Guía de Seguridad de las TIC
CCN-STIC 1482

Procedimiento de Empleo Seguro
FortiSwitch v7.6

Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:23:57 +02'00'

ÍNDICE

1 INTRODUCCIÓN

1. El **FortiSwitch 7.6** es un switch que permite interconectar los segmentos físicos de red y habilitar la circulación de datos entre dichos segmentos. Trabaja a nivel de Capa 2 del modelo de interconexiones de sistemas abiertos (ISO/IEC 7498-1) y dirige el tráfico según direccionamiento físico (Media Access Control) de ethernet. Puede ampliar o reducir sus necesidades de rendimiento de operaciones con facilidad de uso y bajo costo de propiedad para satisfacer las demandas de las aplicaciones con uso intensivo de ancho de banda, desde pequeñas oficinas hasta grandes centros de datos.
2. Este dispositivo se distribuye en forma de equipo dedicado o appliance que incluye el software y el hardware necesarios para su operación segura.
3. Posee una potente arquitectura hardware que tiene los siguientes puertos físicos:
   a) Puertos del 1 al 16 son 802.3af/at 1Gbps
   b) Puertos del 17 al 24 son 802.3af/at/bt tipo 3 clase 6 2.5Gbps
   c) Puertos del 25 al 26 son 2.5Gbps
   d) Puertos del 27 al 30 (SFP+) 10Gbps
   e) 1 puerto USB (A) 2.0
   f) 1 puerto de consola RJ45

2 OBJETO Y ALCANCE

4. La configuración incluida en la presente guía de empleo seguro es la evaluada y cualificada en el Catálogo de Productos y Servicios de STIC (CPSTIC). La versión del firmware evaluada es la **7.6.**
5. El producto **FortiSwitch 7.6** ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte [CPSTIC].

3 ORGANIZACIÓN DEL DOCUMENTO

a. Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
b. Apartado 5. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de instalación del producto.
c. Apartado 6. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. El producto evaluado FortiSwitch 7.6 se distribuye en forma de appliance hardware que incluye el firmware necesario para su operación segura. Antes de proceder con la instalación y configuración del producto, se recomienda verificar la integridad física del dispositivo y la autenticidad del firmware instalado. Se debe comprobar:

   a) **Información de envío.** Se debe comprobar la documentación de envío para verificar que concuerda con la orden de compra original y que el envío ha sido realizado por Fortinet.
   b) **Embalaje externo.** Se debe inspeccionar el embalaje y la cinta de embalaje con la marca de Fortinet. Se debe comprobar que la cinta esté intacta y que no haya sido cortada ni se haya deteriorado en ningún punto. Además, se debe inspeccionar que la caja no presente cortes ni daños que permitan acceder al dispositivo.
   c) **Embalaje interno.** Se debe comprobar el embalaje interior de la misma manera que el embalaje exterior. Adicionalmente, se debe comprobar que la etiqueta presente en el embalaje exterior concuerda con el modelo de dispositivo adquirido.
   d) **Sello de garantía.** Se deberá verificar que la placa de identificación del producto, alojada en el chasis, es consistente con la etiqueta del embalaje del producto.

7. En caso de que exista algún desperfecto o alguna inconsistencia será necesario contactar con el soporte de Fortinet de manera inmediata para recibir instrucciones. No se recomienda realizar la instalación en este caso.

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. El producto FortiSwitch 7.6 deberá instalarse en un entorno físicamente seguro y controlado. El acceso físico a los dispositivos FortiSwitch deberá estar restringido exclusivamente a personal autorizado con funciones de administración o mantenimiento.

9. Se recomienda:

   a) Instalación en CPD o armario de comunicaciones con acceso restringido.
   b) Control de acceso físico mediante autorización expresa.
   c) Protección frente a manipulación física.
   d) Alimentación eléctrica redundante cuando sea posible.
   e) Protección ambiental adecuada (temperatura, humedad y ventilación).
   f) Conexión a redes de administración segregadas.

4.3 REGISTRO Y LICENCIAS

10. El producto FortiSwitch 7.6 no requiere licencias adicionales para operar en la configuración evaluada. Para algunas opciones avanzadas como BGP routing si es necesario. Para más información consultar la sección “Licenses” de [ADMIN_GUIDE].

11. La descarga de firmware, actualizaciones y documentación oficial del producto deberá realizarse exclusivamente desde el portal oficial del fabricante Fortinet: https://support.fortinet.com/.

12. El registro del producto en los servicios cloud del fabricante es opcional y no forma parte de la configuración evaluada.

