Guía de Seguridad de las TIC
CCN-STIC 1485

Procedimiento de Empleo Seguro
FortiAP v7.2.0

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 09:32:13 +02'00'

ÍNDICE

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

El **FortiAP 7.2.0** es un producto orientado a la protección de comunicaciones, proporcionando conectividad a una red local inalámbrica (WLAN) mediante comunicaciones por radiofrecuencia. Los puntos de acceso inalámbricos delegados a FortiAP 7.2.0 brindan un acceso LAN inalámbrico seguro e integrado para la empresa.

Este dispositivo se distribuye en forma de equipo dedicado o appliance que incluye el software y el hardware necesarios para su operación segura.

Posee una potente arquitectura hardware que ofrece las siguientes características:

a) Comunicación Inalámbrica IEEE 802.11a/b/g/n/ac

b) Antenas Internas

c) 1 puerto Ethernet 100/1000/2500 Base-T RJ45

d) 1 puerto Ethernet 10/100/1000 Base-T RJ45

e) Espectro de comunicación entre 2.4G y 5G.

2 OBJETO Y ALCANCE

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 **7.2.0**.

El producto **FortiAP 7.2.0** ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del [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

El producto evaluado FortiAP 7.2.0 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.

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

El FortiAP 7.2.0 deberá instalarse en un entorno físicamente seguro y controlado. El acceso físico a los dispositivos FortiAP 7.2.0 y FortiGate deberá estar restringido exclusivamente a personal autorizado con funciones de administración o mantenimiento.

Se recomienda que los componentes críticos del entorno operacional, incluyendo:

a) dispositivos FortiGate,
b) servidores de autenticación,
c) estaciones de administración,

se desplieguen en ubicaciones con medidas de protección física adecuadas y mecanismos de control de acceso.

4.3 REGISTRO Y LICENCIAS

El producto FortiAP 7.2.0 no requiere licencias adicionales para operar en la configuración evaluada.

La descarga de firmware, actualizaciones y documentación oficial del producto deberá realizarse exclusivamente desde el portal oficial del fabricante [FORTINET].

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

4.4 CONSIDERACIONES PREVIAS

Antes de iniciar la instalación y configuración del producto FortiAP 7.2.0, deberán tenerse en cuenta las siguientes consideraciones de seguridad:

- El producto deberá desplegarse conjuntamente con un dispositivo FortiGate compatible, que será utilizado para la administración centralizada del FortiAP 7.2.0.
- El dispositivo FortiGate deberá encontrarse previamente instalado, configurado y operativo antes de conectar el FortiAP 7.2.0 al entorno de producción.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

El entorno de operación del producto debe estar compuesto por los siguientes elementos hardware en su entorno:

a) FortiGate: Firewall con PoE (Power over Ethernet). Este dispositivo es utilizado para la administración y configuración centralizada del FortiAP.

b) Red FortiLink: Red utilizada para la comunicación entre FortiGate y FortiAP 7.2.0 que hace uso del FortiLink. FortiLink es un protocolo de control y tunelización para FortiAP y FortiSwitches, donde el FortiGate descubre, autoriza, configura, monitoriza y gestiona los dispositivos FortiAP integrados en el entorno operacional.

c) Equipo de Administración: equipo utilizado por los administradores autorizados para la gestión del producto.

d) Servidor RADIUS (opcional): Servidor de autenticación utilizado para despliegues WPA2/WPA3 Enterprise.

El FortiAP 7.2.0 deberá conectarse físicamente al FortiGate mediante interfaces autorizadas dentro del entorno FortiLink.

La administración del FortiAP 7.2.0 se realizará a través del FortiGate, quedando deshabilitada la administración remota directa sobre el FortiAP 7.2.0 en la configuración segura evaluada.

5 FASE DE INSTALACIÓN

5.1 CONEXIÓN MEDIANTE INTERFAZ WEB DEL FORTIGATE

La instalación y despliegue seguro del producto FortiAP 7.2.0 deberá realizarse siguiendo la documentación oficial del fabricante y las recomendaciones incluidas en el presente procedimiento de empleo seguro.

