

Guía de Seguridad de las TIC CCN-STIC 1454

Procedimiento de Empleo Seguro Routers CISCO ASR9000 y NCS4200 Series



Julio 2023



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-23-286-0.

Fecha de Edición: julio 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

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.

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	3
2. OBJETO Y ALCANCE	4
2.1 PRODUCTOS	4
2.1.1 ASR 900 SERIES.....	4
2.1.2 NCS 4200 SERIES.....	5
3. ORGANIZACIÓN DEL DOCUMENTO	6
4. FASE PREVIA A LA INSTALACION.....	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 ENTREGA SEGURA DEL SOFTWARE.....	7
4.3 ENTORNO DE INSTALACIÓN SEGURO	8
4.4 REGISTRO Y LICENCIAS	8
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	9
5. FASE DE INSTALACIÓN.....	10
5.1 USO DE LOS COMANDOS IOS-XE.....	10
5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA	10
6. FASE DE CONFIGURACIÓN	12
6.1 GUARDAR CONFIGURACIÓN EN DISCO.....	12
6.2 AUTENTICACIÓN.....	12
6.3 SERVIDORES DE AUTENTICACIÓN	12
6.4 ADMINISTRACIÓN DEL PRODUCTO.....	13
6.4.1 CONFIGURACIÓN DE ADMINISTRADORES	13
6.4.2 PARÁMETROS DE SESIÓN	14
6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	14
6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS	15
6.7 GESTIÓN DE CERTIFICADOS.....	15
6.8 SINCRONIZACIÓN	16
6.9 ACTUALIZACIÓN DEL SOFTWARE	16
6.10 AUTO-CHEQUEOS.....	17
6.11 AUDITORÍA	18
6.12 COPIAS DE SEGURIDAD	20
6.13 CONFIGURACIÓN DE IPSEC	20
7. FASE DE OPERACIÓN	22
8. CHECKLIST.....	23
9. REFERENCIAS	24
10. ABREVIATURAS	27

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar una guía o procedimiento de configuración y empleo seguro de la familia de routers ASR900 series y NCS4200 series ejecutando la versión de sistema operativo **IOS-XE 16**.
2. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información.

2. OBJETO Y ALCANCE

3. El objeto del presente documento es facilitar la instalación y configuración segura de los routers **Cisco ASR 900 series** y **Cisco NCS4200 Series** ejecutando la versión de **sistema operativo IOS-XE 16**, junto con el aseguramiento del entorno en el que se despliega. Incluye consejos y recomendaciones sobre la activación o desactivación de servicios y funcionalidades disponibles en el sistema operativo para mejorar la seguridad de la red.
4. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del producto, 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 acorde a las políticas vigentes en la organización.
5. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los conmutadores ASR 9K y NCS4200 Series bajo su responsabilidad.

2.1 PRODUCTOS

6. Los enrutadores llevan un software Cisco IOS-XE cuyo nombre tiene la nomenclatura 16.X.Y.



Ilustración 1. Versiones de *Software*

7. La Major Release (16) tiene varias Minor Release: 16.1, 16.2, ..., 16.9. Cada Minor Release tiene varias Maintenance Release: 16.2.1, 16.2.2, etc. Este documento se refiere a cualquier Minor Release de la versión 16.9. Más información sobre las imágenes IOS-XE se encuentra en la guía de Cisco: IOS-XE [REF1].

2.1.1 ASR 900 SERIES

8. Los routers Cisco ASR 900 tienen cuatro (4) series:
 - ASR 902.
 - ASR 903.
 - ASR 907.
 - ASR 920.

9. 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. **Se deberán configurar empleando la versión IOS-XE 16.9.**

2.1.2 NCS 4200 SERIES

10. Los routers Cisco NCS4200 tienen también cuatro (4) series:

- NCS 4201.
- NCS 4202.
- NCS 4206.
- NCS 4216.

11. 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. **Se deberán configurar empleando la versión IOS-XE 16.9.**

3. ORGANIZACIÓN DEL DOCUMENTO

12. Este documento se compone de los siguientes apartados:

- Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, durante la fase previa a la instalación del producto.
- Apartado **5**. En este apartado se recogen aspectos y recomendaciones a considerar, durante la instalación del producto.
- 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.
- Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- Apartado **8**. En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.
- Apartado **9**. En este apartado se incluye el listado de documentos referenciados a lo largo del documento.
- 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

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

- 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.

14. Si se identifica una incidencia en alguno de los puntos anteriores, se debe contactar con el proveedor del equipo (Cisco Systems o un distribuidor autorizado).