4.4 CONSIDERACIONES PREVIAS

13. No son necesarias consideraciones previas adicionales de seguridad antes de iniciar la instalación del producto distintas de las indicadas en las secciones anteriores.
14. La instalación y configuración del producto deberán realizarse siguiendo la documentación oficial de Fortinet correspondiente a FortiSwitch 7.6 en modo standalone/local management.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

15. El entorno de operación del producto debe estar compuesto por los siguientes elementos hardware en su entorno:
    a) Servidor syslog protegido mediante TLS.
    b) Una infraestructura de confianza para la validación de certificados X.509. Esta infraestructura podrá incluir una Autoridad de Certificación (CA) o equivalente, los certificados de CA raíz/intermedia de confianza necesarios y, cuando aplique, mecanismos de comprobación del estado de los certificados, tales como CRL u OCSP. No se requiere que la CA permanezca conectada de forma permanente a la red de operación.
    c) Equipo de Administración: equipo utilizado por los administradores autorizados para la gestión del producto para acceso por GUI y CLI.

5 FASE DE INSTALACIÓN

16. La instalación y despliegue seguro del producto FortiSwitch 7.6 deberá realizarse siguiendo la documentación oficial del fabricante y las recomendaciones incluidas en el presente procedimiento de empleo seguro.
17. Desde un equipo de administración debe conectar un cable ethernet al puerto de *management* del producto.
18. Tras ello, se debe acceder mediante un explorador web a la siguiente dirección https://192.168.1.99 y seremos redirigidos a la siguiente pantalla.

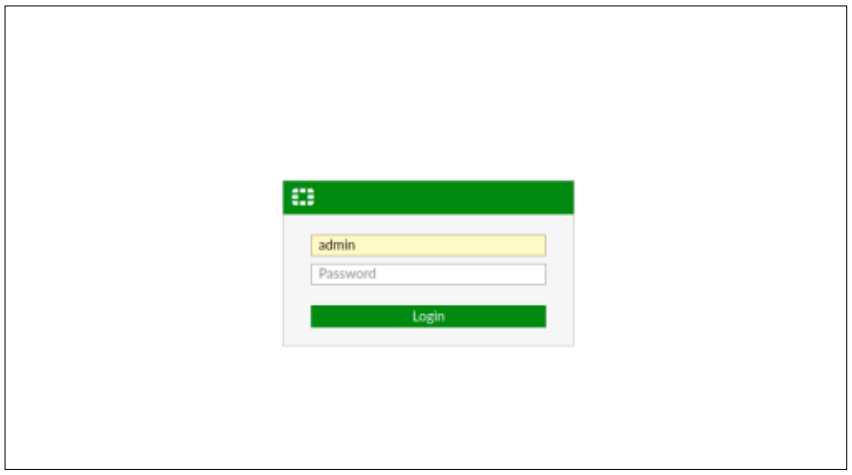

Ilustración 1: Interfaz web de login.

19. En esta pantalla, se escribirá en el campo de usuario “admin” y haremos clic en el botón que dice “Login”.
20. Seguidamente se debe crear una nueva contraseña de administración e introducir dicha contraseña en los campos “New Password” y “Confirm Password” y clicaremos en el botón “OK”. La contraseña deberá cumplir con los requisitos de política de contraseñas especificados en la sección *6.3.2 CONFIGURACIÓN DE ADMINISTRADORES*.

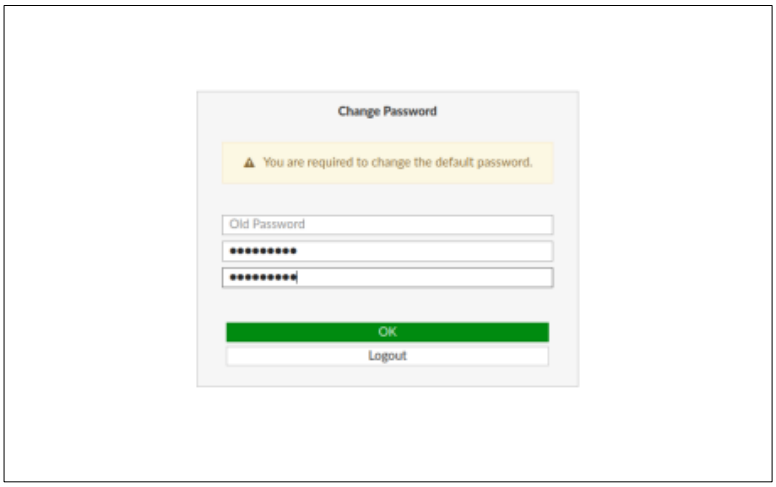

Ilustración 2: Interfaz web para nueva contraseña.

