centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1464

Procedimiento de Empleo Seguro
Cisco Embedded Services 9300 & 3300 Series Switches (ESS9300 & ESS3300). versión IOS-XE 17.9

Febrero 2025

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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-200-2
Fecha de Edición: febrero de 2025

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
2026.01.16 07:45:16 +01'00'

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

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 4
2.1 SOFTWARE 4
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE PREVIA A LA INSTALACION 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTREGA SEGURA DEL SOFTWARE 6
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 9
6 FASE DE CONFIGURACIÓN 10
6.1 USO DE LOS COMANDOS IOS-XE 10
6.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA 10
6.3 GUARDAR CONFIGURACIÓN EN DISCO 11
6.4 ACTUALIZACIÓN DEL SOFTWARE 11
6.5 MODO DE OPERACIÓN SEGURO 12
6.6 ADMINISTRACIÓN DEL PRODUCTO 12
6.6.1 CONFIGURACIÓN DE ADMINISTRADORES 12
6.6.2 ADMINISTRACIÓN REMOTA CON SSH 14
6.6.3 PROTOCOLS HTTP, HTTPS, TELNET 14
6.7 GESTIÓN DE CERTIFICADOS 14
6.8 SERVIDORES DE AUTENTICACIÓN 16
6.9 SINCRONIZACIÓN 17
6.10 AUTO-CHEQUEOS 17
6.11 SNMP 18
6.12 AUDITORÍA 18
6.13 REGISTRO DE EVENTOS 19
6.14 IPSEC 19
6.15 BACKUP 19
7 FASE DE OPERACIÓN 21
8 REFERENCIAS 22
9 ABREVIATURAS 25

1 INTRODUCCIÓN

1. El objetivo de este documento es proporcionar un Procedimiento de Empleo Seguro de switches **Cisco Embedded Services 3300 Series Switches** y **Cisco Embedded Services 9300 Series Switches** ejecutando la versión de sistema operativo **IOS-XE 17.9**
2. Esta guía indica las configuraciones cuando es necesario y referencias a la documentación de Cisco.

2 OBJETO Y ALCANCE

3. El objetivo es poner en conocimiento del administrador de los switches los mecanismos de seguridad necesarios para proteger los sistemas de información y comunicaciones que empleen en sus centros de datos enrutadores de las familias anteriormente mencionadas. Con este conocimiento, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de estas categorías de enrutadores.
4. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del switch, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo con las políticas vigentes en la organización.

2.1 SOFTWARE

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

Ilustración 1. Nomenclatura versiones

1. La *Major Release* (17) tiene varias *Minor Release*: 17.1, 17,2, ..., 17.9.
2. Cada *Minor Release* tiene varias *Maintenance Release*: 17.9.1, 17.9.2, etc.
3. Este documento se refiere a cualquier *Minor Release* de las versiones 17.9.
4. Más información sobre las imágenes IOS-XE se encuentra en la guía de Cisco: IOS-XE [REF1].

3 ORGANIZACIÓN DEL DOCUMENTO

6. Este documento se compone de los siguientes apartados:

   a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

   b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   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 INSTALACION

4.1 ENTREGA SEGURA DEL PRODUCTO

7. El switch debe ser examinado para comprobar que no ha sido manipulado durante su entrega siguiendo los siguientes pasos:

   a) Antes de abrir el paquete donde fue entregado el switch, compruebe que el paquete contenga la serigrafía y logo de Cisco. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

   b) Compruebe que el paquete no ha sido abierto y después vuelto a sellar fijándose en la cinta que lo cierra. Si el paquete parece haber sido abierto y después sellado de nuevo, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

   c) Compruebe que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado). Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.

   d) Preste atención al número de serie del switch especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja, se debe corresponder con el número de serie del dispositivo. Por tanto, compruebe que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

   e) Compruebe que el pedido fue enviado por el proveedor esperado (Cisco o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. Comprobar también que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. 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.

   f) Una vez que el paquete ha sido abierto, inspeccione el dispositivo. Compruebe que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

4.2 ENTREGA SEGURA DEL SOFTWARE

8. El switch se entrega con un software instalado. No obstante, puede que no sea la versión del software recomendada, en cuyo caso el switch deberá actualizarse.

9. El software está disponible en el "Software Center" de Cisco:

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

10. Antes de descargar el software en el puesto de gestión se apunta el checksum SHA512.

11. Ejemplo: En la captura de pantalla abajo, se puede localizar el checksum SHA-512 de la versión 17.6.4 de un Catalyst 9200.

