# Guía de Seguridad de las TIC
# CCN-STIC 1012

# Procedimiento de Empleo Seguro
# Cisco Switches IOS-XE




Noviembre 2026

Edita:

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

Fecha de Edición: Noviembre de 2026

**LIMITACIÓN DE RESPONSABILIDAD**

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

**AVISO LEGAL**

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

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

# ÍNDICE

**1 INTRODUCCIÓN ..... 3**
**2 OBJETO Y ALCANCE ..... 3**
**3 ORGANIZACIÓN DEL DOCUMENTO ..... 3**
**4 FASE PREVIA A LA INSTALACIÓN ..... 4**
4.1 ENTREGA SEGURA DEL PRODUCTO ..... 4
4.2 CONSIDERACIONES PREVIAS ..... 4
4.3 COMPONENTES DEL ENTORNO DE OPERACIÓN ..... 5
**5 FASE DE INSTALACIÓN ..... 6**
**6 FASE DE CONFIGURACIÓN ..... 7**
6.1 MODO DE OPERACIÓN SEGURO ..... 7
6.2 AUTENTICACIÓN ..... 8
6.3 ADMINISTRACIÓN DEL PRODUCTO ..... 8
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA ..... 8
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES ..... 9
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS ..... 11
6.5 MACSEC Y MKA ..... 13
6.6 AUDITORÍA ..... 14
6.6.1 REGISTRO DE EVENTOS ..... 14
6.6.2 ALMACENAMIENTO REMOTO ..... 16
6.7 COPIAS DE SEGURIDAD ..... 19
**7 FASE DE OPERACIÓN ..... 20**
**8 REFERENCIAS ..... 21**
**9 ABREVIATURAS ..... 22**

# ÍNIDCE DE TABLAS

Tabla 1. Componentes ..... 5

# 1 INTRODUCCIÓN

Los switches Cisco con IOS-XE son switches de capa de acceso de tipo empresarial para despliegues de sucursales. Los conmutadores se utilizan para conectar varios dispositivos, como ordenadores, puntos de acceso inalámbricos, impresoras y servidores en la misma red dentro de un edificio o campus. Un switch o conmutador permite que los dispositivos conectados compartan información y se comuniquen entre sí, y es un componente clave de cualquier red.

# 2 OBJETO Y ALCANCE

Esta guía se desarrolla para los switches de Cisco que corren el software IOS-XE 17.12.

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 [CPSTIC].

# 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

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

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

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

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

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

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

## 4.2 CONSIDERACIONES PREVIAS

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

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

a) 9600 baud

b) 8 data bits

c) 1 stop bit

d) No parity

e) None (flow control)

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

## 4.3 COMPONENTES DEL ENTORNO DE OPERACIÓN

Para funcionar en la configuración evaluada, el producto requiere los componentes operativos que se enumeran en la siguiente tabla:

| Componente | Uso |
|---|---|
| Servidor Syslog | Cualquier servidor syslog al que el producto transmita mensajes syslog a través de TLS. |
| Consola local | Cualquier consola que esté conectada directamente al producto a través del puerto serie y que utilice el administrador para facilitar la administración del producto. Se puede acceder a esta interfaz y está disponible de forma local incluso en caso de que se produzca un fallo en la red. |
| Cliente SSHv2 | Cualquier estación de trabajo (PC) que utilice el administrador del producto para llevar a cabo tareas de administración a través de canales protegidos por SSHv2. Se puede utilizar cualquier cliente SSH que sea compatible con SSHv2. |
| Par Media Access Control security (MACsec) | Cualquier par MACsec con el que el producto participe en comunicaciones MACsec. Un par MACsec puede ser cualquier dispositivo que admita comunicaciones MACsec. |

**Tabla 1. Componentes**

En cuanto al servidor de Syslog, se puede utilizar cualquiera al que se pueda acceder a través de TLS 1.2. Instale el servidor Syslog siguiendo las instrucciones de instalación que se incluyen con el software del servidor Syslog escogido.