21. Tras esto se mostrará nuevamente la pantalla de inicio, donde se introducirán las credenciales que hemos creado y haremos clic en “Login”.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

22. Para que el FortiSwitch 7.6 opere en la configuración segura evaluada, deberán aplicarse las siguientes medidas de configuración segura de esta sección.
23. Se deberá habilitar el modo FIPS-CC del FortiSwitch 7.6 ejecutando los siguientes comandos desde el puerto de consola con una cuenta que tenga el perfil de super_admin:

```
config system security
..set mode fips-cc
end
```

24. El sistema preguntará por una nueva contraseña del usuario administrador. La contraseña deberá cumplir con los requisitos de política de contraseñas especificados en la sección *6.3.2 CONFIGURACIÓN DE ADMINISTRADORES*. Tras introducirla, la CLI mostrará un mensaje de aviso para confirmar que se borrará la configuración guardada. Escribimos "y" y pulsamos Enter. El FortiSwitch 7.6 se reiniciará y ahora funcionará en modo FIPS-CC.
25. En el modo FIPS-CC, la administración remota a través de HTTP o Telnet está desactivada. También, el acceso administrativo remoto (vía HTTPS o SSH) está desactivado de forma predeterminada por lo que en caso de usarse se debe habilitar con la siguiente configuración a través de la CLI:

```
config system interface
edit mgmt
set allowaccess https ssh
end
```

26. Conforme al modo FIPS-CC, se debe deshabilitar NTP con la siguiente configuración:

```
config system ntp
..set status disable
end
```

27. Debido a que NTP queda deshabilitado, el administrador deberá establecer y verificar la fecha y hora del sistema de forma manual mediante los mecanismos permitidos por dicha configuración. Para más información consultar la sección "Time" de [ADMIN_GUIDE].
28. Se debe habilitar el cifrado de datos privados y cargar una clave para cifrar los parámetros de seguridad críticos almacenados con la siguiente configuración:

```
config system global
..set private-data-encryption enable
end
```

29. Una vez activado el cifrado de datos privados, se le pedirá al administrador que introduzca y confirme una clave AES de 128 bits que se utilizará para cifrar los parámetros de seguridad críticos almacenados.
30. Para evitar la aparición de servidores DHCP falsos en los diferentes puertos del switch, se debe configurar el "switch-controller-dhcp-snooping" que supervisa el tráfico DHCP y filtra los mensajes no válidos. Para ello hace falta realizar la siguiente configuración a través de la terminal CLI:

```
config system interface
    edit VLAN_NAME
        set switch-controller-dhcp-snooping enable
```

```
        config dhcp-snooping-server-list
            edit NAME_OF_THE_DESIRED_ENTRY
                set server-ip IP_OF_THE_SERVER
            end
    end
```

31. Para evitar ataques de ARP spoofing y posibles MitM (Man in the Middle) se deben configurar la inspección de paquetes ARP "switch-controller-arp-inspection". Para ello se deben ejecutar los siguientes comandos:

```
config system interface
    edit VLAN_NAME
        set switch-controller-arp-inspection enable
    end
    config switch-controller managed-switch
        edit SWITCH_NAME
            config ports
            edit PORT_NAME_ATTACHED_TO_DEVICE
                set arp-inspection-trust untrusted
                next
            end
        next
    end
```

32. Para evitar ataques STP (Spanning Tree Protocol) se debe deshabilitar la configuración STP de cada uno de los puertos, para ello se deben ejecutar los siguientes comandos:

```
config ports
    edit PORT_NUM
        set stp-state disabled
    end
```

33. Para información adicional se recomienda consultar la guía [FIPS_CC_GUIDE].

6.2 AUTENTICACIÓN

34. Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario en la configuración evaluada son los siguientes:

    a) Username/password.

    b) Username/public key para SSH.

35. Los mecanismos de autenticación administrativa permitidos en la configuración evaluada son los siguientes:

    a) GUI web vía HTTPS/TLS: autenticación mediante usuario y contraseña.

    b) CLI remota vía SSH: autenticación mediante usuario y contraseña y/o mediante usuario y clave pública.

    c) Consola local: autenticación mediante cuenta administrativa local, conforme a los perfiles y credenciales configurados en el dispositivo.

36. Para el acceso SSH de administración se recomienda priorizar, cuando sea posible, la autenticación basada en clave pública y restringir el acceso a cuentas administrativas nominales.

37. El FortiSwitch 7.6 proporciona soporte para certificados X.509 utilizados por TLS y permite:

a) Generación de CSR.

b) Generación de claves.

c) Importación de certificados.

d) Importación de certificados CA.