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.**

Details		×
Description :	Cisco ASR 920 Series IOS XE UNIVERSAL-NO PAYLOAD ENCRYPTION	
Release :	Fuji-16.9.8	
Release Date :	01-Sep-2021	
FileName :	asr920-universalk9_npe.16.09.08.SPA.bin	
Min Memory :	DRAM 4096 Flash 2048	
Size :	426.37 MB (447080778 bytes)	
MD5 Checksum :	dd9c888f50be80cb74b5f9d27612159f 	
SHA512 Checksum :	927d69b7d316f16744128faf91b0317f ... 	
Advisories 		




Details		×
Description :	Cisco NCS 4202 IOS XE UNIVERSAL ? WITH PAYLOAD ENCRYPTION	
Release :	Fuji-16.9.8	
Release Date :	01-Sep-2021	
FileName :	ncs4202-universalk9.16.09.08.SPA.bin	
Min Memory :	DRAM 4096 Flash 2048	
Size :	402.76 MB (422322174 bytes)	
MD5 Checksum :	c34f8384482d4218c5416aebc626d63a 	
SHA512 Checksum :	46e91ef6adf1ee9e6f8af73f93972175 ... 	
Advisories 		

Ilustración 2. Verificación del hash de 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 router.
- Puesto de gestión con cliente SSH: dicho puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado, que se emplea para la configuración y administración del router.
- Servidor Radius AAA.
- Servidor Syslog.
- Servidor NTP.
- Servidor de monitorización: para la recepción de los mensajes Syslog del router.

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*.
27. Más información se puede encontrar en la guía de Cisco: *Using the Cisco IOS Command-Line Interface* [REF4].

5.2 CONFIGURACIÓN INICIAL VÍA CABLE DE CONSOLA

28. 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.
29. Se deberán configurar los siguientes parámetros:
 - *Enter host name*. Nombre de dispositivo deseado.
 - *Enter enable secret*. Contraseña empleada para proteger el acceso a los modos de configuración, debe ser conforme a la política de contraseñas definida en el apartado **6.4.1 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 **6.4.1 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.
30. 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. En esta se exige el empleo de RSA con claves de 4096 bits en el protocolo SSH, así como su versión 2.

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

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)#ip address <IP> <Mask>
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#
Router(config)# ip route vrf Mgmt-vrf 0.0.0.0 0.0.0.0 <Gateway>
Router(config)# ip domain name <domain-name>
Router(config)# ip ssh version 2
Router(config)# ip ssh time-out 60
Router(config)# ip ssh authentication-retries 2
Router(config)# ip ssh dh min size 4096
Router(config)# crypto key generate rsa modulus 4096
Router(config)# service password-encryption
Router(config)# username <user-admin> password <password>
Router(config)# enable secret <password>

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

31. 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

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

```
Router# copy run start
```

33. 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.

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

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

6.2 AUTENTICACIÓN

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

- Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver apartado **6.4.1 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 **6.3 SERVIDORES DE AUTENTICACIÓN**.

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

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

6.3 SERVIDORES DE AUTENTICACIÓN

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

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

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

- Para servidores de tipo TACACS+, se deberá configurar la clave de cifrado empleando el comando *key*. Esta se empleará para cifrar las comunicaciones entre el producto y el servidor.
 - 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](#).
39. Debido a que la conexión con los servidores externos puede fallar, se recomienda mantener como método alternativo de respaldo la base de datos local de usuarios, de tal forma que, si no se puede realizar la comunicación con el servidor de autenticación, se siga pudiendo acceder al dispositivo. Para ello emplear el parámetro *local* al final del comando:

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

40. El detalle de configuración de los servidores de autenticación se puede consultar en la guía de Cisco: AAA [REF11].

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 CONFIGURACIÓN DE ADMINISTRADORES

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

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

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

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

44. 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.
45. Los niveles 1-14 se pueden configurar para que comprendan cualquiera de los comandos disponibles. Para ello se debe emplear el siguiente comando, indicando el comando deseado y el nivel al que pertenecerá:

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

46. 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.**
47. El detalle sobre la gestión de usuarios y permisos se puede consultar en la guía de *Cisco: Controlling Router Access with Passwords and Privilege Levels* [REF7].

6.4.2 PARÁMETROS DE SESIÓN

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

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

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

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

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

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

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

```
Router(config)#banner login C Banner C
```

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

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

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

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

54. Se recomienda desactivar SNMP.

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

6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

55. 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.