El producto se distribuye en forma de appliance hardware. La configuración inicial del FortiAP 7.2.0 en la configuración segura evaluada indicada en esta sección no se realiza mediante administración directa del AP, sino a través del dispositivo FortiGate utilizado para la administración centralizada del entorno.

A continuación, se debe comprobar si el dispositivo tiene corriente.

Configurar la máquina con la que se realizará la conexión a la interfaz web del FortiGate con una dirección IP perteneciente a la subred 192.168.1.0/24.

Tras ello, se debe acceder mediante un explorador de internet a la siguiente dirección https://192.168.1.99 y seremos redirigidos a la siguiente pantalla.

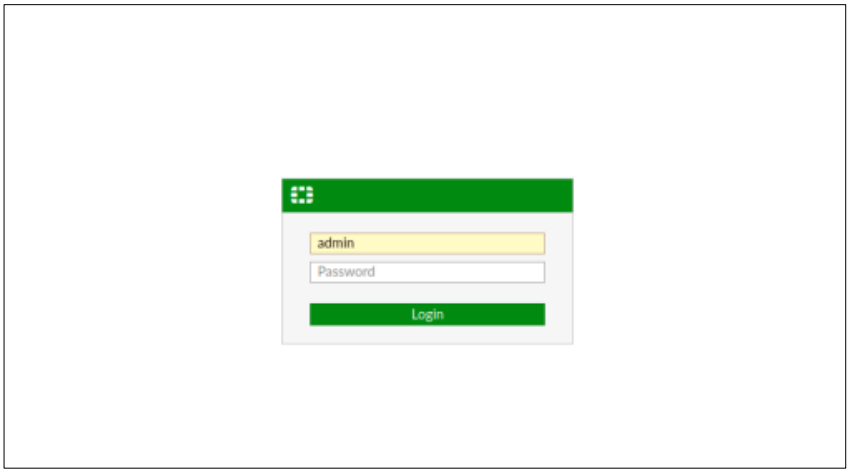

Ilustración 1: Interfaz web de login.

En esta pantalla, se escribirá en el campo de usuario “admin” y haremos clic en el botón que dice “Login”.

Seguidamente se debe crear una nueva contraseña de administración del FortiGate 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.

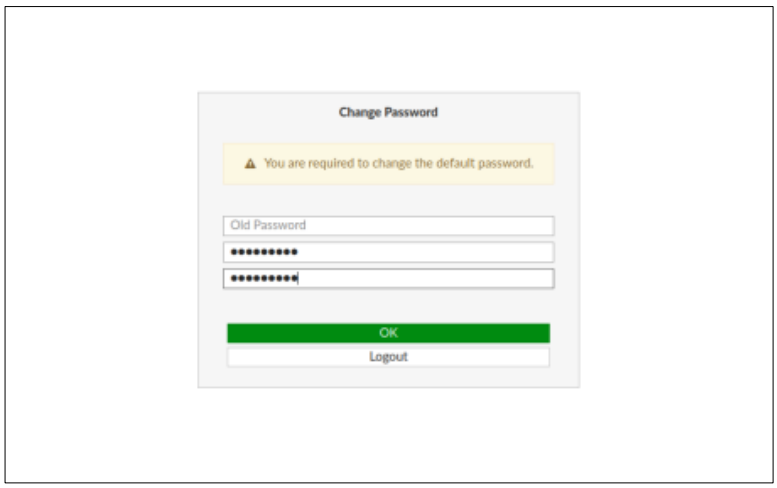

Ilustración 2: Interfaz web de cambio de contraseña.

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

5.2 AUTORIZACIÓN DEL FORTIAP

Antes de autorizar el FortiAP 7.2.0 desde el FortiGate, el AP deberá estar conectado a la interfaz FortiLink para la administración de los APs. Dicha red deberá proporcionar conectividad de gestión entre el FortiAP y el FortiGate, de forma que el FortiGate pueda descubrir el AP y mostrarlo como pendiente de autorización.