38. Los algoritmos soportados son:

a) RSA 2048/3072/4096.
b) ECDSA secp256r1/384r1/521r1.

39. Para más información consultar la sección “Certificates” de las guías [FIPS_CC_GUIDE] y [CC_ST].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

40. La administración del FortiSwitch 7.6 puede realizarse mediante:

a) Consola local.

b) GUI web vía HTTPS.

c) CLI remota via SSH.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

41. El FortiSwitch 7.6 incorpora una cuenta administrativa por defecto denominada *admin*, que permite el acceso a las funciones de administración local y remota del dispositivo. La autenticación administrativa puede realizarse mediante la GUI protegida mediante HTTPS/TLS, mediante CLI utilizando SSH o mediante acceso por consola local.
42. Una vez completada la configuración inicial de la fase de instalación, se recomienda la creación de cuentas administrativas nominales para cada administrador autorizado. Estas cuentas deberán asignarse a perfiles administrativos adecuados, aplicando el principio de mínimo privilegio. La cuenta por defecto *admin*, deberá reservarse para tareas excepcionales de recuperación, contingencia o mantenimiento controlado, y su uso deberá quedar restringido y auditado.
43. La creación de administradores adicionales con permisos diferenciados mediante perfiles administrativos se realiza a través de los *admin profiles*. Los perfiles permiten limitar el acceso a determinadas funciones del sistema conforme al principio de mínimo privilegio.
44. Para más información sobre la configuración de perfiles administrativos y permisos asociados verificar las secciones “Administrators” y “Profiles” de [ADMIN_GUIDE].
45. La política de contraseñas asociadas a cuentas administrativas deberá cumplir, como mínimo, los siguientes requisitos:
    a) Longitud mínima de 12 caracteres.
    b) Complejidad suficiente, incluyendo caracteres de al menos tres de las siguientes categorías: letras mayúsculas, letras minúsculas, números y caracteres especiales.
    c) Prohibición de uso de contraseñas triviales, por defecto, fácilmente deducibles, reutilizadas en otros sistemas o asociadas a información personal o del servicio.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

46. El FortiSwitch 7.6 deberá configurarse minimizando la exposición de interfaces, puertos y servicios no necesarios para la operación prevista.
47. Se recomienda deshabilitar todos aquellos puertos físicos no utilizados.
48. Los puertos utilizados para administración deberán pertenecer exclusivamente a redes de gestión autorizadas.

6.5 GESTIÓN DE CERTIFICADOS

49. El FortiSwitch 7.6 implementa mecanismos criptográficos para el establecimiento de canales seguros y validación de certificados conforme a la configuración evaluada.
50. Los algoritmos y funciones criptográficas identificados en la evaluación del producto son los siguientes:
    a) RSA de 2048, 3072, 4096 bits para generación de claves y generación y verificación de firmas.
    b) ECDSA con curvas P-256, P-384 y P-521 para generación de claves y generación y verificación de firmas.
    c) Funciones hash SHA-256, SHA-384 y SHA-512.
51. El FortiSwitch 7.6 puede generar un CSR con pares de claves RSA de 2048, 3072 y 4096 bits, así como con pares de claves ECDSA P-256, P-384 y P-521. Para más información consultar la sección “Certificates” de [ADMIN_GUIDE].

6.6 ACTUALIZACIONES

52. Las actualizaciones del firmware del producto deberán realizarse exclusivamente utilizando paquetes oficiales obtenidos desde el portal de soporte del fabricante (https://support.fortinet.com/Download/FirmwareImages.aspx)
53. El TOE permite actualización manual del firmware. Las imágenes de firmware son verificadas mediante firma digital antes de su instalación. Si la verificación de la imagen falla al intentar realizar una instalación o actualización mediante la interfaz gráfica de usuario, esta muestra el mensaje «ADVERTENCIA: La validación de la firma de este firmware ha fallado». Aunque el mensaje ofrece al administrador la opción de continuar con la instalación o actualización, en el modo FIPS-CC, hacer clic en «Continuar» no tendrá ningún efecto y la instalación o actualización fallará.
54. Si la actualización falla, el dispositivo se queda con la versión actual, lo cual se puede comprobar ejecutando el comando “get system status”.
55. Para más información consultar la sección “Firmware” de [ADMIN_GUIDE].

6.7 AUTO-CHEQUEOS

56. El producto tiene la capacidad de realizar pruebas para verificar el correcto funcionamiento de las funciones y de la integridad del firmware. Estas pruebas se realizan de forma automática durante el arranque del producto y pueden ser realizadas manualmente a petición de los usuarios autorizados.

