Guía de Seguridad de las TIC
CCN-STIC-1457

Procedimiento de empleo seguro
Enrutadores NOKIA SR y IXR

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.26 08:54:26 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. El presente documento aplica a los equipos de la familia de equipos 7250 IXR (Interconnect Router) y las familias de equipos 7750 SR (Service Router).
2. Los equipos pertenecientes a estas familias son equipos de routing IP/MPLS que se posicionan en distintos puntos de la red. Mientras la familia 7750 SR se posiciona en el núcleo y borde de la red, el 7250 IXR agrega servicios y provee de una capa de acceso cuyo tráfico se enviará a los equipos del núcleo para que sea enrutado a su destino. Ambos conjuntos de equipos incluyen la posibilidad de cifrar las comunicaciones que transitan a través de ellos.
3. Tanto el 7750 SR como el 7250 IXR constan de diferentes elementos que se han optimizado para su aplicabilidad en diversos entornos de despliegue de redes IP/MPLS, soportando un amplio rango de aplicaciones, desde la agregación de tráfico móvil hasta el enrutamiento en el núcleo de red. Estos equipos aprovechan una arquitectura común de software, hardware, gestión y plano de control, lo que permite ofrecer operaciones homogéneas y coherentes en toda la cartera de funcionalidades del producto, para ofrecer operaciones fluidas en toda la cartera de funcionalidades que ofrece el producto.
4. Con el fin de facilitar la comprensión del documento, los **acrónimos utilizados** se encuentran desarrollados en la **Sección 9. Abreviaturas**. Asimismo, las referencias indicadas mediante el formato **[REF-N]** se detallan en la sección 8 correspondiente de **Referencias**, donde se incluye el nombre del documento, su identificador asociado y el enlace directo al mismo en el portal oficial de **Nokia Support**

2 OBJETO Y ALCANCE

5. El objeto del presente documento es establecer las directrices y recomendaciones necesarias para **facilitar la instalación, configuración y uso seguro** de los equipos **Nokia 7750 SR (Service Router)** y **Nokia 7250 IXR (Interconnect Router)**, ambos operando con la **versión de software 24.10R3**.

6. Asimismo, este documento persigue definir un conjunto de **buenas prácticas de seguridad**, orientadas a garantizar la protección de la información, la integridad de los sistemas y la continuidad del servicio, en conformidad con los principios establecidos en el Esquema Nacional de Seguridad (ENS) y las guías CCN-STIC.

7. Esta solución ha sido incluida en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte [REF8].

2.1 PRODUCTOS

8. La familia de equipos 7750 SR está formada por equipos modulares que se componen de una controladora (CPM o SFM -SF/CPM), junto una controladora redundante opcional, y tarjetas de línea (IOM) que incluyen tarjetas de acceso al medio (MDAs). Existen diferentes variantes de los equipos 7750 SR y para la configuración de este documento se ha usado, al igual que en la certificación, un equipo **7750 SR-7**.

9. La familia de equipos 7250 IXR está formada por equipos monolíticos o modulares que se componen de una controladora (CPIOM), en algunos modelos puede haber una controladora redundante opcional, y tarjetas de línea (IOM) que incluyen tarjetas de acceso al medio (MDAs) que pueden ser integradas o modulares. Existen diferentes variantes de los equipos 7250 IXR y para la configuración de este documento se ha usado, al igual que en la certificación, un equipo **7250 IXR-E Small que se referencia como 7250 IXR-E en este documento. Las configuraciones referidas en el documento se aplican de igual manera en ambos equipos, el Nokia 7750 SR-7 y Nokia 7250 IXR-E.**

10. Los equipos físicos y sus componentes se indican en la siguiente tabla:

Appliance	Subcomponente	Descripción
7750 SR-7	3HE08423AA	Tarjeta de control CPM5
	3HE13727AA	Tarjeta de línea IOM5-E
	3HE18361AA	Tarjeta MDA de 16 puertos de 25 GB y 2 puertos de 100GB me16-25gb-sfp28+2-100gb-qsfp28
	3HE03662AA	DC 100A PEM-3 SLOT 1
	3HE05180AA	SR-7 Doble Ventilador
7250 IXR-E SMALL	3HE14783AA	Chasis tipo 7250 IXR-E **imm14-10g-sfp++4-1g-tx**
	3HE14784AA	Fuentes DC/AC

Tabla 1 – Modelos y Componentes de Nokia 7750 SR-7 y 7250 IXR-H

11. Tanto la familia 7750 SR como 7250 IXR consta de puertos de gestión (MGMT) con interfaz RJ45 que permite establecer la conexión del router a una red interna/externa que proporcione conectividad a sistemas de administración/gestión o de usuarios con la

posibilidad de configurar un servidor SSH para establecer una conexión segura hacia/desde los equipos.

2.2 SOFTWARE

12. La familia de equipos Nokia 7750 SR y Nokia 7250 IXR considerados para el documento se contemplan con el sistema operativo versión TIMOS-24.10.R3. La nomenclatura indicada para la versión de software es la siguiente TIMOS-m.n.Yz donde:

    - m — Número Mayor de versión, refiere a los dos últimos dígitos del año de lanzamiento
    - n — Número Menor de versión, refiere al mes de lanzamiento
    - Y:
        - A — Alpha release
        - B — Beta release
        - M — Maintenance release
        - R — Released software
    - z — Número de versión, referente a la versión m.n ejemplo 26.3 (Mayor 26 .Menor 3)

3 ORGANIZACIÓN DEL DOCUMENTO

13. El documento está estructurado en los siguientes apartados:

a) **Apartado 1.** Descripción de la familia de productos Nokia 7750 SR y 7250 IXR-R6.

b) **Apartado 2.** Alcance del documento.

c) **Apartado 3.** Organización del documento.

d) **Apartado 4.** Fase de despliegue.

e) **Apartado 5.** Fase de instalación.

f) **Apartado 6.** Recomendaciones en la fase de configuración y administración.

g) **Apartado 7.** Recomendaciones en la fase de operación.

h) **Apartado 8.** Listado de documentación referenciada en este documento.

i) **Apartado 9.** Listado de abreviaturas que aparecen en este documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. En el momento de la recepción de los equipos, debe verificarse la integridad del producto y comprobar que este, sus componentes y el empaquetado corresponden con los modelos Nokia 7750 SR y Nokia 7250 IXR esperados, en el chasis del equipo debe estar rotulado en su parte frontal el tipo y modelo del equipo.
15. En caso de identificarse alguna irregularidad durante la inspección, el cliente deberá ponerse en contacto inmediatamente con el proveedor para notificar y solucionar los problemas identificados.
16. Las controladoras de los productos se envían con un software preinstalado. Es importante comprobar el software instalado por si fuera necesario una actualización de este software. Tanto la descarga segura como la actualización del software se describe más adelante en el presente documento.

4.2 ENTORNO DE INSTALACIÓN SEGURO

17. El producto debe instalarse en un Centro de Proceso de Datos (CPD) seguro y controlado, de forma que se prevenga el acceso no autorizado al dispositivo y su entorno de operación.
18. El acceso a la sala en la que se ubica el producto debe estar dotado de un sistema de control de acceso que asegure que únicamente el personal autorizado puede acceder al dispositivo.
19. Todos los dispositivos utilizados para la gestión y administración de los equipos Nokia 7750 SR-7 y Nokia 7250 IXR deben tener un nivel de protección físico y lógico similar al producto.
20. Se recomienda consultar la documentación de instalación "*3HE19401AAAATQZZA_V1_7250 IXR-e Chassis Installation Guide Release 23.pdf"* de REF1 para el caso del *7250 IXR-E SMALL* y el documento "3HE18643AAAATQZZA02_V1_7450 ESS-7 and 7750 SR-7 Chassis Installation Guide 22.7.pdf"[REF2] en el caso del 7750 SR-7 para más detalle en las condiciones ambientales y de seguridad física del entorno necesarias para un correcto despliegue y funcionamiento del dispositivo y sus componentes.

4.3 CONSIDERACIONES PREVIAS

21. En el caso del equipo Nokia 7750 SR-7, todos los subcomponentes (IOM-5, SFM5-7, CPM5, me16-25gb-sfp28+2-100gb-qsfp28, Fuentes de alimentación, ventiladores) deben instalarse en los armazones del 7750 SR-7 antes de realizar la instalación y configuración, detalles en documento "3HE18643AAAATQZZA02_V1_7450 ESS-7 and 7750 SR-7 Chassis Installation Guide 22.7.pdf" REF2 en el caso del 7750 SR-7.
22. En el caso del equipo Nokia 7250 IXR-E, todos los subcomponentes están incluidos en el equipo al desembalarlo y sólo es necesaria la instalación de la fuente de alimentación.
23. En el apartado 4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN del presente documento se describen los elementos de administración local y remota. Para más detalle sobre la administración, se debe consultar el apartado 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.

24. Los siguientes elementos y funcionalidades quedan excluidos del empleo seguro del producto:

    a) Autenticación mediante servidor externo (RADIUS, TACAS+)

    b) Administración mediante Gestor

    c) Roles de usuario "*Default*"

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

25. Para la administración de los productos Nokia 7750 SR y Nokia 7250 IXR existen tres tipos de acceso al producto:

    a) acceso local.

    b) acceso local y remoto a través de SSH por puerto de gestión ("MGMT") fuera de banda.

    c) acceso remoto a través de SSH por puerto de tráfico en banda.

    Los modos a) y b) serán descritos en el presente documento. El objetivo final será la administración remota del producto de forma remota en un entorno seguro.

4.4.1 DETALLES EQUIPO 7750 SR-7

26. La figura muestra un esquema frontal del 7750 SR-7. En la tabla se describen los distintos componentes del equipo.

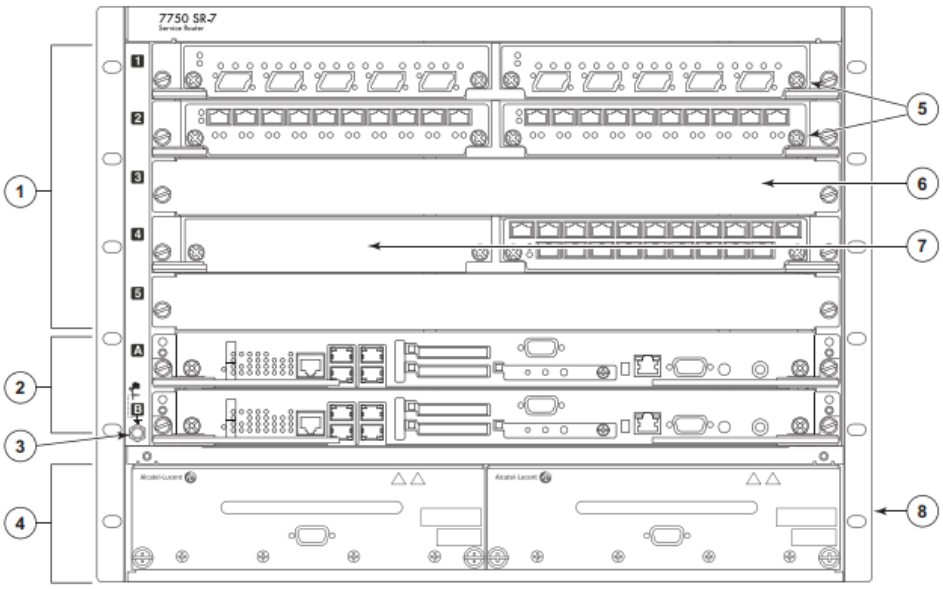

Ilustración 1 – Vista frontal 7750 SR-7

Key	Description
	IOM Slots 1-5
	SF/CPM Slots A y B
	Conector para tierra
	Filtros para las bahías de la alimentación DC

	IOM con MDAs instaladas
	Placa ciega en un slot de IOM vacío
	Placa ciega en un slot de MDA vacío
	Placas para la instalación del chasis en rack

Tabla 2 Slots panel frontal equipo 7750 SR-7

27. El equipo 7750 SR-7 cuenta con dos tarjetas controladoras (SF/CPM – Switch Fabric / Control Processor Module). Son dos tarjetas que se solapan para actuar en conjunto para manejar el control y capacidad de conmutación de tráfico. En la figura se muestra el combo de las tarjetas SFM5-7 (Switch Fabric Module) y CPM5 (SF/CPM – Switch Fabric / Control Processor Module). La tarjeta SFM5-7 es insertada en el slot A y/o B siendo el espacio ofrecida por esta para la controladora CPM5.

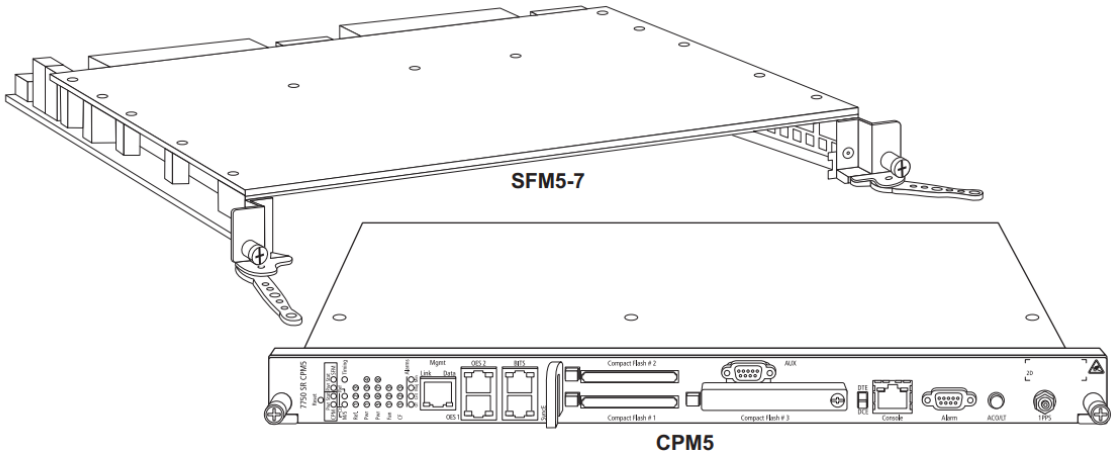

Ilustración 2 Vista frontal combo SFM5-7/CPM5

28. La figura muestra un esquema frontal de la tarjeta controladora CPM5 del 7750 SR-7. En la tabla se describen los distintos componentes del equipo.

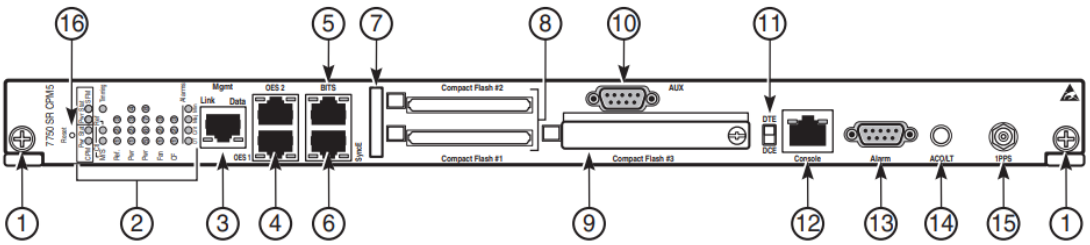

Ilustración 3 Vista frontal tarjeta CPM5

Key	Description
1	Tornillo de fijación a SFM5
2	Leds del sistema
3	Puerto Ethernet de gestión (Out-Of-Band)
4	Puertos 1 y 2 de extensión óptica de shelf, Puerto 2 es para uso futuro
5	Puerto de sincronización BITS

6	Puerto de sincronización sync-E/1588v2
7	Pestaña física para soporte en el retiro físico de la CPM5
8	Slots de tarjetas Compact Flash #1 y #2
9	Slot de tarjetas Compact Flash #3
10	Puerto auxiliar serie (para uso futuro)
11	Selector DTE/DCE del puerto de consola
12	Puerto de consola Serie (Puerto local)
13	Puerto de alarmas
14	Botón de forzado de iluminación de LEDs
15	Puerto de sincronización 1PPS
16	Botón de reset de SF/CPM

Tabla 3 Detalles tarjeta CPM5 de equipos 7750 SR-7

4.4.2 DETALLES EQUIPO 7250 IXR-E

29. En cuanto al 7250 IXR-E , la siguiente figura muestra la estructura del equipo:

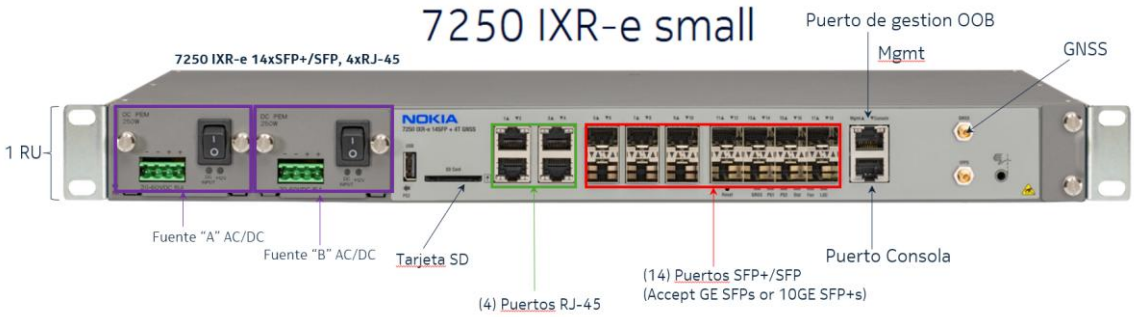

Ilustración 4 Chasis equipo 7250 IXR-E (small)

30. Gestión y administración de equipos. Pueden ser gestionados de tres formas distintas:

a) Equipo 7750 SR-7

i. **Gestión local**: conectando al puerto SERIE serigrafiado como "Console" en la SF/CPM.

ii. **Gestión fuera de banda (Out Of Band)**: conectando vía SSH a la dirección IP configurada en el puerto serigrafiado como "MGMT" en la SF/CPM en el 7750 SR-7. **Este tipo de gestión será usada en el manual y se considera para acceso remoto, se desarrolla la configuración en la sección 6.5.**

iii. Gestión en banda (In Band): es una forma de gestionar el equipo a través del tráfico que entra al equipo en puertos de servicio. **Este tipo de gestión no será usado en el manual de "Empleo Seguro".**

b) Equipo 7250 IXR-E

i. **Gestión local**: conectando al puerto SERIE serigrafiado como "Console" tanto en la SF/CPM en el 7750 SR-7 como en el 7250 IXR-E.

ii. **Gestión fuera de banda (Out Of Band)**: conectando vía SSH a la dirección IP configurada en el puerto serigrafiado como "MGMT" en el panel frontal del 7250

IXR-E. **Este tipo de gestión será usada en el manual y se considera para acceso remoto, se desarrolla la configuración en la sección 6.5.**

iii. Gestión en banda (In Band): es una forma de gestionar el equipo a través del tráfico que entra al equipo en puertos de servicio. **Este tipo de gestión no será usado en el manual de "Empleo Seguro".**

31. Con respecto a la **"Gestión en Banda"** se define como la administración del equipo a través de las interfaces de servicio que transportan el tráfico de producción. Este enfoque implica que la gestión comparte recursos con dicho tráfico, incrementando la exposición a riesgos y dependencias operativas. En el presente documento, esta modalidad se considera fuera del alcance, al no garantizar un canal de gestión segregado; por ello, únicamente se contemplan mecanismos que permitan una separación lógica o física del plano de gestión.

5 INSTALACIÓN

32. Tras la recepción segura de los productos se debe proceder a la instalación física de los mismos.

33. Se debe seguir la guía de instalación de la documentación oficial de Nokia. Se deberán seguir las guías "*3HE19401AAAATQZZA_V1_7250 IXR-e Chassis Installation Guide Release 23.pdf*" de [REF1] para el caso del *7250 IXR-E SMALL* y el documento "3HE18643AAAATQZZA02_V1_7450 ESS-7 and 7750 SR-7 Chassis Installation Guide 22.7.pdf" [REF2] en el caso del 7750 SR-7 para la instalación física de ambos equipos.

34. La instalación de los equipos deberá realizarse en localizaciones que dispongan con las medidas de seguridad físicas necesarias para garantizar la protección frente a accesos no autorizados. A tal efecto, se deberán considerar las siguientes medidas:

a) Control de acceso físico: El acceso a las instalaciones deberá estar restringido y controlado, permitiendo únicamente la entrada a personal debidamente autorizado mediante mecanismos de identificación y registro.

b) Protección perimetral: Las áreas donde se ubiquen los equipos deberán disponer de medidas de protección perimetral, como sistemas de cierre, videovigilancia y detección de intrusiones, que eviten accesos no autorizados.

c) Ubicación y entorno controlado: Los equipos deberán instalarse en ubicaciones seguras, preferiblemente salas técnicas o centros de datos, evitando entornos expuestos o de acceso público.

d) Protección frente a condiciones ambientales: Se deberán garantizar condiciones ambientales adecuadas de temperatura, humedad y ventilación para asegurar el correcto funcionamiento y la integridad de los equipos.

e) Suministro eléctrico seguro: Los equipos deberán contar con una alimentación eléctrica estable y protegida, incluyendo sistemas de respaldo como SAI o fuentes redundantes.

f) Protección contra incendios: Las instalaciones deberán estar equipadas con sistemas de detección y extinción de incendios adecuados para entornos con equipamiento electrónico.

g) Seguridad de los racks y equipos: Los equipos deberán instalarse en racks o armarios con acceso controlado que eviten la manipulación no autorizada de los mismos.

h) Gestión de cableado: El cableado deberá estar debidamente organizado, etiquetado y protegido para prevenir manipulaciones indebidas y facilitar su gestión segura.

i) Protección frente a manipulaciones y sabotaje: Se deberán implementar mecanismos que permitan detectar y prevenir manipulaciones físicas no autorizadas sobre los equipos.

j) Procedimientos operativos: Se deberán definir y aplicar procedimientos formales para regular el acceso, mantenimiento e intervención sobre los equipos, asegurando su registro y trazabilidad.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

35. Para que los dispositivos sean configurables en modo de operación seguro se requiere que el cliente ejecute las configuraciones requeridas para acceso remoto y verificación de estatus del servidor SSH para ser usado durante la configuración en modo seguro. En la sección 6.5 se detallan los pasos a seguir para la configuración del acceso seguro.

36. Cuando el equipo se acaba de instalar, solamente se puede configurar a través del interfaz de consola, por lo que será necesario la actuación, por parte del cliente o de una persona del servicio técnico de Nokia, a través de comandos CLI para configurar el equipo de forma segura (consultar los documentos REF1 y REF2 para más información sobre el CLI)

37. Una vez el operador configure los parámetros para la conexión remota y operación del equipo, el producto sólo podrá ser operado de forma remota a través de esta conexión, y, por tanto, **quedará bastionado por el entorno operacional** y medidas de seguridad adicionales dependiendo de dicho entorno.

6.2 AUTENTICACIÓN

38. El acceso a la administración y funciones del producto requiere de la autenticación de la identidaden del administrador. La autenticación se puede ejecutar a través de usuarios locales o servicios de autenticación remota (TACAS+ y radius) como se indica en los puntos a continuación.

6.2.1 USUARIOS LOCALES

39. Los usuarios se identifican y autentican contra la base de datos local del dispositivo a través de contraseñas. Estas contraseñas se almacenan de forma segura en la configuración del equipo utilizando funciones de hash criptográfico. Por defecto, el sistema emplea el algoritmo bcrypt, el cual está diseñado específicamente para la protección de contraseñas incrementando la resistencia frente a ataques de fuerza bruta. Adicionalmente, el sistema soporta alternativas seguras de hash como PBKDF2 con SHA-2(256) y SHA-3(512), permitiendo adaptarse a distintos requisitos de seguridad. Para más detalles consultar la documentación oficial referenciada en el presente documento [REF5] y [REF6].

40. Una vez autenticado, el usuario podrá realizar cambios de configuración o administrar el sistema en función de su rol administrativo de usuario. Por defecto el equipo tiene configurado únicamente el usuario “admin” con perfil “administrative” (privilegios administrativos completos) el cual podrá acceder al equipo a través del puerto de “Consola”

mencionado anteriormente como también a través del puerto de gestión marcado como "MGMT".

41. Se podrán crear usuarios y perfiles según requerimientos pudiendo limitar el acceso local por consola, el acceso al sistema de ficheros, uso de comandos o configuración del equipo. En el apartado 6.5.2 se muestran ejemplos prácticos de estos casos.

6.2.2 SERVIDORES DE AUTENTICACION

42. Adicional a la autenticación a través de usuarios configurados localmente, la familia de equipos Nokia 7250 SR y 7250 IXR permite la integración con distintos servidores de autenticación externa:

    a) Servidor de tipo Radius

    b) Servidor de tipo TACAS+

43. En caso de requerir configurar y aplicar el uso de estos métodos de autenticación, emplear los pasos correspondientes de configuración de Radius o TACAS+ dentro de "**Configuring security with CLI**" en [REF5] *"3HE20116AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR System Management Guide 24.10.R1.pdf"* y en [REF6] *"3HE20067AAACTQZZA01_V1_7250 IXR System Management Guide 24.10.R1.pdf.* Tener en cuenta que se requerirá de una clave de cifrado "secret" que debe coincidir con la clave configurada en los servidores para dicho equipo.

44. Los equipos de la familia Nokia 7750 SR y 7250 IXR manejan un método de protección de fallo de autenticación por problemas en los servidores o su conectividad. Considerando que la conectividad a los servidores de autenticación puede presentar interrupciones se recomienda siempre mantener el acceso a través de los usuarios locales ya sea como método único o como combinación con los métodos antes descritos. Por defecto los equipos contemplan esta combinación actuando como método de respaldo en caso de fallo de los servidores externos, en cuyo caso al no tener parámetros configurados para radius y TACAS+ la autenticación se ejecuta a través de usuarios locales. En todo caso, se puede ejecutar el siguiente comando para establecer los métodos a utilizar y el orden de preferencia, siendo el mas preferente el primero que este referenciado:

```
# configure system security password authentication-order radius tacplus local
```

ó

```
# configure system security password authentication-order radius local
```

ó

```
# configure system security password authentication-order tacplus local
#admin-save
```

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

45. El producto incluye la posibilidad de ser administrado tanto de forma local como remota:

    a) Para la administración **local**, los equipos constan de dos interfaces: puerto de "Consola" que es un puerto serie y puerto de "Management" que es un puerto

Ethernet cuya conexión al equipo por defecto no será posible**, el mismo está habilitado pero requiere configuración adicional para establecer la conexión, estas configuraciones constituyen la dirección IP de acceso al dispositivo y las rutas estáticas necesarias para tener conectividad desde las distintas redes de administración y gestión de equipos, en la sección 6.5.1** CONFIGURACIÓN DE FICHERO DE OPCIONES DE ARRANQUE **se tienen los pasos para aplicar estas configuraciones**. La interfaz de comandos (CLI), por defecto sólo se encuentra disponible a través del puerto de "Consola". Para la administración local, se debe acceder mediante autenticación con usuario y contraseña.

Para la conexión con el CLI se recomienda consultar los documentos *"3HE20116AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR System Management Guide 24.10.R1.pdf"* REF3 para el 7750 y *"3HE20048AAAATQZZA01_V1_7250 IXR Basic System Configuration Guide 24.3.R1.pdf"* REF4 para el 7250 IXR. En estos documentos se describe una guía básica para la administración de los equipos a través de CLI.

b) Para la administración **remota,** los equipos constan de la posibilidad de establecer una conexión tanto fuera de banda como en banda a través de SSH. Adicional a las capacidades de encriptación y protección de la conexión a través de SSH se tiene la posibilidad de agregar capas de protección con el uso del filtro de acceso de gestión "Management Access Filter (MAF)" para la administración segura a través del CLI.

46. Para una administración segura del producto, se recomienda únicamente el uso de la administración local mediante puerto serie o la administración remota a través de una conexión segura por SSH utilizando la conexión ofrecida por el puerto de gestión "MGMT". Para cada caso. tener en cuenta que sin el acceso remoto a través del puerto "MGMT" se deberá contar con un acceso remoto securizado a un equipo administrador de consolas con su respectiva conexión al puerto consola de los equipos. El acceso a través del puerto MGMT permite un abanico mayor de servicios de administración como por ejemplo SNMP para monitoreo de eventos o de estados de operación del equipo.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

47. Los sistemas Nokia 7750 SR y Nokia 7250 IXR permiten la configuración de distintos **tipos de usuarios (perfiles).** La configuración de perfiles es amplia ya que permite una variación de privilegios según requerimientos del ente operador/gestor de los equipos pudiendo limitar el acceso local por consola, el acceso al sistema de ficheros, uso de comandos o configuración del equipo, en el apartado 6.5.2 se muestran ejemplos prácticos de estos casos. El usuario "**admin**" tiene un perfil "**administrative**" por defecto que permitirá la configuración segura de todos los elementos necesarios para crear un canal seguro para configuración y administración segura.

48. Este usuario "admin" es el **Administrador** de ambos equipos y permite la administración para distintos tipos de usuario con distintos perfiles, los cuales puede crear y gestionar un administrador principal a través de CLI. Los roles determinan el nivel de privilegios de cada usuario. Este usuario "admin" tiene acceso a la configuración de todos los elementos existentes en los equipos.

49. Al conectarse a la consola CLI, inicialmente se deberán introducir las credenciales:

    - Username: **admin**

- Password: **admin**

50. Se dispone de tres modos de operación de la línea de comandos CLI: clásica, md-cli (model-driven cli) e hibrida que permite el uso de los dos primeros de manera indistinta para operar el equipo. En el contexto del presente documento, se recomienda el uso de la CLI clásica, por tratarse de un entorno más extendido, estable y adecuado para procedimientos operativos y de seguridad estandarizados.

51. Por su parte, el modo MD-CLI proporciona capacidades avanzadas basadas en modelos de datos, una mayor estructuración de la configuración y una mejor integración con herramientas de automatización mediante estándares como YANG, NETCONF o RESTCONF; no obstante, su utilización requiere un nivel técnico superior y un mayor conocimiento del modelo de datos subyacente. Para un análisis detallado de las funcionalidades y ventajas del modo MD-CLI, se deberá consultar la documentación oficial referenciada en el presente documento [REF5] y [REF6].

52. El Se recomienda reconfigurar el modo de operación a clásica en vez de tener el equipo con el modo md-cli que viene por defecto para la versión 24.10.R3, para más detalles respecto a este modo consultar. Los siguientes comandos se ejecutan para realizar el cambio:

```
# edit-config global
# configure system management-interface configuration-mode classic
# commit
# //
```

53. Posteriormente se deberán modificar dichas credenciales por defecto mediante los siguientes comandos:

```
# configure system security user “admin” password <password>
```

54. En caso de querer configurar nuevos usuarios se podrán crear con un perfil específico, como, por ejemplo, *“adminmistrative”* tal y como se indica a continuación (mirar los puntos ***“Configuring local command authorization profiles”*** *y* ***“Configuring local users”*** en [REF5] *“3HE20116AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR System Management Guide 24.10.R1.pdf”* y en [REF6] *“3HE20067AAACTQZZA01_V1_7250 IXR System Management Guide 24.10.R1.pdf”* para una descripción detallada de la creación de perfiles y usuarios tanto en el 7750 SR como en el 7250 IXR:

```
# configure system security user <nuevo-usuario> password <password>
# configure system security user <nuevo-usuario> access console
# configure system security user <nuevo-usuario> console member "administrative"
```

6.3.3 PARAMETROS DE SESIÓN

55. Adicionalmente, se deberán configurar los siguientes parámetros de sesión y políticas de contraseña:

    a) **Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:
        - Longitud mínima de la contraseña: doce (12) caracteres:

```
# configure system security password complexity-rules minimum-length 12
```

        - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales (del tipo: “!”, “@”, “#”,“$”, “%”, “^”, “&”, “*”, “(“, “)”). Debe utilizarse al menos un carácter de los cuatro (4) grupos.

```
# configure system security password complexity-rules required lowercase 1 uppercase 1 numeric 1 special-character 1
```

- Número de caracteres diferentes que ha de tener la nueva contraseña respecto de contraseñas anteriores. Por ejemplo, si establecemos el valor en 5, y la contraseña anterior es V4len.12345! la nueva contraseña podría ser V4len.67890!:

```
# configure system security password minimum-change 5
```

- Tiempo de validez en días de las contraseñas tras el cual expiran: por ejemplo, dos meses (60 días).

```
# configure system security password aging 60
```

- Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: máximo 1 día, 23 horas, 59 minutos y 59 segundos.

```
# configure system security password configure system security password minimum-age days 1 hrs 23 min 59 sec 59
```

b) **Configuración de los parámetros de sesión,** mediante el comando *'configure system login-control'***.** Deberá cumplir con los siguientes requisitos mínimos:

- Tiempo de inactividad de las sesiones: cinco (5) minutos.

```
# configure system login-control idle-timeout 5
```

- Tiempo de bloqueo tras los intentos fallidos de inicio de sesión: se activa un mecanismo frente a ataques aumentando el tiempo entre dos inicios de sesión en caso de fallo de inicio de sesión.

```
# configure system login-control exponential-backoff
```

- Configuración del mensaje de aviso y consentimiento en el inicio de sesión (**login banner**).

```
# configure system login-control pre-login-message "<mensaje mostrado al hacer un login>"
```

56. Los cambios realizados se aplicarán automáticamente. Será necesario usar el siguiente comando para que no se pierdan los cambios tras un reinicio:

```
# admin save
```

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

57. Los equipos 7750 SR y 7250 IXR necesitarán para su correcta operación segura la gestión de las siguientes entidades:

- **Dirección IP de gestión:** La dirección IP de gestión se configura como parte de la información de arranque del equipo y se asocia al puerto ethernet de la controladora serigrafiado como "MGMT". Esta dirección IP será la utilizada para el acceso remoto del equipo y se configura en el fichero de opciones de arranque ("BOF" por sus siglas en ingles Boot Option File).
- **Rutas estáticas de gestión:** Se configuran rutas estáticas que incluyan las distintas redes fuente de del tráfico de gestión, redes que alojen a los sistemas de administración de

elementos de Red y los operadores autorizados. Estas rutas se configuran en el fichero de opciones de arranque.

58. Con el objeto de reducir la superficie de exposición del producto, , cualquier otra interfaz de administración, funcionalidad o servicio no contemplado expresamente en el presente documento se considera fuera del alcance del mismo y, por tanto, no será objeto de análisis ni de recomendaciones específicas en este contexto. En este sentido, dichas interfaces y servicios se asumen deshabilitados o no utilizados en la configuración evaluada. Para un detalle completo de estas capacidades y su configuración, se deberá consultar la información recogida en las referencias [REF5] y [REF6] del presente documento.

6.5 CONFIGURACIÓN PARA CONEXIÓN SEGURA

6.5.1 CONFIGURACIÓN DE FICHERO DE OPCIONES DE ARRANQUE

59. Para establecer una conexión remota a través del puerto de gestion “MGMT” de los equipos es necesario proveer/configurar la dirección IP a través de la cual se gestionará/administrará el equipo de manera remota. De igual manera se requiere configurar de las rutas estáticas necesarias, por defecto o específicas que permitan la conectividad del equipo hacia/desde las redes de gestión. Estas configuraciones se ejecutan sobre el fichero de opciones de arranque (BOF por sus siglas en inglés), su aplicación se ejecuta como parte del proceso de arranque de los equipos y por defecto no cuenta con dirección IP ni rutas estáticas.

60. La figura muestra un esquema de conexión típica para la gestión remota de un equipo Nokia 7750 SR y 7250 IXR. En el esquema, el equipo Nokia 7750 SR-7 se conecta a una red local 10.10.10.0/24 a través del puerto “MGMT”, la red local es accesible desde una red externa privada o pública. Se requiere configurar el fichero de opciones de arranque para establecer la dirección IP de gestion y rutas estáticas necesarias. La configuración se hace por CLI desde el interfaz serie de consola, con el objetivo final de tener una conexión segura a través SSH.

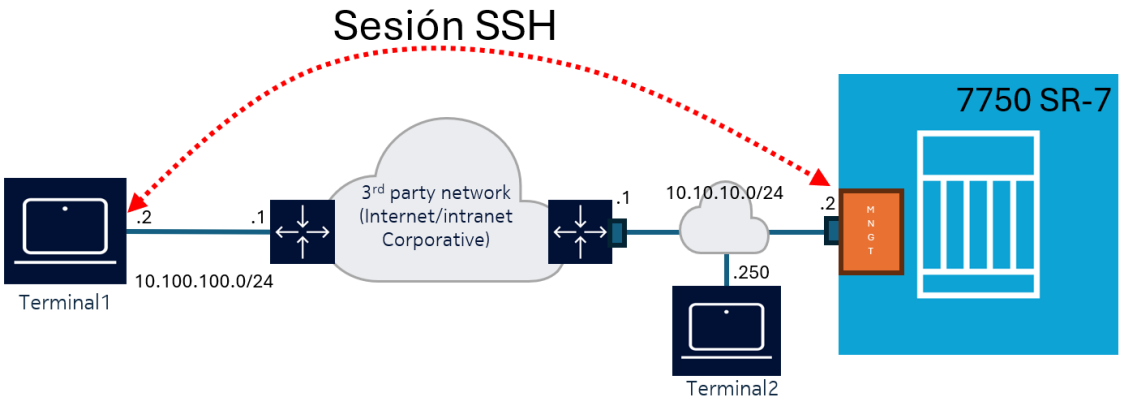

Ilustración 5 Sesión SSH

61. A través de la conexión local del puerto consola se ejecutan como ejemplo según la figura los siguientes comandos para gestión local desde la red 10.10.10.0/24 y gestión remota desde la red 10.100.100.0/24, debe existir conectividad previa entre estas redes:

    a) Dirección IP de gestión:

```
# bof address 10.10.10.2/24
```

(es posible configurar una ruta por defecto: 0.0.0.0/0 next-hop 10.10.10.1, no se recomienda por seguridad)

```
# show bof
# bof save
```

b) Ruta estática hacia red 10.100.100.0/24:

```
# bof static-route 10.100.100.0/24 next-hop 10.10.10.1
```

(en caso de no usar ruta por defecto, agregar ruta estática por cada subred de interés para la administración del equipo)

c) Revisar parámetros configurados y guardar configuración del BOF:

```
# show bof
# bof save
```

62. Una vez configuradas la dirección IP, rutas estáticas y establecida la conexión física del equipo a través del puerto de gestión a la red local es posible establecer la conexión remota segura a través de SSH, tanto desde la red local del equipo como desde la red remota que pertenece a la ruta estática configurada.

63. Los equipos por defecto tienen habilitado el servidor SSH

6.5.2 CONFIGURACIÓN DE USUARIOS Y PERFILES ADICIONALES:

64. El sistema operativo permite la administración y creación de usuarios y perfiles acorde a las necesidades y privilegios de los distintos usuarios asignando a cada usuario únicamente los permisos necesarios según sus funciones (principio de privilegio mínimo).

65. Los perfiles permiten controlar de forma granular las acciones que cada usuario puede ejecutar sobre el equipo, incluyendo el acceso a comandos operativos y de configuración.

66. A continuación, se muestran ejemplos de configuración para distintos tipos de usuarios.

a) Usuario administrador (acceso completo): Usuario con permisos totales sobre el sistema. Permite acceso completo a configuración, gestión de seguridad y ejecución de cualquier comando:

```
#
configure system security profile "admin-full"
   default-action permit-all
exit

configure system security user "admin1"
   password "PasswordSegura123"
   access console ftp ssh snmp
   profile "admin-full"
exit
### El password se almacena encriptado en MD5, no será visible luedo de introducir el comando
####
```

b) **Usuario técnico (sin acceso a modificaciones de parámetros de seguridad):** Usuario con acceso completo salvo a comandos críticos de seguridad. Permite configuración general del equipo y se restringe el acceso a cambio en los parámetros de seguridad:

```
#
configure system security profile "tecnico-limitado"
   default-action permit-all
   entry 10
      match command "configure system security"
      action deny
   exit
exit

configure system security user "tecnico"
   password "PasswordSegura123"
   access console ssh
   profile "tech-limited"
exit
### El password se almacena encriptado en MD5, no será visible luedo de introducir el comando
####
```

c) **Usuario operador/monitoreo (solo lectura):** Usuario limitado a comandos de visualización (show). Permite ejecutar comandos de revisión de estado del sistema sin acceso a modificaciones en la configuración del equipo:

```
#
configure system security profile "tecnico-limitado"
   default-action permit-all
   entry 10
      match command "configure system security"
      action deny
   exit
exit

configure system security user "tecnico"
   password "PasswordSegura123"
   access console ssh
   profile "tecnico-limitado"
exit
### El password se almacena encriptado en MD5, no será visible luedo de introducir el comando
####
```

6.5.3 CONFIGURACIÓN DE FILTRO DE ACCESO

67. La familia de equipos Nokia 7750 SR y 7250 IXR pueden limitar el acceso al CLI a través de la creación de filtros mediante direcciones IP (IPv4 y IPv6) y MACs de forma que solo puedan acceder a la gestión del equipo las direcciones de interés y se descarte cualquier intento de acceso no deseado

    Ejemplo de configuración del filtro MAF (Management Access Filter):

Se vuelve a mostrar la figura de la estructura de conexión para la cual se desarrolla como ejemplo sencillo para configurar el filtro de forma que el Terminal1 pueda acceder al equipo Nokia 7750 SR mientras que el terminal2 no podrá acceder aun cuando este está en la misma red

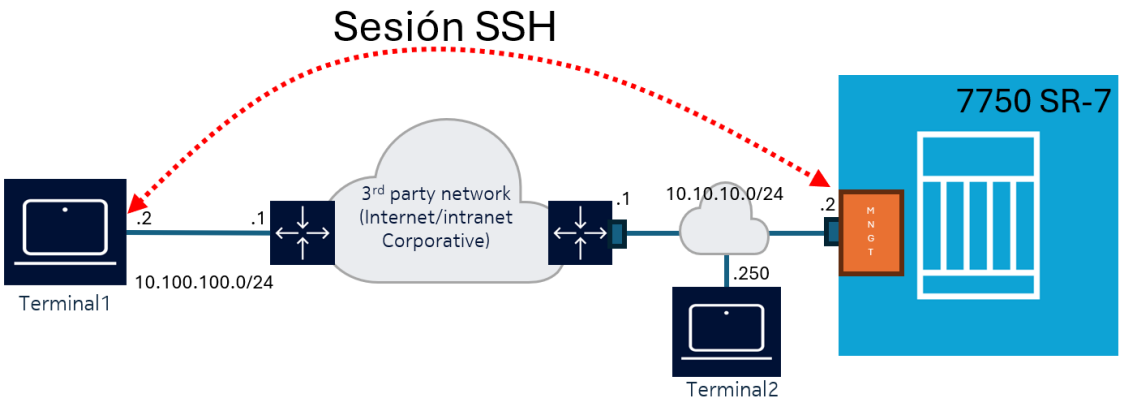

Ilustración 6 Sesión SSH

68. La operación del MAF establece que a todo tráfico de entrada se revisa la dirección IP de los paquetes y se compara con las entradas de los filtros de manera ordenada, aplicando la acción de la primera coincidencia. Este orden puede afectar que ciertas entradas no sean evaluadas si se tienen entradas muy generales previa a unas más específicas. En tal sentido, la recomendación es incluir las entradas más específicas en entradas previas a las generales. La numeración de las entradas no es obligatoria hacerla en secuencia, pudiendo manejar la numeración a conveniencia y cuando se tomen en cuenta casos futuros.

69. Considerando el ejemplo a desarrollar y las consideraciones para aplicar los filtros de manera correcta, se muestra la secuencia de comandos para permitir el acceso de la red del Terminal1, de la red local de la gestión del equipo y prohibir el acceso al Terminal2.

a) Se deshabilita para manipular y agregar entradas sin afectar sesiones en ejecución

```
# configure system security management-access-filter ip-filter shutdown
# configure system security management-access-filter ip-filter default-action permit
```

b) Se configura entrada para direcciones IP de red local y la acción "permit" desde red local . Se utiliza un número de entrada alto para permitir en entradas previas, limitar accesos de subredes o host incluidas en el segmento de red permitido

```
# configure system security management-access-filter ip-filter entry 10 src-ip 10.10.10.0/24
# configure system security management-access-filter ip-filter entry 10 action permit
```

c) Se configura entrada para direcciones IP de la Red del Terminal1 y la acción "permit" desde red local

```
# configure system security management-access-filter ip-filter entry 9 src-ip 10.100.100.0/24
# configure system security management-access-filter ip-filter entry 9 action permit
```

d) Se configura entrada para direcciones IP del Terminal2 y la acción "deny" desde red local. Esta entrada se desarrolla en el documento como muestra de las posibilidades de restricción, incluso si la dirección IP origen es de la misma subred.

```
# configure system security management-access-filter ip-filter entry 1 src-ip 10.10.10.250/32
# configure system security management-access-filter ip-filter entry 1 action deny
```

e) Se Habilita para activar la operación del filtro con acción por defecto "deny". Se activa el filtro y solo coincidencias con acción "permit" serán permitidas

```
# configure system security management-access-filter ip-filter default-action deny
# configure system security management-access-filter ip-filter no shutdown
```

Nota: Una gestión errónea de este apartado puede dejar incomunicado el nodo. Es altamente recomendable entrenar la sintaxis y la secuencia de comandos en un entorno de preproducción.

6.6 SINCRONIZACIÓN HORARIA

70. La sincronización horaria se podrá realizar en ambos equipos con la misma configuración (esto es válido para todos los procedimientos que vamos a describir salvo que se haga mención expresa de que son diferentes).

71. Existe la funcionalidad de administración de tiempo mediante protocolo NTP. Para su uso, debe haberse asegurado previamente que el servidor se encuentra en el entorno de administración protegido de igual forma que el resto de los equipos del sistema. Por ejemplo, suponiendo que en la red se tiene alcanzable y disponible un servidor NTP con dirección IP 10.100.100.2 podremos configurar los equipos para que tomen la sincronización de tiempo a través de la conectividad existente desde este servidor.

72. Para la configuración del servidor NTP se debe acceder al dispositivo por CLI como usuario administrador y seguir el procedimiento con los siguientes comandos:

    1. Configuramos el servidor mencionado como NTP server:

```
# configure system time ntp server 10.100.100.2 prefer
```

    2. Habilitar el Servidor NTP:

```
# configure system time ntp no shutdown
```

    3. Para ver los detalles del Servidor NTP configurado:

```
# show system ntp all
```

6.7 ACTUALIZACIONES

6.7.1 DESCARGA SEGURA DEL SOFTWARE

73. El software de los equipos Nokia 7750 SR y Nokia 7250 IXR está disponible para descarga electrónica a través del Portal de soporte de NOKIA (https://customer.nokia.com/support).

74. Pasos a seguir para la descarga SW:

- Abra el Portal de soporte de Nokia (https://customer.nokia.com/support) en su navegador.
- Introduzca sus credenciales de inicio de sesión. Las credenciales son definidas por el tipo de contrato de soporte del cliente (credenciales corporativas con correos bajo dominio del cliente o bajo el soporte de un técnico empleado de Nokia, el cliente debe estar dado de alta en la lista de empresas con contratos actuales con Nokia)

- Busque los productos en el campo de búsqueda o navegando por los iconos de las letras del abecedario.
- Cuando encuentra los productos, le aparecerá la siguiente ventana para el 7250 IXR:

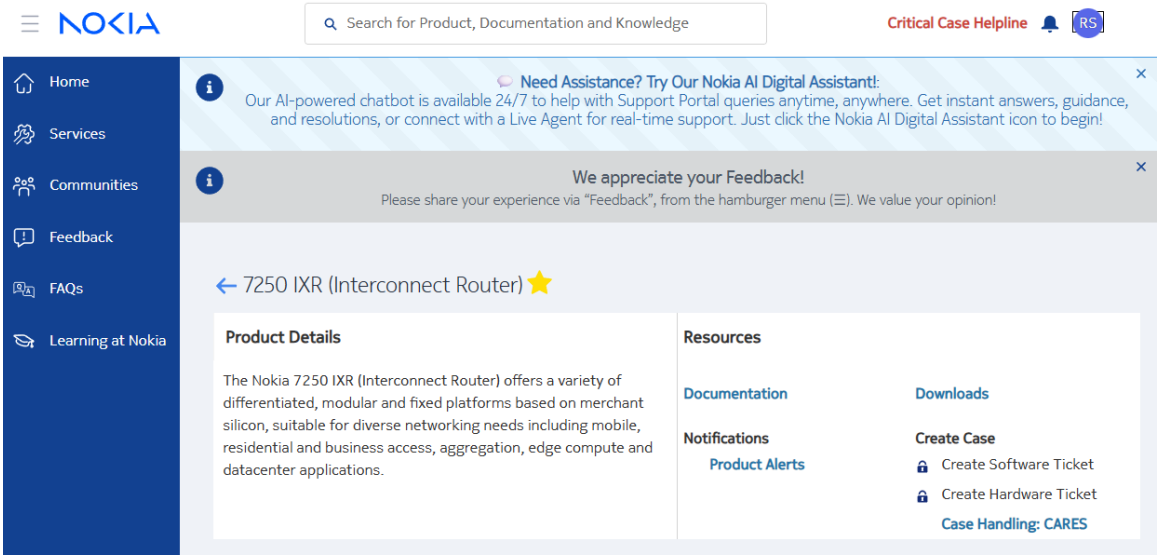

Ilustración 7 7250 IXR

- Y la siguiente para el 7750 SR:

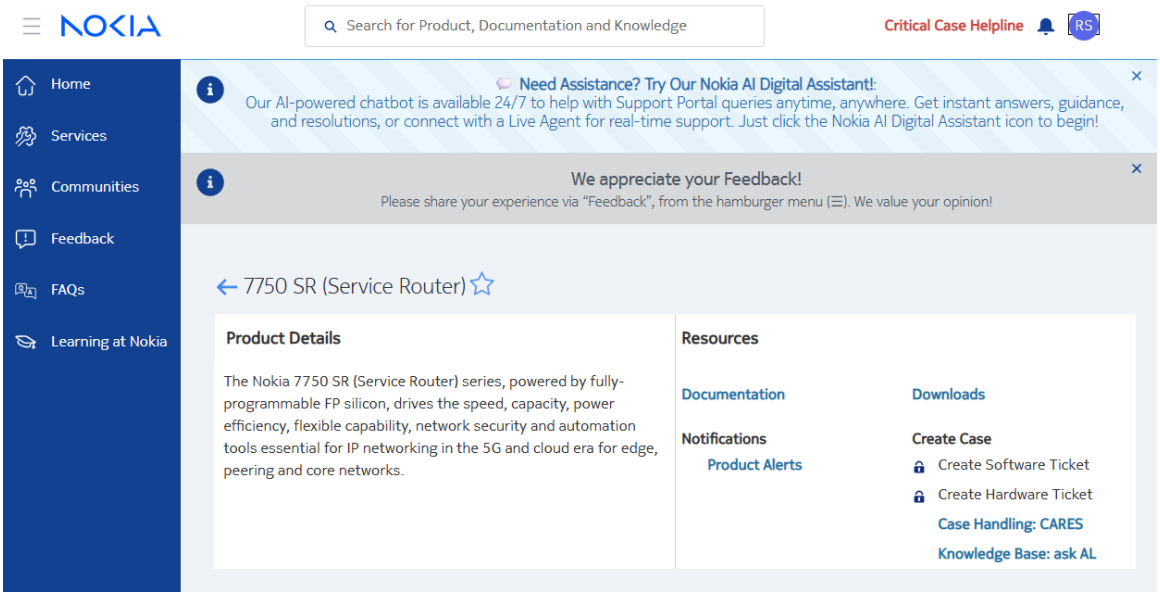

Ilustración 8 7750 SR

- Pulse en el enlace "Downloads" y seleccione la versión que quiere descargar:

75. Se muestran las versiones disponibles para su producto seleccionado.
    - En Please select a Product / Sub-category: el producto se completa automáticamente. Desde el segundo menú desplegable, seleccionar 24.10.

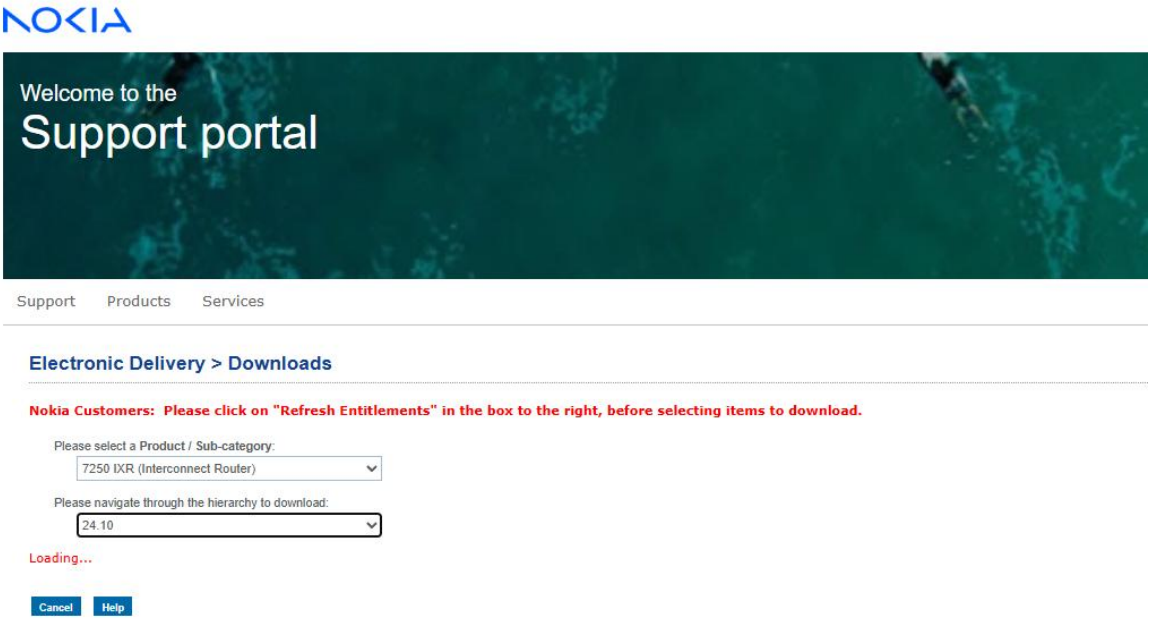

Ilustración 9 Support portal

- Se despliegan en el campo siguiente las versiones disponibles, seleccionar la versión específica que quiere descargar. Por ejemplo, R3.

76. Los paquetes de SW disponibles aparecen. En las siguientes figuras, se muestran las opciones para 7750 SR y 7250 IXR:

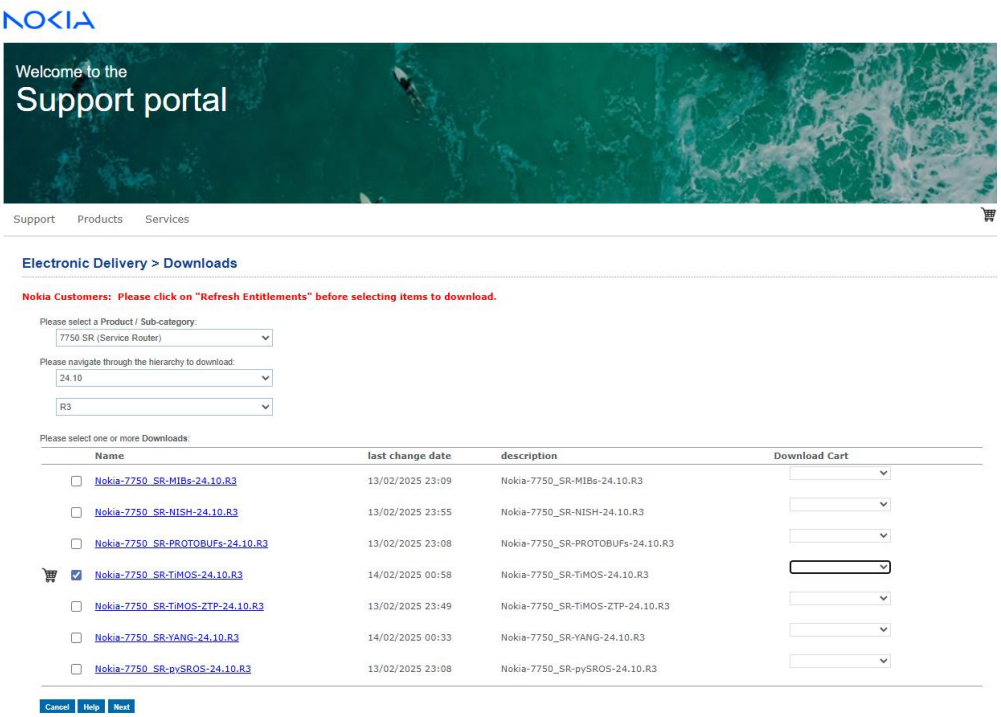

Ilustración 10 Support portal

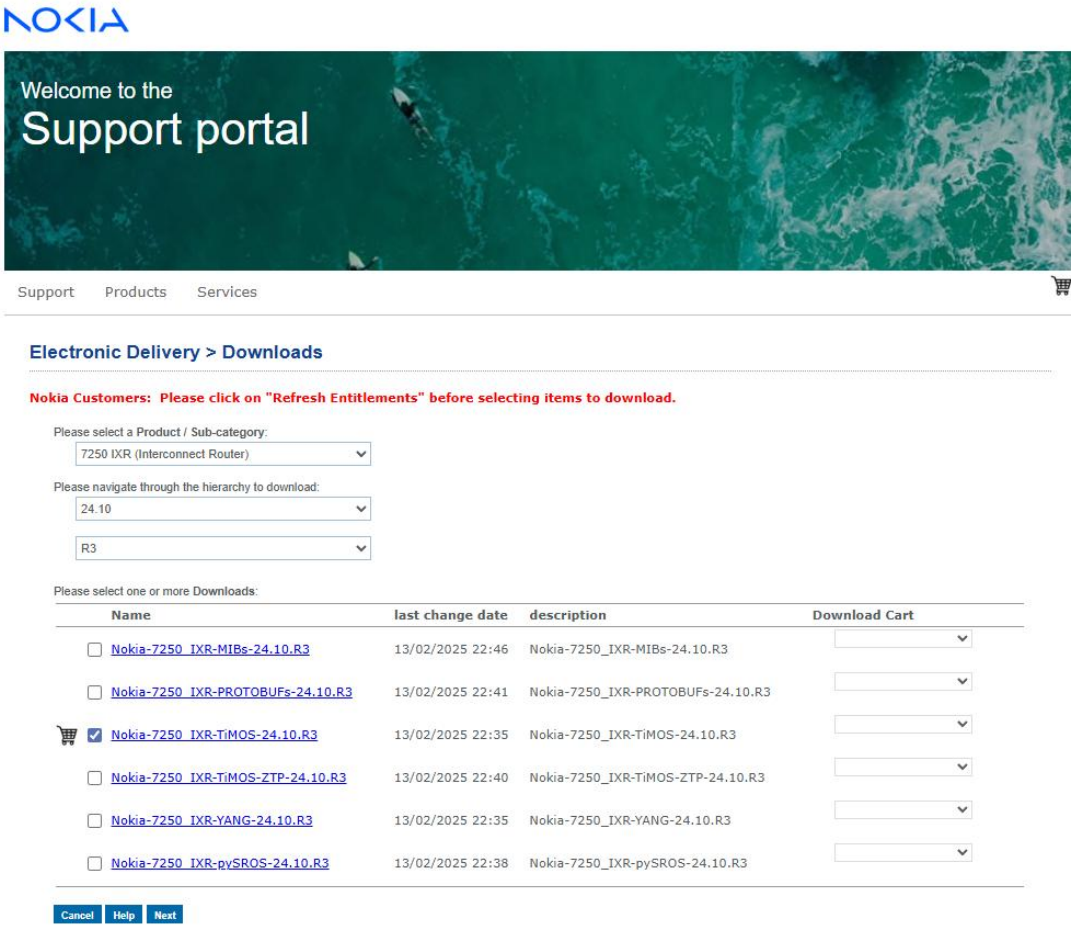

Ilustración 11 Support portal

- Revisar las descargas disponibles:

1. Seleccione la casilla de verificación del paquete de software adecuado. En general Nokia-7750 SR-TiMOS-<versión> y Nokia-7250 IXR-TiMOS-<versión>.

2. Lea la información adicional.

3. En el menú desplegable Carrito de descargas, seleccione Agregar al carrito.

4. Haga clic en Siguiente.

77. Nota: La pantalla muestra el APN del SW y el valor hash SHA-256 del archivo a ser descargado Asegúrese de que el APN mostrado sea correcto antes de descargar el archivo. **Registre el valor hash SHA-256 para verificar manualmente la integridad del archivo después de la descarga**

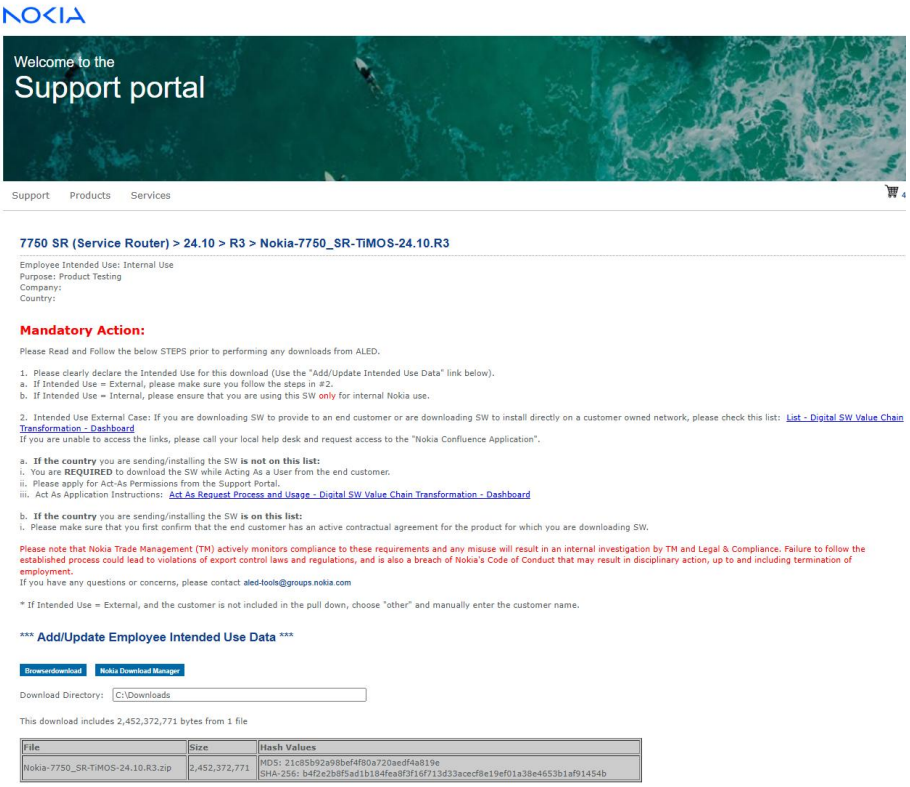

Ilustración 12 Support portal

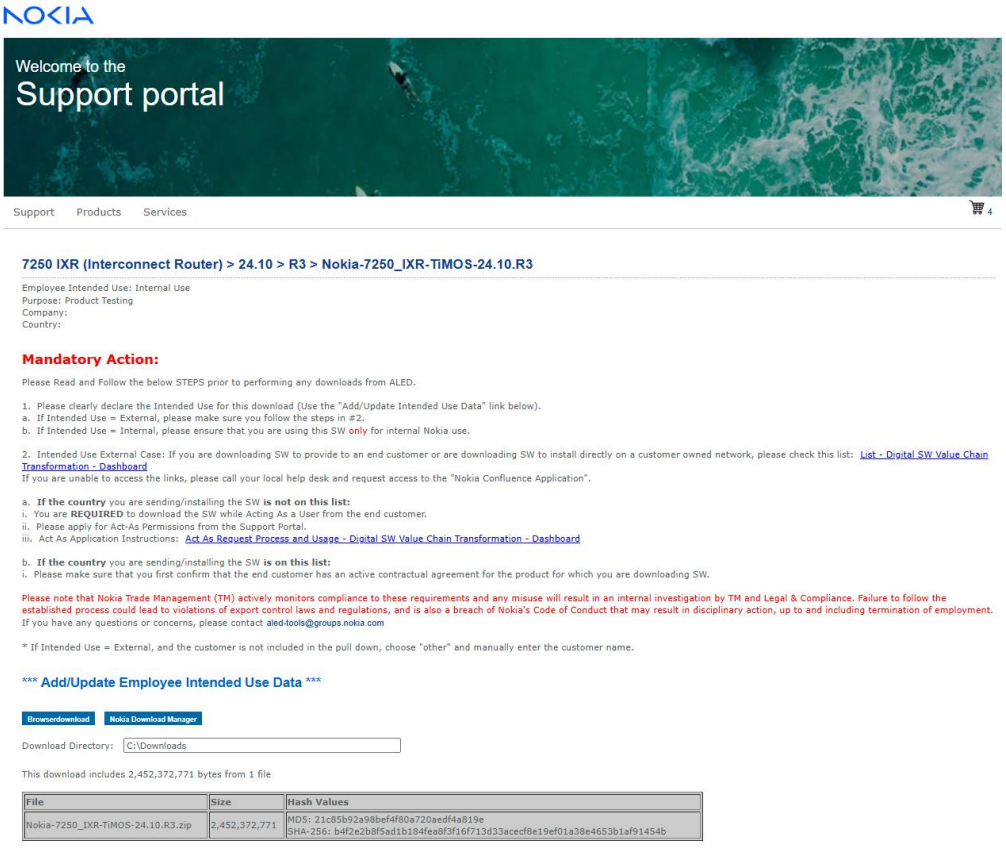

Ilustración 13 Support portal

78. Click en Nokia Download Manager

79. Se muestra la ventana Leyes de exportación, desplazar hasta el final y marcar “I Accept” y click en submit.

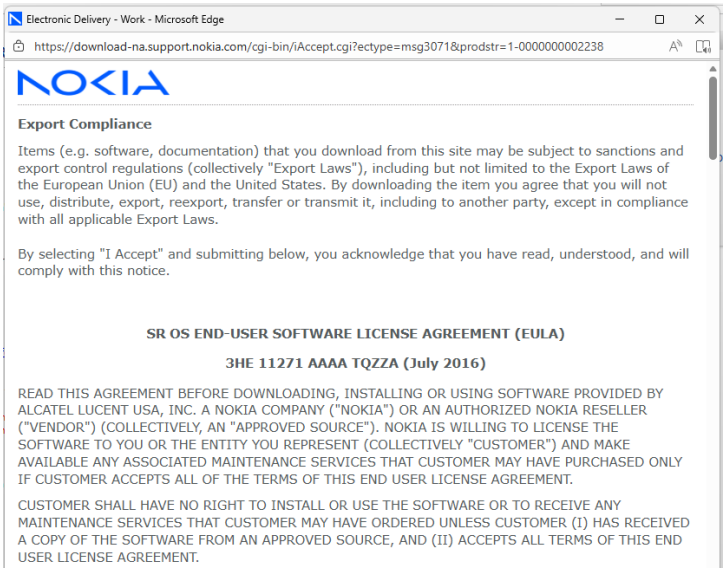

Ilustración 14 Leyes de exportación

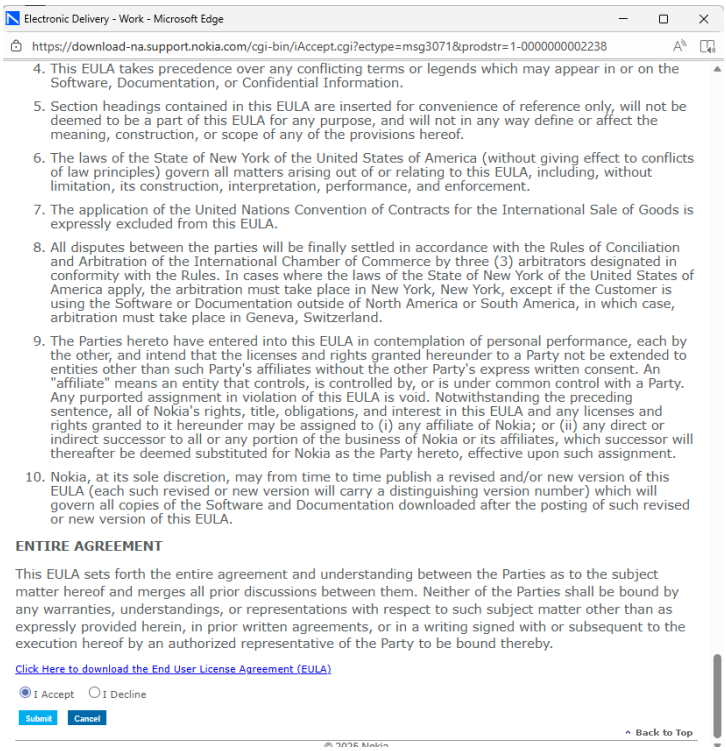

Ilustración 15 Leyes de exportación

80. Aparece la ventana con el mensaje “Select Download location” para descargar a una carpeta local, click en “Browse” y seleccionar carpeta para descargar el paquete:

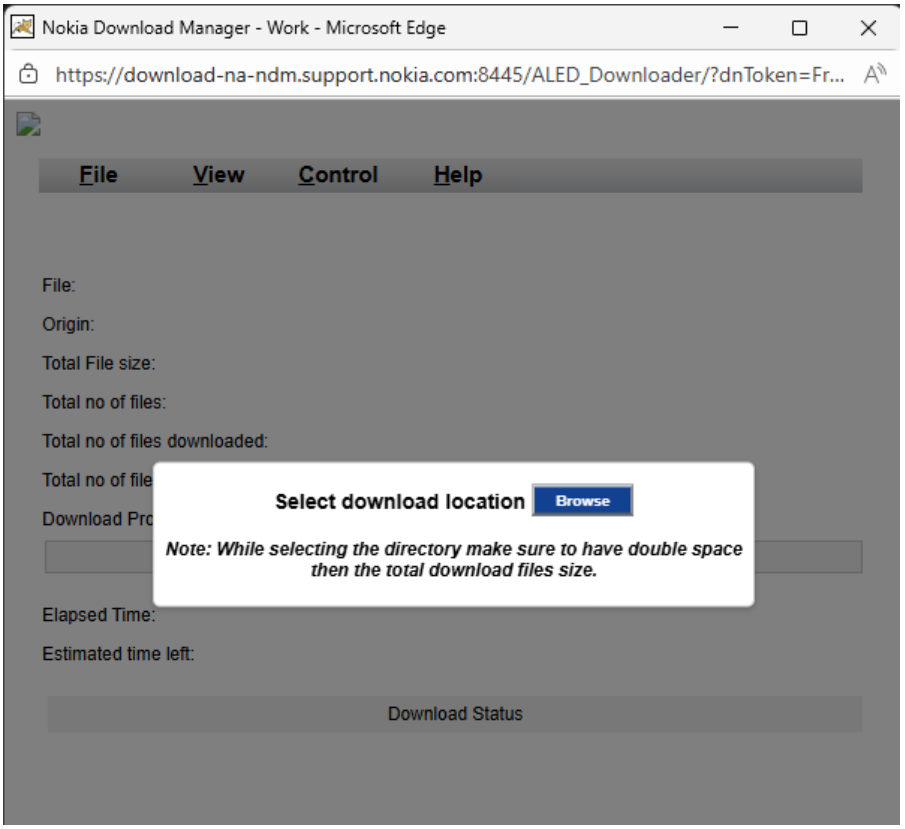

Ilustración 16 Download Manager

81. Se despliega ventana con el estado de la descarga:

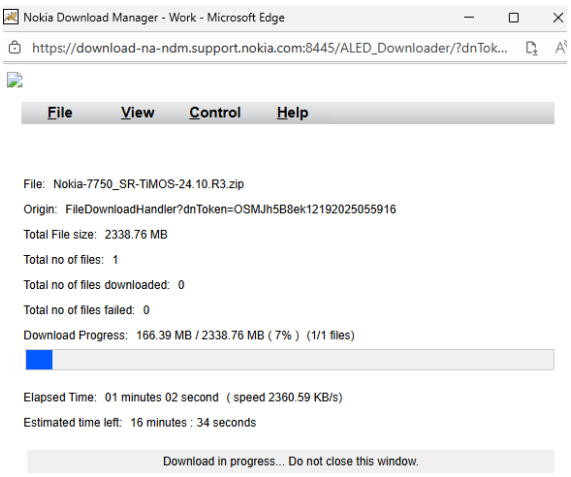

Ilustración 17 Download Manager

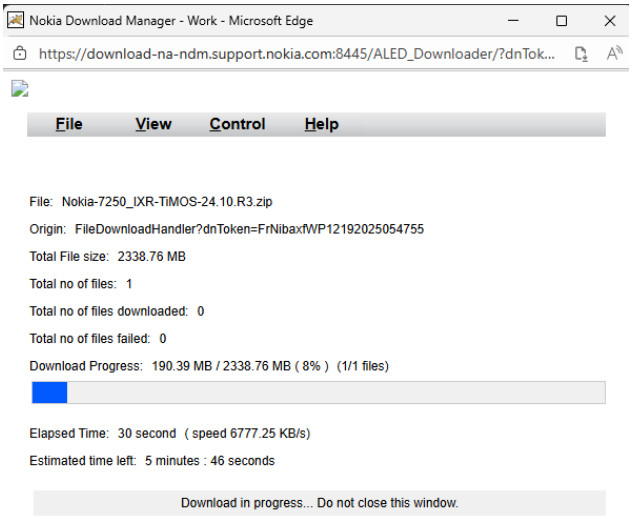

Ilustración 18 Download Manager

82. Aparece el mensaje Download Completed:
    - Si aparece el mensaje, el paquete ha sido descargado y verificado para su uso seguro.
    - Reintentar la descarga si el proceso falla.

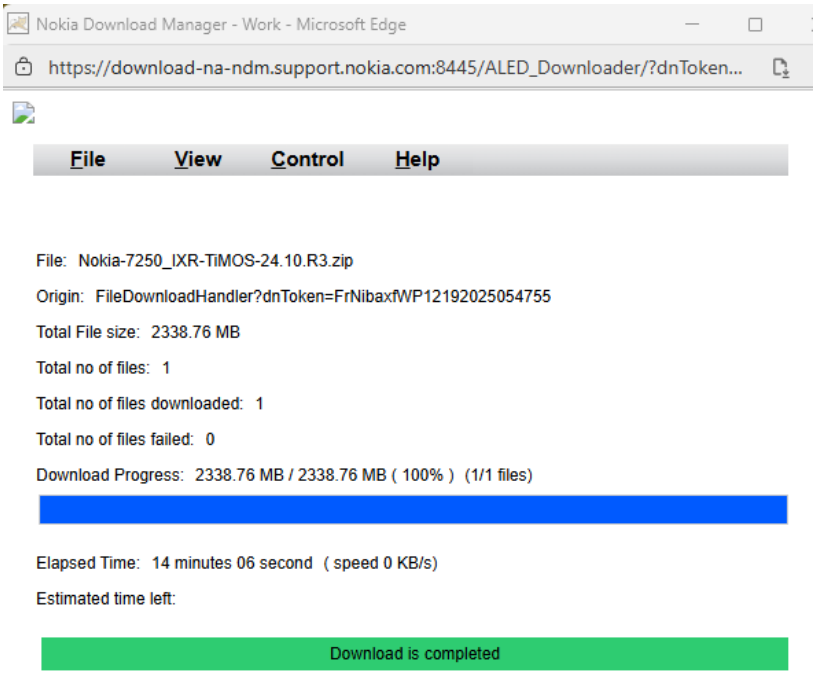

Ilustración 19 Download Manager

83. Si el mensaje no aparece, y lo intenta alguna vez más contactar con el soporte técnico de NOKIA (http://www.nokia.com/en_int/contact-us)

6.7.2 ACTUALIZACION DE SW DE LOS EQUIPOS

84. Las actualizaciones de SW se realizar de forma segura (de forma manual por un usuario Administrador) a través de una conexión SSH siguiendo el punto **Standard Software Upgrade Procedure** del documento [REF7] *"3HE201520009TQZZA01_V1_SR OS 24.10.R3 Software Release Notes.pdf".*

85. Este proceso es idéntico para 7750 SR y 7250 IXR; se ilustra la actualización de software de 7250 IXR.

- Se verifica versión del equipo

```
#show version
```

- Desde terminal o servidor con conectividad y usuario con credenciales de administrador, copiaremos la carpeta con los ficheros del sistema operativo previamente descargado según lo mostrado en la *sección 6.7.1*, al Nokia 7250 IXR-E, se copian los archivos de la carpeta. Crear en equipo destino la carpeta correspondiente

- En equipo Nokia:

```
# file md /images/TIMOS-<new-version>
```

- En equipo terminal o servidor con acceso al equipo

```
# scp \TIMOS-<new-version>\<file> admin@10.10.10.2:/TIMOS-<new-version>/<file>
```

- Comprobamos la integridad de los ficheros

```
# file version cf3:\images\TIMOS-<new-version>\boot.ldr check
```

- Cambiamos el fichero BOF para arrancar con la nueva release.

```
# bof secondary-image cf3:\images\ TIMOS-<old-version>\
# bof primary-image cf3:\images\TIMOS-<new-version>\
# bof save
```

- Copiamos el fichero "boot.ldr" al fichero raíz:

```
# file copy cf3:\images\TIMOS-<new-version>\boot.ldr cf3:\boot.ldr
```

- En equipos con redundancia de controladoras sincronizar el entorno de arranque

```
# admin redundancy synchronize boot-env
```

- Reiniciamos el equipo para que arranque con el nuevo software:

```
# admin reboot upgrade active now
```

- Tras el reinicio, el sistema arrancará con la nueva versión de software.

6.8 AUTO-CHEQUEOS

86. Durante el proceso de arranque, los equipos realizan chequeos del software, hardware y memoria de manera que se abortará el arranque en caso de que no pase dichos chequeos.

87. En fase normal de operación, el equipo generará distintas notificaciones como reacción a distintos problemas que puedan surgir tanto en el hardware (problemas de recursos) como en otros elementos de la operación.
88. El siguiente punto, describe cómo configurar estas notificaciones para que sean enviadas a través del canal seguro al receptor que vea conveniente el administrador.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

89. Revisar "Event *adn Accounting Logs"* en [REF5] *"3HE20116AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR System Management Guide 24.10.R1.pdf"* y en [REF6] *3HE20067AAACTQZZA01_V1_7250 IXR System Management Guide 24.10.R1"* para una descripción detallada de la gestión de los logs tanto en el 7750 SR como en el 7250 IXR.
90. Los eventos que ocurren en el sistema se dividen en cuatro fuentes de eventos:
    - General (General Log): Se generan eventos generales del equipo: referentes a las diferentes tarjetas, puertos, servicios.
    - De seguridad (Security Log): Se generan eventos de seguridad: intentos de acceso al equipo con éxito, fallidos.
    - De acciones de usuario (change log): Se generan diferentes eventos en el que se muestran cambios realizados en el sistema e indica el usuario que ha realizo la acción.
    - Debug (Debug log): Se generan eventos de debug pedidos por el usuario (no tratados en este documento).

6.9.2 ALMACENAMIENTO LOCAL

91. Por defecto, existen dos registros de eventos en memoria: logs 100 y 99, que registran eventos importantes del equipo en un modo round robin con una profundidad de 500 eventos.
92. Estos registros de log tienen el siguiente formato:

```
A:7250-IXR-E# show log log-id 99
===============================================================================
Event Log 99 log-name 99
===============================================================================
Description : Default System Log
Memory Log contents  [size=500   next event=47  (not wrapped)]

46 2025/12/18 08:44:52.281 UTC WARNING: SYSTEM #2002 Base Configuration Save Succeeds
"Configuration file saved to: cf3:\config.cfg"

45 2025/12/18 08:44:26.107 UTC MAJOR: SYSTEM #2077 Base SYSTEM
```

"Management interface configuration mode change to classic has completed"

44 2025/12/18 08:44:26.010 UTC WARNING: SYSTEM #2121 Base Commit
"Commit to configure by admin (MD-CLI) from Console succeeded."

43 2025/12/18 08:44:25.975 UTC MAJOR: SYSTEM #2076 Base SYSTEM
"A management interface configuration mode change (reason manual) from modelDriven to classic was initiated."

42 2025/12/17 21:17:20.920 UTC WARNING: SNMP #2005 management management
"Interface management is operational"

41 2025/12/17 21:17:20.919 UTC WARNING: SNMP #2005 Base A/1
"Interface A/1 is operational"

40 2025/12/17 21:17:12.720 UTC WARNING: SNMP #2004 management management
"Interface management is not operational"

Los registros tienen el siguiente formato:

<Id del registro> <Fecha> <Severidad> : <Aplicación> <EventControl> <descripción del evento>

---

93. El identificador de registro es el número secuencial del evento.
94. La fecha, por defecto está en UTC
95. La severidad manejada tanto por la familia 7750-SR como 7250 IRX se establece de la siguiente manera:

SR OS event severity	Syslog severity numerical code	Syslog severity name	Syslog severity definition
—	0	emergency	System is unusable
critical	1	alert	Action must be taken immediately
major	2	critical	Critical conditions
minor	3	error	Error conditions
warning	4	warning	Warning conditions
—	5	notice	Normal but significant condition
cleared or indeterminate	6	info	Informational messages
—	7	debug	Debug-level messages

96. Las aplicaciones que generan eventos se pueden mostrar con el comando:

```
# show log applications
```

97. Los identificadores de los eventos y el nombre de los mismos se pueden mostrar con el comando:

```
# show log event-control
```

98. Para mostrar el contenido de los logs existentes 99 y 100 podemos ejecutar los comandos:

```
# show log log-id 99
# show log log-id 100
```

99. Para crear por ejemplo un log adicional (log 33) de eventos de seguridad y almacenarlos en el sistema de archivos locales se ejecutan los siguientes comandos:

```
-Configurar la ubicación e identificador de fichero del log:
# configure log file-id 44 location cf3:

-Configurar el identificador del log e indicar el tipo de evento a registrar:

# configure log log-id 33 from security

-Asociar el log con el identificador de fichero
# configure log log-id 33 to file 44

-Activar la recolección de eventos
# configure log log-id 33 no shutdown
```

Ejemplo:

```
A:7750-SR7# file dir log


Volume in drive cf3 on slot B has no label.

Volume in drive cf3 on slot B is formatted as FAT16

Directory of cf3:\log

12/17/2025  08:58a    <DIR>         ./
12/17/2025  08:58a    <DIR>         ../
12/17/2025  11:22a               300 log3344-20260525-135642-CEST
          1 File(s)              300 bytes.
          2 Dir(s)          87883776 bytes free.

A:7750-SR7# show log log-id 33 # revisar log id 33


===============================================================================
Event Log 33 log-name 33
===============================================================================
```

```
Description : (Not Specified)

5 2026/05/25 11:57:34.634 UTC MINOR: SECURITY #2011 management tecnico
"User tecnico from 10.152.115.157 failed authentication"



4 2026/05/25 11:57:29.154 UTC MINOR: SECURITY #2011 management tecnico
"User tecnico from 10.152.115.157 failed authentication"

3 2026/05/25 11:57:25.694 UTC MINOR: SECURITY #2011 management tecnico
"User tecnico from 10.152.115.157 failed authentication"

2 2026/05/25 11:57:00.268 UTC MINOR: SECURITY #2009 management admin
"User admin from 10.152.115.157 logged in"

1 2026/05/25 11:56:59.219 UTC MINOR: SECURITY #2009 management admin
"User admin from 10.152.115.157 logged in"

#Revisar contenido de fichero creado en local:
A:7750-SR7#file type cf3:log/log3344-20260525-135642-CEST
File: log3344-20260525-135642-CEST
-------------------------------------------------------------------------------
status          : in progress
log id          : 33
system ip address : 10.215.35.1
created         : MON MAY 25 13:56:42 2026 CEST
completed       :
first record    : 1
last record     :


1 2026/05/25 11:56:59.219 UTC MINOR: SECURITY #2009 management admin
"User admin from 10.152.115.157 logged in"

2 2026/05/25 11:57:00.268 UTC MINOR: SECURITY #2009 management admin
"User admin from 10.152.115.157 logged in"

3 2026/05/25 11:57:25.694 UTC MINOR: SECURITY #2011 management tecnico
"User tecnico from 10.152.115.157 failed authentication"

4 2026/05/25 11:57:29.154 UTC MINOR: SECURITY #2011 management tecnico
"User tecnico from 10.152.115.157 failed authentication"

5 2026/05/25 11:57:34.634 UTC MINOR: SECURITY #2011 management tecnico
```

```
"User tecnico from 10.152.115.157 failed authentication"

===============================================================================
=
```

6.9.3 ALMACENAMIENTO REMOTO

100. Los registros se pueden enviar a un servidor remoto. Se podría pensar en distintas formas de enviar los eventos de log hacia un almacenamiento remoto:

- Copiar Fichero Locales: Los ficheros locales generados anteriormente podrían ser copiados a una máquina remota con un simple SCP.
- Syslog remoto: se puede configurar para que los eventos de log se envíen a un servidor remoto. Se describe el procedimiento.

101. El procedimiento sería el siguiente:

1. En primer lugar, definimos el servidor de syslog donde queremos mandar los eventos:

```
# configure log syslog 1
# exit
# configure log syslog 1 description "Servidor de Syslog"
# configure log syslog 1 address <direccion-ip-servidor-syslog>
# configure log syslog 1 level info
# configure log syslog 1 log-prefix "7250IXR-7750SR”
```

2. El siguiente paso será crear un log que envíe los eventos al Syslog 1 recien creados:

```
# configure log log-id 50
# exit
# configure log log-id 50 from security
# configure log log-id 50 to syslog 1
# configure log log-id 50 no shutdown
```

3. A partir de este momento, los eventos de seguridad (intentos de ingreso en el sistema) serán reportados al servidor de syslog definido.
4. Se recomienda realizar auditorías periódicas de estos eventos (tanto en local como en remoto) para una correcta gestión de los equipos.

6.10 BACKUP

102. Revisar los documentos *“3HE20090AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR Basic System Configuration Guide 24.10.R1”* REF3 para el 7750 y *“3HE20048AAAATQZZA01_V1_7250 IXR Basic System Configuration Guide 24.3.R1”* REF4 para una detallada descripción de los elementos involucrados en el backup.

103. Para realizar un backup del 7750 SR y el 7250 IXR, se tienen que tener en cuenta los ficheros sensibles dentro del equipo.

1. Fichero de inicio (boot option file): bof.cfg
2. Fichero de configuración: es el fichero “primary-config” que aparece en el bof.cfg

3. (Opcional) Ficheros de software: son los ficheros existentes en el directorio que aparece en el bof.cfg como “primary-image“
4. (Opcional) Fichero “cf3:\boot.ldr”

104. El procedimiento de backup sería el siguiente:

1. Copiamos el fichero bof.cfg a una máquina segura (desde el equipo), se utiliza máquina del ejemplo y se indica en el comando el uso de la instancia “management” para indicar que el acceso se ejecuta desde la conexión de gestión fuera de banda:

```
# file scp bof.cfg nokia@10.100.100.2:/tmp/bof.cfg router “management”
```

Ejemplo:

```
A:7250-IXR-E# file scp bof.cfg nokia@10.100.100.2:/tmp/bof.cfg router "management"
The authenticity of host '10.100.100.2' can't be established.
RSA key fingerprint is SHA256:L425wbtMFl9BHWyYu4Zs5Xm0YyKeO5rDPUeSwopU43o.
RSA key fingerprint is MD5:74:1f:5a:05:34:eb:60:d0:d7:19:df:38:d9:a7:94:fd.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
nokia@10.100.100.2's password:
bof.cfg                                   100%  625     0.6KB/s   00:00
A:7250-IXR-E#
```

2. Comprobamos cuál es el fichero de configuración y lo salvamos:

```
# file type config.cfg | match primary-config
# file scp cf3:\<fichero-config> nokia@10.100.100.2:/tmp/<fichero-config>.cfg router “management”
```

Ejemplo:

```
A:7250-IXR-E# show bof | match primary-config
    primary-config   cf3:\config.cfg
A:7250-IXR-E#
A:7250-IXR-E# file scp config.cfg nokia@10.100.100.2:/tmp/bof.cfg router "management"
nokia@10.100.100.2's password:
config.cfg                                100% 7809     7.6KB/s   00:00
A:7250-IXR-E#
```

3. Comprobamos dónde están los ficheros de imagen de software y los salvamos todos los ficheros del directorio (en nuestro caso para el 7250, boot.ldr)

```
# file type bof.cfg | match primary-image
# file scp cf3:\<directorio>\<fichero-imagen01> nokia@10.100.100.2:/tmp/<fichero-imagen01> router “management”
# file scp cf3:\<directorio>\<fichero-imagen0N> nokia@10.100.100.2:/tmp/<fichero-imagen0N> router “management”
```

Ejemplo:

```
A:7250-IXR-E# show bof | match primary-image
    primary-config   cf3:\images\TiMOS-SR-24.10.R3\
A:7250-IXR-E#
```

```
A:7250-IXR-E# file scp cf3:\images\TiMOS-SR-24.10.R3\boot.ldr nokia@10.100.100.2:/tmp/
images\TiMOS-SR-24.10.R3\boot.ldr router "management"
nokia@10.100.100.2's password:
config.cfg                    100% 7809     7.6KB/s   00:00
A:7250-IXR-E#
```

4. Salvamos el fichero “cf3:\boot.ldr” que debería ser igual que el que salvamos en el punto anterior.

```
# file scp cf3:\boot.ldr nokia@10.100.100.2:/tmp/boot.ldr router “management”
```

Ejemplo:

```
A:7250-IXR-E# file scp cf3:\boot.ldr nokia@10.100.100.2:/tmp/ images\TiMOS-SR-
24.10.R3\boot.ldr router "management"
nokia@10.100.100.2's password:
config.cfg
```

105. En la máquina destino estarían ahora todos los ficheros susceptibles de guardar en un backup de un equipo 7250 IXR o 7750 SR. Se recomienda hacer un backup en soporte físico de dichos ficheros.

7 FASE DE OPERACIÓN

106. Como se ha comentado a lo largo del documento, los equipos son capaces de generar notificaciones en función de los elementos que se pudieran degradar dentro del equipo.

107. Los siguientes comandos para monitorizar distintas partes del software pueden ser de ayuda para mejorar el mantenimiento del equipo.

1. Comprobación del fichero de opciones de arranque:

```
# show bof
```

2. Comprobación de los elementos de chasis, fuentes de alimentación, ventiladores:

```
# show chassis [detail]
# show chassis power-supply
# show chassis environment
```

3. Verificación del estado de las SF/CPM:

```
# show uptime
# show card
# show system cpu
# show system info
# show system memory-pools
```

4. Verificación del estado de las IOMs:

```
# show card <slot-number> detail
# show card state
```

5. Verificación del estado de las MDAs:

```
# show mda <slot-id> detail
```

108. Recordar la conveniencia de monitorizar los logs de memoria, así como las notificaciones de eventos que aparece en el syslog remoto de forma periódica.

8 REFERENCIAS

109. En la tabla se muestran los diferentes documentos de referencia mencionados en los distintos puntos del documento, los mismos se pueden descargar desde la página web oficial de soporte al cliente de Nokia https://customer.nokia.com/support/s/ :

REF1 3HE19401AAAATQZZA_V1_7250 IXR-e Chassis Installation Guide Release 23.pdf

REF2 3HE18643AAAATQZZA02_V1_7450 ESS-7 and 7750 SR-7 Chassis Installation Guide 22.7.pdf

REF3 3HE20090AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR Basic System Configuration Guide 24.10.R1

REF4 3HE20048AAAATQZZA01_V1_7250 IXR Basic System Configuration Guide 24.3.R1.pdf

REF5 3HE20116AAACTQZZA01_V1_7450 ESS 7750 SR 7950 XRS and VSR System Management Guide 24.10.R1.pdf

REF6 3HE20067AAACTQZZA01_V1_7250 IXR System Management Guide 24.10.R1.pdf

REF7 3HE201520009TQZZA01_V1_SR OS 24.10.R3 Software Release Notes.pdf

REF8 CPSTIC
https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

8.1 DESCARGA Y ACCESO A DOCUMENTACIÓN.

110. La documentación de referencia indicada en la sección previa está disponible para descarga electrónica a través del Portal de soporte de NOKIA (https://customer.nokia.com/support).

111. Pasos a seguir para la descarga SW:

- Abra el Portal de soporte de Nokia (https://customer.nokia.com/support) en su navegador.
- Introduzca sus credenciales de inicio de sesión. Las credenciales son definidas por el tipo de contrato de soporte del cliente (credenciales corporativas con correos bajo dominio del cliente o bajo el soporte de un técnico empleado de Nokia, el cliente debe estar dado de alta en la lista de empresas con contratos actuales con Nokia).

Ilustración 20 Descarga

- Seleccionar “All Products” y en la casilla de búsqueda indicar la familia de equipos de interés.

Ilustración 21 Descarga

- Se desplagará una nueva sección donde ubicamos “Resourses” y seleccionamos “Documentation”.

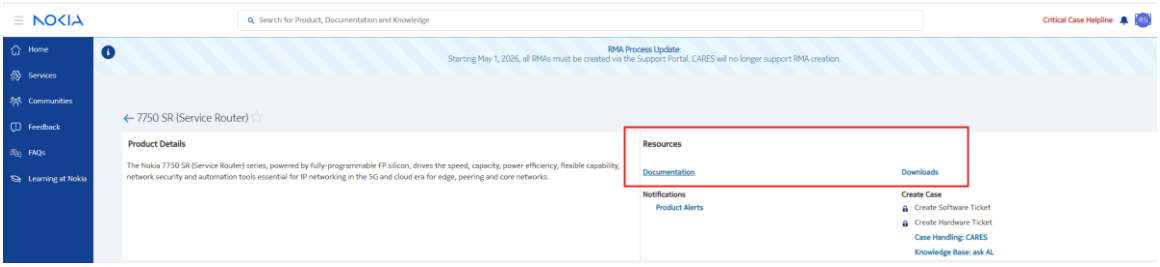

Ilustración 22 Descarga

- Se desplegará la sección de documentos de la familia que permite filtrar por versiones, modelos, categoría, tipo de contenido y formato (pdf/html/zip). Se puede utilizar el cuadro de búsqueda para filtrado de interés, por ejemplo, utilizando el nombre de los documentos indicados en la sección de referencias

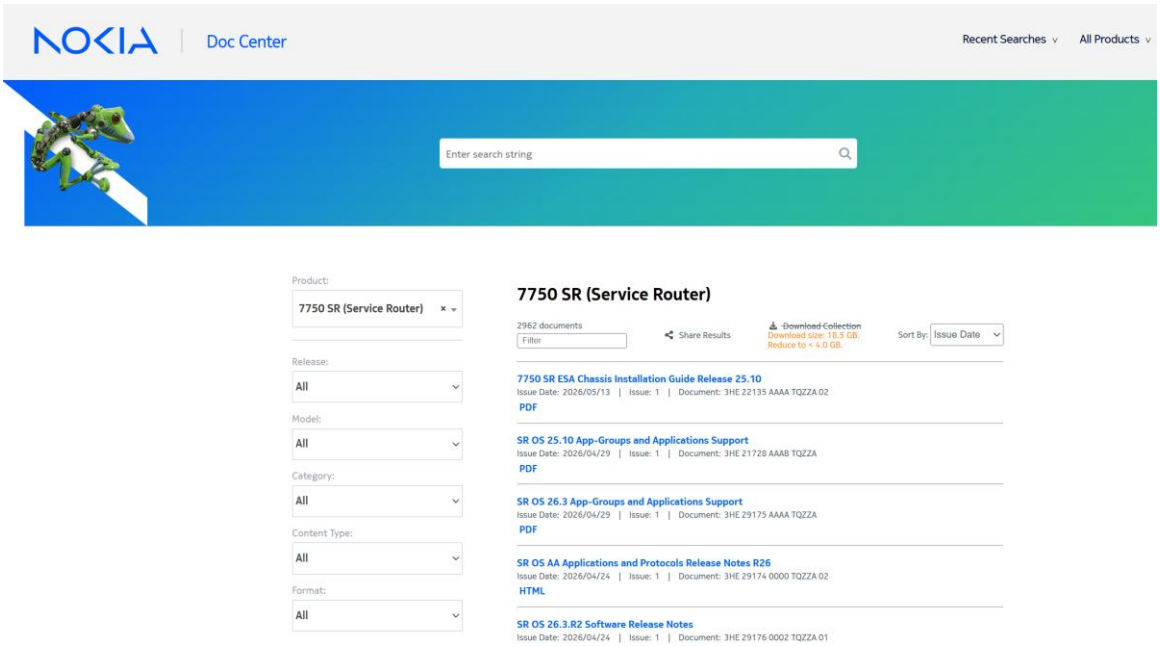

Ilustración 23 Descarga

9 ABREVIATURAS

BOF	Boot Option File
CC	Commom Criteria
CLI	Command Line Interface
CPM	Control Processor Module
CSM	Control and Switching Module
DC	Direct Current
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards
GRT	Global Routing Table
IMM	Integrated Media Module
IOM	Input Output Module
IP	Internet Protocol
IXR	Interconnect Router
MDA	Media Dependent Adapter
MPLS	Multi Protocol Label Switching
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PEM	Power Entry Module
RADIUS	Remote Authentication Dial In User Service
SCP	Secure Copy
SF	Switch Fabric
SF/CPM	Switch Fabric/Control Processor Module
SFP	Small Form-factor Pluggable
SR	Service Router
SSH	Secure Shell
SW	Software