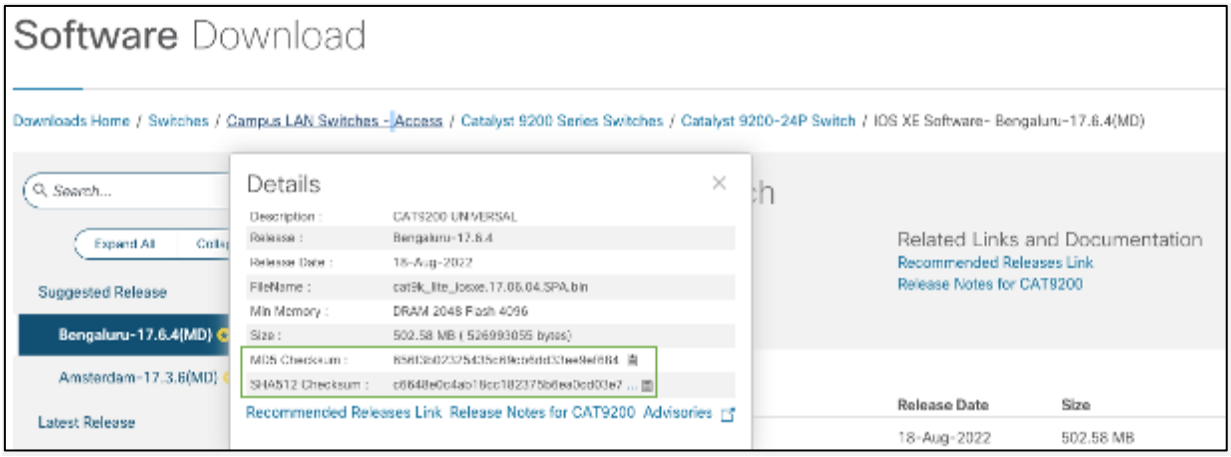

Ilustración 2. Checksum publicado

12. Una vez descargado en el puesto de gestión, se calcula el checksum del Software y se compara con el checksum apuntado. Si los hashes no concuerdan, significa que un fallo ha ocurrido durante la transferencia. Se volverá a descargar el software
13. La instalación del nuevo Software se detalla más adelante en este documento.
14. Aquí hay ejemplos de los detalles para estos productos en IOS-XE 17.9.5:

Modelo	Nombre de imagen	Hash (SHA512 Cheksum)
ESS-3300-NCP	ess3x00-universalk9.17.09.05.SPA.bin	f3bfefa87427dcbf34078a2913dce37ac4e9266638113fae329f207f28fc06432c489383a2d49b815cacb6a897fee03cab529f0167d98dcf0997ee6b1342cc68
ESS-3300-CON	ess3x00-universalk9.17.09.05.SPA.bin	f3bfefa87427dcbf34078a2913dce37ac4e9266638113fae329f207f28fc06432c489383a2d49b815cacb6a897fee03cab529f0167d98dcf0997ee6b1342cc68
ESS-3300-24T-NCP	ess3x00-universalk9.17.09.05.SPA.bin	f3bfefa87427dcbf34078a2913dce37ac4e9266638113fae329f207f28fc06432c489383a2d49b815cacb6a897fee03cab529f0167d98dcf0997ee6b1342cc68
ESS-3300-24T-CON	ess3x00-universalk9.17.09.05.SPA.bin	f3bfefa87427dcbf34078a2913dce37ac4e9266638113fae329f207f28fc06432c489383a2d49b815cacb6a897fee03cab529f0167d98dcf0997ee6b1342cc68
ESS-9300-10X-E	ie9k_iosxe.17.09.05.SPA.bin	c7d7710d983ea9014348a7364c6e8fe3835093390c564e05716e5745e1559b0c490a6d08354d6bffcac6fa70d3b6de00413f34139d8b445cb0b814f01eb40a46

Tabla 1.Checksum para cada binario de IOS-XE 17.9.5

4.3 ENTORNO DE INSTALACIÓN SEGURO

15. Se debe instalar el switch dentro de un Centro de Proceso de Datos (CPD) que cuente con un sistema de control de acceso limitado únicamente a las personas autorizadas. Para asegurarse de que solo estas personas tengan acceso al switch (incluso fuera del horario laboral), la sala que alberga el CPD también debe contar con un sistema de control.