57. El administrador puede ejecutar las autocomprobaciones manualmente en cualquier momento. Para ejecutar todas las pruebas, introduzca el siguiente comando de la CLI:

```
execute system security kat all
```

58. En caso de detectarse un fallo durante la ejecución de los auto-chequeos el FortiSwitch 7.6 pasa modo de error FIPS. En caso de fallos en las autocomprobaciones que no estén relacionados con la integridad del firmware, la unidad desactiva todas las interfaces, incluida la consola, y detiene el sistema operativo del firmware. Para reanudar el modo de funcionamiento normal FIPS-CC, es necesario apagar y volver a encender la unidad. Si las autocomprobaciones se superan tras el reinicio, la unidad reanudará el funcionamiento normal FIPS-CC.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

59. El FortiSwitch 7.6 registra eventos relativos a:
    a) Login/logout administrativo.
    b) Cambios de configuración.
    c) Gestión de certificados y claves.
    d) Eventos HTTPS y SSH.
    e) Actualizaciones de firmware.
60. Cada registro incluye:
    a) Timestamp.
    b) Tipo de evento.
    c) Usuario asociado.
    d) Resultado del evento.

6.8.2 ALMACENAMIENTO LOCAL

61. El FortiSwitch 7.6 almacena registros localmente. El almacenamiento local está habilitado por defecto en el modo FIPS-CC por lo que no es necesario configuración adicional.
62. Los registros de auditoría se almacenan en la memoria del sistema local.
63. Las entradas del almacenamiento local no se conservan cuando el sistema se reinicia (el búfer no es persistente); sin embargo, las entradas enviadas a un syslog externo permanecen sin cambios. El búfer de memoria local tiene una capacidad limitada y solo muestra las entradas de registro más recientes.
64. Una vez agotada toda la memoria disponible, el sistema comienza a sobrescribir los mensajes de registro más antiguos.
65. Dado que el almacenamiento local de registros no es persistente y dispone de capacidad limitada, se deberá configurar el envío de eventos de auditoría a un servidor syslog externo protegido mediante TLS.

6.8.3 ALMACENAMIENTO REMOTO

66. El FortiSwitch 7.6 permite exportar registros mediante syslog protegido mediante TLS.
67. La configuración se realiza mediante CLI con el comando “config log syslogd setting” o mediante GUI. Para más información consultar la sección “Syslog Server” de [ADMIN_GUIDE] y “Secure Syslog configuration” de [FIPS_CC_GUIDE].

6.9 BACKUP

68. Tras la instalación, se deberá realizar una copia de seguridad de la configuración del producto. Asimismo, se recomienda la realización de forma periódica de copias de seguridad tras cualquier cambio relevante de configuración, actualización de firmware o modificación de parámetros de seguridad.
69. Para realizar una copia de seguridad completa de manera manual se deberá ejecutar el siguiente comando desde la CLI:

```
execute backup full-config
```

70. La restauración de una copia de seguridad únicamente deberá realizarse por administradores autorizados y verificando previamente que la copia corresponde a una configuración permitida dentro del alcance de la configuración evaluada.
71. Para más información, consultar la sección “Backup” de [ADMIN_GUIDE].

7 REFERENCIAS

[ADMIN_GUIDE]	Administration Guide—Standalone Mode FortiSwitchOS 7.6.0 (https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/68894855-5526-11ef-bfe5-fa163e15d75b/FortiSwitchOS-7.6.0-Administration_Guide%E2%80%94Standalone_Mode.pdf).
[FIPS_CC_GUIDE]	NDcPP v3.0e FortiSwitch Technote FortiSwitch 7.6 (https://www.niap-ccevs.org/api/file/get_public_file/?file_id=35620).
[CC_ST]	Fortinet FortiSwitch v7.6 Security Target (https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/st_vid11572-st.pdf).
[CPSTIC]	Catálogo de Productos y Servicios TIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8 ABREVIATURAS

AES	Advanced Encryption Standard.
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol.
CA	Certificate Authority
CC	Common Criteria.
CLI	Command Line Interface.
CPD	Centro Procesamiento de Datos.
CPSTIC	Catálogo de Productos y Servicios de STIC.
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol.
ECDSA	Elliptic Curve Digital Signature Algorithm.
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standards.
GUI	Graphical User Interface.
HTTPS	HyperText Transfer Protocol Secure
MitM	Man-in-the-Middle
NTP	Network Time Protocol.
OCSP	Online Certificate Status Protocol
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
STP	Spanning Tree Protocol
TLS	Transport Layer Security