Guía de Seguridad de las TIC
CCN-STIC 1465

Procedimiento de Empleo Seguro
Cisco Routers 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 14:07:00 +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
2.1 SOFTWARE 5
3 ORGANIZACIÓN DEL DOCUMENTO 6
4 FASE PREVIA A LA INSTALACIÓN 7
4.1 ENTREGA SEGURA DEL PRODUCTO 7
4.2 ENTREGA SEGURA DEL SOFTWARE 7
4.3 ENTORNO DE INSTALACIÓN SEGURO 8
4.4 REGISTRO Y LICENCIAS 8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 8
5 FASE DE INSTALACIÓN 10
5.1 USO DE LOS COMANDOS IOS-XE 10
5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA 10
6 FASE DE CONFIGURACIÓN 12
6.1 GUARDAR CONFIGURACIÓN EN DISCO 12
6.2 MODO DE OPERACIÓN SEGURO 12
6.3 AUTENTICACIÓN 12
6.3.1 SERVIDORES DE AUTENTICACIÓN 13
6.4 ADMINISTRACIÓN DEL PRODUCTO 13
6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA 13
6.4.2 CONFIGURACIÓN DE ADMINISTRADORES 13
6.4.3 PARÁMETROS DE SESIÓN 14
6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 15
6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 15
6.7 GESTIÓN DE CERTIFICADOS 16
6.8 SINCRONIZACIÓN 16
6.9 ACTUALIZACIÓN DEL SOFTWARE 17
6.10 AUTO-CHEQUEOS 17
6.11 AUDITORÍA 18
6.11.1 REGISTRO DE EVENTOS 18
6.12 CONFIGURACIÓN DE IPSEC 19
6.13 COPIAS DE SEGURIDAD 21
7 FASE DE OPERACIÓN 22
8 CHECKLIST 23
9 REFERENCIAS 25
10 ABREVIATURAS 27

ÍNDICE DE TABLAS

Tabla 1. Transformaciones IPsec 20
Tabla 2. Transformaciones IKEv2 21
Tabla 3. Checklist 24

ÍNDICE DE FIGURAS

Ilustración 1. Versiones de Software 5
Ilustración 2 Verificación HASH durante la descarga del software 8

1 INTRODUCCIÓN

Los routers Cisco con IOS-XE son equipos diseñados para entornos industriales exigentes. Son resistentes y duraderos, capaces de soportar condiciones extremas, además de ser fácil de configurar y administrar, lo que lo hace adecuado para entornos industriales donde se requiere una infraestructura de red robusta y confiable.

2 OBJETO Y ALCANCE

El objeto del presente documento es facilitar la instalación y configuración segura de los routers de Cisco ejecutando la versión de sistema operativo **IOS-XE 17.12**, junto con el aseguramiento del entorno en el que se despliega.

El producto ha sido incluido en el catálogo CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF15]. **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-XE cuyo nombre tiene la nomenclatura 17.12.Y.



Ilustración 1. Versiones de Software

La Major Release (17) tiene varias Minor Release: 17.9, 17.12, etc.

Cada Minor Release tiene varias Maintenance Release: 17.12.1, 17.12.2, 17.12.4, etc.

Este documento se refiere a la Minor Release 17.12.

Más información sobre las imágenes IOS-XE se encuentra en la guía de Cisco: IOS-XE [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 6. 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

El producto debe ser examinado para comprobar que no ha sido manipulado durante su entrega siguiendo los siguientes pasos. En caso de encontrar algún problema, contactar con el proveedor del equipo (Cisco o un distribuidor autorizado):

a) Antes de abrir el paquete donde fue entregado el producto, comprobar que el paquete contenga la serigrafía y logo de Cisco.

b) Comprobar que el paquete no ha sido abierto y después vuelto a sellar examinando la cinta que lo cierra.

c) Comprobar que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.

d) Verificar que el número de serie del producto especificado en la documentación del pedido coincide con el recibido. El número de serie que figura en la etiqueta blanca de la caja debe corresponder con el número de serie del dispositivo, y con el indicado en la factura recibida.

e) Comprobar que el pedido fue enviado por el proveedor esperado. Para ello, verificar el código de envío/paquete junto con la empresa de transporte. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío, por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.

4.2 ENTREGA SEGURA DEL SOFTWARE

El producto se entrega con un software instalado. No obstante, puede que no sea la versión del software recomendada, en cuyo caso el producto deberá actualizarse para emplear las versiones de software indicadas en el apartado 2.1 SOFTWARE.