# 5 FASE DE INSTALACIÓN

Si va a encender el producto, coloque el interruptor de encendido en la posición ON. Preste atención a los ventiladores; debería oírlos funcionar inmediatamente. Asegúrese de que el LED de OK de la fuente de alimentación esté en verde y de que el LED de FAIL no esté encendido.

En caso de que el LED de FAIL esté encendido, deberá contactar con el soporte técnico de Cisco.

Los indicadores LED del panel frontal proporcionan información sobre la alimentación, la actividad y el estado, lo cual resulta útil durante el arranque.

Observe el proceso de inicialización. Cuando finalice el arranque del sistema (el proceso tarda unos segundos), el producto comenzará a inicializarse.

```
Loading from ROMMON with a System Image in Bootflash
```

Una vez finalizada la inicialización, aparecerá lo siguiente:

```
Press RETURN to get started!
```

# 6 FASE DE CONFIGURACIÓN

## 6.1 MODO DE OPERACIÓN SEGURO

Se le pedirá al administrador que acceda al cuadro de diálogo de configuración inicial. Introduzca "no" y confirme que desea cancelar la instalación automática. La configuración de este documento seguirá unos pasos manuales para realizar la configuración inicial.

```
Would you like to enter the initial configuration dialog?
[yes/no]: no

Would you like to terminate autoinstall? [yes]:yes

Press RETURN to get started!
```

Acceda al modo privilegiado EXEC:

```
SWITCH> enable
```

Entre en la configuración de la teminal:

```
SWITCH# configure terminal
```

Configure un nombre de dominio:

```
SWITCH(config)# hostname mySWITCH
```

Configure la habilitación de *Enable Secret Password*:

```
SWITCH(config)# enable algorithm-type scrypt secret <the
unencrypted (cleartext) 'enable' secret>
```

Configure una interfaz de gestión Gigabit Ethernet:

```
SWITCH(config)# do show running-config vrf
```

Si no se ha creado automáticamente un interfaz de gestión siga los pasos que se indican a continuación para crear una:

```
SWITCH(config)# vrf definition Mgmt-vrf
SWITCH(config-vrf)# address-family ipv4
SWITCH(config-vrf)# exit-address-family
SWITCH(config-vrf)# address-family ipv6
SWITCH(config-vrf)# exit-address-family
SWITCH(config-vrf)# exit
```

Configure una ruta predeterminada para conectarte al producto y una ruta predeterminada para la interfaz de gestión.

```
SWITCH(config)# ip route <prefix> <mask> <default gateway/next hop>
SWITCH(config)# ip route vrf Mgmt-vrf <prefix> <mask> <default gateway/next hop>
```

Configure la consola para requerir autenticación mediante usuario y contraseña.

```
SWITCH(config)# line console 0
SWITCH(config-line)# login authentication default
```

Guarde la configuración inicial en la NVRAM ejecutando el comando "wr mem" o "copy system:running-config nvram:startup-config".

En el modo EXEC con privilegios, escriba:

```
SWITCH# config terminal
```

Introduzca la clave de autorización para el modo FIPS:

```
SWITCH(config)# fips authorization-key
12345678901234567890123456789012
```

Salga del modo de configuración y volver al modo EXEC privilegiado:

```
SWITCH(config)# end
```

## 6.2 AUTENTICACIÓN

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

- **Autenticación de usuarios mediante credenciales locales.** Este mecanismo se utiliza para la autenticación de usuarios, tanto administradores como no administradores, que acceden al producto mediante los mecanismos de acceso locales habilitados. La autenticación se basa en credenciales compuestas por nombre de usuario y contraseña.
- **Autenticación mediante PKI.** Este mecanismo se utiliza para la autenticación de las sesiones SSH establecidas con el producto. La autenticación se realiza mediante certificados y claves asociadas a una Infraestructura de Clave Pública (PKI), cuando se utiliza este método de acceso.

## 6.3 ADMINISTRACIÓN DEL PRODUCTO

### 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

Para la administración del producto se usará la línea de comandos, tanto de manera local como de forma remota mediante SSHv2.

