Guía de Seguridad de las TIC
CCN-STIC 1013

Procedimiento de Empleo Seguro
Adtran FSP 3000R7 Network Element release 22.5.2



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:01 +01:00

Fecha de Edición: Noviembre de 2026

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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 6
3 ORGANIZACIÓN DEL DOCUMENTO 6
4 CONFIGURACIÓN EVALUADA 7
4.1 COMPONENTES DEL PRODUCTO EN LA CONFIGURACIÓN EVALUADA 7
4.2 COMPONENTES Y APLICACIONES QUE NO SE INCLUYEN EN LA CONFIGURACIÓN EVALUADA 8
5 FASE PREVIA A LA INSTALACIÓN 14
5.1 ENTREGA SEGURA DEL PRODUCTO 14
5.2 ENTORNO DE INSTALACIÓN SEGURO 14
5.3 COMPONENTES DEL ENTORNO DE OPERACIÓN 14
6 FASE DE INSTALACIÓN 16
7 FASE DE CONFIGURACIÓN 17
7.1 MODO DE OPERACIÓN SEGURO 17
7.2 AUTENTICACIÓN 18
7.3 ADMINISTRACIÓN DEL PRODUCTO 19
7.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 19
7.3.2 CONFIGURACIÓN DE ADMINISTRADORES 20
7.4 CONFIGURACIÓN CRIPTOGRÁFICA 20
7.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 22
7.6 GESTIÓN DE CERTIFICADOS 22
7.7 ACTUALIZACIONES 24
7.8 AUTO-CHEQUEOS 26
7.8.1 COMPROBACIÓN DE LA INTEGRIDAD DEL SOFTWARE 27
7.8.2 COMPROBACIÓN CRIPTOGRÁFICA 27
7.9 AUDITORÍA 27
7.9.1 REGISTRO DE EVENTOS 27
7.9.2 ALMACENAMIENTO LOCAL 28
7.9.3 ALMACENAMIENTO REMOTO 28
8 REFERENCIAS 30
9 ABREVIATURAS 32

ÍNDICE DE ILUSTRACIONES

Ilustración 1 Plataforma NCU3 5
Ilustración 2. Módulos opcionales 5
Ilustración 3. Entorno operacional del dispositivo 15
Ilustración 4. Auditoría relativa al auto-chequeo 26
Ilustración 5. Auditoría relativa al auto-chequeo (pruebas criptográficas) 26

ÍNDICE DE TABLAS

Tabla *1*. Propiedades del producto 4
Tabla *2*. Componentes del producto evaluados 7
Tabla *3*. Componentes de soporte para el entorno operacional 8
Tabla *4*. Especificaciones de los modelos del producto (management) 9
Tabla 5. Especificaciones de los modelos del producto (operational) 10

Tabla 6. Manuales del FSP 3000R7 11
Tabla *7*. Servicios Criptográficos 12
Tabla *8*. Suites de Cifrado del dispositivo en el modo de operación seguro 18
Tabla *9*. Roles y privilegios del dispositivo 18
Tabla 10. Ficheros de auditoria según el tipo de evento 28

1 INTRODUCCIÓN

El producto es un dispositivo de red compuesto por el Adtran FSP3000 (hardware) y la versión 22.5.2 del sistema operativo. El sistema operativo del sistema Adtran FSP 3000R7 se encuentra en la Unidad de Control de Red 3 (NCU-3). El producto, también denominado FSP 3000R7 a partir de este momento, es una herramienta de gestión de redes ópticas. El producto es una solución de transporte óptico escalable que se adapta a las demandas de ancho de banda de la red en la que se instala y garantiza la transferencia segura de datos a través de la red.

El producto puede desplegarse como cualquiera de los tres tipos de modelo siguientes: aunque el hardware entre los modelos cambia de tamaño para dar cabida a ranuras de módulos adicionales, el procesador sigue siendo el mismo. Todos los modelos utilizan el mismo software.

Property	SH1HU	SH7HU	SH9HU
Power	AC/DC/Mix	AC/DC/Mix	AC/DC/Mix
Processor	NCU-3 (NXP QorIQ e5500 model T1042E)	NCU-3 (NXP QorIQ e5500 model T1042E)	NCU-3 (NXP QorIQ e5500 model T1042E)
Size	1 rack unit	7 rack units	9 rack units
Module Slots	2	16	16

Tabla 1. Propiedades del producto

En su configuración evaluada, el sistema operativo FSP 3000R7 es un dispositivo de red autónomo compuesto por la plataforma de hardware NCU-3 y módulos opcionales para la conectividad de red operativa.

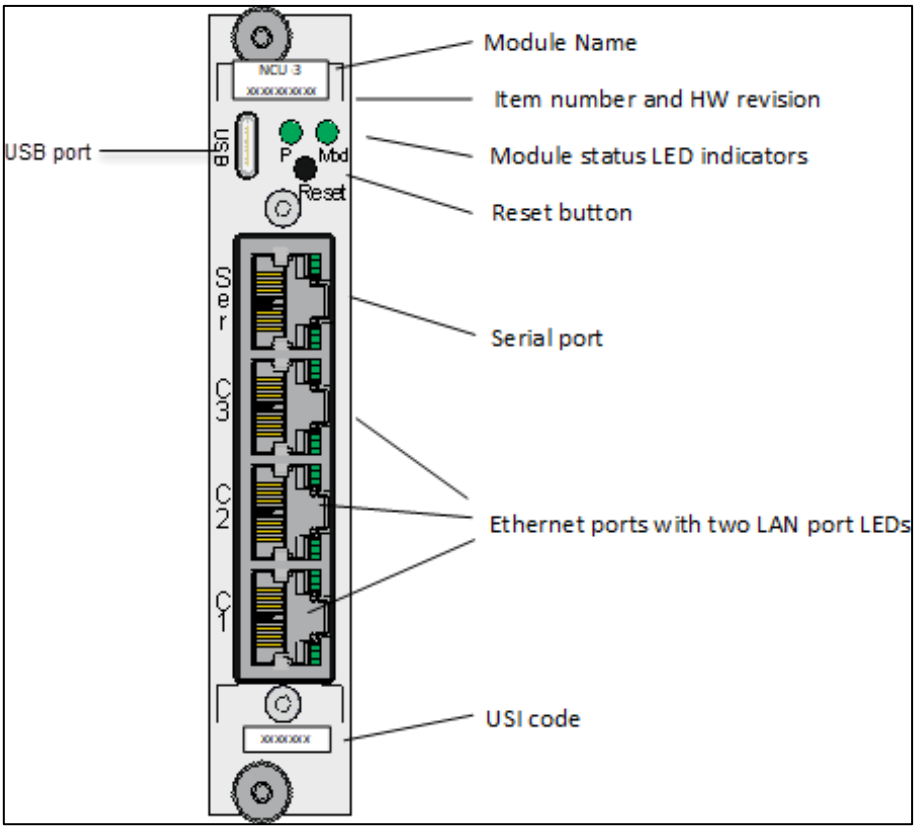


Ilustración 1 Plataforma NCU3



Ilustración 2. Módulos opcionales

2 OBJETO Y ALCANCE

El objeto del presente documento es facilitar la instalación y configuración segura del router **Adtran FSP 3000R7 con** el sistema operativo release **22.5.2**, junto con el aseguramiento del entorno en el que se despliega.

El producto Adtran FSP 3000R7 ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF20].

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado 4. En este apartado se recogen los aspectos y componentes de la configuración evaluada del producto.

