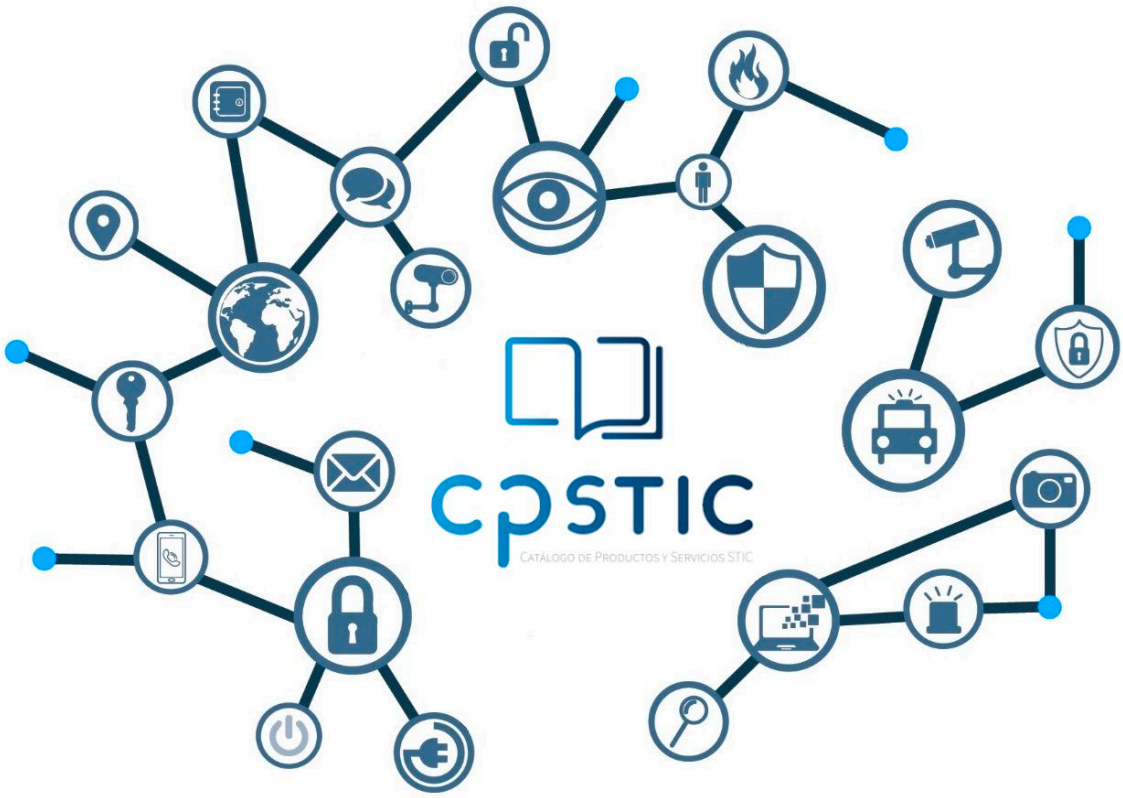
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1461

Procedimiento de empleo seguro
Cisco ISR 4K / ASR 1000 Series / Catalyst 8300/8500, IOS-XE 17.9



Febrero 2024

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: 083-24-103-6.
Fecha de Edición: febrero de 2024.

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
2024.03.01 11:21:10 +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
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

1. INTRODUCCIÓN

1. Los routers Cisco Integrated Services Router 4000 Series (ISR4K), ASR 1000 Series y Catalyst 8300/8500 series son plataformas que permiten la configuración de funcionalidades de *switching* y *routing*.

2. OBJETO Y ALCANCE

2. El objeto del presente documento es facilitar la instalación y configuración segura de los routers **Cisco Integrated Services Router 4000 Series (ISR4K), ASR 1000 Series y Catalyst 8300/8500 series** ejecutando la versión de **sistema operativo IOS-XE 17.9**, junto con el aseguramiento del entorno en el que se despliega.

