centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1450

Procedimiento de Empleo Seguro
Cisco Catalyst 9000 y Catalyst IE3000

Junio 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.13 12:35:23 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-185-7.
Fecha de Edición: julio de 2023

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

ÍNDICE **2**
1. INTRODUCCIÓN **3**
2. OBJETO Y ALCANCE **4**
2.1 PRODUCTOS 4
2.1.1 CATALYST 9000 SERIES 4
2.1.2 CATALYST IE3000 SERIES 6
2.2 SOFTWARE 7
3. ORGANIZACIÓN DEL DOCUMENTO **8**
4. FASE PREVIA A LA INSTALACION **9**
4.1 ENTREGA SEGURA DEL PRODUCTO 9
4.2 ENTREGA SEGURA DEL *SOFTWARE* 9
4.3 ENTORNO DE INSTALACIÓN SEGURO 10
4.4 REGISTRO Y LICENCIAS 10
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 10
5. FASE DE INSTALACIÓN **12**
5.1 USO DE LOS COMANDOS IOS-XE 12
5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA 12
6. FASE DE CONFIGURACIÓN **14**
6.1 GUARDAR CONFIGURACIÓN EN DISCO 14
6.2 MODO DE OPERACIÓN SEGURO 14
6.3 AUTENTICACIÓN 14
6.4 SERVIDORES DE AUTENTICACIÓN 15
6.5 ADMINISTRACIÓN DEL PRODUCTO 15
6.5.1 CONFIGURACIÓN DE ADMINISTRADORES 15
6.5.2 PARÁMETROS DE SESIÓN 16
6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 17
6.7 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 17
6.8 GESTIÓN DE CERTIFICADOS 18
6.9 SINCRONIZACIÓN 18
6.10 ACTUALIZACIÓN DEL *SOFTWARE* 19
6.11 AUTO-CHEQUEOS 19
6.12 AUDITORÍA 20
6.13 COPIAS DE SEGURIDAD 22
6.14 CONFIGURACIÓN DE IPSEC 22
7. FASE DE OPERACIÓN **24**
8. CHECKLIST **25**
9. REFERENCIAS **26**
10. ABREVIATURAS **29**

1. INTRODUCCIÓN

1. Los switches Cisco Catalyst 9000 series y Cisco Catalyst IE3000 series son plataformas que permiten la configuración de funcionalidades de *switching* y *routing*.
2. **Dichos switches han sido cualificados e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC). Se recomienda consultarlo para conocer los modelos concretos y las versiones del sistema operativo cualificadas en cada momento.**

2. OBJETO Y ALCANCE

3. El objeto del presente documento es facilitar la instalación y configuración segura de los switches **Cisco Catalyst 9000 series y Cisco Catalyst IE3000** series ejecutando la versión de **sistema operativo IOS-XE 17**, junto con el aseguramiento del entorno en el que se despliega.

2.1 PRODUCTOS

2.1.1 CATALYST 9000 SERIES

4. Los switches Catalyst 9000 tienen cinco (5) series:
    - Catalyst 9200.
    - Catalyst 9300.
    - Catalyst 9400.
    - Catalyst 9500.
    - Catalyst 9600.
5. Cada serie tiene varios modelos que se distinguen en función del número de puertos, tipo de puertos, ancho de banda, etc. La configuración es la misma en todos los modelos.

Serie	Modelos
Catalyst 9200	C9200-24T C9200-24P C9200-24PB C9200-24PXG C9200-48T C9200-48P C9200-48PL C9200-48PB C9200-48PXG C9200L-24T-4G C9200L-24P-4G C9200L48T-4G C9200L-48P-4G C9200L-48PL-4G C9200L-24T-4X C9200L-24P-4X C9200L-48T-4X C9200L-48P-4X C9200L-48PL-4X C9200L-24PXG-4X C9200L-48PXG-4X C9200L-24PXG-2Y C9200L-48PXG-2Y