56. 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
Router(config)# ip domain name <domain-name>

se configura SSH versión 2

Router(config)# ip ssh version 2

Timeout de espera de respuesta del cliente
Router(config)# ip ssh time-out 60

Número de intentos de autenticación
Router(config)# ip ssh authentication-retries 2

Grupo Diffie-Hellman 16
Router(config)# ip ssh dh min size 4096

Longitud de la clave RSA
Router(config)# crypto key generate rsa modulus 4096
```

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

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

6.7 GESTIÓN DE CERTIFICADOS

58. 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.
59. Para el último paso, una vez configurados los certificados correspondientes, deberán ejecutarse los siguientes comandos.

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

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

6.8 SINCRONIZACIÓN

61. **Todos los sistemas y sus productos utilizados por la organización deben estar sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.
62. El producto dispone de un reloj hardware y reloj software. Sin embargo, **se recomienda la configuración NTP con autenticación, empleando MD5**. (SHA2 no disponible en esta versión).

```
Router(config)#ntp server <IP del servidor>
Router(config)#ntp authenticate
Router(config)#ntp authentication-key number <key-id> md5 <key>
```

63. El detalle de configuración de NTP se puede consultar en la guía de *Cisco: NTP [REF12]*.

6.9 ACTUALIZACIÓN DEL SOFTWARE

64. Las actualizaciones de Software pueden consultarse en el *Software Center* de Cisco: <https://software.cisco.com/download/home>
65. El producto permite verificar la versión del software instalada empleando el siguiente comando.

```
Router#Show version
```

66. 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>
```

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

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

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

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

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

```
Router#Show version
```

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

6.10 AUTO-CHEQUEOS

71. El producto es capaz de realizar comprobaciones automáticas del comportamiento de sus funciones durante el arranque o reinicio del dispositivo. El test automático incluye los siguientes apartados:

- Test automáticos en el encendido:
 - Test de integridad del *firmware/software*.
 - Test de respuesta conocida:
 - AES.
 - 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.

72. 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.
73. 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.
74. El producto permite también invocar los test criptográficos bajo demanda con el comando siguiente:

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

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

6.11 AUDITORÍA

76. 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.
77. El *logging* en la sesión SSH se puede activar y desactivar. Para asegurar que se encuentra habilitado, emplear el siguiente comando.

```
Router#terminal monitor
```

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

```
Router#show logging
```

79. El detalle sobre los mensajes de log se puede consultar en la guía de *Cisco: Upgrade* [REF14].
80. En caso de alcanzarse el límite de almacenamiento, los logs más recientes sobrescribirán a los más antiguos. Se puede aumentar el tamaño del búfer a un valor que depende de la memoria disponible en el producto.

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

81. 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.

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

```
Router#clear log
```

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

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

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

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

85. 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 **6.13 CONFIGURACIÓN DE IPSEC**, para ver el detalle de configuración del protocolo.
86. Se puede configurar el tipo de mensajes generados, en función al nivel definido. Este se puede modificar empleando los comandos *Logging monitor <level>* y *logging trap <level>*, para el acceso SSH y el servidor syslog respectivamente. A continuación, se muestra el detalle de los distintos niveles disponibles.

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

87. El detalle de configuración de los registros de auditoría se puede consultar en la guía de *Cisco: System Message Logs* [REF13].

6.12 COPIAS DE SEGURIDAD

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

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

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

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

90. **Se recomienda siempre almacenar las copias de seguridad en una ubicación externa para mayor seguridad.**
91. El detalle de configuración de la función *Archive* se puede consultar en la guía de *Cisco: Archive* [REF14].

6.13 CONFIGURACIÓN DE IPSEC

92. El producto proporciona capacidades de conexión IPsec. El detalle de configuración se puede consultar en la guía de *IPsec* - REF9.
93. **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.
94. A continuación, se muestran los parámetros recomendados.

- Transformaciones de IPsec:

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Transformación AH	<i>ah-sha-hmac</i>	ah-sha-hmac (solo se permite SHA-1 para funciones HMAC).	No.
Transformación de cifrado ESP	<i>esp-3des</i> <i>esp-aes</i> <i>esp-des</i> <i>esp-null</i> <i>esp-seal</i>	esp-aes (permitido con claves iguales o mayores a 128 bits)	Sí. Se recomienda utilizar AES.
Transformación de autenticación ESP	<i>esp-md5-hmac</i> <i>esp-sha-hmac</i>	esp-sha-hmac (solo se permite SHA-1 para funciones HMAC).	Sí. Se recomienda no utilizar MD5.