4.4 REGISTRO Y LICENCIAS

16. El sistema de licencias se nombra Smart Licensing.
17. Cada cliente tiene una cuenta Smart Licensing en el portal de Cisco. https://software.cisco.com/
18. Con esta cuenta, el cliente dispone del Smart Software Manager.
19. El switch comunica al Smart Software Manager de manera online (a través de un servidor Proxy) u offline (solución satélite) las informaciones siguientes:
    - uso de funcionalidades que necesitan licencias.
    - números de identificación de productos asociados.
    - números de serie.
20. En el Smart Software Manager se encuentran las licencias compradas.
21. Cuando el Smart Software Manager recibe las informaciones sobre el uso de las funcionalidades necesitando licencias, sube el contador de licencias usadas.
22. De este modo no hace falta instalar licencias en el switch de manera manual.
23. La gestión de licencia se hace siguiendo las instrucciones de la guía de Cisco para licenciamiento [REF2].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

24. El switch requiere los siguientes componentes en el entorno operacional:
    - Puesto de gestión por consola
    - Este puesto hace referencia a cualquier estación de trabajo que permita una conexión por consola serie en el switch.
    - Puesto de gestión con cliente SSH
    - Este 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
    - Este puesto recibe los mensajes Syslog del switch.

5 FASE DE INSTALACIÓN

25. La instalación física del switch se hace siguiendo las instrucciones de las guías de Cisco: Hardware Installation Guide [REF3].

6 FASE DE CONFIGURACIÓN

26. El switch necesita una configuración inicial realizada por el cable de consola entregado con el switch. Esta configuración inicial permite luego una conexión Ethernet por SSHv2 para seguir con la configuración avanzada.

6.1 USO DE LOS COMANDOS IOS-XE

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

28. Para más información consultar la guía de Cisco: Using the Cisco IOS Command-Line Interface [REF4].

6.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA

29. Después de conectar el cable de consola entre el puesto de gestión y el puerto de serie del switch, se arranca el equipo. Aparece un menú configuración del sistema: "System Configuración Dialog". Este menú permite introducir la configuración inicial. Pasar por el menú configuración del sistema es opcional. Se recomienda interrumpirlo para luego configurar la parte inicial por CLI. Este método permite seguir las primeras recomendaciones de seguridad relacionadas con SSHv2 (ejemplo: tamaño de clave RSA a 4096 bits).

30. Para interrumpir el menú de configuración del sistema, se contesta "no" y "yes" a las dos preguntas siguientes.

```
        --- System Configuration Dialog ---

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!

Switch>

Switch>
Switch>en
Switch#
```

31. La configuración inicial siguiente permite una conexión SSHv2 por la red de gestión.

32. La explicación de los comandos se realiza más adelante en el documento.

```
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
```

33. Más información se encuentra en la guía de Cisco: Basic System Management Configuration Guide [REF5].

6.3 GUARDAR CONFIGURACIÓN EN DISCO

34. Para guardar la configuración inicial o cualquier cambio de configuración en la memoria NVRAM, se utiliza el comando siguiente.

```
Switch# copy run start
```

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

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

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

6.4 ACTUALIZACIÓN DEL SOFTWARE

37. El Software se actualiza si la imagen no es la recomendada.

38. El comando siguiente permite verificar la versión.

```
Switch#Show version
```

39. Para transferir la imagen del puesto de gestión al disco duro (bootflash) del switch, se usa SCP. No se recomienda el uso de TFTP o FTP.

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

40. Una vez en el disco del switch, se calcula el checksum del Software y se compara con el checksum apuntado durante la entrega del Software

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

41. Al entrar el comando siguiente, el switch hace un reload.

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

42. El nuevo Sofware se comprueba con el comando siguiente.

```
Switch#Show version
```

43. Más información se encuentra en la guía de Cisco: Upgrade [REF6]

6.5 MODO DE OPERACIÓN SEGURO

44. El switch debe ejecutarse en el modo de operación FIPS.
45. FIPS se implementa con el comando de configuración siguiente.