La red 192.168.1.0/24 indicada en el apartado anterior corresponde únicamente a un posible escenario de acceso inicial al FortiGate con configuración de fábrica. No constituye un requisito para la autorización del FortiAP ni debe considerarse la red de operación en producción, salvo que coincida expresamente con la arquitectura definida por la organización.

Una vez que el FortiAP haya sido detectado por el FortiGate, existirán dos opciones para autorizarlo. En la primera opción, se puede acceder a la sección de WiFi & Switch Controller --> Managed FortiAP 7.2.0 y hacer clic derecho en el FortiAP. Ahí se hará clic en “Authorize” y se espera a que los dispositivos se vinculen.

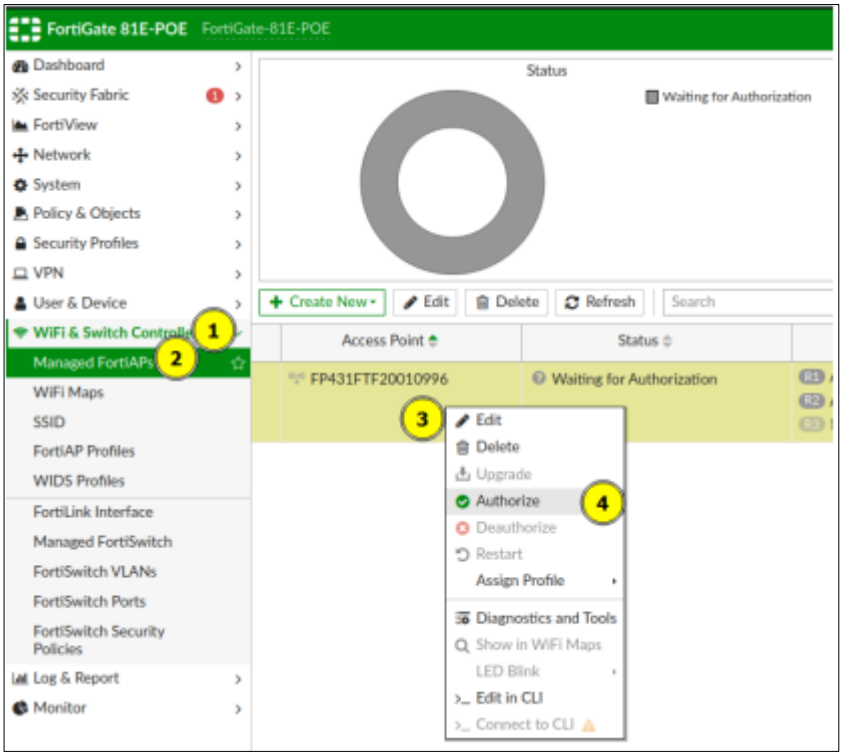

Ilustración 3: Proceso autorización del FortiAP.

Para la otra opción que existe, en la pantalla principal de Dashboard-->Status. Se hace clic en el icono del FortiAP 7.2.0 y después clic en “Authorize”.

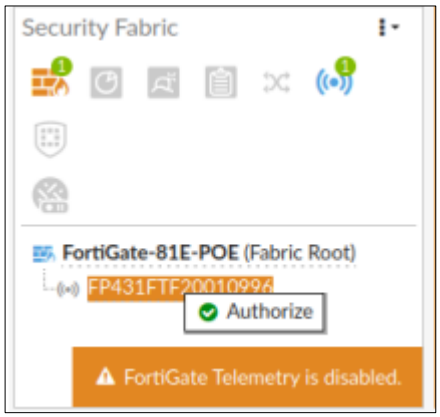

Ilustración 4: Método alternativo de autorización del AP.

Una vez realizado los pasos en una de las dos opciones, tendremos que esperar un par de minutos a que se establezca la conexión entre los dispositivos. Cuando el FortiGate haya identificado el dispositivo FortiAP, en la sección WiFi & Switch Controller --> Managed FortiAPs ya podremos gestionar al AP. El FortiAP 7.2.0 debería aparecer como “Online” en la columna de estatus.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

Para que el producto opere en la configuración segura evaluada, deberán aplicarse las siguientes medidas de configuración que consisten en habilitar el modo FIPS con los siguientes pasos:

Se debe acceder a la terminal CLI desde la interfaz web expuesta por el FortiGate.