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

c) Apartado 6. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

d) Apartado 7. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 CONFIGURACIÓN EVALUADA

4.1 COMPONENTES DEL PRODUCTO EN LA CONFIGURACIÓN EVALUADA

La siguiente tabla describe los componentes del producto en la configuración evaluada:

Componente del TOE	Descripción del Componente	Modelo Hardware	Versión del Software
Adtran FSP 3000R7 Sistema Operativo	Utilizado por el administrador de seguridad para la gestión del transporte de la red óptica	SH1HU, SH7HU, SH9HU	Rel 22.5.2

Tabla 2. Componentes del producto evaluados

Nota$_1$: Los tres modelos ofrecen las mismas funciones de seguridad. Las únicas diferencias son el tamaño y el número de ranuras, que se utilizan para proporcionar más conexiones al dispositivo de red. Estas diferencias pueden consultarse en [REF17].

Estos componentes y la funcionalidad que proporcionan están fuera del alcance de las pruebas de evaluación, pero son necesarios para apoyar la funcionalidad probada del producto. La siguiente tabla enumera los componentes y aplicaciones utilizados en el entorno operativo para la configuración evaluada del producto.

Componente	Definición
Terminal	Un terminal es un dispositivo que maneja la entrada y visualización de datos cuando se conecta al puerto serie de un dispositivo. También se puede acceder a la CLI del producto de forma local con una conexión física al producto mediante el conector eléctrico tipo RJ45 o el puerto serie y se debe utilizar un emulador de terminal VT100 que sea compatible con las comunicaciones serie. Sinónimo del término consola local. Este componente del producto debe soportar la interfaz E1 definida en la Tabla 3: Metodología y criterios de evaluación.
Estación de trabajo de gestión remota	Cualquier ordenador de uso general utilizado por un administrador para gestionar el producto. Para que el producto pueda ser administrado remotamente se requiere que la estación de trabajo de administración tenga: • Navegador compatible para acceder a la GUI Web del producto Cliente SSHv2. • Cliente SSHv2 instalado para acceder a la CLI del producto. El producto actúa como servidor para todos los protocolos. Las comunicaciones TCP desde la estación de trabajo de administración remota hasta el TOE están protegidas mediante • **SSH** para el acceso remoto a la CLI. • **HTTPS** para el acceso remoto a la GUI Web. Este componente TOE es necesario para soportar las interfaces E2 y E3.

Servidor de auditoría	El TOE actúa como cliente TLS cuando se conecta a un servidor de auditoría para enviar los registros de auditoría para su almacenamiento remoto. Este componente del TOE debe admitir la interfaz E4 definida en la figura 3 para enviar copias de los datos de auditoría que se almacenarán en una ubicación remota a efectos de redundancia de datos.
Servidor de autoridad de certificación (CA)	Un servidor que actúa como emisor de confianza de certificados digitales y distribuye una CRL que identifica los certificados revocados. Este componente del producto es necesario para soportar la interfaz E5 definida en la figura 3.
Servidor NTP	El TOE puede conectarse a un servidor NTP para mantener marcas de tiempo precisas para el producto y los registros de auditoría generados. Este componente del TOE debe admitir la interfaz E6 definida en la figura 3.
Red OTH o WDM	La red OTH o WDM representa la jerarquía de transporte óptico y los componentes de división de longitud de onda. La figura 3 identifica estas interfaces como una única interfaz. La interfaz con la red OTH o WDM gestionada es una conexión independiente con el entorno operativo de la empresa que gestiona el producto. No hay SFR para abordar la gestión de la red OTH o WDM por parte del TOE. Por lo tanto, la interfaz E7 a estos componentes está fuera del alcance de la evaluación complementaria para su inclusión en CPSTIC. Esta interfaz y sus componentes se incluyen únicamente a efectos de exhaustividad.

Tabla 3. Componentes de soporte para el entorno operacional

4.2 COMPONENTES Y APLICACIONES QUE NO SE INCLUYEN EN LA CONFIGURACIÓN EVALUADA

Las siguientes funcionalidades, componentes y aplicaciones del producto no forman parte de la configuración evaluada. Estos elementos no proporcionan funcionalidades de seguridad adicionales para el producto evaluado y se clasifican en las siguientes categorías:

a) Componentes no instalados.

b) Componentes instalados que requieren una licencia independiente para su activación.

c) Componentes instalados que no forman parte de la TSF.

No hay componentes, aplicaciones y/o funcionalidades que no estén instalados. Asimismo, no hay componentes, aplicaciones o funcionalidades excluidos que requieran una licencia independiente para su activación.

Algunos componentes instalados forman parte del producto adquirido, pero cuyas funcionalidades no forman parte de la funcionalidad de la TSF considerada en la evaluación realizada frente al perfil de protección.

El Adtran FSP 3000R7 incluye una serie de capacidades proporcionadas a través de los módulos del Plano de Datos Operativos identificados en la Tabla 8, destinadas a dar soporte a su funcionalidad principal. Estas capacidades quedan fuera del alcance del Perfil de Protección reivindicado [REF15] y, por tanto, no forman parte del TSF, ya que no existe ningún SFR aplicable a ellas.

La siguiente tabla describe los modelos de producto y sus diferenciadores clave que forman parte de la evaluación.

Propiedad	SH1HU	SH7HU	SH9HU	Definición de acrónimo
Alimentación	AC/DC/Mix	AC/DC/Mix	AC/DC/Mix	NCU-Unidad de control de red
Procesador	NCU-3 (NXP QorIQ T1042E)	NCU-3 (NXP QorIQ T1042E)	NCU-3 (NXP QorIQ T1042E)	
Conexión de consola local	RJ45 Jack Serial Connector	RJ45 Jack Serial Connector	RJ45 Jack Serial Connector	
	1 USB Port	1 USB Port	1 USB Port	
Conexión de red de gestión	3 RJ45 Ethernet	3 RJ45 Ethernet	3 RJ45 Ethernet	
Tamaño	1 rack unit	7 rack unit	9 rack unit	
Ranuras para módulos	2	16	19	
Comunes	FAN/1HU, PSU/1HU-AC, PSU/1HU-DC	FAN/Plug-in, PSU/7HU-AC, PSU/7HU-DC	CEM/9HU, FAN/9HU, PSU/9HU-AC, PSU/9HU-DC	PSU/HU-Unidad de fuente de alimentación/Unidad de carcasa CEM-Módulo de equipo común

Tabla 4. Especificaciones de los modelos del producto (management)

La funcionalidad de seguridad fuera del ámbito está contenida en el plano operativo. Toda la funcionalidad del plano operativo no es compatible con SFR, incluidos los módulos de cifrado definidos en la tabla siguiente. La siguiente tabla identifica los módulos enchufables disponibles para cada tipo de modelos de la serie Adtran FSP 3000R7.