### 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

Los administradores deben definir la política "aaa common-criteria policy" y aplicarla a cada cuenta local. De este modo, se garantiza que, al cambiar la contraseña, se solicite la contraseña anterior antes de permitir la introducción de una nueva, y que las contraseñas tengan un mínimo de 12 caracteres.

Cree la política de contraseñas de seguridad AAA y acceda al modo de política de configuración de criterios comunes.

```
SWITCH(config)# aaa common-criteria policy <policy name>
```

Establezca la longitud mínima de las contraseñas en 12 caracteres:

```
SWITCH(config-cc-policy)# min-length 12
```

Establezca un periodo de validez de la contraseña de 60 días.

```
SWITCH(config-cc-policy)# lifetime day 60
```

Cuando caduque la contraseña, se le pedirá al usuario que la cambie.

Escriba "exit" para volver al modo de configuración principal:

```
SWITCH(config-cc-policy)# exit
```

Para verificar la política de contraseñas de Common Criteria, introduzca:

```
SWITCH(config)# do show aaa common-criteria policy <policy
name>
```

Para habilitar el modelo de control de acceso de autenticación, autorización y contabilidad (AAA), ejecute el siguiente comando:

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

Para configurar la autenticación predeterminada al iniciar sesión de modo que utilice la autenticación local, utilice el siguiente:

```
SWITCH(config)# aaa authentication login default local
```

Para configurar el método de autorización predeterminado de modo que utilice credenciales locales, utilice el siguiente comando:

```
SWITCH(config)# aaa authorization exec default local
```

El administrador debe crear y utilizar una nueva cuenta a la que se le aplique la política de contraseñas de Common Criteria.

Para añadir una cuenta de administrador, utilice el comando “username” en el modo de configuración. Deberá especificar la política de contraseñas de Common Criteria:

```
SWITCH(config)# username <user> privilege 15 common-criteria-
policy <policy name> algorithm-type <scrypt> secret password
<the unencrypted (cleartext) password for the user>
```

Las contraseñas no deben contener palabras comunes, caracteres repetidos ni patrones fáciles de adivinar. Siga estas pautas a la hora de crear contraseñas seguras:

a) La contraseña no debe contener el nombre de usuario asociado, y el nombre de usuario no debe escribirse al revés.

b) Los caracteres de la contraseña no deben repetirse más de tres veces seguidas.

c) La contraseña no debe ser “cisco”, “ocsic”, “admin”, “nimda” ni ninguna variante obtenida cambiando las mayúsculas y minúsculas de las letras que la componen, ni sustituyendo la “i” por “1”, “|” o “!”, ni sustituyendo la “o” por “0”, ni sustituyendo la “s” por “$”.

d) La contraseña debe estar compuesta por letras mayúsculas, letras minúsculas, números y caracteres especiales (! @ # $ % ^ & * ( ) ; : “ ‘ | + - = . , / \ > < _ ` ~ { } ). La contraseña debe tener una longitud mínima de 12 caracteres.

Para bloquear los intentos de ataque por fuerza bruta, es necesario configurar el controlador para que detecte los errores de autenticación. El administrador debe definir el número máximo de intentos fallidos de inicio de sesión en un periodo de tiempo determinado. Además, el administrador debe definir el periodo de tiempo durante el cual se bloqueará la cuenta infractora.

Especifique el número máximo de intentos fallidos (3) en un intervalo de tiempo (65535 segundos) y el intervalo de tiempo (300 segundos) durante el cual se bloqueará la cuenta infractora.

```
SWITCH(config)# aaa authentication rejected 3 in 65535 ban
300
```

Salga del modo de configuración y vuelva al modo EXEC privilegiado:

```
SWITCH(config)# end
```

Todas las sesiones en la consola local y en el puerto auxiliar deben cerrarse una vez transcurrido el intervalo de tiempo de inactividad de la sesión especificado por el administrador. Siga los pasos que se indican a continuación para configurar dicho intervalo.