2.1 PRODUCTOS

2.1.1 CISCO INTEGRATED SERVICES ROUTER 4000 SERIES (ISR4K)

3. Los routers ISR4K tienen 6 series:

   - ISR 4321.
   - ISR 4331.
   - ISR 4351.
   - ISR 4431.
   - ISR 4451.
   - ISR 4461.

4. 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 17.9.**

ISR 4221	Modelos
	ISR4221/K9

Tabla 1 – Modelos serie ISR 4221

ISR 4331	Modelos
	ISR4331/K9

Tabla 2 – Modelos serie ISR 4331

ISR 4351	Modelos
	ISR4351/K9

Tabla 3 – Modelos serie ISR 4351

ISR 4431	Modelos
	ISR4431/K9

Tabla 4 – Modelos serie ISR 4431

ISR 4451	Modelos
	ISR4451-X/K9

Tabla 5 – Modelos serie ISR 4451

ISR 4461	Modelos
	ISR4461/K9

Tabla 6 – Modelos serie ISR 4461

2.1.2 ASR 1000 SERIES

5. Los routers ASR 1000 Series tienen 6 series:
    - ASR 1001.
    - ASR 1002.
    - ASR 1004.
    - ASR 1006.
    - ASR 1009.
    - ASR 1013
6. 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 17.9.**

ASR 1001	Modelos
	ASR1001-X ASR1001-X= ASR 1001-HX ASR 1001-HX=

Tabla 7 – Modelos serie ASR 1001

ASR 1002	Modelos
	ASR1002-X ASR1002-X= ASR1002-HX ASR1002-HX=

Tabla 8 – Modelos serie ASR 1002

ASR 1004	Modelos
	ASR1004 ASR1004=

Tabla 9 – Modelos serie ASR 1004

ASR 1006	Modelos
	ASR1006 ASR1006= ASR1006-X ASR1006-X=

Tabla 10 – Modelos serie ASR 1006

ASR 1009	Modelos
	ASR1009-X ASR1009-X=

Tabla 11 – Modelos serie ASR 1009

ASR 1013	Modelos
	ASR1013 ASR1013=

Tabla 12 – Modelos serie ASR 1013

2.1.3 CATALYST 8300/8500

7. Los routers Catalyst 8300/8500 Series tienen 1 serie:
    - Catalyst 8300/8500
8. 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 17.9.**

Catalyst 8300/8500	Modelos
	Catalyst 8300/8500 Series Edge Platforms

Tabla 13 – Modelos series Catalyst 8300/8500

2.2 SOFTWARE

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

Figura 1 – Versiones de Software

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

3. ORGANIZACIÓN DEL DOCUMENTO

14. Este documento se compone de los siguientes apartados:

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

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

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

d) Apartado **7**. En este apartado se incluye el listado de documentos referenciados a lo largo del documento.

e) Apartado **8**. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACION

4.1 ENTREGA SEGURA DEL PRODUCTO

15. 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.

4.2 ENTREGA SEGURA DEL SOFTWARE

16. 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.
17. El software está disponible en el *Software Center* de Cisco [REF17]:

    https://software.cisco.com/download/home
18. 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**.

Figura 2 – Verificación Hash descargas

4.3 ENTORNO DE INSTALACIÓN SEGURO

19. 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

20. 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*.
21. 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.
22. 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**.
23. El detalle de configuración de licencias se puede consultar en la guía *Cisco: Licenses* [REF2].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

24. 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

25. La instalación física del producto se debe realizar siguiendo las instrucciones de las guías de *Cisco: Hardware Installation Guide* [REF3].
26. 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

27. Antes de configurar el producto, se necesita entender el formato de los comandos y los modos *Exec*.
28. 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