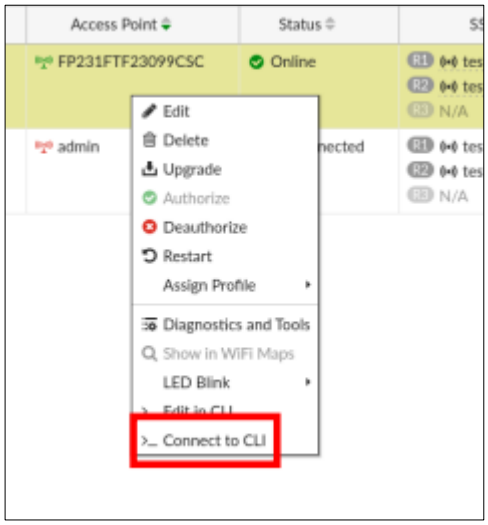

Ilustración 5: Acceso a la CLI del AP a través de la interfaz web.

Dentro de la terminal CLI se pedirá autenticarse con las credenciales del usuario con el que se ha iniciado sesión en la interfaz web. Una vez se ha iniciado sesión se debe ejecutar el siguiente comando para habilitar el modo FIPS:

```
cfg -a FIPS_CC=1
```

Una vez se haya configurado el FortiAP 7.2.0 a través del CLI, se deberá deshabilitar la configuración remota del FortiAP 7.2.0. Tras esto, el FortiAP solo podrá ser configurado a través de la interfaz web expuesta por el FortiGate

Para realizar dicha configuración se debe acceder a la sección FortiAP Profiles, donde se debe seleccionar el perfil que se le aplica al AP, este puede ser consultado en el apartado Managed FortiAP, de la sección Wifi & Switch Controller.

Una vez conocemos el perfil aplicado al AP accederemos a la sección FortiAP Profiles, y editaremos el que aplica al AP a configurar. En caso de que no se cuente con ningún perfil, se puede crear uno pulsando sobre el botón “Create New”.

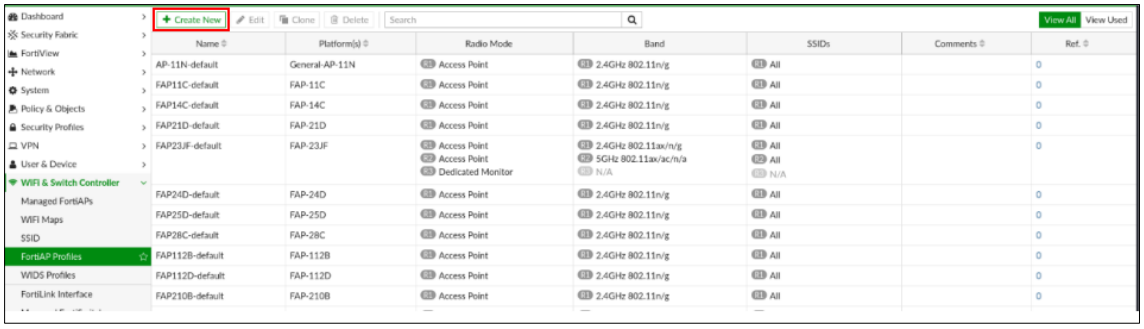

Ilustración 6: Creación del FortiAP Profile.

Dentro de la configuración del perfil se deberán deshabilitarse los mecanismos de administración remota no requeridos desde el perfil del FortiAP: HTTPS, SSH y SNMP.