Acceda al modo de configuración de línea de la consola.

```
SWITCH(config)# line console 0
```

Especifique el valor del tiempo de espera en 5 minutos.

```
SWITCH(config-line)# exec-timeout 5
```

Acceda al modo de configuración de línea del puerto auxiliar:

```
SWITCH(config-line)# line aux 0
```

Especifique el valor del tiempo de espera en 5 minutos.

```
SWITCH(config-line)# exec-timeout 5
```

## 6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Para configurar la interfaz SSH, siga los siguientes pasos.

En el modo EXEC con privilegios, escriba:

```
SWITCH# configure terminal
```

Especifique el nombre de dominio del host correspondiente al producto:

```
SWITCH(config)# ip domain name cisco.com
```

Genere una clave criptográfica RSA para SSH. Asigna un nombre, por ejemplo, “SSH-KEY”.

```
SWITCH(config)# crypto key generate rsa label SSH-KEY modulus
3072
```

Asigne el par de claves a SSH:

```
SWITCH(config)# ip ssh rsa keypair-name SSH-KEY
```

Habilite SSHv2. Esto también desactivará el uso de SSHv1.

```
SWITCH(config)# ip ssh version 2
```

Configure el intercambio de claves del servidor SSH:

```
SWITCH(config)# ip ssh server algorithm kex diffie-hellman-
group14-sha1
```

Especifique los algoritmos de cifrado permitidos y el orden en que deben admitirse:

```
SWITCH(config)# ip ssh server algorithm encryption aes256-
gcm@openssh.com aes128-gcm@openssh.com
```

Especifique los algoritmos de código de autenticación de mensajes (MAC) permitidos y el orden en que deben ser compatibles:

```
SWITCH(config)# ip ssh server algorithm mac hmac-sha2-256
```

El administrador debe configurar el producto para la autenticación mediante clave pública SSH. Esto es necesario para evitar una posible situación en la que los errores al introducir la

contraseña por parte de los administradores remotos provoquen que no se pueda acceder a la cuenta de administrador durante un periodo de tiempo temporal. Durante el periodo de bloqueo definido, el producto permite que la cuenta de administrador inicie sesión de forma remota mediante la autenticación mediante clave pública SSH.

Antes de continuar, tenga a mano la clave pública SSH. La clave pública se genera desde su cliente SSH.

Configure algoritmos de clave pública para la autenticación basada en clave pública de SSH:

```
SWITCH(config)# ip ssh server algorithm publickey ssh-rsa
```

Configure los algoritmos de la clave del host para la autenticación basada en clave pública de SSH:

```
SWITCH(config)# ip ssh server algorithm hostkey rsa-sha2-256
rsa-sha2-512
```

Acceda al modo de configuración de clave pública:

```
SWITCH(config)# ip ssh pubkey-chain
```

Especifique la cuenta de usuario de administrador que se va a configurar para la autenticación mediante clave pública SSH:

```
SWITCH(conf-ssh-pubkey-user)# username admin
```

Acceda al modo de configuración de datos de clave pública:

```
SWITCH(conf-ssh-pubkey-user)# key-string
```

Pegue la parte de datos de la clave pública generada por el cliente SSH. Nota: Si es necesario, puede dividir la clave en varias líneas.

```
SWITCH(conf-ssh-pubkey-data)# <paste your public key>
```

Vuelva al modo de configuración pulsando “exit” tres veces:

```
SWITCH(conf-ssh-pubkey-data)# exit
SWITCH(conf-ssh-pubkey-user)# exit
SWITCH(conf-ssh-pubkey)# exit
```

Las conexiones SSH con las mismas claves de sesión no pueden utilizarse durante más de una hora ni superar un gigabyte de datos transmitidos. En los pasos que se indican a continuación, configure los valores de renovación de claves en función del tiempo y del volumen (en kilobytes).

```
SWITCH(config)# ip ssh rekey time 59
SWITCH(config)# ip ssh rekey volume 1000000
```