29. Después de conectar el cable de consola entre el equipo 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.
30. Se deberán configurar los siguientes parámetros:
    - *Enter host name*. Nombre de dispositivo deseado.
    - *Enter enable secret*. Contraseña empleada para proteger el acceso a los modos de configuración, debe ser conforme a la política de contraseñas definida en el apartado 6.5.2 CONFIGURACIÓN DE ADMINISTRADORES.
    - *Enter virtual terminal password*. Contraseña empleada para proteger el acceso a la terminal virtual permitiendo acceso al producto mediante consola. debe ser conforme a la política de contraseñas definida en el apartado 6.5.2 CONFIGURACIÓN DE ADMINISTRADORES.
    - *Configure SNMP Network Management*. Por defecto configurado en NO, de tal forma que el servidor SNMP estará deshabilitado. Dejar el valor por defecto.
    - *Enter interface name used to connect to the management network from the above interface summary*. Seleccionar la interfaz que se desea emplear para conectar a la red.
31. 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
```

32. 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

33. 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
```

34. 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.

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

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

6.2 MODO DE OPERACIÓN SEGURO

36. El producto debe ejecutarse en el modo de operación seguro. Para ello, **se debe ejecutar el siguiente comando**. El fabricante indica que la longitud de la clave **no** es configurable:

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

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

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

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

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

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

```
Router# show fips status
```

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

6.3 AUTENTICACIÓN

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

    - Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver apartado 6.5.2 CONFIGURACIÓN DE ADMINISTRADORES.

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

42. **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
```

6.4 SERVIDORES DE AUTENTICACIÓN

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

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

44. 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 [REF18].

45. 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
```

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

6.5 ADMINISTRACIÓN DEL PRODUCTO

6.5.1 ADMINISTRACIÓN LOCAL Y REMOTA

47. El producto permite la conexión directa mediante consola, y la conexión remota empleando el protocolo SSHv2.

48. En el apartado 6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS se indica que 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. La configuración segura del protocolo SSHv2 se indica en el apartado 6.7 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.

49. En el apartado 6.6 de este documento se indican los comandos a introducir para deshabilitar el protocolo HTTP. Asimismo, en este apartado se indican los comandos a seguir para deshabilitar el protocolo SNMP.

6.5.2 CONFIGURACIÓN DE ADMINISTRADORES

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

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

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

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

53. **Se deberá configurar la política de contraseñas segura**. Para ello emplear los siguientes comandos, de tal forma que deban contener al menos 12 caracteres y un tiempo de validez de 60 días y emplear al menos una letra minúscula, una mayúscula, un número y un carácter especial.

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

54. Adicionalmente, los administradores deberán asegurar **de forma procedural**:
    - No se puedan reutilizar las últimas 5 contraseñas.
    - No se podrá volver a modificar una contraseña hasta pasados 10 días.
55. Para crear un nuevo usuario, se debe emplear el siguiente comando:

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

56. 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.

57. 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>
```

58. 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**.

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

6.5.3 PARÁMETROS DE SESIÓN

60. 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
```

61. 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
```

62. Una vez bloqueado un usuario, se deberá desbloquear manualmente. Dicha operación de desbloqueo deberá ser realizada por un usuario con permisos de administración.

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

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

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

6.6 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

64. **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 https server
```

65. 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
```

66. Se recomienda desactivar SNMP.

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

6.7 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

67. 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.

68. 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

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

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

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

69. 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
```

6.8 GESTIÓN DE CERTIFICADOS

70. 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.

71. 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
```

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

6.9 SINCRONIZACIÓN

73. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.
74. El producto dispone de un reloj hardware y reloj software. Sin embargo, **se recomienda la configuración NTP con autenticación**, **empleando siempre SHA2**.

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

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

6.10 ACTUALIZACIÓN DEL SOFTWARE

76. Las actualizaciones de Software pueden consultarse en el *Software Center* de Cisco [REF17]:

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

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

```
Router#Show version
```

78. 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>
```

79. 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>
```

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

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

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

```
Router#Show version
```

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

6.11 AUTO-CHEQUEOS

83. El producto 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.
86. 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.
87. El producto permite también invocar los test criptográficos bajo demanda con el comando siguiente:

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

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

6.12 AUDITORÍA

89. El producto genera mensajes de *logging* que se pueden distribuir a la consola, a la sesión VTY (SSH), a un búfer o a un servidor Syslog. **No se recomienda el uso de la consola**.
90. El *logging* en la sesión SSH se puede activar y desactivar. Para asegurar que se encuentra habilitado, emplear el siguiente comando.