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

46. Se necesita un reload del equipo para activarlo.

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

47. Se comprueba con los comandos siguientes.

```
Switch# show fips status
```

48. Más información se encuentra en la guía de Cisco: FIPS [REF7]

6.6 ADMINISTRACIÓN DEL PRODUCTO

6.6.1 CONFIGURACIÓN DE ADMINISTRADORES

49. Cada administrador del switch necesita un nombre de usuario y contraseña.
50. Esto permite garantizar la trazabilidad de las acciones realizadas y controlar el acceso.
51. Una contraseña "Enable secret" permite entrar en modo "Enable" para la configuración y comandos avanzados.
52. Se configura 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
```

53. Se configura la contraseña "Enable secret" para almacenar de forma segura las contraseñas con SHA-256.

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

54. Se cifran las contraseñas de los usuarios.

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

55. Las contraseñas deben tener al menos 12 caracteres y un tiempo de validez de 60 días. Se puede forzar el número de minúsculas, números y símbolos especiales de la contraseña.

```
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 <n1>
Switch(config-cc-policy)# upper-case <n2>
Switch(config-cc-policy)# special-case <n3>
Switch(config-cc-policy)# numeric-count <n4>
Switch(config-cc-policy)#exit
Switch(config)# username <user-admin> common-criteria-policy <nombre-policy>
password <password>
```

56. Cada administrador del switch necesita un nombre de usuario y contraseña. Se configura el usuario con el privilegio 1 que es el privilegio por defecto. Los niveles de privilegio de los usuarios están numerados del 1 al 15. El nivel de privilegio 15 tiene acceso a todos los comandos.

57. Los niveles 1-14 se pueden ajustar para que comprendan cualquiera de los comandos disponibles.

58. Si un usuario de nivel 1 quiere pasar al nivel 15, puede entrar el password enable.

```
Switch(config)# username <user-admin> password <password>
```

59. Se bloquea el usuario después de 3 intentos fallidos.

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

60. Una vez un usuario bloqueado, los comandos siguientes permiten desbloqueralo.

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

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

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

62. Se configura el tiempo de inactividad de sesión a 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)#
Switch(config-line)# exec-timeout 5
```

63. Más información se encuentra en la guía de Cisco: Controlling Switch Access with Passwords and Privilege Levels [REF8]

6.6.2 ADMINISTRACIÓN REMOTA CON SSH

64. La administración remota se realiza con el protocolo SSHv2.
65. Se necesita la configuración de los siguientes algoritmos y funciones:
    - SSH versión 2
    - el uso del grupo 16 de DH
    - el tamaño de clave RSA 4096 bits
66. Los parámetros siguientes están configurados por defecto:
    - los algoritmos de cifrado AES-128, AES-192, 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
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
```

67. Más información se encuentra en la guía de Cisco: SSH [REF9]

6.6.3 PROTOCOLS HTTP, HTTPS, TELNET

68. Se desactiva HTTP server y HTTPS.

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

69. Telnet no está permitido por defecto.

6.7 GESTIÓN DE CERTIFICADOS

70. El switch proporciona capacidades de conexión IPsec.
71. La fase de negociación de IPSEC se necesita realizar con IKEv2 y no con IKEv1.
72. La configuraciones necesitan Transformaciones de IPsec y Transformaciones de IKEv2.