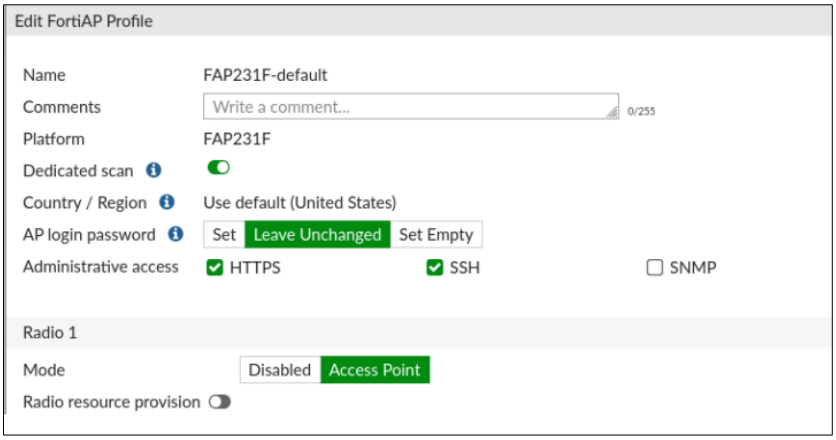

Ilustración 7: Configuración de perfil del FortiAP.

6.2 AUTENTICACIÓN

Los mecanismos de autenticación que utiliza el producto para autenticar a un usuario son los siguientes:

a) Credenciales administrativas gestionadas a través del dispositivo FortiGate utilizado para la administración del FortiAP 7.2.0.

b) Autenticación de usuarios inalámbricos mediante WPA2/WPA3.

c) Autenticación IEEE 802.1X mediante servidor RADIUS externo para despliegues WPA2/WPA3 Enterprise. Su configuración se describe en la sección 6.6 SERVIDORES DE AUTENTICACIÓN.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

La administración del producto deberá realizarse a través del dispositivo FortiGate autorizado utilizando interfaces de administración seguras.

La administración remota podrá realizarse mediante:

a) interfaz web HTTPS,

b) interfaz CLI mediante SSHv2.

La administración remota directa sobre el FortiAP 7.2.0 deberá permanecer deshabilitada en la configuración segura evaluada. Para deshabilitar los mecanismos de administración remota del FortiAP 7.2.0 deberá hacerse tal y como se indica en el apartado *6.1 MODO DE OPERACIÓN SEGURO*.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

En este caso no es necesario hacer ninguna configuración en específico, ya que la gestión de administradores del entorno FortiAP 7.2.0 se realiza a través del dispositivo FortiGate utilizado para la administración centralizada de los mismos.

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

En este caso no es necesario hacer ninguna configuración en específico para el producto, sin embargo, se recomienda que el producto se configure minimizando la exposición de interfaces, puertos y servicios no necesarios para la operación prevista.

Se recomienda utilizar una interfaz de red específica del FortiGate, física o lógica mediante VLAN, para la gestión de los dispositivos FortiAP. Dicha interfaz deberá formar parte de una red de gestión segregada, destinada exclusivamente a la administración y monitorización de los componentes autorizados del entorno.

6.5 GESTIÓN DE CERTIFICADOS

El FortiAP 7.2.0 implementa mecanismos criptográficos para el establecimiento de canales seguros y validación de certificados conforme a la configuración evaluada.

Los algoritmos y funciones criptográficas identificados en la evaluación del producto son los siguientes:

a) RSA de 2048 bits para generación y verificación de firmas. El FortiAP 7.2.0 soporta también longitudes de clave superiores, incluyendo 3072 y 4096 bits. No obstante, la compatibilidad concreta de dichas configuraciones deberá verificarse conforme a la documentación oficial del fabricante y, en caso necesario, consultarse directamente con el fabricante para validar su soporte dentro del entorno operacional previsto.

b) ECDSA con curvas P-256, P-384 y P-521.

c) Funciones hash SHA-256, SHA-384 y SHA-512.

d) DTLS 1.2 para establecimiento de canales seguros.

6.6 SERVIDORES DE AUTENTICACIÓN

El FortiAP 7.2.0 soporta autenticación externa mediante servidores RADIUS para despliegues WPA2/WPA3 Enterprise utilizando IEEE 802.1X.

La configuración del servidor RADIUS puede realizarse desde la sección "User & Device -> RADIUS Servers" dentro de la interfaz de administración del FortiGate. Para más información consultar la sección "WPA2 Security" de [CONFIGURATION_GUIDE].

6.7 ACTUALIZACIONES

Las actualizaciones del firmware del producto deberán realizarse exclusivamente utilizando paquetes oficiales obtenidos desde el portal de soporte del fabricante [SOPORTE].