Acceda al modo de configuración de línea para configurar los ajustes de la línea del terminal virtual 0 4:

```
SWITCH(config)# line vty 0 4
```

Especifique las líneas vty 0-4 para utilizar únicamente SSH:

```
SWITCH(config-line)# transport input ssh
```

Especifique un valor de tiempo de espera para las líneas VTY 0-4:

```
SWITCH(config-line)# exec-timeout 5
```

Escriba “exit”:

```
SWITCH(config-line)# exit
```

Acceda al modo de configuración de líneas para configurar las líneas de terminal virtual 5-15:

```
SWITCH(config)# line vty 5 15
```

Especifique las líneas vty para utilizar únicamente SSH:

```
SWITCH(config-line)# transport input ssh
```

Especifique un valor de tiempo de espera para las líneas VTY 5-15:

```
SWITCH(config-line)# exec-timeout 5
```

Salga del modo de configuración y vuelve al modo EXEC privilegiado:

```
SWITCH(config)# end
```

Escriba “show running-config” y compruebe que todas las líneas vty incluyan “transport input SSH” y tengan un valor de tiempo de espera configurado.

```
SWITCH# show running-config
```

Los siguientes protocolos de gestión remota (HTTP, HTTPS, SNMP) no se han probado en la configuración evaluada y deben desactivarse:

```
SWITCH(config)# no ip http server
SWITCH(config)# no ip http secure-server
SWITCH(config)# no snmp-server
```

## 6.5 MACSEC Y MKA

El producto autentica y cifra los paquetes que intercambia con un par MACsec. El protocolo de acuerdo de claves MACsec (MKA) proporciona las claves de sesión necesarias y gestiona las

claves de cifrado requeridas para proteger los datos que intercambian los pares. De forma predeterminada, MACsec está desactivado y no hay políticas MKA configuradas en el producto.

Para garantizar que los datos CAK de MACsec estén protegidos contra la divulgación no autorizada, siga estos pasos.

En el modo EXEC con privilegios, escriba:

```
SWITCH# config terminal
```

Cree el siguiente applet de Embedded Event Manager para la configuración en ejecución:

```
SWITCH(config)#event manager applet SHOW_RUN_NO_KEY_STRING
SWITCH(config-applet)# event cli pattern "show run" sync yes
SWITCH(config-applet)# action 1.0 cli command "enable"
SWITCH(config-applet)# action 2.0 cli command "show run |
exclude key-string"
SWITCH(config-applet)# action 3.0 puts "$_cli_result"
SWITCH(config-applet)# action 4.0 set $_exit_status "0"
SWITCH(config-applet)# exit
```

Cree el siguiente applet de Embedded Event Manager para la configuración de inicio:

```
SWITCH(config)#event manager applet
SHOW_STARTUP_NO_KEY_STRING
SWITCH(config-applet)# event cli pattern "show start" sync
yes
SWITCH(config-applet)# action 1.0 cli command "enable"
SWITCH(config-applet)# action 2.0 cli command "show start |
exclude key-string"
SWITCH(config-applet)# action 3.0 puts "$_cli_result"
SWITCH(config-applet)# action 4.0 set $_exit_status "0"
SWITCH(config-applet)# end
```

## 6.6 AUDITORÍA

### 6.6.1 REGISTRO DE EVENTOS

La función de notificación y registro de cambios de configuración realiza un seguimiento de los cambios realizados en la configuración en ejecución del software de Cisco. Siga estos pasos para asegurarse de que se registren todos los eventos de auditoría necesarios.