73. Transformaciones de 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, el uso de AH es irrelevante para la funcionalidad de seguridad.
Transformación de cifrado ESP	esp-3des (necesita 3 claves de 56 bits sin repetición) esp-aes (permitido para claves mayores o iguales a 128 bits) esp-des (no permitido por tener una longitud de clave de 64 bits con solo 56 bits útiles) esp-null (no se permite trabajar sin criptografía) esp-seal (no aparece en CCN-STIC-807)	esp-aes (permitido con claves iguales o mayores a 128 bits)	Sí. Se recomienda utilizar AES.
Transformación de autenticación ESP	esp-md5-hmac (no permitido) esp-sha-hmac (solo se permite SHA-1 para funciones HMAC).	esp-sha-hmac (solo se permite SHA-1 para funciones HMAC).	Sí. Se recomienda no 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.

Tabla 2. Transformaciones de IPSec

74. Transformaciones de IKEv2:

TIPOS DE TRANSFORMACIÓN PARA IKEV2	OPCIONES DE TRANSFORMACIÓN PARA IKEV2	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Autenticación	rsa-sig (por defecto) (firma RSA 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) pre-share (no permitido)	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) (no permitido) 3des (no permitido por tener una longitud de clave de 64 bits con solo 56 bits útiles) aes 128 (permitido por respetar el tamaño mínimo de clave de 128 bits) aes 256 (permitido por respetar el tamaño mínimo de clave de 128 bits)	aes 128 (permitido por respetar el tamaño mínimo de clave de 128 bits) aes 256 (permitido por respetar el tamaño mínimo de clave de 128 bits)	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) (no permitido) sha256 (permitido por respetar tamaño mínimo de salida de 256 bits) sha384 (permitido por respetar tamaño mínimo de salida de 256 bits)	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

Tabla 3. Transformaciones de IKE v2

75. Más información se encuentra en la guía de Cisco: IPSEC [REF10] - PKI [REF11]

6.8 SERVIDORES DE AUTENTICACIÓN

76. El switch puede estar configurado para la autenticación de usuarios con servidores Radius, Tacacs, Kerberos.

77. En este caso la comunicación irá protegida IPsec.
78. En caso de que falle la comunicación on el servidor externo, se recomienda tener como solución de backup la base de datos local de usuarios.
79. Más información se encuentra en la guía de Cisco: AAA [REF12]

6.9 SINCRONIZACIÓN

80. El switch tiene un reloj hardware y reloj software.
81. Adicionalmente se recomienda la configuración NTP con autenticación.

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

82. Más información se encuentra en la guía de Cisco: NTP [REF13]

6.10 AUTO-CHEQUEOS

83. El switch es capaz de realizar comprobaciones automáticas del comportamiento de sus funciones durante el arranque o reinicio del dispositivo.
84. 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

85. 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. Si ocurriese un error durante estos test, el módulo criptográfico implicado forzaría a la plataforma IOS 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.

86. El switch tiene la capacidad de invocar test criptográficos bajo demanda con el comando siguiente:

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

87. Si ocurre un error durante algún test, se genera un log de sistema llamado SELF_TEST_FAILURE.

6.11 SNMP

88. Se recomienda desactivar SNMP.

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

6.12 AUDITORÍA

89. El switch genera mensajes de logging que se pueden distribuir a la consola, a la sesión VTY (SSH), a un búfer, a un servidor Syslog.
90. No se recomienda el uso de la consola.
91. Se activa y desactiva el logging en la sesión SSH con los comandos siguientes:

```
Switch#terminal monitor

Switch#no terminal monitor
```

92. La configuración del búfer está activa por defecto.
93. Los mensajes se visualizan con el comando siguiente.

```
Switch#show logging
```

94. El búfer local es circular: los mensajes más nuevos sobrescriben los mensajes más antiguos una vez que el búfer está lleno.
95. Se puede aumentar el tamaño del búfer a un valor que depende de la memoria disponible en el switch.

```
Switch#show proc memory sorted

Switch(config)#logging buffer <x bytes>
```

96. Se puede limpiar el búfer.

```
Switch#clear log
```

97. Para que el switch envíe los mensajes de logging a un servidor Syslog, se configura el comando siguiente.

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

98. Se puede configurar el tipo de mensajes según la necesidad del administrador.

```
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>
```

99. Más información se encuentra en la guía de Cisco: System Message Logs [REF14]

6.13 REGISTRO DE EVENTOS

100. El switch puede ser configurado para registrar cualquier evento que occurra por sesión.

```
Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# hidekeys    (las contraseñas no se almacenan
en texto plano)
Switch(config-archive)#end
```

101. Más información se encuentra en la guía de Cisco: System Message Logs [REF14]

6.14 IPSEC

102. Para securizar la comunicación entre switch y servidor IPsec proporciona los siguientes servicios de seguridad de red:

- Confidencialidad de datos: el remitente de IPsec puede cifrar los paquetes antes de transmitirlos a través de una red.
- Integridad de datos: el receptor de IPsec puede autenticar los paquetes enviados por el remitente de IPsec para asegurarse de que los datos no hayan sido alterados durante la transmisión.
- Autenticación del origen de datos: el receptor de IPsec puede autenticar la fuente de los paquetes IPsec enviados. Este servicio depende de la integridad de datos.
- Anti-replay: el receptor de IPsec puede detectar y rechazar paquetes reproducidos.

103. Más información sobre el proceso completo se encuentra en la guía de Cisco: Cisco Embedded Services 3300/9300 Series Switches running IOS XE 17.9 CC Configuration Guide 5.1 IPsec Overview [REF16].

6.15 BACKUP

104. El backup de la configuración en un servidor externo se realiza con SCP

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

105. Otra opción es el uso de la funcionalidad Archive que permite mantener las versiones de configuración. Se pueden guardar en el switch o en un servidor externo.

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

106. Más información se encuentra en la guía de Cisco: Archive [REF15]

7 FASE DE OPERACIÓN

107. Durante la fase de operación del switch, el administrador debe llevar a cabo las siguientes tareas de mantenimiento:

- Mantenimiento del control de acceso al switch.
- 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) y, si es necesario, aplicar un patch (Minor Release o Maintenance Release).
- https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&keyword=catalyst&sort=-day_sir#~Vulnerabilities
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos contra borrados y modificaciones no autorizados, y solamente el personal de seguridad autorizado podrá acceder a ellos.

8 REFERENCIAS

CÓDIGO	REFERENCIA
[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 Embedded Service 9300 series y Cisco Embedded Service 3300 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]	*Cisco Embedded Services 3300 Series Switches Configuration Guide* *https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess3300/software_config/b-cisco-embedded-services-3300-series-configuration.html* *Cisco Embedded Services 3300 Series Hardware Technical Guide* *https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess3300/hardware/b-cisco-embedded-services-3300-series-switches-hardware-technical-guide/m-product-overview.html* *Cisco Embedded Service 9300 Series Switches Configuration Guide* *https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/config/b-cisco-embedded-service-9300-series-switches-configuration-guide.html* *Cisco ESS-9300-10X Embedded Switch Hardware Technical Guide* *https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/hardware/tech-guide/b-cisco-catalyst-ess-9300-10x-embedded-switch-hardware-technical-guide/m-product-overview.html*
[REF4]	*Using the Cisco IOS Command-Line Interface* *Cisco Embedded Service 9300 series y Cisco Embedded Service 3300 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 Embedded Service 9300 series y Cisco Embedded Service 3300 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*

CÓDIGO	REFERENCIA
[REF6]	*Upgrade* *Cisco Embedded Service 3300 series* *Apartado "Upgrading the Switch Software"* *https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_9/17-9-x-release-notes-iot-switch.html* *Cisco Embedded Service 9300 series* *Apartado "Upgrading the Switch Software"* *https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie9300/software/17_9/17-9-x-ie93xx-rn.html*
[REF7]	*FIPS* *Cisco IOS XE Cupertino 17.9.x (Catalyst 9500 switches)* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-9/configuration_guide/sec/b_179_sec_9500_cg/secure_operation_in_fips_mode.html?dtid=osscdc000283*
[REF8]	*Controlling Switch Access with Passwords and Privilege Levels* *Cisco Embedded Service 9300 series y Cisco Embedded Service 3300 series* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-9/configuration_guide/sec/b_179_sec_9300_cg/controlling_switch_access_with_passwords_and_privilege_levels.html?dtid=osscdc000283*
[REF9]	*SSH* *Cisco Embedded Service 9300 series y Cisco Embedded Service 3300 series. Secure Shell Version 2 Support.* *https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-v2-0.html?bookSearch=true*
[REF10]	*IPSEC* *IP Routing Configuration Guide Cisco IOS-XE 17 Chapter: IPv6 Routing: OSPFv3 Authentication Support with IPsec* *https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/ip-routing/b-ip-routing/m_ip6-route-ospfv3-auth-ipsec.html?dtid=osscdc000283*
[REF11]	*PKI* *Cisco Embedded Services 9300 series y Cisco Embedded Services 3300 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*

CÓDIGO	REFERENCIA
[REF12]	*AAA Chapter configuring authentication, security configuration guide 17.9* *https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9600/software/release/17-9/configuration_guide/sec/b_179_sec_9600_cg/configuring_authentication.html*
[REF13]	*NTP* *Cisco Embedded Services 9300 series y Cisco Embedded Services 3300 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 Embedded Service 9300 series* *https://www.cisco.com/c/en/us/td/docs/switches/lan/embedded/ess9300/config/b-cisco-embedded-service-9300-series-switches-configuration-guide/m9-173-sm-log-cg.html* *System Message Guide – IOS XE Cupertino 17.9.x* *https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-9-x/b-system-message-guide-17-9-x.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]	Cisco Embedded Services 3300/9300 Series Switches running IOS XE 17.9 CC Configuration Guide 5.1 IPsec Overview *https://www.niap-ccevs.org/MMO/Product/st_vid11394-agd.pdf*

9 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