El proceso de actualización del FortiAP 7.2.0 se realiza mediante el dispositivo FortiGate utilizado, desde la sección de WiFi & Switch Controller --> Managed FortiAPs. Dentro de esta sección, se hace clic derecho en el dispositivo y seleccionaremos la opción que dice "Upgrade".

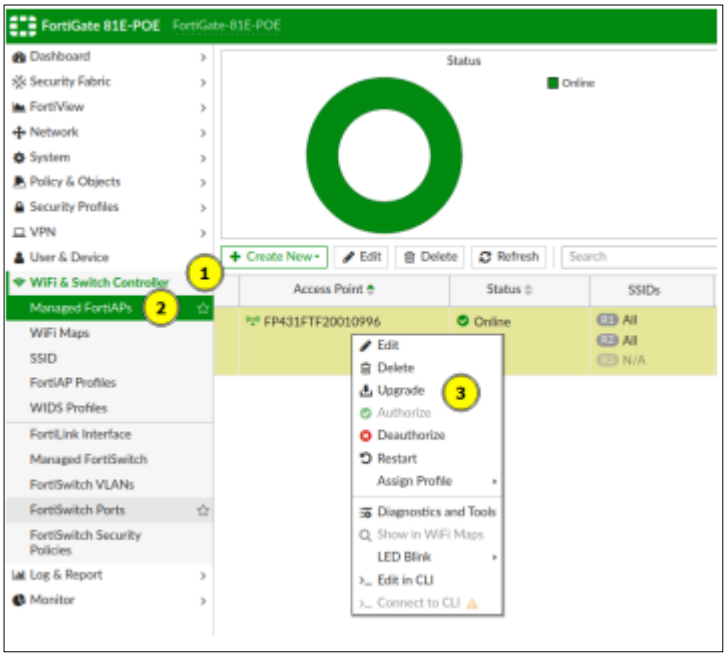

Ilustración 8: Menú de actualización del firmware.

Se hace clic en la opción "Browse" y cargaremos el archivo de actualización. Clic en "Upgrade" y esperaremos a que el FortiAP 7.2.0 descargue y aplique la actualización.

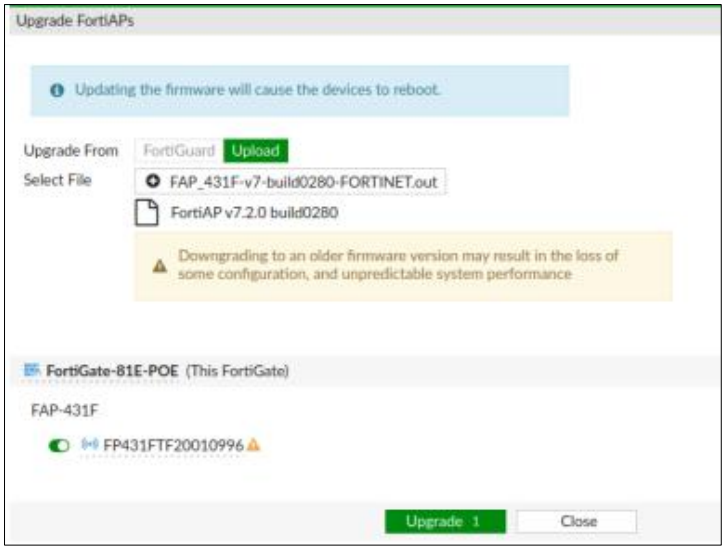

Ilustración 9: Menú de actualización del firmware.

Para más información consultar la sección "FortiAP unit firmware upgrade" de [CONFIGURATION_GUIDE].

6.8 AUTO-CHEQUEOS

El FortiAP 7.2.0 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. No se pueden realizar de forma manual de forma que, para una verificación bajo demanda, habría que reiniciar el producto.