TIPOS DE TRANSFORMACIÓN PARA IPSEC	OPCIONES DE TRANSFORMACIÓN PARA IPSEC	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Transformación de compresión IP	<i>comp-lzs</i>	Todas	No.
Modos	<i>tunnel (por defecto)</i> <i>transport</i>	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.

- Transformaciones de IKEv2:

TIPOS DE TRANSFORMACIÓN PARA IKEV2	OPCIONES DE TRANSFORMACIÓN PARA IKEV2	OPCIONES RECOMENDADAS	ES REQUERIDA SU CONFIGURACIÓN
Autenticación	rsa-sig (por defecto) rsa-encr pre-share	rsa-sig (con una longitud de clave igual o superior a 3072 bits) rsa-encr (nonces cifrados con RSA con una longitud de clave igual o superior a 3072 bits)	Sí. Se recomienda usar RSA y no claves precompartidas.
Cifrado	des (por defecto) 3des aes 128 256	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

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

7. FASE DE OPERACIÓN

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

- **Mantenimiento del control de acceso** al producto.
- **Comprobaciones periódicas del hardware y software** para asegurar que no se ha introducido hardware o software no autorizado.
- **Seguir las alertas de seguridad de Cisco** ([Security Advisories](#)) 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 podrá acceder a ellos.

8. CHECKLIST

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

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 ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/gsg/b_Smart_Licensing_QuickStart/b_Smart_Licensing_Quick_Start_chapter_00.html
- REF3** *Hardware Installation guide*
Cisco ASR 902 Series Hardware Installation Guide
<https://www.cisco.com/c/en/us/td/docs/routers/asr902/hardware/guide/b-asr902-hig.html>
Cisco ASR 903 Series Hardware Installation Guide
https://www.cisco.com/c/en/us/td/docs/wireless/asr_900/hardware/installation/b-asr903u-hig.html
Cisco ASR 907 Series Hardware Installation Guide
<https://www.cisco.com/c/en/us/td/docs/routers/asr907/hardware/installation/guide/b-asr907-hig.html>
Cisco ASR 920 Series Hardware Installation Guide
<https://www.cisco.com/c/en/us/td/docs/routers/asr920/hardware/installation/guide/b-asr920-ic-hig/m-overview.html>
- REF4** *Using the Cisco IOS Command-Line Interface*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xs-17/fundamentals-xe-17-book/m_cf-cli-basics.html
- REF5** *Basic System Management Configuration Guide*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xs-17/fundamentals-xe-17-book/m_cf-config-overview-0.html
- REF6** *Upgrade*
Cisco ASR 900 series
Apartado " Upgrading to a New Software Release"
https://www.cisco.com/c/en/us/td/docs/routers/asr903/release/notes/b-rn-xe-16-7-asr900/167x_introduction.html#concept_ovh_wvj_5bb

- REF7** *Controlling Router Access with Passwords and Privilege Levels*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/controlling_switch_access_with_passwords_and_privilege_levels.html
- REF8** *SSH*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/routers/asr903/software/guide/chassis/16-12-1/b-config-guide-xe-16-12-1-asr900/b-config-guide-xe-16-12-1-asr900_chapter_01.html
- REF9** *IPSEC*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xs/asr900/16-12-1/b-sec-ipsec-xe-16-12-asr900/b-sec-ipsec-xe-16-12-asr900_chapter_00.html
- REF10** *PKI*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xs/asr900/16-12-1/b-sec-ipsec-xe-16-12-asr900/b-sec-ipsec-xe-16-12-asr900_chapter_00.html
- REF11** *AAA*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xs/16-12/sec-usr-rad-xe-16-12-book/sec-rad-aaa-server-groups.html
- REF12** *NTP*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/routers/asr903/software/guide/timing/16-12-1/b-timing-sync-xe-16-12-asr900/m_bsm-ntp-asr920.html
- REF13** *System Message Logs*
Cisco ASR 900 series
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xs/asr903/17-1-1/b-system-logging-xe-17-1-asr900/m_configuring_onboard_failure_logging.html#ID1

REF14 *Archive*

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/configuration/xr/asr9000/16-12-1/b-config-mgmt-xe-16-12-asr900/b-config-mgmt-xe-16-12-asr900_chapter_011.html

REF15 *Error and System Messages*

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/16_xr/smg/xe-16-10/b-sem-16-10-1.html

10.ABREVIATURAS

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