Serie	Modelos
	C9200-NM-4G C9200-NM-4X C9200-NM
Catalyst 9300	C9300-24T C9300-48T C9300-24P C9300-48P C9300-24U C9300-48U C9300-24UX C9300-48UX C9300-48UN C9300-24UB C9300-24UXB C9300-48UB C9300-24H C9300-48H C9300-24S C9300-48S C9300L-24T-4G C9300L-24T-4X C9300L-48T-4G C9300L-48T-4X C9300L-24P-4G C9300L-24P-4X C9300L-48P-4G C9300L-48P-4X C9300L-48PF-4G C9300L-48PF-4X C9300L-24UXG-4X C9300L-24UXG-2Q C9300L-48UXG-4X C9300L-48UXG-2Q C9300-NM-4G C9300-NM-8X C9300-NM-2Q C9300-NM-4M C9300-NM-2Y
Catalyst 9400	C9404R C9407R C9410R C9400-SUP-1XL C9400-SUP-1 C9400-SUP-1XL-Y C9400-LC-24S C9400-LC-48S C9400-LC-24XS C9400-LC-48P

Serie	Modelos
	C9400-LC-48T C9400-LC-48U C9400-LC-48UX C9400-LC-48H
Catalyst 9500	C9500-12Q C9500-24Q C9500-40X C9500-16X C9500-32C C9500-32QC C9500-24Y4C C9500-48Y4C C9500-NM-8X C9500-NM-2Q
Catalyst 9600	C9606R C9600-SUP-1 C9600-LC-24C C9600-LC-48YL C9600-LC-48TX C9600-LC-24S

2.1.2 CATALYST IE3000 SERIES

6. Los switches Catalyst IE3000 tienen cuatro (4) series:
    - Catalyst IE3200.
    - Catalyst IE3300.
    - Catalyst IE3400.
    - Catalyst IE3400H.
7. Cada serie tiene varios modelos que se distinguen en función del nombre de puertos, tipo de puertos, ancho de banda, etc. La configuración es la misma en todos los modelos.

Series Catalyst IE	Modelos
Catalyst IE3200	IE-3200-8T2S-E IE-3200-8P2S-E
Catalyst IE3300	IE-3300-8T2S IE-3300-8P2S IE-3300-8T2X IE-3300-8U2X
Catalyst IE3400	IE-3400-8T2S-E IE-3400-8T2S-A IE-3400-8P2S-E IE-3400-8P2S-A

Series Catalyst IE	Modelos
Catalyst IE3400H	IE-3400H-8FT-E IE-3400H-16FT-E IE-3400H-24FT-E IE-3400H-8T-E IE-3400H-16T-E IE-3400H-24T-E

2.2 SOFTWARE

8. Los switches llevan un Software Cisco IOS-XE cuyo nombre tiene la nomenclatura 17.X.Y.

Ilustración 1. Versiones de Software.

9. La *Major Release* (17) tiene varias *Minor Release*: 17.1, 17,2, ..., 17.6.
10. Cada *Minor Release* tiene varias *Maintenance Release*: 17.6.1, 17.6.2, etc.
11. Este documento se refiere a cualquier *Minor Release* de las versiones 17.6 y 17.3.
12. Más información sobre las imágenes IOS-XE se encuentra en la guía de Cisco: IOS-XE [REF1].

3. ORGANIZACIÓN DEL DOCUMENTO

13. Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar durante la fase previa a la instalación del producto.

b) Apartado **5**. En este apartado se recogen aspectos y recomendaciones a considerar durante la 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.

e) Apartado **8**. En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

f) Apartado **9**. En este apartado se incluye el listado de documentos referenciados a lo largo del documento.

g) Apartado **10**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACION

4.1 ENTREGA SEGURA DEL PRODUCTO

14. 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, se debe contactar con el proveedor del equipo (Cisco o un distribuidor autorizado). Se deben seguir los siguientes pasos:

    - Antes de abrir el paquete donde fue entregado el producto, **comprobar que el paquete contenga la serigrafía y logo de Cisco.**
    - **Comprobar que el paquete no ha sido abierto** y después vuelto a sellar examinando la cinta que lo cierra.
    - **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.
    - 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.
    - **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*

15. 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 PRODUCTOS**.
16. El *software* está disponible en el *Software Center* de Cisco:

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

17. 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**.