En caso de fallo en la verificación el proceso de arranque se bloquearía, y se pasaría a arrancar desde la partición de backup. El FortiAP 7.2.0 cuenta con dos particiones para que en caso de que la partición primaria se corrompiese por algún motivo durante la ejecución, este pudiera arrancar de igual manera desde la partición secundaria. En caso de que la segunda partición también estuviera corrupta, el AP no terminaría de arrancar y no se conectaría al FortiGate, quedando solo abierto el acceso local para la carga de un firmware válido mediante TFTP.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

El FortiAP 7.2.0 genera registros de auditoría relativos a eventos de seguridad y operación del sistema conforme a la configuración evaluada.

Entre los eventos registrados por el AP se incluyen:

a) Al inicio y finalización de las funciones de auditoría.

b) Login y logout de usuarios registrados.

c) Cambio en las credenciales de usuarios.

d) Cambios en la configuración del producto.

e) Peticiones de asociación.

f) Peticiones de autenticación.

g) Fallos de autenticación.

h) Desconexión de clientes.

Los registros de auditoría incluyen información relativa a:

a) fecha y hora del evento,

b) tipo de evento identificado,

c) resultado del evento,

d) usuario que produce el evento.

Los registros generados por el FortiAP 7.2.0 son enviados al dispositivo FortiGate utilizado para la administración centralizada del entorno operacional, donde se realiza su almacenamiento persistente y gestión de auditoría.

6.9.2 ALMACENAMIENTO LOCAL

El FortiAP 7.2.0 no realiza almacenamiento persistente local de registros de auditoría.

Los registros generados por el FortiAP 7.2.0 se almacenan únicamente de forma temporal en memoria RAM antes de ser enviados al dispositivo FortiGate utilizado para la administración centralizada del entorno operacional.

6.9.3 ALMACENAMIENTO REMOTO

El almacenamiento remoto de registros de auditoría puede realizarse mediante las capacidades de registro del dispositivo FortiGate utilizado para la administración centralizada del FortiAP 7.2.0.

La configuración de servidores syslog externos de auditoría deberá realizarse desde las funcionalidades de registro del dispositivo FortiGate. Para configurar el envío de estos registros de auditoría a un servidor syslog externo consultar la sección “Configuring a Syslog Profile” de [CONFIGURATION_GUIDE].

6.10 BACKUP

La configuración operativa del FortiAP 7.2.0 en la configuración segura evaluada se gestiona de forma centralizada desde el dispositivo FortiGate. Por este motivo, las copias de seguridad de la configuración deberán realizarse desde el FortiGate utilizado para la administración del entorno.

El backup de configuración del FortiGate deberá incluir, cuando aplique, los perfiles FortiAP, la configuración de SSID, los parámetros de seguridad WLAN, la configuración de servidores RADIUS, las opciones de gestión, las políticas asociadas y cualquier otro parámetro necesario para restaurar la operación segura del entorno FortiAP.

Tras la instalación, se deberá realizar una copia de seguridad de la configuración del producto. Asimismo, se recomiendo la realización de forma periódica de copias de seguridad tras cualquier cambio relevante de configuración, actualización de firmware o modificación de parámetros de seguridad.

7 REFERENCIAS

[CONFIGURATION_GUIDE]	Configuration Guide FortiWiFi and FortiAP 7.2.0 (https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/89ea0dba-bc2e-11ec-9fd1-fa163e15d75b/FortiWiFi_and_FortiAP-7.2.0-Configuration_Guide.pdf).
[QUICKSTART_GUIDE]	FortiAP 7.2.0 U431F/U433F Quick Start Guide (https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/3bdcf4a9-acb8-11e9-901c-00505692583a/FortiAP-U433F-431F.pdf).
[CPSTIC]	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN. https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic
[FORTINET]	Portal oficial https://support.fortinet.com/
[SOPORTE]	Portal de soporte del fabricante https://support.fortinet.com/Download/FirmwareImages.aspx

8 ABREVIATURAS

AP	Access Point
CA	Certificate Authority
CC	Common Criteria.
CLI	Command Line Interface.
CPSTIC	Catálogo de Productos y Servicios de STIC.
DTLS	Datagram Transport Layer Security
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
IEEE	Institute of Electrical and Electronics Engineers
MitM	Man-in-the-Middle
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial-In User Service
RAM	Random-access memory
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access