El software está disponible en el Software Center de Cisco [REF17]

En la pantalla de descarga del software, se puede consultar el hash SHA512 del fichero a descargar. Se deberá realizar el hash del fichero descargado y verificar que coincide con el indicado en la página de descarga.

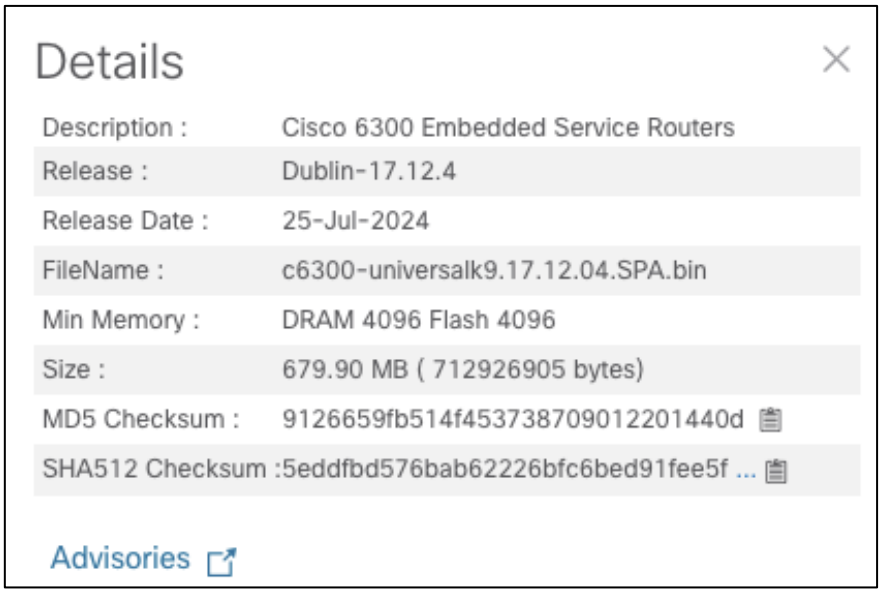


Ilustración 2 Verificación HASH durante la descarga del software

4.3 ENTORNO DE INSTALACIÓN SEGURO

El producto debe instalarse en una ubicación físicamente segura donde solo se permita acceso físico al personal autorizado. Por ejemplo, en el CPD de la organización.

4.4 REGISTRO Y LICENCIAS

El sistema de licencias de Cisco se llama Smart Licensing. Cada cliente tiene una cuenta en el portal de Cisco. Con esta cuenta, la organización dispone del Smart Software Manager.

El producto comunica al Smart Software Manager de manera online (a través de un servidor proxy) u offline (solución satélite) la siguiente información:

- Uso de funcionalidades que necesitan licencias.
- Números de identificación de productos asociados.
- Números de serie.

En el Smart Software Manager se encuentran las licencias compradas. Cuando el Smart Software Manager recibe la información sobre el uso de las funcionalidades necesitando licencias, sube el contador de licencias usadas. Por lo tanto, no hace falta instalar licencias en el producto.

El detalle de configuración de licencias se puede consultar en la guía Cisco: Licenses [REF2].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El producto requiere los siguientes componentes en el entorno operacional:

- Puesto de gestión por consola: dicho puesto hace referencia a cualquier estación de trabajo que permita una conexión por consola serie en el Router.
- Puesto de gestión con cliente SSH: dicho puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado, que se emplea para la configuración y administración del Router.

La administración del equipo se debe realizar aplicando medidas adicionales de seguridad. Por ejemplo, desde la red interna de la organización, restringiendo las direcciones IP origen de la conexión, aplicando capas de protección adicionales como comunicaciones a través de canales VPN con un nivel de cifrado adecuado, etc.

- Servidor radius AAA.
- Servidor syslog.
- Servidor NTP.
- Servidor de monitorización: para la recepción de los mensajes syslog del Router.

5 FASE DE INSTALACIÓN

La instalación física del producto se debe realizar las instrucciones de las guías de Cisco: *Cisco Embedded Service 6300 Series Router Hardware Technical Guide* [REF3].

El producto requiere una configuración inicial a través del cable de consola entregado con el producto. Esta configuración inicial permite luego una conexión Ethernet por SSHv2 para seguir con la configuración avanzada.

La administración del equipo se debe realizar aplicando medidas adicionales de seguridad. Por ejemplo, desde la red interna de la organización, restringiendo las direcciones IP origen de la conexión, aplicando capas de protección adicionales como comunicaciones a través de canales VPN con un nivel de cifrado adecuado, etc.

5.1 USO DE LOS COMANDOS IOS-XE

Antes de configurar el producto, se necesita entender el formato de los comandos y los modos Exec.