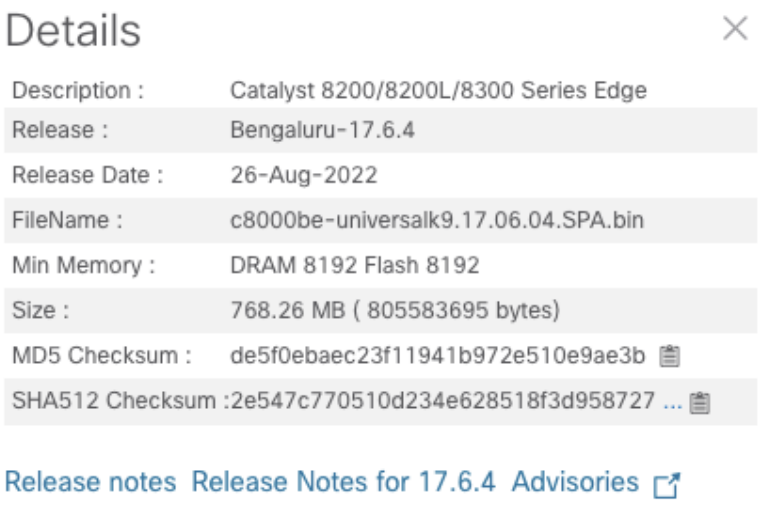

Ilustración 1. Verificación hash descargas

4.3 ENTORNO DE INSTALACIÓN SEGURO

18. 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

19. El sistema de licencias se llama *Smart Licensing* y cada cliente tiene una cuenta en el portal de Cisco. Con esta cuenta, la organización dispone del *Smart Software Manager*.
20. 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.
21. 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**.
22. El detalle de configuración de licencias se puede consultar en la guía *Cisco: Licenses* [REF2].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. 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 switch.
- 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 switch.
- Servidor Radius AAA.
- Servidor Syslog.
- Servidor NTP.
- Servidor de monitorización para la recepción de los mensajes Syslog del switch.

5. FASE DE INSTALACIÓN

24. La instalación física del producto se debe realizar las instrucciones de las guías de *Cisco: Hardware Installation Guide* [REF3].

25. 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.

5.1 USO DE LOS COMANDOS IOS-XE

26. Antes de configurar el producto, se necesita entender el formato de los comandos y los modos *Exec*. Se puede encontrar información al respecto en la guía de *Cisco: Using the Cisco IOS Command-Line Interface [REF4].*

5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA

27. 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 Configuración Dialog*. Este menú permite introducir la configuración inicial.

28. 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 **6.5.1 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 **6.5.1 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.

29. 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. Se exige el empleo de RSA con claves de 4096 bits en el protocolo SSH, así como su versión 2.

```
Switch#conf t
Switch(config)# hostname <Switch>
Switch(config-if)#interface GigabitEthernet0/0
Switch(config)# interface GigabitEthernet0/0
```

```
Switch(config-if)#ip address <IP> <Mask>
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#
Switch(config)# ip route vrf Mgmt-vrf 0.0.0.0 0.0.0.0 <Gateway>
Switch(config)# ip domain name <domain-name>
Switch(config)# ip ssh version 2
Switch(config)# ip ssh time-out 60
Switch(config)# ip ssh authentication-retries 2
Switch(config)# ip ssh dh min size 4096
Switch(config)# crypto key generate rsa modulus 4096
Switch(config)# service password-encryption
Switch(config)# username <user-admin> password <password>
Switch(config)# enable secret <password>
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default local
Switch(config)# aaa authorization exec default local
Switch(config)#exit
Switch# copy run start
```

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

6. FASE DE CONFIGURACIÓN

6.1 GUARDAR CONFIGURACIÓN EN DISCO

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

```
Switch# copy run start
```

32. 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.

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

```
Switch# show running-config
```

6.2 MODO DE OPERACIÓN SEGURO

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

```
Switch(config)#fips authorization-key <key 128 bits>
```

35. Adicionalmente, se recomienda activar el *logging* extendido mediante:

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

36. Se necesita un *reload* del equipo para activarlo.

```
Switch# copy run start
Switch# reload
```

37. Verificar que se ha activado correctamente con los comandos siguientes.

```
Switch# show fips status
```

38. El detalle sobre la configuración el modo seguro se puede consultar en la guía de *Cisco: FIPS* [REF7].

6.3 AUTENTICACIÓN

39. 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 **6.5.1 CONFIGURACIÓN DE ADMINISTRADORES**.
    - Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración y gestión de dichos servidores, ver apartado **6.4 SERVIDORES DE AUTENTICACIÓN**.

