR 9000 permite configurar la comunicación con servidores externos de autenticación, incluyendo la definición de servidores, claves compartidas y parámetros de retransmisión.

Para ello se deberá consultar la "*System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*" **[**REF4**]**, donde se describen las configuraciones seguras para:

- Uso de protocolos de autenticación centralizada (RADIUS/TACACS+).
- Configuración de claves compartidas entre el producto y el servidor de autenticación.
- Uso de canales seguros para el acceso administrativo (SSHv2) que complementan la autenticación externa.

6.7 SINCRONIZACIÓN

El producto permite la sincronización horaria mediante el uso de servidores de tiempo externos, lo cual es necesario para el correcto funcionamiento de los registros de auditoría y mecanismos de seguridad.

Para la configuración de la sincronización, se deberá consultar la "*System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*" [REF8].

6.8 ACTUALIZACIONES

Cisco ASR 9000 permite la actualización segura de software, la realización de estas operaciones se encuentra detallada en "*System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers*" [REF9].

Las secciones "*Installing and Upgrading Software*" y "*Managing System Images*" describen el proceso de instalación y actualización del software del sistema, incluyendo la carga de nuevas imágenes, su verificación y activación en el dispositivo.

6.9 AUTO-CHEQUEOS

El producto realiza automáticamente los auto-chequeos durante el proceso de arranque (*startup*), antes de poner en funcionamiento los servicios de seguridad, tal y como se describe en "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*" **[**REF7**]**.

6.10 ALTA DISPONIBILIDAD

Cisco ASR 9000 soporta mecanismos de alta disponibilidad mediante componentes redundantes, tales como procesadores de ruta (Route Processors) y fuentes de alimentación redundantes. La configuración de alta disponibilidad del producto se describe en la siguiente documentación:

- *"System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers"* [REF9].
- *"Cisco ASR 9000 Series Aggregation Services Routers Hardware Installation Guide"* [REF5].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El producto permite el registro de eventos de auditoría relacionados con la seguridad, como se describe en "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*" [REF7].

Además, los registros incluyen información como la fecha y hora del evento, el proceso que lo genera, el tipo de evento y su resultado.

6.11.2 ALMACENAMIENTO LOCAL

Cisco ASR 9000 permite almacenar registros localmente mediante buffers internos de syslog para su posterior consulta por parte de administradores autorizados. Se recomienda configurar un tamaño de almacenamiento suficiente y habilitar el registro de todos los eventos relevantes de seguridad para evitar la pérdida de información de auditoría. Los pasos se describen en "*Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance*" [REF7].

6.11.3 ALMACENAMIENTO REMOTO

Cisco ASR 9000 permite el envío de registros a servidores syslog remotos. Para garantizar la confidencialidad e integridad de los registros durante la transmisión, se recomienda utilizar TLS 1.2 o superior, evitando el uso de mecanismos no cifrados para el transporte de eventos de auditoría.

6.12 BACKUP

Se recomienda realizar copias de seguridad, al menos, de los siguientes elementos:

- Configuración activa del producto.
- Configuración almacenada de forma persistente.
- Certificados digitales instalados.
- Claves y configuraciones criptográficas asociadas a PKI.
- Imágenes software y paquetes instalados necesarios para la recuperación del sistema.

El procedimiento para la gestión de archivos y realización de copias de seguridad se describe en la documentación del fabricante:

- "*System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x*" [REF8].
- "*System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers*" [REF9].

Las copias de seguridad deberán realizarse mediante protocolos seguros, como **SCP** o **SFTP**, evitando el uso de protocolos no cifrados. Asimismo, se recomienda realizar copias de seguridad de forma periódica y tras cualquier cambio relevante en la configuración o actualización del sistema.

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 (*Security Advisories* [REF10]) 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 Software Lifecycle Support Statement - IOS XR

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xr-software/product_bulletin_c25-478699.html

REF3 CISCO Software

https://software.cisco.com/download/home

REF4 Licenses

https://www.cisco.com/c/en/us/td/docs/iosxr/licensing/article/ios-xr-smart-licensing.html#deploying-smart-licensing

REF5 Hardware Installation guide:

Cisco ASR 9000 Series Aggregation Services Routers Hardware Installation Guide

https://www.cisco.com/c/en/us/support/routers/asr-9000-series-aggregation-services-routers/series.html

Cisco ASR 9000 Series Aggregation Services Router SIP and SPA Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/iosxr/asr9000/hardware-install/sip-spa-hig/b-asr9000-sip-and-spa-hardware-installation-guide.html

Cisco ASR 9000 Series Aggregation Services Router Satellite Systems Installation Guide

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/hardware/satellite/installation/guide/b-asr9000-satellite-hig.html

Cisco ASR 9000 Series Fixed-Port Routers Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/iosxr/asr9000/hardware-install/9001-hig/b-asr9001-hardware-installation-guide.html

REF6 Command Reference List for IOS-XR

https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xr-software/products-command-reference-list.html

REF7 Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11, Common Criteria Operational User Guidance

https://www.niap-ccevs.org/products/11484

REF8 System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/system-security/configuration/guide/b-system-security-cg-asr9000-711x.html

REF9 System Setup and Software Installation Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x

https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/711x/system-setup/configuration/guide/b-system-setup-cg-asr9000-711x.html

REF10 Cisco Security Advisories
https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&keyword=catalyst&sort=-day_sir#~Vulnerabilities

9 ABREVIATURAS

CA	Autoridad de Certificación
CCN	Centro Criptológico Nacional
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
FTP	File Transfer Protocol
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure
IKEv1	Internet Key Exchange Version 1
RSA	Rivest-Shamir-Adleman
RSP	Route Switch Processor
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network