Más información se puede encontrar en la guía de Cisco: *Command Reference Guides for Access and Edge Routers* [REF4].

5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA

Después de conectar el cable de consola entre el puesto de gestión y el puerto de serie del producto, se arranca el equipo. Aparece un menú configuración del sistema: **System Configuration Dialog**. Este menú permite introducir la configuración inicial.

Se deberán configurar los siguientes parámetros:

- *Enter host name*. Nombre de dispositivo deseado.
- *Enter enable secret*. Contraseña empleada para proteger el acceso a los modos de configuración, debe ser conforme a la política de contraseñas definida en el apartado 6.4.2 CONFIGURACIÓN DE ADMINISTRADORES.
- *Enter virtual terminal password*. Contraseña empleada para proteger el acceso a la terminal virtual permitiendo acceso al producto mediante consola. debe ser conforme a la política de contraseñas definida en el apartado 6.4.2 CONFIGURACIÓN DE ADMINISTRADORES.
- *Configure SNMP Network Management*. Por defecto configurado en NO, de tal forma que el servidor SNMP estará deshabilitado. Dejar el valor por defecto.
- Enter interface name used to connect to the management network from the above interface summary. Seleccionar la interfaz que se desea emplear para conectar a la red.

Una vez finalizada la configuración inicial, se deben introducir los siguientes comandos para permitir la conexión por la red de gestión mediante SSHv2, para llevar a cabo la configuración completa del producto.

La administración remota del equipo se debe realizar aplicando medidas adicionales de seguridad. Por ejemplo, desde la red interna de la organización, restringiendo las direcciones IP origen de la conexión, aplicando capas de protección adicionales como comunicaciones a través de canales VPN con un nivel de cifrado adecuado, etc.

En esta configuración se exige el empleo de RSA con claves de 4096 bits en el protocolo en la versión 2 del protocolo ssh. Así como la utilización el algoritmo de encriptación aes128-cbc o aes256-cbc junto con utilización de hmac-sha2 como mecanismo MAC.

```
Router#conf t
Router(config)# hostname <Router>
Router(config-if)#interface GigabitEthernet0/0
Router(config)# interface GigabitEthernet0/0
Router(config-if)#ip address <IP> <Mask>
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)# ip domain name <domain-name>
Router(config)# ip ssh version 2
Router(config)# ip ssh time-out 60
Router(config)# ip ssh authentication-retries 2
Router(config)# ip ssh dh min size 4096
Router(config)# ip ssh server algorithm encryption aes256-cbc aes128-
cbc
Router(config)# ip ssh server algorithm mac hmac-sha512 hmac-sha2-256
Router(config)# crypto key generate rsa modulus 4096
Router(config)# service password-encryption
Router(config)# username <user-admin> password <password>
Router(config)# enable secret <password>
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local
Router(config)#exit
Router# copy run start
```

El detalle sobre la configuración inicial del producto se puede consultar en la guía de Cisco*: System* Management *Configuration Guide* [REF5].

6 FASE DE CONFIGURACIÓN

6.1 GUARDAR CONFIGURACIÓN EN DISCO

Todas las configuraciones o modificaciones introducidas en el producto o deben guardarse manualmente en la memoria NVRAM. Para ello se debe emplear el siguiente comando.

```
Router# copy run start
```

Si el producto se reinicia cuando se han realizado los cambios sin guardar la nueva configuración, estos se perderán y el producto utilizará la última configuración guardada.

Para comprobar la configuración actual, se utiliza el comando siguiente.

```
Router# show running-config
```

6.2 MODO DE OPERACIÓN SEGURO

El producto debe ejecutarse en el modo de operación seguro. Para ello, se debe ejecutar el siguiente comando:

```
Router(config)#platform ipsec fips-mode
```

Adicionalmente, se recomienda activar el logging extendido mediante:

```
Router(config)#logging console errors
```

Se necesita un reinicio del equipo para activarlo.

```
Router# copy run start
Router# reload
```

Verificar que se ha activado correctamente con los comandos siguientes:

```
Router# show fips status
```

El detalle sobre la configuración el modo seguro se puede consultar en la guía de Cisco: Security Configuration Guide: Secure Operation in FIPS Mode [REF6].

6.3 AUTENTICACIÓN

Los mecanismos de autenticación utilizados por el producto son los siguientes:

- Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver apartado 6.4.2 CONFIGURACIÓN DE ADMINISTRADORES. Así mismo, se recomienda que cada administrador disponga de una cuenta individual para el acceso al producto. El uso de cuentas compartidas debe evitarse con el fin de garantizar la correcta identificación de las acciones realizadas y su adecuada trazabilidad, como se indica en la sección 4.1 de [REF17].
- Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración y gestión de dichos servidores, ver sección 6.3.1 SERVIDORES DE AUTENTICACIÓN.

Se recomienda emplear la autenticación local, por lo que se debe configurar la funcionalidad AAA para la gestión local de los usuarios.

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default local
Router(config)# aaa authorization exec default local
```

6.3.1 SERVIDORES DE AUTENTICACIÓN

El producto permite la integración con distintos servidores de autenticación externos:

- Servidores de tipo RADIUS.
- Servidores de tipo TACACS+.

Se deberán seguir las siguientes recomendaciones en caso de emplear alguna de las opciones:

- Para servidores de tipo TACACS+, se deberá configurar la clave de cifrado empleando el comando *key*. Esta se empleará para cifrar las comunicaciones entre el producto y el servidor (ver [REF7]).
- Para servidores de tipo RADIUS, se deberá configurar el producto para emplear RADSEC. Se puede consultar el detalle de los pasos en [REF18].

Debido a que la conexión con los servidores externos puede fallar, se recomienda mantener como método alternativo de respaldo la base de datos local de usuarios, de tal forma que, si no se puede realizar la comunicación con el servidor de autenticación, se siga pudiendo acceder al dispositivo. Para ello emplear el parámetro local al final del comando:

```
Router(config)#aaa authentication login default group radius/tacacs+
local
```

El detalle de configuración de los servidores de autenticación se puede consultar en la guía de Cisco: AAA [REF7].

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

Se recomienda realizar la administración del producto de forma local desde la consola.

El protocolo SSH deberá estar deshabilitado por defecto en el producto. Solo en caso de que sea estrictamente necesario llevar a cabo la administración remota vía CLI, se podrá habilitar temporalmente SSH, y adoptando medidas de protección adicionales.

6.4.2 CONFIGURACIÓN DE ADMINISTRADORES

Cada usuario administrador del producto dispone de un usuario y contraseña para acceder al sistema. Adicionalmente, la contraseña Enable secret permite en entrar en modo *Enable* para la configuración y comandos avanzados.

Para configurar la contraseña *Enable secret* y almacenarla empleando SHA-256, utilizar el siguiente comando:

```
Router(config)# enable secret <password>
```

Emplear el siguiente comando para almacenar cifradas con SHA-256 las contraseñas de los usuarios.

```
Router(config)#service password-encryption
```

Se deberá configurar la política de contraseñas segura. Para ello emplear los siguientes comandos, de tal forma que deban contener al menos 15 caracteres y un tiempo de validez de 60 días y emplear al menos una letra minúscula, una mayúscula, un número y un carácter especial.

Adicionalmente, se habilitará el comando aaa password restriction, que impide el uso de contraseñas idénticas al nombre de usuario, contraseñas triviales conocidas, así como secuencias repetidas excesivamente de caracteres. Esta medida complementa la política de complejidad definida anteriormente.

```
Router(config)#aaa common-criteria policy <nombre-policy>
Router(config-cc-policy)#min-length 15
Router(config-cc-policy)#lifetime day 60
Router(config-cc-policy)# lower-case 1
Router(config-cc-policy)# upper-case 1
Router(config-cc-policy)# special-case 1
Router(config-cc-policy)# numeric-count 1
Router(config-cc-policy)#exit

! Activar restricciones adicionales de contraseña
Router(config)# aaa password restriction

Router(config)# username <user-admin> common-criteria-policy <nombre-
policy>  password <password>
```

Adicionalmente, los administradores deberán asegurar de forma procedural:

- No se puedan reutilizar las últimas 5 contraseñas.
- No se podrá volver a modificar una contraseña hasta pasados 10 días.

Para cada usuario se debe definir el nombre de usuario, su contraseña de acuerdo con la política definida y el nivel de privilegios del mismo. Los niveles de privilegio de los usuarios están numerados del 1 al 15. El nivel de privilegio 15 tiene acceso a todos los comandos.

Los niveles 1-14 se pueden configurar para que comprendan cualquiera de los comandos disponibles. Para ello se debe emplear el siguiente comando, indicando el comando deseado y el nivel al que pertenecerá:

```
Router(config)# privilege exec level <x> <command>
```

Un usuario de nivel 1 puede ejecutar cualquier comando empleando la contraseña password enable definida. Por lo tanto, esta contraseña deberá ser segura y estar únicamente en conocimiento de los administradores autorizados.

El detalle sobre la gestión de usuarios y permisos se puede consultar en la guía de Cisco: Controlling Router Access with Passwords and Privilege Levels [REF8].

6.4.3 PARÁMETROS DE SESIÓN

Configurar el tiempo de inactividad de las sesiones en 5 minutos en la consola y en la *line vty* (para SSH):

```
Router(config)# line console
Router(config-line)# exec-timeout 5
Router(config)# line vty 0 31
Router(config-line)# exec-timeout 5
```

Para configurar el bloqueo de usuarios tras 3 intentos de autenticación fallidos, emplear el siguiente comando.