Propiedad	SH1HU	SH7HU	SH9HU
Chassis / Shelf Configuration			
Passive shelf	SH1HU/PASSIVE/FT 1 rack unit 4 module slots	SH1HU/PASSIVE/FT 1 rack unit 4 module slots	SH1HU/PASSIVE/FT 1 rack unit 4 module slots
Management and switch modules			
Management and switch modules	SCU-II, UTM, PSCU, OSCM-PN, HDSCM-PN, OPPM	SCU-II, UTM, PSCU, OSCM-PN, HDSCM-PN, OPPM	SCU-II, UTM, PSCU, OSCM- PN, HDSCM-PN,OPPM
Optical Modules			
Reconfigurable optical modules	4ROADM,MROADM,PSM40, PSM80,4-OPCM	9ROADM,4ROADM,MROADM,PSM40, PSM80,4-	9ROADM,4ROADM,MROADM,PSM40, PSM80,4-OPCM

		OPCM	
Optical amplifiers	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)	GCB, V(L)GC(B), RAMAN, AMP, EDFA, 2EDFA, MA(L)P(B), MTP(B)
Access modules	2WCA, 5WCA, 6WCA	2WCA, 5WCA, 6WCA	2WCA, 5WCA, 6WCA
Client / Service Modules			
Core 100G modules	WCC, 4TCC, 10TCC	None	WCC, 4TCC, 10TCC
Core <100G modules	2(16)TCC, 2(4)WCC	2(16)TCC, 2(4)WCC	2(16)TCC, 2(4)WCC
Enterprise 100G modules	10TCE	None	10TCE
Enterprise <100G modules	9TCE	9TCE	9TCE
Encryption modules	9TCE+AES, 10TCE+AES, WCC+AES	9TCE+AES	9TCE+AES, 10TCE+AES, WCC+AES
Auxiliary Optical Modules			
Dispersion compensation modules	DCF, DCG	DCF, DCG	DCF, DCG
Passive filter modules	OSFM(A),(x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM	OSFM(A),(x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM	OSFM(A), (x)PSM, (x)PM, (x)PSM(x), ILM, (x)CSM

Tabla 5. Especificaciones de los modelos del producto (operational)

Para la versión 22.5.2 del sistema operativo Adtran FSP 3000R7, en estos manuales de usuario se ofrece orientación para los usuarios. En las notas de la versión R22.5.2 se ofrecen referencias adicionales.

Componente del producto	Descripción del Componente	Modelo Hardware	Versión del Software
Manuales pertinentes para la evaluación complementaria del STIC			
Installation and Commission-ing Manual ([REF4])	FSP3000R7_R22.5_Installation_and_Commissioning_ Manual_IssueA.pdf	22.5 Issue A	December 2023
Secure System Configuration ([REF5])	FSP3000R7_R22.5_Secure_System_Configuration_Guide _IssA.pdf	22.5 Issue A	2023
Otros manuales de productos			

Hardware Description ([REF6])	FSP3000R7_R22.5_Hardware_Description_IssueB.pdf	22.5 Issue B	February 2024
High-Density Subshelf Hardware Guide ([REF7])	FSP3000R7_R22.5_High-Density_Subshelf_Guide_IssA.pdf	22.5 Issue A	December 2023
Maintenance and Troubleshoot-ing Manual ([REF8])	FSP3000R7_R22.5_Maintenance_and_Troubleshooting_Manual_IssA.pdf	22.5 Issue A	December 2023
Management Data Guide ([REF9])	FSP3000R7_R22.5_Management Data Guide_IssA.pdf	22.5 Issue A	2023
Module and System Specification ([REF10])	FSP3000R7_R22.5_Module_System_Specification_Issue A.pdf	22.5 Issue B	February 2024
NETCONF User Guide ([REF11])	FSP3000R7_R22.5_NETCONF_User_Guide_IssA.pdf	22.5 Issue A	December 2023
Network Element Director Online Help ([REF12])	FSP3000R7_R22.5_Network_Element_Director_Help_Iss A.zip	22.5 Issue A	2023
Provisioning and operations Manual ([REF13])	FSP300R7_R22.5_Provisioning_and_Operations_Manual_IssA.pdf	22.5 Issue A	December 2023
Safety Guide ([REF14])	FSP3000R7_R22.5_Safety_Guide_IssA.pdf	22.5 Issue A	December 2023

Tabla 6. Manuales del FSP 3000R7

Para obtener más información sobre los manuales que incluyen secciones relacionadas con la seguridad, consulte los documentos de orientación sobre garantías (AGD) correspondientes.

El límite lógico del producto se divide en las siguientes características de seguridad que han sido delimitadas por el perfil de protección [REF15].

- Auditoría de seguridad
- Soporte criptográfico
- Gestión de la seguridad
- Protección del TSF
- Vías/canales de confianza

El producto contiene mecanismos para generar datos de auditoría para registrar eventos predefinidos en el mismo. El producto tiene la capacidad de almacenar registros de auditoría localmente y liberará espacio de almacenamiento de auditoría borrando los

archivos archivados según el orden de entrada y salida. El administrador de seguridad puede configurar el reenvío de eventos a un servidor de auditoría externo. En la configuración evaluada, los datos de auditoría se transmiten de forma segura al servidor de auditoría utilizando un canal de comunicación TLS v1.2.

El producto ofrece criptografía para las comunicaciones seguras SSH y TLS (v1.2 y v1.3). OpenSSL se utiliza para todas las comunicaciones TLS y SSH. El producto destruye inmediatamente las claves cuando ya no se utilizan. La siguiente tabla identifica los servicios criptográficos:

SFR	Implementación de OpenSSL CAVP ##A4284
FCS_CKM.1	ECC schemes using NIST curves P-256, P-384 and P-521 following FIPS PUB 186-4
	FFC using safe-prime groups per NIST Special Publication 800-56A Revision 3 and RFC 3526
FCS_CKM.2	Elliptic curve-based key establishment per NIST Special Publication 800-56A Revision 3
	FFC using safe-prime per NIST Special Publication 800-56A Revision 3 and groups listed in RFC 3526.
FCS_COP.1/DataEncryption	AES GCM 256 bits
FCS_COP.1/SigGen	ECDSA FIPS 186-4 Signature Services 256 bits or greater
FCS_COP.1/Hash	SHA-256, SHA-384 and SHA-512
FCS_RBG_EXT.1	CTR DRBG (AES-256)

Tabla 7. Servicios Criptográficos

El producto utiliza un control de acceso basado en roles de usuario (sección User Authentication and Authorization del documento [REF12]) para evitar la gestión y el acceso no autorizados a los datos del TSF. El producto mantiene el rol de administrador de seguridad, que puede administrar el TOE local y remotamente.

El producto garantiza la seguridad e integridad de todos los datos que se almacenan localmente y a los que se accede de forma remota. Las contraseñas no se almacenan en texto plano, sino que se cifran mediante SHA-512. Un administrador de seguridad tiene la capacidad de consultar la versión que se está ejecutando actualmente del software producto y debe iniciar manualmente el proceso de actualización. Antes de la instalación, el producto verifica automáticamente el certificado X509 utilizado para firmar la actualización del software. En la configuración de evaluación, si el certificado no es válido por cualquier motivo o falta, la actualización no se instala. El producto implementa un mecanismo de autocomprobación que se ejecuta automáticamente durante la puesta en marcha inicial para verificar el correcto funcionamiento del producto y de las funciones criptográficas. El TOE proporciona su propia hora a través de su reloj interno configurable administrativamente o a través de una conexión a un servidor NTP.

Los usuarios pueden acceder a la CLI para las funciones de administración de forma local a través de una conexión física con el producto o de forma remota a través de una conexión SSH en la que el producto actúa como servidor SSH. Los usuarios también pueden acceder

a la GUI web para funciones administrativas a través de una conexión HTTPS en la que el producto actúa como servidor HTTPS/TLS.

El producto actúa como cliente TLS para iniciar el canal seguro a un servidor de auditoría externo.