Asegúrese de que el registro esté activado:

```
SWITCH(config)#logging on
```

Acceda al modo de configuración del archivo:

```
SWITCH(config)# archive
```

Acceda al submodo de configuración de registro:

```
SWITCH(config-archive)# log config
```

Habilite el registrador de configuración:

```
SWITCH(config-archive-log-cfg)# logging enable
```

Oculte la contraseña al mostrar los comandos registrados:

```
SWITCH(config-archive-log-cfg)# hidekeys
```

Introduzca el número de entradas que desea conservar. El rango va de 1 a 1000; el valor predeterminado es 100. Seleccione 1000.

```
SWITCH(config-archive-log-cfg)# logging size 1000
```

Habilite el envío de comandos registrados al servidor syslog remoto.

```
SWITCH(config-archive-log-cfg)# notify syslog
```

Salga del modo de configuración y volver al modo EXEC privilegiado

```
SWITCH(config-archive-log-cfg)# end
```

Configure el tamaño del búfer de registro local. El tamaño del búfer de registro local se puede configurar en un rango de [4096-2147483647] bytes. Nota: Se recomienda no establecer un tamaño de búfer demasiado grande, ya que el producto podría quedarse sin memoria para otras tareas. Se recomienda establecerlo en al menos 150000000

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

Si el espacio de almacenamiento local para los datos de auditoría está lleno, el producto sobrescribirá el registro de auditoría más antiguo para dejar espacio al nuevo.

Para generar registros de los intentos fallidos de inicio de sesión, escriba:

```
SWITCH(config)# login on-failure log
```

Para incluir el año en la marca de tiempo de todos los registros de auditoría del registro de mensajes, escriba:

```
SWITCH(config)# service timestamps log datetime year
```

Para generar registros de los intentos de inicio de sesión correctos, introduzca:

```
SWITCH(config)# login on-success log
```

Establezca el nivel de registro del servidor syslog en “debug”:

```
SWITCH(config)# logging trap debugging
```

Para generar todos los eventos de auditoría necesarios, es preciso introducir los siguientes comandos de depuración cada vez que se reinicie el producto:

```
SWITCH# debug crypto pki validation
SWITCH# debug crypto pki transaction
SWITCH# debug crypto pki api
SWITCH# debug crypto pki messages
SWITCH# debug crypto engine
SWITCH# debug ssl openssl errors
```

Para generar los eventos de auditoría adicionales necesarios, es preciso configurar los siguientes comandos:

```
SWITCH(config)# ip ssh logging events
SWITCH(config)# crypto logging session
```

Los eventos de auditoría se pueden consultar en la CLI introduciendo:

```
SWITCH# show logging
```

Los eventos de auditoría incluyen la siguiente información:

a) Fecha y hora.

b) Acción realizada.

c) Resultado del evento.

d) Usuario que ha realizado la acción.

A continuación, se muestra un ejemplo de un registro de auditoría cuando se realiza un intento de autenticación local en la consola:

```
<189>618: C9407RSUP2: Aug 17 2023 17:14:12: %SEC_LOGIN-5
LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL]
[localport: 0] at 13:14:12 EDT Thu Aug 17 2023
```

### 6.6.2 ALMACENAMIENTO REMOTO

El producto utiliza TLS para transmitir de forma segura los datos de auditoría generados a un servidor syslog externo. El producto requiere un servidor de auditoría (syslog) en el entorno operacional para transmitir mensajes syslog a través de TLS. El producto valida el certificado X.509 presentado por el servidor syslog remoto, pero no requiere un certificado X.509 para el propio producto. El administrador deberá asegurarse de que el servidor syslog remoto esté

correctamente configurado con un certificado X.509 válido. Si el certificado del servidor syslog remoto no está correctamente configurado con un certificado X.509 válido, el producto no establecerá la conexión con el servidor syslog. En este caso, el administrador deberá solucionar el problema antes de continuar.

Cree un modo de mapa de certificados.

```
SWITCH(config)# crypto pki certificate map <attribute map tag> | <sequence-number>
```

Especifique el campo SAN (nombre alternativo del sujeto) junto con el criterio de coincidencia "igual a" y el valor con el que debe coincidir para el servidor syslog remoto. Los siguientes ejemplos muestran los valores con los que debe coincidir para peer.cisco.com y la dirección IP del par:

```
SWITCH(ca-certificate-map)# alt-subject-name eq < peer.cisco.com>
SWITCH(ca-certificate-map)# alt-subject-name eq < IP Address of Peer in SAN field>
```