```
Router(config)#aaa local authentication attempts max-fail 3
```

Una vez bloqueado un usuario, se deberá desbloquear manualmente.

```
Router#show aaa local user lockout
Router#clear aaa local user lockout  username <username>
```

Se deberá configurar un mensaje de aviso que se muestra cuando se conecta un usuario. La letra "C" en el ejemplo abajo es un delimitador arbitrario.

```
Router(config)#banner login C eso es un banner C
```

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Se deberá deshabilitar el servidor web. Para ello se deben emplear los siguientes comandos, desactivando tanto HTTP como HTTPS.

```
Router(config)#no ip http server
Router(config)#no ip http secure-server
```

Telnet se encuentra deshabilitado por defecto y no debe habilitarse su uso. Adicionalmente para prevenir su uso, se puede forzar el uso de SSH en todas las interfaces.

```
Router(config)#line vty 0 10
Router(config)#transport Input ssh
```

Se recomienda desactivar SNMP.

```
Router(config)# no snmp-server
```

6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

La administración remota del equipo se debe realizar aplicando medidas adicionales de seguridad. Por ejemplo, desde la red interna de la organización, restringiendo las direcciones IP origen de la conexión, aplicando capas de protección adicionales como comunicaciones a través de canales VPN con un nivel de cifrado adecuado, etc.

La administración remota se realiza empleando el protocolo 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 4096 bits.
- Los algoritmos de AES-128-CBC y AES-256-CBC
- Las funciones SHA2-256, SHA2-512.

Para aplicar dichas configuraciones se ejecutarán los siguientes comandos:

```
Domain-name
Router(config)# ip domain name <domain-name>
Se configura SSH versión 2
Router(config)# ip ssh version 2
Timeout de espera de respuesta del cliente
Router(config)# ip ssh time-out 60
```

```
Numéro de intentos de autenticación
Router(config)# ip ssh authentication-retries 2
Grupo Diffie-Hellman 16
Router(config)# ip ssh dh min size 4096
Longitud de la clave RSA
Router(config)# crypto key generate rsa modulus 4096
Configuración de AES-128-CBC y AES-256-CBC como algoritmos de cifrado
Router(config)# ip ssh server algorithm encryption aes256-cbc aes128-
cbc
Configuración de hmac-sha2 como algoritmo MAC. Para establecer esta
configuración, utilice el siguiente comando:
Router(config)# ip ssh server algorithm mac hmac-sha512 hmac-sha2-256
```

Por último, se deben configurar los valores de rekey del protocolo SSH para renovar las claves tras una hora o 1 Gb de volumen.

```
Router(config)#Ip ssh rekey time 60 volume 1
```

6.7 GESTIÓN DE CERTIFICADOS

El producto emplea certificados X.509 para autenticar a los pares IPsec. Deberán seguirse los siguientes pasos generales:

a) Crear un CSR (*Certificate Signing Request*). Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:

   i. Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.
   ii. Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.

b) Conectar con la CA correspondiente empleando una conexión IPsec.

c) Almacenar los certificados en el almacenamiento local.

d) Configurar la revocación de certificados mediante CRL o OCSP, según se desee.

e) Finalmente configurar el certificado para su uso con IKE.

Para el último paso, una vez configurados los certificados correspondientes, deberán ejecutarse los siguientes comandos.

```
Router(config)# crypto isakmp policy 1
Router(config)# authentication rsa-sig
```

El detalle de configuración de los certificados se puede consultar en la guía de Cisco: IPSEC [REF9] - PKI [REF10].

6.8 SINCRONIZACIÓN

Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

El producto dispone de un reloj hardware y reloj software. Sin embargo, se recomienda la configuración NTP con autenticación, empleando siempre SHA2.

```
Router(config)#ntp server <IP del servidor>
Router(config)#ntp authenticate
Router(config)#ntp authentication-key number <key-id> sha2 <key>
```

El detalle de configuración de NTP se puede consultar en la guía de Cisco: NTP [REF11].

6.9 ACTUALIZACIÓN DEL SOFTWARE

El producto permite verificar la versión del software instalada empleando el siguiente comando.