```
Router#terminal monitor
```

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

```
Router#show logging
```

92. El detalle sobre los mensajes de log se puede consultar en la guía de *Cisco: System Message Logs* [REF14].
93. A continuación, se incluye un ejemplo del formato de los registros de auditoría:

- *seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)*
- *seq no:timestamp: %facility-severity-MNEMONIC:description*

Figura 3 – Ejemplo formato registros de auditoría

94. 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>
```

95. 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.

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

```
Router#clear log
```

97. **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
```

98. 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>
```

99. **Será necesario configurar un túnel IPsec para proteger la conexión con el servidor Syslog y evitar el envío de los logs en claro**. Consultar el apartado 6.14 CONFIGURACIÓN DE IPSEC, para ver el detalle de configuración del protocolo.

100. 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>
```

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

6.13 COPIAS DE SEGURIDAD

102. **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
```

103. 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>
```

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

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

6.14 CONFIGURACIÓN DE IPSEC

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

107. **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.

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

7. 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*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/qsg/b_Smart_Licensing_QuickStart/b_Smart_Licensing_QuickStart_chapter_00.html
https://www.cisco.com/c/en/us/td/docs/routers/sl_using_policy/b-sl-using-policy/introduction.html

REF3 *Hardware Installation guide*
Cisco 4000 Series ISR
https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html

Cisco ASR 1000 Series
https://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/asr1routers/asr-1000-series-hig.html

Cisco Catalyst 8300
https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/hardware_installation/b-catalyst-8300-series-edge-platforms-hig/m_c_sm.html

Cisco Catalyst 8500
https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/hardware-installation-guide/b_C8500_HIG.html

REF4 *Using the Cisco IOS Command-Line Interface*
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*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17/fundamentals-xe-17-book/m_cf-config-overview-0.html

REF6 *Upgrade*
Cisco 4000 Series ISR
https://www.cisco.com/c/en/us/td/docs/routers/access/4400/release/xe-17-9/isr4k-rel-notes-xe-17-9.html#con_43195

Cisco ASR 1000 Series
https://www.cisco.com/c/en/us/td/docs/routers/asr1000/software/configuration/xe-17/asr1000-sw-config-xe-17/issu-1.html
Cisco Catalyst 8300
https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/software_config/cat8300swcfg-xe-17-book/isr9000swcfg-xe-16-12-book_chapter_0111.html#concept_0EDA6D6296B74D3B9743A77302187643
Cisco Catalyst 8500
https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/software-configuration-guide/c8500-software-config-guide/issu-1.html

REF7 *FIPS*
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9200/software/release/17-6/configuration_guide/sec/b_176_sec_9200_cg/secure_operation_in_fips_mode.html

REF8 *Controlling Router Access with Passwords and Privilege Levels*
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-cfg-authentifcn-0.html#GUID-9E649014-9534-4DE9-9130-2ABBBBC54011

REF9 *SSH*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book/sec-secure-shell-v2.html
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book/sec-secure-shell-algorithm-ccc.html

REF10 *IPSEC*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-17/sec-sec-for-vpns-w-ipsec-xe-17-book-cat8000.html

REF11 *PKI*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book/sec-pki-overview.html

REF12 *AAA*
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-domain-stripping-xe.html

REF13 *NTP*
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*
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-3/configuration_guide/sys_mgmt/b_173_sys_mgmt_9400_cg/configuring_system_message_logs.html

REF15 *Archive*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-17/config-mgmt-xe-17-book/cm-config-versioning.html

REF16 *Error and System Messages*
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-9-x/b-system-message-guide-17-9-x.html

REF17 *Página de descargas de Cisco*
https://software.cisco.com/download/home

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

8. 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