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

```
Switch(config)# aaa new-model
```

```
Switch(config)# aaa authentication login default local
Switch(config)# aaa authorization exec default local
```

6.4 SERVIDORES DE AUTENTICACIÓN

41. El producto permite la integración con distintos servidores de autenticación externos:
    - Servidores de tipo RADIUS.
    - Servidores de tipo TACACS+.
42. Se deberán seguir las siguientes recomendaciones en caso de emplear alguna de las integraciones:
    - 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.
    - Para servidores de tipo RADIUS, se deberá configurar el producto para emplear RADSEC. Se puede consultar el detalle de los pasos a seguir en el siguiente enlace.
43. 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:

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

44. El detalle de configuración de los servidores de autenticación se puede consultar en la guía de *Cisco: AAA* [REF12].

6.5 ADMINISTRACIÓN DEL PRODUCTO

6.5.1 CONFIGURACIÓN DE ADMINISTRADORES

45. Cada usuario administrador del producto dispone de un usuario y contraseña para acceder al sistema. Adicionalmente, la contraseña *Enable secret* permite acceder a configuración y comandos avanzados.
46. Para configurar la contraseña *Enable secret* y almacenarla empleando SHA-256, utilizar el siguiente comando:

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

47. **Se debe emplear el siguiente comando para almacenar cifradas con SHA-256 las contraseñas de los usuarios**.

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

48. **Se deberá configurar la política de contraseñas segura**. Para ello emplear los siguientes comandos, de tal forma que deban contener al menos 12 caracteres y un

tiempo de validez de 60 días y emplear al menos una letra minúscula, una mayúscula, un número y un carácter especial.

```
Switch(config)#aaa common-criteria policy <nombre-policy>
Switch(config-cc-policy)#min-length 12
Switch(config-cc-policy)#lifetime day 60
Switch(config-cc-policy)# lower-case 1
Switch(config-cc-policy)# upper-case 1
Switch(config-cc-policy)# special-case 1
Switch(config-cc-policy)# numeric-count 1
Switch(config-cc-policy)#exit
Switch(config)# username <user-admin> common-criteria-policy <nombre-policy> password <password>
```

49. 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.
50. Para crear un nuevo usuario, se debe emplear el siguiente comando:

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

51. Para cada usuario se debe definir el nombre de usuario, su contraseña de acuerdo a 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.
52. 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:

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

53. 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**.
54. El detalle sobre la gestión de usuarios y permisos se puede consultar en la guía de *Cisco: Controlling Switch Access with Passwords and Privilege Levels* [REF8].

6.5.2 PARÁMETROS DE SESIÓN

55. **Se debe configurar el tiempo de inactividad de las sesiones.** Para configurarlo el tiempo en 5 minutos en la consola y en la *line vty* (para SSH):

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

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

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

57. Una vez bloqueado un usuario, se deberá desbloquear manualmente.

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

58. **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.

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

6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

```
Switch(config)#no ip http server
Switch(config)#no ip https server
```

60. 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.

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

61. Se recomienda desactivar SNMP.

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

6.7 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

62. 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.

63. Adicionalmente, los siguientes parámetros están configurados por defecto:

    - Los algoritmos de cifrado AES-128, AES-192 y AES-256.
    - Las funciones SHA2-256, SHA2-512.

```
Domain-name
Switch(config)# ip domain name <domain-name>
se configura SSH versión 2
Switch(config)# ip ssh version 2
Timeout de espera de respuesta del cliente
```

```
Switch(config)# ip ssh time-out 60
Numéro de intentos de autenticación
Switch(config)# ip ssh authentication-retries 2
Grupo Diffie-Hellman 16
Switch(config)# ip ssh dh min size 4096
Longitud de la clave RSA
Switch(config)# crypto key generate rsa modulus 4096
```

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

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

6.8 GESTIÓN DE CERTIFICADOS

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

- Crear un CSR (*Certificate Signing Request*). **Se deberá utilizar uno de los siguientes parámetros para la creación del certificado**:
  - Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.
  - Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.
- Conectar con la CA correspondiente empleando una conexión IPsec.
- Almacenar los certificados en el almacenamiento local.
- Configurar la revocación de certificados mediante CRL o OSCP, según se desee.
- Finalmente configurar el certificado para su uso con IKE.