```
Router#show version
```

Una vez descargada la imagen de software, se debe transferir desde la ubicación de descarga al dispositivo Cisco **empleando el protocolo SCP**. No se deben emplear TFTP o FTP.

```
Puesto_de_gestion#     scp     <software     image>     admin@<IP     de
GigabitEthernet0/0>:<software image>
```

Una vez en el disco del producto, se debe calcular el hash SHA512 del fichero descargado y verificar que coincide con el mostrado en la página de descarga.

```
Router#verify sha512 <software image>
```

Finalmente, emplear el siguiente comando para cargar la nueva imagen de software.

```
Router#install add  <software image> activate commit
```

Verificar la nueva versión de software instalada con el comando siguiente.

```
Router#Show version
```

Las actualizaciones de Software pueden consultarse en el Software Center de Cisco [REF17]

6.10 AUTO-CHEQUEOS

El producto es capaz de realizar comprobaciones automáticas del comportamiento de sus funciones durante el arranque o reinicio del dispositivo.

El test automático incluye los siguientes apartados:

- Test automáticos en el encendido:
  - Test de integridad del *firmware/software.*
  - Test de respuesta conocida:
    - AES.
    - RNG/DRBG.
    - HMAC.
    - RSA.
    - SHA-1/256/512.
- Autocomprobaciones condicionales (se ejecutan periódicamente durante la ejecución normal del sistema):
  - Test de generación continua de números aleatorios para DRBG.
  - Test de generación continua de números aleatorios para el motor de entropía.
  - Test de consistencia *RSA Pairwise*.
  - Test contra bypass.

Adicionalmente, durante las comprobaciones se inhibe el acceso a los algoritmos criptográficos. También, estas pruebas se realizan después de inicializar los módulos criptográficos, pero antes de inicializar las interfaces externas; esto previene las complicaciones de seguridad derivadas de introducir datos antes de completar los test y entrar en el modo de operación seguro.

Si ocurriese un error durante estas pruebas, el módulo criptográfico implicado forzaría a la plataforma a reiniciarse junto con el sistema operativo y el módulo en cuestión. Esta operación garantiza que no se puedan utilizar los algoritmos criptográficos a no ser que todos los test tengan un resultado satisfactorio.

El producto permite también invocar las pruebas criptográficas bajo demanda con el comando siguiente:

```
Router#test crypto self-test
```

Si ocurre un error durante alguna prueba, se genera un log de sistema con el código SELF_TEST_FAILURE.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

El producto genera mensajes de logging que se pueden distribuir a la consola, a la sesión VTY (SSH), a un búfer o a un servidor syslog. No se recomienda el uso de la consola.

El logging en la sesión SSH se puede activar y desactivar. Para asegurar que se encuentra habilitado, emplear el siguiente comando:

```
Router#terminal monitor
```

La configuración del búfer está activa por defecto y se pueden visualizar los mensajes de la siguiente forma:

```
Router#show logging
```

El detalle sobre los mensajes de log se puede consultar en la guía de Cisco: Embedded syslog Manager [REF13].

En caso de alcanzarse el límite de almacenamiento, los logs más recientes sobrescribirán a los más antiguos. Se puede aumentar el tamaño del búfer a un valor que depende de la memoria disponible en el producto.

```
Router#show proc memory sorted
Router(config)#logging buffer <x bytes>
```

Por defecto, el producto no guarda un timestamp junto a los registros de auditoría, por lo que será necesario configurar esta funcionalidad. Para ello, emplear el comando service timestamps log datetime, de tal forma que se salven los registros con una marca de tiempo del momento en el que se genera el mensaje.

En caso necesario, un usuario administrador puede eliminar los registros manualmente empleando el siguiente comando:

```
Router#clear log
```

Es necesario configurar el producto para no almacenar las contraseñas en claro en los registros de auditoría. Para ello, emplear los siguientes comandos:

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-cfg)# logging enable
Router(config-archive-log-cfg)#  hidekeys        (las  contraseñas  se
almacenan con SHA-256)
```

```
Router(config-archive)#end
```

Debido al espacio limitado de almacenamiento local, se recomienda realizar el envío de los registros a un servidor de auditoría externo mediante syslog. Para ello, emplear el siguiente comando incluyendo la dirección IP del servidor al que se quieren enviar.

```
Router(config)#logging host <IP del servidor>
```

Será necesario configurar un túnel IPsec para proteger la conexión con el servidor syslog y evitar el envío de los logs en claro. Consultar el apartado 6.12 CONFIGURACIÓN DE IPSEC, para ver el detalle de configuración del protocolo.

Se puede configurar el tipo de mensajes generados, en función al nivel definido. Este se puede modificar empleando los *comandos* *Logging monitor <level> y logging trap <level>*, para el acceso SSH y el servidor syslog respectivamente. A continuación, se muestra el detalle de los distintos niveles disponibles.

```
Router(config)#logging buffered ?
  <0-7>              Logging severity level
  <4096-2147483647>  Logging buffer size
  alerts             Immediate action needed           (severity=1)
  critical           Critical conditions               (severity=2)
  debugging          Debugging messages                (severity=7)
  discriminator      Establish MD-Buffer association
  emergencies        System is unusable                (severity=0)
  errors             Error conditions                  (severity=3)
  filtered           Enable filtered logging
  informational      Informational messages            (severity=6)
  notifications      Normal but significant conditions (severity=5)
  warnings           Warning conditions                (severity=4)
  xml                Enable logging in XML to XML logging buffer
  <cr>               <cr>
```

El detalle de configuración de los registros de auditoría se puede consultar en la guía de Cisco: System Message Logs [REF14].

6.12 CONFIGURACIÓN DE IPSEC

El producto proporciona capacidades de conexión IPsec. El detalle de configuración se puede consultar en la guía de IPsec - [REF10].

La fase de negociación de IPSEC se debe realizar con IKEv2 y no con IKEv1. Las configuraciones necesitan Transformaciones de IPsec y Transformaciones de IKEv2.

```
Router(config)#no crypto isakmp enable
```

A continuación, se muestran los parámetros recomendados.

- Transformaciones de IPsec:

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Transformación AH	No se recomienda el uso de AH. Se recomienda utilizar ESP con mecanismos de integridad modernos.		
Transformación de cifrado ESP	esp-aes 128 esp-aes 192 esp-aes 256	esp-gcm 256	Sí. Se recomienda utilizar GCM (ya que incorpora

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
	esp-gcm 128 esp-gcm 192 esp-gcm 256		por defecto integridad y autenticidad).
Transformación de autenticación ESP	esp-sha-hmac esp-sha256-hmac esp-sha512-hmac	esp-sha256-hmac esp-sha512-hmac	Sí. Se recomienda no usar esp-sha-hmac
Transformación de compresión IP	comp-lzs	Todas	No.
Modos	tunnel (por defecto) transport	Todas	**Se recomienda usar el modo de túnel.**
Tiempo de vida	Segundos y/o KB	Las SA de IPsec (fase 2) se recomienda limitarlas a: - 100.000 - 200.000 KB - 28.800 segundos (8 horas) Las IKE SA (fase 1) se recomienda limitarlas a: - 86.400 segundos (24 horas)	Sí.

Tabla 1. Transformaciones IPsec

- Transformaciones de IKEv2:

TIPOS DE TRANSFORMACIÓN PARA IKEV2	OPCIONES DE TRANSFORMACIÓN PARA IKEV2	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Autenticación	rsa-sig (por defecto) rsa-encr pre-share	rsa-sig (con una longitud de clave igual o superior a 3072 bits) rsa-encr (nonces cifrados con RSA con una longitud de clave igual o superior a 3072 bits)	Sí. **Se recomienda usar RSA y no claves precompartidas**.
Cifrado	des (por defecto) 3des aes 128 aes 256	aes 128 aes 256	Sí. **Deberá utilizarse AES**.
Grupo	1, 2, 5, 14, 15, 16, 19, 20, 24	15, 16, 19 o 20.	Sí. **Deberán utilizarse los grupos 15, 16, 19 o 20**.
Hash	sha (por defecto sha 1) sha256 sha384	sha256 (permitido por respetar tamaño mínimo de salida de 256 bits) sha384 (permitido por respetar tamaño mínimo de salida de 256 bits)	Sí**. Deberá utilizarse SHA256 o SHA384**.
Tiempo de vida	Número de segundos	El límite recomendado para IKEv2 SA (SA de IKE	Sí

TIPOS DE TRANSFORMACIÓN PARA IKEV2	OPCIONES DE TRANSFORMACIÓN PARA IKEV2	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
		fase 1) es de 24 horas (86400 segundos).	

Tabla 2. Transformaciones IKEv2

El detalle de configuración del protocolo IPsec se puede consultar en la guía de Cisco: IPSEC [REF9] - PKI [REF10]. Se deberán configurar los parámetros recomendados.

6.13 COPIAS DE SEGURIDAD

Se recomienda realizar copias de seguridad periódicas de la configuración del producto. Estas se llevan a cabo salvando la configuración del Router en un servidor externo, empleando SCP. No se deben emplear otros protocolos de intercambio de ficheros.

```
Puesto_de_gestion# scp admin@<IP de GigabitEthernet0/0>:startup-config
conf-date
```

También es posible salvar la configuración en el propio producto o en un servidor externo, mediante la funcionalidad Archive que permite mantener las versiones de configuración. Se pueden guardar en el Router o en un servidor externo, empleando SCP siempre.

```
Router(config)# archive
Router(config-archive)# path scp:<path>
```

Se recomienda siempre almacenar las copias de seguridad en una ubicación externa para mayor seguridad.

El detalle de configuración de la función Archive se puede consultar en la guía de Cisco: Archive.

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* REF19) 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 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación del paquete recibido	☐	☐	
Verificación de la integridad de la descarga	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de usuarios	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Configuración del banner de acceso	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Configuración de servicios no empleados	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de SSHv2	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
SINCRONIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
COPIAS DE SEGURIDAD			
Creación de los backups	☐	☐	
AUDITORÍA			

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración del envío de los logs a un servidor *Syslog*	☐	☐	

Tabla 3. Checklist

9 REFERENCIAS

[REF1] Software Lifecycle Support Statement - IOS XE
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xe-16/bulletin-c25-2378701.html

[REF2] Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
https://www.cisco.com/c/en/us/td/docs/routers/sl_using_policy/b-sl-using-policy/introduction.html

[REF3] Cisco ESR6300 Hardware Installation Guide
https://www.cisco.com/c/en/us/td/docs/routers/embedded/6300/hardware/tech-guide/b-cisco-embedded-service-6300-series-router-hardware-technical-guide/m-implementation-options.html

[REF4] Command Reference
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/command/command-references.html

[REF5] System Management Configuration Guide
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management.html

[REF6] Security Configuration Guide: Secure Operation in FIPS Mode
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/secure_operation_in_fips_mode.html

[REF7] AAA, Radius, Tacacs+.

AAA
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/configuring_authentication.html

Radius
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/configuring_radius.html

Tacacs+
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/configuring_tacacs_.html

[REF8] Security Configuration Guide, Cisco IOS XE Cupertino 17.9.x: Controlling Router Access with Passwords and Privilege Levels
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/controlling_switch_access_with_passwords_and_privilege_levels.html

[REF9] IPsec Configuration Guide
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/configuring_ipsec.html

[REF10] PKI
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/sec/b_1712_sec_9300_cg/configuring_authorization_and_revocation_of_certificates_in_a_pki.html

[REF11] NTP
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_bsm-ntp4-mib.html

[REF12] Embedded syslog manager
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_esm-syslog.html

[REF13] Configuration Change Notification and Logging
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_cm-config-logger-0.html

[REF14] Configuration Versioning
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_cm-config-versioning.html

[REF15] https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

[REF16] Cisco Embedded Services Router (ESR) 6300 v17.12
Common Criteria Configuration Guide Version 1.0 30/05/2024

[REF17] Upgrades
https://software.cisco.com/download/home

[REF18] Security Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches) - Configuring RadSec [Support] - Cisco

[REF19] https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&keyword=catalyst&sort=-day_sir#~Vulnerabilities

10 ABREVIATURAS

AAA	Autenticación, Autorización y Auditoría
AES	Advanced Encryption Standard
AH	Authentication Header
CA	Autoridad de Certificación
CC	Common Criteria
CCN	Centro Criptológico Nacional
CLI	Interfaz de Línea de Comandos
CPD	Centro de Proceso de Datos
CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y la Comunicación
CRL	Lista Revocación Certificados
CSR	Certificate Signing Request
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DBRGDRBG	Digital Random Number Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
ENS	Esquema Nacional de Seguridad.
ESP	Encapsulating Security Payload
ESR	Embedded Service Router
FIPS	Estándares Federales de Procesamiento de la Información
HMAC	Hash-based Message Authentication Code
HTTP/HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IOS-XE	Internetwork Operating System - Extended Enterprise
IP	Internet Protocol
IPsec	Internet Protocol Security
MAC	Message Authentication Code
MKA	MACsec Key Agreement
NTP	Network Time Protocol
NVRAM	Non-Volatile Random Access Memory
OCSP	Online Certificate Status Protocol

PKI	Public Key Infrastructure
RADSEC	RADIUS over TLS
RFC	Request for Comments
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest–Shamir–Adleman
SA	Security Association
SCP	Secure Copy Protocol
SHA512	Secure Hash Algorithm 512 bits
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHv2	Secure Shell version 2
TACACS+	Terminal Access Controller Access-Control System Plus
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language