5 FASE PREVIA A LA INSTALACIÓN

5.1 ENTREGA SEGURA DEL PRODUCTO

Durante el proceso de entrega deberán llevarse a cabo una serie de tareas de comprobación para garantizar que el producto recibido no haya sido manipulado indebidamente:

- **Etiqueta de envío**: deberá comprobarse que la etiqueta de envío identifica correctamente el nombre del cliente, su dirección y el dispositivo.
- **Embalaje externo**: deberá inspeccionarse la caja de envío externa y la cinta adhesiva. Se comprobará que la cinta adhesiva no esté cortada ni se haya deteriorado en ningún punto. Así mismo, la caja no deberá presentar cortes ni daños que permitan acceder al dispositivo.

En caso de identificarse algún problema durante la inspección, el cliente deberá ponerse en contacto inmediatamente con Adtran Networks SE., al que se le indicará el número de pedido, el número de seguimiento y una descripción del problema.

El producto no dispone de etiquetas anti-tampering. Por lo tanto, es necesario realizar una serie de comprobaciones para garantizar que la caja recibida la envió Adtran Networks SE. y no existe una suplantación de identidad. Para ello se aconseja al comprador verificar que efectivamente se ha realizado un pedido de compra al fabricante Adtran Networks SE. y el dispositivo recibido es exactamente el que se ha pedido al fabricante.

5.2 ENTORNO DE INSTALACIÓN SEGURO

Los dispositivos se deberán instalar dentro de un Centro de Procesamiento de Datos (CPD), cuyo acceso estará restringido a un grupo de personas con autorización explícita. Para garantizarlo, la sala que alberga el CPD contará con un sistema de control de acceso que asegure que solo el personal autorizado pueda ingresar al dispositivo, incluso fuera del horario laboral.

Será necesario que se sigan las recomendaciones indicadas en el presente documento, así como en las guías de instalación que se proporcionan junto al producto.

5.3 COMPONENTES DEL ENTORNO DE OPERACIÓN

El router Adtran **FSP 3000R7** debe implementar el sistema operativo con la release **22.5.2**.

Para realizar la configuración inicial del dispositivo será necesario un ordenador que permita al administrador realizar la administración de manera local o remota del dispositivo tal y cómo se indica en Ilustración 3. Entorno operacional del dispositivo.

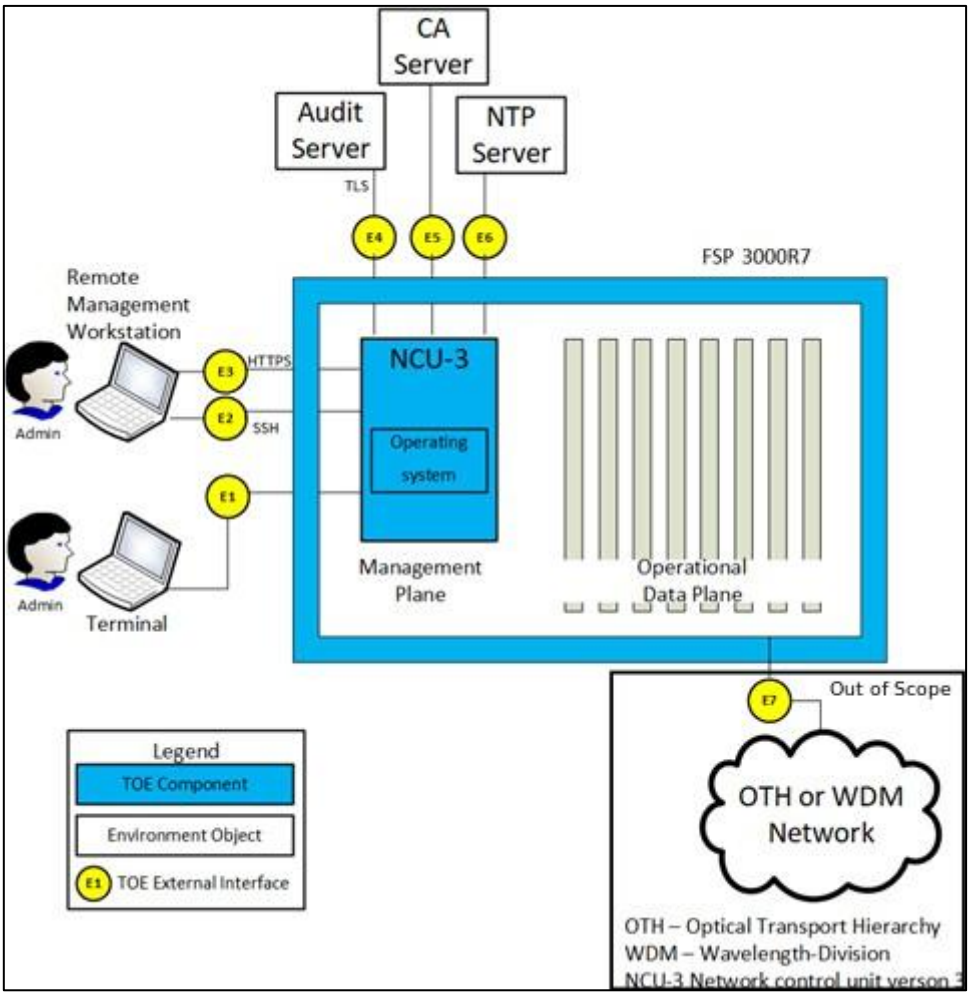


Ilustración 3. Entorno operacional del dispositivo

El ordenador utilizado por el administrador debe de disponer de un cliente SSH para realizar la comunicación con el dispositivo de manera remota.

6 FASE DE INSTALACIÓN

La fase de instalación del producto se considera únicamente como la instalación física del producto. Una vez la instalación física del producto se ha realizado, se pasará a la parte de configuración.

7 FASE DE CONFIGURACIÓN

Una vez instalado el router es necesario configurarlo. A continuación, se muestran los pasos a seguir para configurar el producto. Para más información consultar las guías [REF1], [REF2] y [REF3].

7.1 MODO DE OPERACIÓN SEGURO

Para activar el modo de operación seguro el usuario deberá de seguir los pasos descritos en el presente documento.

En concreto es obligatorio seguir las secciones indicadas a continuación, para que el dispositivo realice las siguientes funciones:

- Sección 7.4 CONFIGURACIÓN CRIPTOGRÁFICA: No permitirá el establecimiento de cualquier tipo de conexión que utilice suites de cifrado diferentes a las autorizadas durante la configuración.
- Sección 7.2 AUTENTICACIÓN: Las contraseñas se almacenarán protegidas con algoritmos sólidos (funciones hash/resumen). Así mismo, la política de contraseñas forzara a que las contraseñas de los usuarios estén compuestas por 15 caracteres como mínimo y contengan al menos una letra minúscula, una letra mayúscula, un número y un carácter especial.
- Sección 7.3.2 CONFIGURACIÓN DE ADMINISTRADORES: Implementará mecanismos de prevención de fuerza bruta por medio de blacklist.

Conecte el puerto de consola (COM) a una computadora portátil o PC utilizando un cable RJ-45. Utilizar la velocidad de conexión serie por 9600 bps.

Inicie sesión como administrador haciendo uso de las credenciales por defecto:

```
username: ADMIN
password: CHGME.1A
```

Nota$_2$: Durante esta configuración inicial, el producto obliga al usuario a cambiar la contraseña por defecto por una contraseña no por defecto. Una vez que el modo de operación seguro (Enhanced Security Mode está activado, la contraseña por defecto (CHGME.1A) nunca será aceptada como una contraseña válida en cualquier intento futuro de cambiar la contraseña.

Para activar el modo de operación seguro será necesario navegar hasta el siguiente menú: *System Security Management > Security Settings > General*. En el campo *Security Mode* seleccionar el modo *Enhanced*, y aplicar los cambios.

El dispositivo hará uso de las siguientes suites de cifrado para los diferentes tipos de conexiones:

	Criptografía TLS (software)	Criptografía SSH (software)
Algoritmos de Encriptación		
AES-128-GCM	Sí	No
AES-256-GCM	Sí	Sí
Algoritmos de autenticación por clave publica		
ecdsa-sha2-nistp256	Sí	Sí

ecdsa-sha2-nistp384	Sí	Sí
ecdsa-sha2-nistp521	Sí	Sí
Intercambio de clave para SSH		
diffie-hellman-group15-sha512	-	Sí
diffie-hellman-group16-sha512	-	Sí
diffie-hellman-group18-sha512	-	Sí
ecdh-sha2-nistp256	-	Sí
ecdh-sha2-nistp384	-	Sí
ecdh-sha2-nistp521	-	Sí

Tabla 8. Suites de Cifrado del dispositivo en el modo de operación seguro

7.2 AUTENTICACIÓN

Se utilizan contraseñas que contengan al menos una letra mayúscula, una letra minúscula, un número y un carácter especial con una longitud mínima de 15 caracteres como mecanismo de autenticación para los usuarios del producto.

Por otra parte, durante la configuración inicial, el producto forzará al usuario a cambiar la contraseña por defecto del usuario administrador.

Esta autenticación será la que se utilice tanto para el inicio de sesión de manera local por el puerto serie como de manera remota haciendo uso de SSH.

Para que el mecanismo de autenticación funcione según los requisitos de cualificación del producto se deben realizar las siguientes acciones:

- Configurar la política de contraseña correcta. Esto hará que se exija una contraseña de una longitud mínima de 15 caracteres y al menos una letra minúscula, una mayúscula, un carácter numérico y un carácter especial. Para ello será necesario acceder al TOE como el usuario administrador y navegar hasta la siguiente ruta: *System Security Management > Security Settings > Login > Min Password Length*, y escribir en el campo un valor entre 15 y 128.

Nota$_3$: El resto de requisitos de la política de contraseñas están activados una vez configurado el modo de operación seguro.

Nota$_4$: Existen dos tipos de roles predefinidos en el producto:

Rol predefinido	Privilegios
Administrator	Tiene capacidad para desempeñar todas las funciones de gestión definidas por el PP ([REF15]).
Provision	Las capacidades administrativas se limitan a la actualización del software del producto.

Tabla 9. Roles y privilegios del dispositivo

Para crear una cuenta de usuario habrá que conectarse al producto y navegar a la siguiente ruta: *System Security Management > User Management*. Seleccionar la opción de *Add* y seleccionar el rol de usuario. Después, seleccionar la opción *Next* y después *Next*.

Especificar la contraseña del usuario e introducir un valor entre el 1 y el 10 para el campo *Login Fail Count*. Después de esto seleccionar *Apply*.

Se recomienda que las cuentas con rol de administrador sean nominales y de uso exclusivo por una única persona, evitando el uso de cuentas compartidas.

Configurar el tiempo de inactividad máximo entre 30 y 3600 segundos. Para realizar este cambio habrá que conectarse al producto y navegar a la siguiente ruta: *System Security Management > Security Settings > Timeouts*. En el campo *Craft Session Timeout* introducir un valor entre 30 y 3600. Después de esto seleccionar *Apply*.

7.3 ADMINISTRACIÓN DEL PRODUCTO

En el caso de que se desee realizar la administración de manera remota se deberán realizar las siguientes configuraciones:

- Configurar una dirección IP donde quieras realizar las tareas de administración:
  - Conectarse al producto y navegar a la siguiente ruta: *System Management > System IP Settings > System IP*, introducir la dirección IP *192.168.1.1* y aplicar los cambios.

Por defecto SSH y la interfaz Web están desactivados, por tanto, para activarlos es necesario realizar las siguientes acciones de configuración:

- Conectarse al producto y navegar a la siguiente ruta: *System Security Management > SSH Configuration > Ciphers > General*, seleccionando el valor de *Custom* para el campo *SSH Ciphers Profile* y aplicar los cambios.
- Conectarse al producto y navegar a la siguiente ruta: *System Management > System General Setings > Controls*, seleccionando el valor de *Enable* para el campo *Web Interface* y aplicar los cambios.

Para que se apliquen estos cambios será necesario reiniciar el producto, conectándose al dispositivo y seleccionando la opción de *Reboot NCU*.

Para que el producto tenga un correcto funcionamiento a la hora de realizar las conexiones remotas es necesario realizar un paso final de configuración, una vez reiniciado la interfaz web estará disponible en la dirección IP configurada (192.168.1.1). Una vez conectado y autenticado a la interfaz web del TOE, navegar a la siguiente ruta: *Configure > Shelf 1 > Slot A > Ethernet Ports*, editar el puerto ya existente (pj. C1), seleccionar el valor de *Unnumbered* para el campo *IP Configuration*, y aplicar los cambios. En caso de que la opción no esté disponible recrear el puerto y realizar los pasos de configuración sobre el nuevo puerto. Después de realizar estas configuraciones es necesario realizar un reinicio del TOE.

7.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

El producto ofrece administración del dispositivo de manera local por medio del puerto de consola, haciendo uso de un cable RJ-45 y administración remota por medio de los protocolos SSHv2 y TLS a través de una interfaz web.

Gracias a las configuraciones del apartado anterior (sección 7.3 ADMINISTRACIÓN DEL PRODUCTO) un administrador puede acceder al producto de manera local o remota (tanto por SSH como por la interfaz web).

7.3.2 CONFIGURACIÓN DE ADMINISTRADORES

El fabricante detalla en sus guías dos tipos diferentes de usuario que implementa el dispositivo. Estos son descritos en la Tabla 9. Roles y privilegios del dispositivo del presente documento.

En el párrafo 0 de la sección 7.2, el administrador deberá **configurar una política de contraseña conforme a lo requerido en la cualificación**. Antes de crear un usuario, se deberán de seguir los pasos descritos en dicho párrafo.

Después de configurar la política de contraseñas, el administrador podrá crear un usuario utilizando el mismo nombre de usuario definido anteriormente. Es fundamental especificar los privilegios asociados al usuario dentro del sistema mediante el parámetro *role*. Para ello el administrador debe ejecutar los siguientes pasos:

a) Conectarse al producto y navegar a la siguiente ruta: System Security Management > User Management. Seleccionar la opción de Add y seleccionar el rol de usuario.

b) Después, seleccionar la opción *Next* y después *Next*.

c) Especificar la contraseña del usuario e introducir un valor entre el 1 y el 10 para el campo *Login Fail Count*.

d) Después de esto seleccionar *Apply.*

Como mecanismo para evitar ataques de autenticación por fuerza bruta, la siguiente configuración permitirá al producto bloquear usuarios (incluso administradores) cuando superen los intentos de autenticación permitidos por conexión remota, manteniendo que no se pueda bloquear a los administradores por conexión local:

a) Conectarse al producto y navegar a la siguiente ruta: *System Security Management > Security Settings > Login*.

b) Dentro del campo *Account Lockout* seleccionar la opción de *Allow Lock of All Users*.

c) Dentro del campo *Serial Access Lockout* seleccionar la opción de *Do Not Lock Admins*, de esta manera el producto puede bloquear los intentos de fuerza bruta pero los usuarios administradores podrán conectarse por serie.

d) Para activar el mensaje de advertencia antes de la autenticación habrá que conectarse al producto y navegar a la siguiente ruta: *System Security Management > Security Setting > Login*.

e) El valor *Prompt* se seleccionará para el campo *Login Presentation*.

7.4 CONFIGURACIÓN CRIPTOGRÁFICA

Realizar los siguientes pasos para configurar que sólo las ciphersuites permitidas sean las disponibles en el dispositivo.

Para realizar las configuraciones generales del protocolo TLS hay que realizar los siguientes pasos:

a) Conectarse al producto y navegar a la siguiente ruta: *System Security Management > TLS Configuration > General*.

b) Los campos *V1_3* y *V1_2* tienen que estar seleccionados.

c) El valor del campo *TLS Ciphers Profile* debe de tener el valor de *Custom*.

d) El valor del campo *ECDHE curves Profile* debe de tener el valor de *Custom*.

Para configurar las ciphersuites de TLS v1.2 hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > TLS Configuration > TLS1_2*.

b) Seleccionar las siguientes ciphersuites del listado como aceptadas:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Para configurar las ciphersuites de TLS v1.3 hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > TLS Configuration > TLS1_3*.

b) Seleccionar las siguientes ciphersuites del listado como aceptadas:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

Para configurar las curvas elípticas usadas para las comunicaciones TLS hay que realizar lo siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > TLS Configuration > ECDHE Curves*.

b) Seleccionar las siguientes curvas elípticas del listado como aceptadas:

- SECP256R1
- SECP384R1
- SECP521R1

Para configurar los algoritmos de *Host key/Auth key* de SSH hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > SSH Configuration > Ciphers > Host Key/Auth Key*.

b) Seleccionar los siguientes algoritmos del listado como aceptadas:

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

Para configurar los algoritmos de *Key Exchange* de SSH hay que realizar lo siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > SSH Configuration > Ciphers > Key Exchange*.

b) Seleccionar los siguientes algoritmos del listado como aceptadas:

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group15-sha512
- diffie-hellman-group16-sha512

- diffie-hellman-group18-sha512

Para configurar los algoritmos de *Encryption* de SSH hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > SSH Configuration > Ciphers > Encryption*.

b) Seleccionar los siguientes algoritmos del listado como aceptadas:

- AEAD_AES_256_GCM
- aes256-gcm@openssh.com

Para configurar los algoritmos de *MAC* de SSH hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: *System Security Management > SSH Configuration > Ciphers > MAC*.

b) Dejar todos los valores sin marcar ninguno.

7.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

El producto presenta ciertos protocolos adiciones que deben ser deshabilitados por el administrador del mismo durante su instalación/puesta en marcha:

- TELNET
- FTP
- HTTP
- SNMP
- TL1
- GNMI
- NETCONF
- CP REST

Para desactivarlos será necesario ejecutar los siguientes pasos:

a) Conectarse al producto y navegar a la siguiente ruta: *System Security Management > Security Settings > Protocols*.

b) Los siguientes campos tienen que tener el valor asignado de *Disable*: *Telnet Interface*, *FTP Client* y *FTP Server.*

c) Conectarse al producto y navegar a la siguiente ruta: System Management > System General Settings > Controls.

d) Los siguientes campos tienen que tener el valor asignado de Disable: HTTP Redirect to HTTPS, SNMPv1 and v2c, SNMPv3, TL1 Interface y GNMI Interface.

e) Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > Controls > Interfaces*.

f) Los siguientes campos tienen que tener el valor asignado de *Disable*: *CP REST Interface* y *NETCONF Interface*.

7.6 GESTIÓN DE CERTIFICADOS

El producto utiliza certificados X.509 para la autenticación del *syslog*, además de para firmar las imágenes de actualización.

El producto permite al administrador la capacidad de generar y asignar un certificado para el protocolo HTTPS de la interfaz web.

Para configurar el certificado X.509v3 usado para el servidor web HTTPS hay que realizar los siguiente:

a) Conectarse al producto y navegar hasta la siguiente ruta: System Security Management > Public Key Infraestructure (PKI) > Keys > Create private key.

b) Selecciona una de los IDs de llaves disponibles para generar una nueva. Especificar la llave como *ECDSA*.

c) Seleccionar *Next*.

d) Especificar el valor de *Key Curve Name*, que debe ser uno de los siguientes valores: *prime256v1*, *secp384r1* y *secp521r1*.

e) Seleccionar *Next*.

f) Especificar el valor *Web Services* para el campo *Key Profile*.

g) Seleccionar *Next.*

h) Seleccionar *Next.*

i) Seleccionar *Next.*

j) Seleccionar *Apply.*

k) Navegar hasta la siguiente ruta: System Security Management > Public Key Infraestructure (PKI) > Certificates.

l) Seleccionar los certificados ya existentes, aparte del creado en estos pasos, y borrarlos.

m) Seleccionar el certificado que fue creado a lo largo de estos pasos y seleccionar el menú de *Activate*.

n) En el campo *Activate* seleccionar el valor de *Activate*.

o) Seleccionar *Apply*.

También es necesario configurar los certificados para el servicio de *syslog*. Para realizar estas configuraciones hay que realizar los siguientes pasos:

a) Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > Security > Certificate Authorities*.

b) Añadir una nueva Certificate Authority.

c) Seleccionar un identificador valido de la lista.

d) Especificar una etiqueta para la CA.

e) Especificar el valor de *Strict Base CRL (all)* para el campo *CRL Method*.

f) Especificar el valor del campo *CRL Update Interval*, el recomendado es de 30 minutos.

g) Especificar el valor de Required para los campos Extended Key Usage, Basic Constraints y Subject Name.

h) Pulsar el botón de *Add*.

i) Navegar a la siguiente ruta: Node > Security Applications > Syslog > Syslog Secure Connection.

j) Especificar el *Server Authority* generado a lo largo de estos pasos.

k) Seleccionar *Apply*.

Es posible generar certificados desde el producto para asignar a los diferentes usuarios o servicios. Para realizar estas configuraciones hay que realizar los siguientes pasos:

a) Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > Security > Certificate & Keys*.

b) En la pestaña de *Keys* seleccionar la opción de *Add*.

c) Seleccionar un identificador valido.

d) Seleccionar el valor de *ECDSA* para el campo *Key Algorithm*.

e) Seleccionar el valor de *secp384r1* para el campo *Key Curve Name*.

f) Especificar la IP del producto como el valor para el campo *Common Name*.

g) Seleccionar *Add*.

h) Seleccionar el valor de *Manual (CSR only)* para el campo *Renewal Mode*.

i) Seleccionar la clave nueva generado durante estos pasos de la lista de claves.

j) Seleccionar el valor de *Request* para el campo *Key and Certificate Renewal*.

k) Firmar de manera manual la clave generada por la CA.

l) En el área de certificados seleccionar la llave correspondiente con la que se acaba de firmar.

m) Dentro de la ventana de *Configure Details*, en el área de *Certificate Activation*, seleccionar la opción de *Activate*.

n) Seleccionar *Apply*.

El producto permite la opción de importar el certificado CA a la *CA Trusted Store*. Para realizar estas configuraciones hay que realizar los siguientes pasos:

a) Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > Security > Certificate & Keys > Certificates*.

b) Añadir un nuevo certificado.

c) Seleccionar un identificador valido de la lista *drop-down*.

d) Especificar una etiqueta.

e) Copiar los datos del certificado en el campo de texto.

f) Elegir la opción de Trusted (Root Authority) para el campo Trusted Setting.

g) Asociar el certificado con la CA correspondiente.

h) Seleccionar *Add*.

7.7 ACTUALIZACIONES

La actualización del software debe realizar siguiendo la guía [REF3].

Se recomienda hacer uso de un ordenador adicional para realizar la descarga y firma del firmware.

Es necesario descargar la versión correcta del software desde el portal web de *Adtran Customer*. Una vez descargada la imagen del producto se requerirá una comprobación del SHA-256 del fichero descargado y del hash publicado en la web.

El TOE no realiza comprobaciones automáticas para detectar nuevas actualizaciones de software o firmware. La identificación de nuevas versiones debe ser llevada a cabo manualmente por el administrador mediante la consulta del portal de clientes de Adtran. Por su parte, la versión actualmente instalada en el TOE puede visualizarse a través de las interfaces de administración del producto.

Una vez extraído los contenidos del paquete de actualización, realizar una firma del fichero con extensión "*.CON*" utilizando el siguiente comando:

```
openssl cms -md sha384 -sign -binary -in F#######RC##.CON - outform DER
-out F#######RC##.SIG -signer foo.pem -inkey foo.pem -nosmimecap
```

Una vez que se ha comprobado que el fichero de actualización es el fidedigno, y se ha realizado un proceso de firma sobre el paquete de actualización, será necesario ejecutar los siguientes pasos:

a) En primera instancia, configurar la validación por software de los paquetes de instalación:
   - conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: Node > Security > Certificate Authorities.
   - Definir una nueva Certificate Authority.
   - Especificar el valor de Strict Base CRL (all) para el campo CRL Method.
   - Especificar el valor de 30 Minutes para el campo CRL Update Interval.
   - Dentro del área de Certificate Validation Requirements especificar el valor de ECDSA para el campo de Public Key Algorithm y el valor de Required para el campo de Basic Constraints, Extended Key Usage.
   - Seleccionar Add.
   - Navegar a la siguiente ruta: Node > Security Applications > SW Install.
   - Dentro del área de Secure Sw Installation especificar el valor Enable para el campo Signature Validation, la Certificate Authority definida en estos pasos para el campo Software Sign Authority, y el valor Default (Secure Only) para el campo SW Install Digest.

b) Configurar la capacidad de trasferir los paquetes de actualización al producto a través de la interfaz web:
   - Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > General > Controls > Functionality*.
   - Especificar el valor de *Upload & Download* para el campo *Local Computer Transfer*.
   - Seleccionar *Apply*.

Para llevar a cabo la instalación del paquete de actualización hay que realizar los siguientes pasos:

- Conectarse al producto a través de la interfaz web y navegar a la siguiente ruta: *Node > Software > NCU > Transfer Software to Standby Area*.
- Especificar el valor de *Local Computer* para el campo *Source Location*.

- Importar toda la selección de ficheros del paquete tal que: **.PGM*, **.COM* y **.SIG*.
- Una vez los ficheros se han importado seleccionar *Transfer to Standby*.
- En la página de *NCU*, seleccionar el valor de *Activate* en el campo *Activate Software in Standby Area*.

Una vez que el producto se reinicie, se iniciará con la nueva versión.

7.8 AUTO-CHEQUEOS

El producto realiza los siguientes procedimientos de autocomprobación antes de iniciar el sistema operativo para garantizar la integridad del sistema de archivos, el software del producto y las funciones criptográficas.

Para verificar las comprobaciones automáticas realizadas durante el arranque o reinicio, el administrador debe conectarse por consola (remota o local) al dispositivo y revisar la información generada por el sistema en dicho proceso.

La salida generada durante el arranque se puede encontrar en registros de auditoría del producto, incluyendo información detallada similar a la siguiente:

```
UTC root filesystem /dev/sda7 clean
UTC root filesystem /dev/sda7 mounted OK.
UTC Algorithm Test Start.
UTC Initrd intrgrity Test PASS.
UTC Alg pass test:
UTC /tmp/algtest/test_file: OK
UTC /tmp/algtest/test_dir: OK
UTC /tmp/algtest/test_dir/test_symlink: OK
UTC /tmp/algtest/test_file_not_found: OK
UTC /tmp/algtest/test_file_wrong_owner: OK
UTC /tmp/algtest/test_file_wrong_perms: OK
UTC /tmp/algtest/test_file_wrong_size: OK
```

Ilustración 4. Auditoría relativa al auto-chequeo

```
Crypto Test Start.
Execute positive test sha-384-hash
Positive test sha-384-hash: PASS
Execute negative test sha-384-hash-out
Negative test sha-384-hash-out: PASS
Execute negative test sha-384-hash-in
Negative test sha-384-hash-in: PASS
Execute positive test sha-512-hash
Positive test sha-512-hash: PASS
Execute negative test sha-512-hash-out
Negative test sha-512-hash-out: PASS
Execute negative test sha-512-hash-in
Negative test sha-512-hash-in: PASS
Execute positive test hmac
Positive test hmac: PASS
Execute negative test hmac-out
Negative test hmac-out: PASS
Execute negative test hmac-key
Negative test hmac-key: PASS
Execute negative test hmac-msg
Negative test hmac-msg: PASS
Execute positive test ecdsa-get-pubkey
```

Ilustración 5. Auditoría relativa al auto-chequeo (pruebas criptográficas)

7.8.1 COMPROBACIÓN DE LA INTEGRIDAD DEL SOFTWARE

El producto valida la integridad del software en el sistema de archivos verificando el estado actual de los archivos constantes en la partición raíz con el archivo de manifiesto que se generó e incluyó en el software como parte del proceso de compilación. El manifiesto contiene la siguiente información:

- Archivos binarios ejecutables
- Archivos de texto ejecutables (scripts)
- Bibliotecas compartidas
- Todos los archivos constantes de la partición raíz
- Hashes SHA-384 para comparación
- Propiedad para la comparación
- Permisos de archivos para la comparación

Esta comprobación dará lugar a errores que indican un problema de integridad con uno o más de los archivos de software producto. Un fallo de esta comprobación da lugar al estado no operativo.

7.8.2 COMPROBACIÓN CRIPTOGRÁFICA

El producto ejecuta Pruebas de Respuesta Conocida para las siguientes funcionalidades criptográficas:

- CTR_DRBG
- AES256-GCM
- Generación de claves Diffie-Hellman Safe Primes
- Verificación de claves Diffie-Hellman Safe Primes
- Cálculo del secreto compartido Diffie-Hellman Safe Primes
- Generación de claves ECDSA
- Verificación de claves ECDSA
- Verificación de firmas ECDSA
- HMAC-SHA-384
- SHA-384
- SHA-512

Basándose en la metodología FIPS 140-2, el fallo de las comprobaciones criptográficas tiene como resultado que el producto NO realiza ningún servicio criptográfico. Esta comprobación da lugar a errores que identifican las operaciones criptográficas fallidas. Un fallo de esta comprobación da como resultado el estado no operativo.

7.9 AUDITORÍA

7.9.1 REGISTRO DE EVENTOS

Los ficheros de auditoria se comprimen para que se ocupe menos espacio en la memoria del producto, cada uno de los registros de auditoria en su respectivo directorio en el producto. Cuando un archivo de llena, se crea otro archivo nuevo hasta alcanzar un número máximo configurable. Luego, se inicia una rotación donde el archivo más antiguo se sobrescribe.

El proceso de rotación de registros funciona de la siguiente manera (ejemplo con el nombre del archivo `events.txt`):

- Si `events.txt` alcanza su tamaño máximo, se copia a `events.txt.1.gz` u se crea un nuevo `events.txt`.
- La próxima vez `events.txt.1.gz` se convierte en `events.txt.2.gz` y `events.txt` pasa a ser `events.txt.1.gz`.

Dependiendo del tipo de registro de auditoría, el producto almacenara una cantidad de registros de auditoría. Teniendo en cuenta que ya haya llegado a la cantidad máxima de ficheros de registro, a la siguiente vez se eliminará el registro con el número más alto.

Por lo tanto, los registros se encuentran en los archivos `events.txt`, `events.txt.1.gz`, `events.txt.2.gz`… hasta el número máximo de posibles ficheros de auditoria por función.

Cada tipo de registro de evento son almacenados de manera diferente siguiendo las siguientes reglas:

Tipo de archivo de registro de auditoría	Tamaño mínimo del archivo de registro de auditoría para activar el archivado	Número máximo de entradas de registro de auditoría por archivo de registro (M)	Número máximo de archivos de registro de auditoría archivados (N)	Espacio máximo de almacenamiento del archivo de registro de auditoría (actual + archivado)
Condition log (Event)		100	19	2 MB (*)
Database change log		50	19	2 MB (*)
Security log (System)	>80K		9	800 KB

Tabla 10. Ficheros de auditoria según el tipo de evento

(*) Los registros de condiciones y cambios de la base de datos se guardan en una partición compartida SRAM de 2 MB.

7.9.2 ALMACENAMIENTO LOCAL

Para almacenar todos los eventos en los registros de auditoria en el sistema de archivos persistente, el administrador debe ejecutar los siguientes pasos:

a) Conectarse al producto y navegar a la siguiente ruta: *System Security Management > Security Settings > General*. Seleccionar la opción de *Enable* para el campo de *Audit Logs*.

7.9.3 ALMACENAMIENTO REMOTO

Para enviar todos los eventos a un servidor de auditoria (*syslog*) el administrador debe ejecutar los siguientes pasos:

a) Conectarse al producto y navegar a la siguiente ruta: System Management > System General Settings > Syslog.

b) Seleccionar *Add*.

c) Especificar la IP del servidor de auditoria en el campo apropiado.

d) Asignar el valor de Enable para los campos Send Alarms, Send Database Changes y Send Security Events.

e) Seleccionar *Apply*.

f) Navegar a la siguiente ruta: System Security Management > Security Settings > General.

g) Asignar el valor de *Enable* para el campo *Audit Logs*.

h) Seleccionar *Apply*.

Una vez configurado el servidor Syslog y habilitado el envío de eventos, los registros de auditoría se transmiten al servidor remoto mediante un canal de comunicación TLS v1.2, proporcionando confidencialidad e integridad durante la transmisión.

8 REFERENCIAS

[REF1]	Extra explanations to reach the evaluated configuration Version 1.0 2024-06-20	N/A
[REF2]	Document explaining the installation process and the commissioning of the product Issue A	N/A
[REF3]	Administrative Guidance document for FSP 3000R7 R22.5.2 Version 1.0 2024-05-08	N/A
[REF4]	Installation and Commission- ing Manual 22.5 Issue A December 2023	N/A
[REF5]	Secure System Configuration 22.5 Issue A 2023	N/A
[REF6]	Hardware Description 22.5 Issue A February 2024	N/A
[REF7]	High-Density Subshelf Hardware Guide 22.5 Issue A December 2023	N/A
[REF8]	Maintenance and Troubleshoot- ing Manual 22.5 Issue A December 2023	N/A
[REF9]	Management Data Guide 22.5 Issue A 2023	N/A
[REF10]	Module and System Specification22.5 Issue A February 2024	N/A
[REF11]	User Guide22.5 Issue A December 2023	N/A
[REF12]	Network Element Director Help 22.5 Issue A 2023	N/A
[REF13]	Provisioning and operations Manual	N/A

	22.5 Issue A December 2023	
[REF14]	Safety Guide 22.5 Issue A December 2023	N/A
[REF15]	collaborative Protection Profile for Network Devices. version 2.2e 23-March-2020	https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/CPP_ND_V2.2E.pdf
[REF16]	Security Target Description Adtran FSP 3000R7 versión 1.1	
[REF17]	Fiber Service Platform 3000R7 Hardware Description, Product Release: 22.5, Document Issue: B, Document Number: 80000075272	
[REF18]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.	https://oc.ccn.cni.es/documentos/criterios-y-metodologias/79-ccn-stic-2001-definicion-de-la-certificacion-nacional-esencial-de-seguridad-lince/file
[REF19]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.	https://oc.ccn.cni.es/documentos/criterios-y-metodologias/80-ccn-stic-2002-metodologia-de-evaluacion-para-la-certificacion-nacional-esencial-de-seguridad-lince/file
[REF20]	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

Nota: Las referencias marcadas como N/A están disponibles de forma privada para nuestros clientes en el portal del fabricante MyAdtran (https://my.adtran.com)

9 ABREVIATURAS

AES	Advanced Encryption Standard
GCM	Galois/Counter Mode
AGD	Assurance Guidance Document
bps	Bits Per Second
CA	Certificate Authority
CEM	Common Equipment Module
CLI	Command Lince Interface
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos y Servicios de Tecnologías de la Información y las Comunicaciones del CCN
CRL	Certificate Revocation List
CSM	Channel Splitter Module
CSR	Certificate Signing Request
CTR DRBG	Counter Mode Deterministic Random Bit Generator
DCF	Dispersion Compensation Fiber
DCG	Dispersion Compensation Gratings
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EDFA	Erbium Doped Fiber Amplifier
ENS	Esquema Nacional de Seguridad
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GCB	Gain Controlled Balanced amplifier
GUI	Graphical User Interface
HDSCM	High Density Supervisory Channel Module
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ILM	Interleaver Module
IP	Internet Protocol
IPv4	Internet Protocol version 4
LAN	Red de Área Local
MA(L)P(B)	Micro Amplifier (Low) Pre (Booster) Amplifier

MAC	Message Authentication Code
Mbps	Megabits per second
MTP(B)	MicroTerminal Pre (Booster) Amplifier
NCU	Network Control Unit
NDcPP	Network Device Collaborative Protection Profile
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OPCM	Optical Power Control Module
OPPM	Optical Path Protection Module
OSCM	Optical Supervisory Channel Module
OSFM(A)	Optical Supervisory Filter Module (with ALM/OTC Coupler)
OTC	Optical Time-domain Coupler
OTH	Optical Transport Hierarchy
PKI	Public Key Infrastructure
PM	Protection Splitter Module
PSCU	Passive Shelf Control Unit
PSM	Power Splitter Module
PSU	Power Supply Unit
PYME	Pequeña y Mediana Empresa
RAMAN	Raman Amplifier
RBG	Random Bit Generator
RFC	Request for Comments
RJ45	Registered Jack 45
ROADM	Reconfigurable Optical Add/Drop Module
RSA	Rivest-Shamir-Adleman
SCU	Shelf Control Unit
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SSH	Secure Shell
SW	Software
TCC	TDM Channel Module Core
TCE	TDM Channel Module Enterprise
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Objetivo de la evaluación (Target of Evaluation)

TSF	TOE Security Function
UTM	Utility Module
UTP	Par Trenzado No Blindado (Unshielded Twisted Pair)
V(L)GC(B)	Variable (Low) Gain Controlled Balanced amplifier
WAN	Red de Área Amplia
WCA	Wavelength Converter Module Access
WCC	Wavelength Channel Module Core