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

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

67. El detalle de configuración de los certificados se puede consultar en la guía de *Cisco: IPSEC* [REF10] - *PKI* [REF11].

6.9 SINCRONIZACIÓN

68. **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*.

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

```
Switch(config)#ntp server <IP del servidor>
Switch(config)#ntp authenticate
```

```
Switch(config)#ntp authentication-key number <key-id> sha2 <key>
```

70. El detalle de configuración de NTP se puede consultar en la guía de *Cisco: NTP* [REF13].

6.10 ACTUALIZACIÓN DEL *SOFTWARE*

71. Las actualizaciones de Software pueden consultarse en el *Software Center* de Cisco:

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

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

```
Switch#Show version
```

73. 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>
```

74. 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**.

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

75. Finalmente, emplear el siguiente comando para cargar la nueva imagen de *Software.*

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

76. Verificar la nueva versión de *Software* instalada con el comando siguiente.

```
Switch#Show version
```

77. El detalle sobre la actualización del producto se puede consultar en la guía de *Cisco: Upgrade* [REF6].

6.11 AUTO-CHEQUEOS

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

79. El test automático incluye los siguientes apartados:

- Test automáticos en el encendido:
  - Test de integridad del *firmware/software.*
  - Test de respuesta conocida:
    - AES.
    - DRBG.
    - HMAC.
    - ECC (IOS 16.6).
    - FFC (IOS 16.6).

        - RSA.
        - SP 800-56B RSA *key wrap/unwrap* (IOS 16.6).
        - 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.

80. Se comprueban todos los módulos (*hardware* y *software*). Adicionalmente, durante las comprobaciones se inhibe el acceso a los algoritmos criptográficos. También, estos test 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.
81. Si ocurriese un error durante estos test, 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.
82. El producto permite también invocar los test criptográficos bajo demanda con el comando siguiente:

```
Switch#test crypto self-test
```

83. Si ocurre un error durante algún test, se genera un log de sistema con el código *SELF_TEST_FAILURE*.

6.12 AUDITORÍA

84. 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.
85. El *logging* en la sesión SSH se puede activar y desactivar. Para asegurar que se encuentra habilitado, emplear el siguiente comando.

```
Switch#terminal monitor
```

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

```
Switch#show logging
```

87. El detalle sobre los mensajes de log se puede consultar en la guía de *Cisco: Upgrade* [REF15].

88. 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.

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

89. 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.

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

```
Switch#clear log
```

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

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

92. 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.

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

93. **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 **6.14 CONFIGURACIÓN DE IPSEC**, para ver el detalle de configuración del protocolo.

94. 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.

```
Switch(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>
```

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

6.13 COPIAS DE SEGURIDAD

96. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto**. Estas se llevan a cabo salvando la configuración del switch 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
```

97. 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 switch o en un servidor externo, empleando SCP siempre.

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

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

99. El detalle de configuración de la función *Archive* se puede consultar en la guía de *Cisco: Archive* [REF15].

6.14 CONFIGURACIÓN DE IPSEC

100. El producto proporciona capacidades de conexión IPsec. **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.

101. A continuación, se muestran los parámetros recomendados para Ipsec:

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Transformación AH	*ah-sha-hmac*	ah-sha-hmac (solo se permite SHA-1 para funciones HMAC).	No.
Transformación de cifrado ESP	*esp-3des* *esp-aes* *esp-des* *esp-null* *esp-seal*	**ESP-AES** (permitido con claves iguales o mayores a 128 bits)	**Sí. Se recomienda utilizar AES.**

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Transformación de autenticación ESP	*esp-md5-hmac* *esp-sha-hmac*	**esp-sha-hmac** (solo se permite SHA-1 para funciones HMAC).	**Sí. No se debe utilizar MD5.**
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 (SAs de fase 2 en IKEv2) pueden ser restringidas dentro del rango 100-200 MB (100,000 a 200,000 KB). El límite de tiempo recomendado para las SA de IKEv2 es inferior a 8 horas (28800 segundos).	Sí.