Escriba "exit" para volver al modo de configuración principal.

```
SWITCH(ca-certificate-map)# exit
```

Cree, configure y autentique el punto de confianza raíz:

```
SWITCH(config)# crypto pki trustpoint <root trustpoint name>
SWITCH(ca-trustpoint)# enrollment terminal pem
SWITCH(ca-trustpoint)# revocation-check none
SWITCH(ca-trustpoint)# match eku server-auth
SWITCH(ca-trustpoint)# exit
SWITCH(config)# crypto pki authenticate <root trustpoint name>
```

Introduzca el certificado de la CA raíz codificado en base 64. Termine con una línea en blanco o con la palabra "quit" en una línea sola. Cuando se te solicite, escribe "yes" para aceptar el certificado de la CA. El producto debería responder con:

```
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Cree, configure y autentique el punto de confianza intermedio:

```
SWITCH(ca-trustpoint)# crypto pki trustpoint <subordinate
 trustpoint name>
SWITCH(ca-trustpoint)# enrollment terminal pem
SWITCH(ca-trustpoint)# revocation-check none
SWITCH(ca-trustpoint)# chain-validation continue <root
trustpoint name>
SWITCH(ca-trustpoint)# match certificate <attribute map tag>
SWITCH(ca-trustpoint)# match eku server-auth
SWITCH(ca-trustpoint)# exit
```

Autentique el punto de confianza:

```
SWITCH(config)# crypto pki authenticate <subordinate
trustpoint name>
```

Introduzca el certificado de la CA raíz codificado en base 64. Termine con una línea en blanco o con la palabra "quit" en una línea sola. Cuando se te solicite, escribe "yes" para aceptar el certificado de la CA. El producto debería responder con:

```
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Configure los puntos de confianza para que comprueben las revocaciones mediante la lista CRL:

```
SWITCH(config)# crypto pki trustpoint <root trustpoint name>
SWITCH(ca-trustpoint)# revocation-check CRL
SWITCH(ca-trustpoint)# crl cache none
SWITCH(ca-trustpoint)# match key-usage cRLSign
SWITCH(ca-trustpoint)# exit
SWITCH(config)# crypto pki trustpoint <subordinate trustpoint
name>
SWITCH(ca-trustpoint)# revocation-check CRL
SWITCH(ca-trustpoint)# crl cache none
SWITCH(ca-trustpoint)# match key-usage cRLSign
SWITCH(ca-trustpoint)# exit
```

Cree un perfil TLS para Syslog:

```
SWITCH(config)# logging tls-profile <profile name>
```

Configure la versión de TLS en 1.2

```
SWITCH(config-tls-profile)# tls-version TLSv1.2
```

Configure los siguientes conjuntos de cifrado:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

Escriba “exit” para volver al modo de configuración principal.

```
SWITCH(config-tls-profile)# exit
```

Utilizando la interfaz Ethernet de gestión VRF, asegúrese de que su servidor de nombres DNS contenga una entrada para el nombre de dominio completo (FQDN) del servidor Syslog.

```
SWITCH(config)# ip name-server vrf Mgmt-vrf <IP Address of
DNS Server>
```

## 6.7 COPIAS DE SEGURIDAD

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
```

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>
```

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

# 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 (CISCOSEC *Security Advisories*) 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


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

DOC https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html#anchor244

CISCOSEC https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities

# 9 ABREVIATURAS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CA | Certification Authority |
| CAK | Connectivity Association Key |
| CLI | Command Line Interface |
| CPSTIC | Catálogo de Productos y Servicios STIC |
| DNS | Domain Name System |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| ENS | Esquema Nacional de Seguridad |
| FQDN | Fully Qualified Domain Name |
| GCM | Galois/Counter Mode |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol Secure |
| LED | Light Emitting Diode |
| MAC | Media Access Control |
| PC | Personal Computer |
| RSA | Rivest–Shamir–Adleman |
| SAN | Subject Alternative Name |
| SHA | Secure Hash Algorithm |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| TLS | Transport Layer Security |
| USB | Universal Serial Bus |