102. A continuación, se muestran los parámetros recomendados para 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 fase 1) es de 24 horas (86400 segundos).	Sí

103. El detalle de configuración del protocolo IPsec se puede consultar en la guía de *Cisco: IPSEC* [REF10] - *PKI* [REF11]. **Se deberán configurar los parámetros recomendados.**

7. FASE DE OPERACIÓN

104. 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.
- Seguimiento de las alertas de seguridad de Cisco (*Security Advisories*) y, si es necesario, aplicar un parche (*Minor Release* o *Maintenance Release*).
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos contra borrados y modificaciones no autorizados y solamente el personal de seguridad autorizado deberá 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			
Configuración del envío de los logs a un servidor *Syslog*	☐	☐	
OPERACIÓN			
Mantenimiento del control de acceso	☐	☐	
Comprobaciones periódicas del hardware y software	☐	☐	
Seguimiento de las alertas de seguridad	☐	☐	
Mantenimiento de los registros de auditoría	☐	☐	

9. REFERENCIAS

REF1 *IOS-XE*

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-xe-16/bulletin-c25-2378701.html

REF2 *Licenses*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/qsg/b_Smart_Licensing_QuickStart/b_Smart_Licensing_QuickStart_chapter_00.html

https://www.cisco.com/c/en/us/td/docs/routers/sl_using_policy/b-sl-using-policy/introduction.html

REF3 *Hardware Installation guide*

Cisco Catalyst 9200 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/hardware/install/b-c9200-hig.html

Cisco Catalyst 9300 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b_c9300_hig.html

Cisco Catalyst 9400 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/hardware/install/b_c9400_hig.html

Cisco Catalyst 9500 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig.html

Cisco Catalyst 9600 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/hardware/install/b_9600_hig.html

Cisco Catalyst 9800 Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-40/installation-guide/b-wlc-ig-9800-40.html

Cisco Catalyst IE3x00 Rugged Series Switches Hardware Installation Guide

https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/Hardware/installation/guide/b_ie3x00_hig/b_ie2k-ip67-hig_chapter_01.html

REF4 *Using the Cisco IOS Command-Line Interface*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17/fundamentals-xe-17-book/m_cf-cli-basics.html

REF5 *Basic System Management Configuration Guide*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17/fundamentals-xe-17-book/m_cf-config-overview-0.html

REF6 *Upgrade*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

Apartado "Upgrading the Switch Software"

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/release_notes/ol-17-6-9300.html#id_67613

REF7 *FIPS*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-6/configuration_guide/sec/b_176_sec_9200_cg/secure_operation_in_fips_mode.html

REF8 *Controlling Switch Access with Passwords and Privilege Levels*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sec/b_176_sec_9300_cg/controlling_switch_access_with_passwords_and_privilege_levels.html

REF9 *SSH*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book/sec-secure-shell-v2.html

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book/sec-secure-shell-algorithm-ccc.html

REF10 *IPSEC*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-17/sec-sec-for-vpns-w-ipsec-xe-17-book-cat8000.html

REF11 *PKI*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-pki-overview.html

REF12 *AAA*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sec/b_176_sec_9300_cg/configuring_authentication.html

REF13 *NTP*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/syst-mgmt/b-system-management/m_bsm-time-calendar-set.html

REF14 *System Message Logs*

Cisco Catalyst 9000 series y Cisco Catalyst IE3x00 series

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sys_mgmt/b_176_sys_mgmt_9300_cg/configuring_system_message_logs.html

REF15 *Archive*

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-17/config-mgmt-xe-17-book/cm-config-versioning.html

REF16 *Error and System Messages*

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-6-x/b-system-message-guide-17-6-x.html

10.ABREVIATURAS

AAA	Autenticación, Autorización y Auditoría
AH	*Authentication Header*
CA	Autoridad de Certificación
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CLI	Interfaz de Línea de Comandos
CRL	Lista Revocación Certificados
DBRG	*Digital Random Number Generator*
DH	*Diffie-Hellman*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
ENS	Esquema Nacional de Seguridad
ESP	*Encapsulating Security Payload*
FIPS	Estándares Federales de Procesamiento de la Información
HTTP/HTTPS	*Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
MKA	*MACsec Key Agreement*
NTP	*Network Time Protocol*
NVRAM	*Non-Volatile Random Access Memory*
PKI	*Public Key Infrastructure*
RFC	*Request for Comments*
ROM	*Read-Only Memory*
SA	*Security Association*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
USB	*Universal Serial Bus*
VPN	*Virtual Private Network*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL