centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1436

Procedimiento de empleo seguro
Nokia 1830 Photon Service Switch (PSS) v9.1

Febrero 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.02.17 18:04:02 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-065-5.
Fecha de Edición: febrero de 2023

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

ÍNDICE

1. INTRODUCCIÓN

1. El conmutador de servicio fotónico Nokia 1830 PSS es una plataforma escalable que ofrece conectividad multiservicio de multiplexación óptica por división de longitud de onda densa (DWDM) de gran capacidad. Incluye cifrado, baja latencia y detección de intrusiones ópticas, lo que garantiza la confidencialidad e integridad de los datos, así como el soporte de comunicaciones.
2. La familia 1830 PSS consta de diferentes plataformas que se han optimizado para su aplicabilidad en diversos entornos de despliegue de redes ópticas, desde la interconexión de centros de procesamiento de datos hasta el escalado de grandes redes ópticas multiservicio, multicapa, regionales y de larga distancia.
3. Son compatibles con múltiples aplicaciones de red de transporte, que incluyen: transporte y agregación metro multiservicio, implementaciones de larga distancia y núcleo óptico, configuraciones de conmutación fotónica con enrutamiento incoloro, sin dirección y sin contención con Flexgrid, agregación/conmutación en capa L1, medidas reflectométricas OTDR de las fibras ópticas, y otros mecanismos de protección.

2. OBJETO Y ALCANCE

4. El objeto del presente documento es facilitar la instalación y configuración segura de los **dispositivos 1830 PSS con la versión software 9.1 de las series 1830 PSS-32 y 1830 PSS-8.**

5. Los modelos hardware y sus componentes se indican en la siguiente tabla:

Appliance	Subcomponente	Descripción
1830 PSS-32	32EC2E PSS-16/PSS-32	Controlador del equipo
	11QPEN4	Tarjeta de cifrado
	11DPM12	Transpondedor
	10G MR XFP	Línea XFP, 1310nm, medio alcance, OTU2
	10GBASE-SR XFP	Cliente XFP corto alcance, 850nm, 10GE
	1AB396080001	Atenuador fVOA (*fast Variable Optical Attenuator*)
	X8FCLC-L	XFP I-64.1/8.5GFC IT (8G FC XFP SM)
	X8FCSN-I	8G FC XFP MM
	XL-64TU XFP	DWDM Sintonizable CT (50GHz 10G XFP)
	PF (-48V DC) PSS-32, 20A	Alimentación
	8DG-59319-AB	Bastidor
	8DG-59240-AB	Panel de usuario
	8DG-61510-AA	Kit de etiquetado de seguridad
	8DG-63269-JAAA-TSZZA	Manual de seguridad
	8DG-59418-AA	Placas de relleno de tarjeta
	8DG-59243-AB	Ventilador de Alta Capacidad
1830 PSS-8	8EC2E PSS-8	Controlador del equipo
	11QPEN4	Tarjeta de cifrado
	11DPM12	Transpondedor
	10G MR XFP	Línea XFP, 1310nm, medio alcance, OTU2

Appliance	Subcomponente	Descripción
	10GBASE-SR XFP	Cliente XFP corto alcance, 850nm, 10 GE
	1AB396080001	Atenuador fVOA (*fast Variable Optical Attenuator*)
	X8FCLC-L	XFP I-64.1/8.5GFC IT (8G FC XFP SM)
	X8FCSN-I	8G FC XFP MM
	XL-64TU XFP	DWDM Sintonizable CT (50GHz 10G XFP)
	PF (-48V DC) PSS-8, 20A	Alimentación
	3KC-48901-AA	Bastidor
	8DG-61510-AA	Kit de etiquetado de seguridad
	8DG-63269-JAAA-TSZZA	Manual de seguridad
	8DG-59418-AA	Placas de relleno de tarjeta
	3KC-49926-AA	Filtro de Aire
	3KC-48850-AA	Bandeja de ventilador

Tabla 1 – Modelos y Componentes de Nokia 1830 PSS

6. El producto consta de una tarjeta 11QPEN4, la cual proporciona cifrado de nivel de transporte para la interconexión de centros de datos a través de fibra óptica. La tarjeta admite el cifrado de línea OTU2 con AES-256 que se puede utilizar para proporcionar cifrado de uno o más puertos de cliente conectables, incluidos 10GE, OTU2, canales de fibra 8G y 10G, y señales de cliente 5G *InfiniBand* (DDR).
7. La tarjeta 11DPM12 es una tarjeta con funciones de agregación, la cual no incluye funciones de seguridad adicionales.
8. **Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC), en la categoría "Switches".**

3. ORGANIZACIÓN DEL DOCUMENTO

9. La estructura de capítulos del documento es la siguiente:

   a) **Apartado 1.** Descripción de la familia de productos Nokia 1830 PSS.

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

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

   d) **Apartado 4.** Fase de despliegue e instalación. Recoge recomendaciones de seguridad en dicha fase.

   e) **Apartado 5**. Fase de configuración. Recoge recomendaciones de seguridad en dicha fase.

   f) **Apartado 6.** Fase de operación. Recoge recomendaciones de seguridad en dicha fase.

   g) **Apartado 7.** *Checklist* de las tareas a realizar y el estado de cada una de ellas.

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

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

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. En el momento de la recepción del *appliance*, debe verificarse la integridad del producto y comprobar que su modelo, componentes y empaquetado corresponden con el modelo Nokia 1830 PSS esperado.
11. El dispositivo se entrega con etiquetas de sellado de seguridad, las cuales deben encontrarse pegadas e intactas en el producto en el momento de su recepción, de forma que se pueda asegurar que el producto no ha sido manipulado. El embalaje debe estar sellado con una etiqueta que dice "*Vacío a menos que lo retire el cliente final*". Si la etiqueta del embalaje muestra alguna evidencia de manipulación, no se considera seguro el uso del producto.
12. Se debe comprobar que el puerto USB de cada controladora (32EC2E y 8EC2E) está sellado por una etiqueta azul a prueba de manipulaciones para impedir el acceso al puerto. Si la etiqueta muestra alguna evidencia de manipulación, no se considera seguro el uso del producto.
13. 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.
14. El controlador del producto se envía con el software 9.1 preinstalado. El controlador funciona exclusivamente en **modo fijo**, el cual establece que el producto sea conforme con los requerimientos de seguridad necesarios. Dicho modo no puede desactivarse, y se indica la versión segura del producto con el nombre **ECE 9.1 (versión 9.1 con configuración segura activada)**. Las configuraciones de seguridad adicionales necesarias se describirán en el presente documento.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. 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.
16. El acceso físico al lugar donde 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.
17. Todos los dispositivos utilizados para la gestión y administración de los sistemas 1830 PSS deben tener un nivel de protección físico y lógico similar al producto.
18. Se recomienda consultar el apartado "*Safety requirements in specific deployment phases*" de la guía oficial del producto [REF3] (PSS-8) o [REF4] (PSS-32) para más detalle en las condiciones ambientales y de seguridad física del entorno necesarias para un correcto despliegue y funcionamiento del dispositivo.

4.3 CONSIDERACIONES PREVIAS

19. Todos los subcomponentes (11QPEN4, 11DPM12 y placas de relleno) deben instalarse en los armazones del 1830 PSS antes de realizar la instalación y configuración de seguridad.
20. El dispositivo Nokia 1830 PSS dispone de funcionalidades opcionales de administración remota. Los componentes de administración remota, en caso de utilizarse, **deben estar protegidos por el entorno operacional**. Concretamente, serían los siguientes sistemas:
    a) Network Management System (NMS).
    b) Security Management Server (SMS).
21. En el apartado 4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN del presente documento se incluyen más detalles sobre estos elementos de administración remota. Para más detalle sobre la administración, se debe consultar el apartado 5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.
22. Los siguientes elementos y funcionalidades quedan excluidos del empleo seguro del producto:
    a) Interfaz Web GUI/Soporte TLS.
    b) Autenticación mediante servidor externo (RADIUS).
    c) Administración mediante TL1.
    d) Roles de usuario "*Provisioner*" y "*Observer*".
    e) Soporte GCC.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. Para la administración remota del producto, se debe configurar una red de administración en un entorno seguro y bastionar dicha red de forma que los sistemas de administración queden protegidos de forma física y lógica, dado que esta red transporta claves de sesión sensibles. Para ello se deberán utilizar dispositivos/herramientas VPN cualificados.

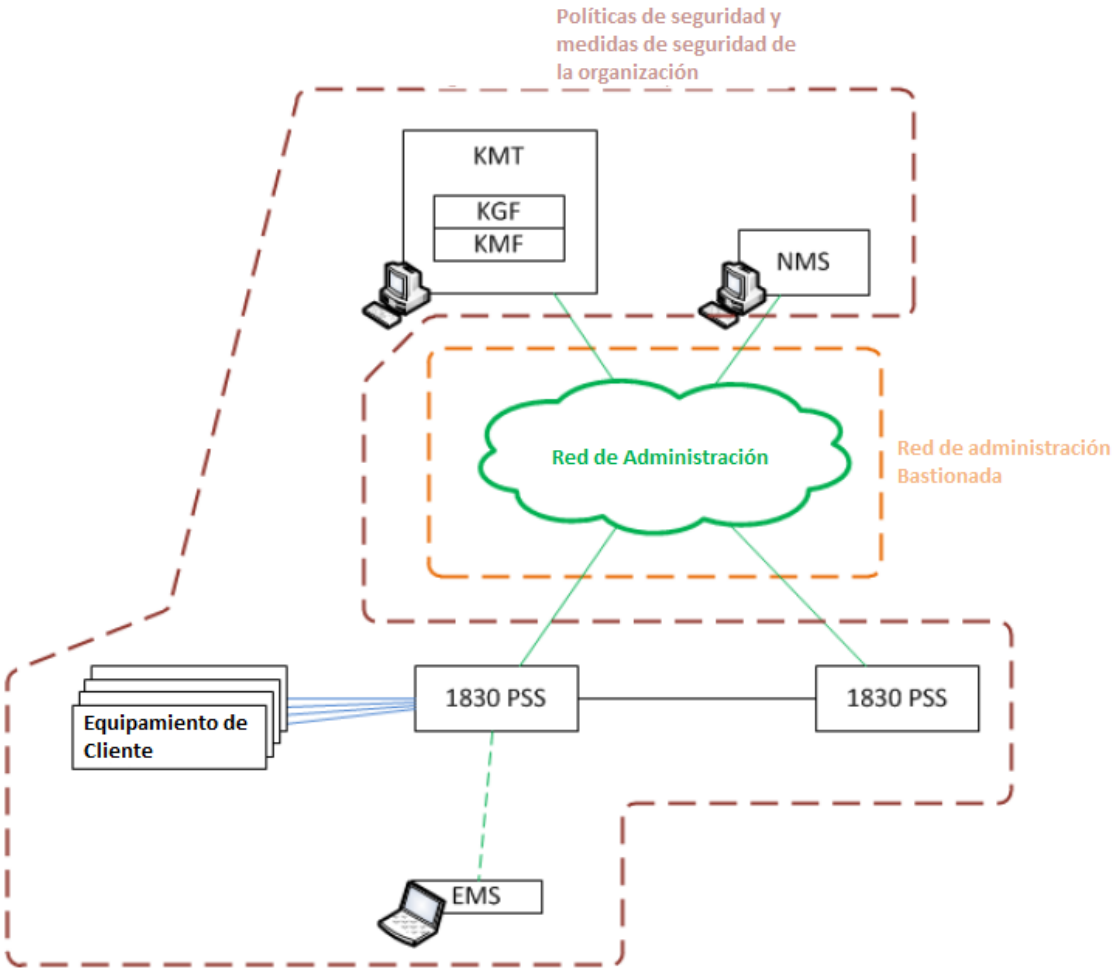

Ilustración 1 – Ejemplo de Arquitectura de Red de Operación del Producto.

24. El producto se integra en un entorno donde se comunica con los siguientes elementos:
    a) **Sistema o red de administración**, local o remota.
    b) **Equipamiento vecino** (*Neighbor Equipement* o **NE**). Equipo óptico (en ocasiones, otro producto PSS) conectado mediante fibra óptica, dicho canal utiliza el protocolo OTU2 con cifrado de datos.
    c) **Equipamiento cliente externo** para el intercambio de datos mediante fibra óptica. Este tráfico **no** se transmite cifrado y no es configurable desde el producto.
    d) **Servidor externo de auditoría,** donde se enviarán los registros de auditoría mediante el protocolo SNMPv3.
    e) **Servidor NTP,** configurable opcionalmente para la sincronización de tiempo de los dispositivos.
25. En el entorno de administración se han de tener en cuenta los siguientes elementos para una administración local segura del producto (EMS) y, opcionalmente, remota (ver Ilustración 1):

a) **EMS (*Equipment Management System*):** equipo externo para administrar y operar el producto a través de la interfaz local de administración (puerto serie).

b) **NMS (*Network Management System*):** equipo externo para administrar y operar el producto a través de la interfaz remota de administración. Utiliza los protocolos SNMPv3, SFTP (sobre SSHv2) y NTP. SFTP habilita la posibilidad de actualizar software, realizar copias de seguridad de las bases de datos desde el propio NMS y recolectar logs SNMP y de auditoría.

c) **KMT (*Key Management Tool*):** equipo externo para administrar las funciones criptográficas del producto a través de la interfaz remota de administración. Utiliza SNMPv3 para la comunicación con el producto. Sus funcionalidades incluyen generación de claves o KGF (*Key Generation Functionality*) y administración de las mismas o KMF (*Key Management Functionality*). Se recomienda que se utilicen dispositivos de gestión de claves cualificados.

   Nokia dispone de un *appliance* de operaciones KMT remoto: **Nokia 1830 SMS** (Security Management Server). El empleo y configuración de este dispositivo queda fuera del alcance del procedimiento de empleo seguro de este producto y no se incluye dentro de la configuración segura de este procedimiento.

d) **Cliente SSH:** Cliente SSHv2 para la configuración, administración y solución de problemas a través de CLI.

e) **Servidor SFTP**: se puede habilitar el cliente SFTP para añadir archivos de actualización software, realizar copias de seguridad de bases de datos desde el NMS y recolectar logs SNMP y de auditoría.

26. Consultar el apartado 5.3 ADMINISTRACIÓN DEL PRODUCTO para los detalles de los equipos de administración de la red.

4.5 INSTALACIÓN

27. Tras la recepción segura del producto se debe proceder a la instalación física del *appliance.*

28. Se debe seguir la guía de documentación oficial de Nokia: consultar el apartado *"Procedure 1: Provision 1830 PSS for CC EAL3+ secured operation"* para el despliegue e instalación del producto. Se deberán seguir las guías "*2 Equipment Installation Overview"* de [REF3] (PSS-8) o [REF4] (PSS-32) a la hora de proceder a su instalación física.

29. Una vez se haya instalado el producto, deben instalarse etiquetas a prueba de manipulaciones para garantizar la seguridad e integridad durante su operación. Para la instalación de las etiquetas seguir el apartado "*Procedure 2: Install tamper-evident labels*" de la guía de la documentación oficial [REF1].

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

30. Para que el dispositivo sea configurable en modo de operación seguro se requiere que el cliente entre en un acuerdo de servicio activo con Nokia para el *appliance* Nokia 1830 PSS versión 9.1.

31. Como se menciona en apartado 4.1 ENTREGA SEGURA DEL PRODUCTO, el equipo se encuentra configurado en modo de operación seguro por defecto en el momento de su entrega (modo fijo), por lo que no se requiere la activación manual del modo de operación seguro por parte del usuario administrador. Se puede comprobar la versión del equipo con el comando '*show version*' a través de CLI (consultar apartado 5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA para más información sobre la interfaz de comandos CLI).

32. En caso de utilizarse los protocolos mencionados, el producto **debe quedar bastionado por el entorno operacional** y medidas de seguridad adicionales dependiendo de dicho entrono.

5.2 AUTENTICACIÓN

33. El acceso a la administración y funciones del producto requiere de la autenticación de la identidad del administrador.

34. Los usuarios se identifican y autentican contra la base de datos local del dispositivo a través de contraseñas. Una vez autenticado, el usuario podrá realizar cambios de configuración o administrar el sistema en función de su rol administrativo de usuario. Consultar el apartado 5.3.2 CONFIGURACIÓN DE ADMINISTRADORES para más información sobre los roles de usuario.

35. Consultar el apartado "*Authentication*" de [REF1] para más información sobre los mecanismos de autenticación.

36. En caso de administración remota, los equipos de administración NMS y KMT se autentican mediante el uso de claves simétricas del modo *AuthPriv* de SNMPv3. Ambos equipos de administración utilizarán claves diferentes.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

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

    a) Para la administración **local**, el *appliance* posee dos interfaces: puerto serie y puerto ethernet. La interfaz de comandos (CLI) se encuentra disponible a través de ambos puertos. Para la administración local, se debe acceder mediante autenticación con usuario y contraseña. El sistema encargado de esta administración es el EMS.

Para la conexión con el CLI se recomienda consultar el apartado "*Connect to NE for CLI access*" de [REF3] (PSS-8) o [REF4] (PSS-32). Se recomienda consultar y seguir el apartado "*Introduction to 1830 CLI*" de la documentación oficial [REF2] para conectarse a la interfaz de comandos. [REF2] incluye una guía de todos los comandos disponibles para la administración del 1830 PSS a través de CLI.

b) Para la administración **remota,** el *appliance* posee interfaces cifradas para las funciones de administración SNMPv3. A estas interfaces mencionadas acceden los equipos NMS y KMT. Ambos equipos utilizan claves criptográficas para la protección del protocolo SNMPv3. Las claves (*AuthKey* y *PrivKey*) se configuran durante el comisionado del producto, y se pueden editar tal y como se indica en el apartado 7.10 SNMP. La autenticación se realiza mediante el protocolo SNMPv3.

38. Para una administración segura del producto, se recomienda únicamente el uso de la administración local mediante puerto serie o puerto ethernet (EMS).

39. Para el uso de la administración remota (NMS, KMT) de forma segura **se debe bastionar el canal con la red de administración:** se debe garantizar, mediante el entorno operacional y medidas adicionales de seguridad (por ejemplo: implementación de una VPN IPsec cualificada y configurada de forma segura), la confidencialidad, integridad y fiabilidad de la conexión de administración remota. Se deberá realizar un análisis de riesgos para determinar las medidas de seguridad adecuadas a implementar en función de los dispositivos e información que se encuentren en el entorno específico.

40. En caso de que no se pueda garantizar un canal y entorno seguro para la administración remota, se desaconseja su uso y únicamente se consideraría segura la administración local.

41. Las únicas interfaces y protocolos que se deben utilizar en caso de administración remota son SNMPv3 y SSHv2 (CLI y SFTP). Para más información sobre las interfaces y administración SNMP, consultar el apartado *"SNMP Interface"* de [REF1]

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

42. El sistema Nokia 1830 PSS tiene dos **tipos de usuarios:**

    a) Usuarios NE (*Network Element*) para elementos de red.

    b) Usuarios SNMPv3, en el caso de administración remota mediante SNMPv3**.**

43. El producto soporta **diferentes roles** de administración para ambos tipos de usuario, los cuales puede crear y gestionar un administrador principal a través de CLI. Los roles determinan el nivel de privilegios de cada usuario. Los roles de administración que deben configurarse en el dispositivo son los siguientes:

    a) **Administrador:** usuario principal del producto, encargado de llevar a cabo la instalación, configuración y posterior operación y administración del sistema. Puede crear y modificar otras cuentas de usuario. Se recomienda tener un usuario administrador principal (*root*) y otro usuario administrador NMS con el mismo rol administrador excluyendo las funcionalidades de creación y modificación de usaurios.

b) **Oficial de Criptografía (*Crypto officer*):** usuario encargado de la administración de las claves criptográficas. Este rol proporciona todos los servicios que son necesarios para la gestión segura del módulo criptográfico.

44. La identificación de usuario (*user Id*) y las reglas de usuario y contraseña son diferentes para los usuarios de NE y SNMPv3. En administración remota, los usuarios SNMP acceden desde el KMT y el NMS. Para el KMT se utilizará el rol de Oficial de Criptografía y para el NMS utilizará el rol de Administrador.

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

    - Username: **admin**
    - Password: **admin**

46. Cuando el usuario accede con sus credenciales aparecerá precediendo a la línea de comandos un mensaje de aviso de sesión. Siempre aparecerá dicho mensaje por defecto y no es configurable. Consultar el apartado *"Connect to NE for CLI access"* de [REF3] y [REF4] para más información sobre el mensaje.

47. Una vez que el administrador haya accedido a la interfaz CLI se deberán modificar dichas credenciales por defecto mediante los siguientes comandos:

    # config admin users edit service status disabled

    # config admin users edit admin passwd

48. Se deberán configurar y crear los administradores mediante el comando '*config admin*', tal y como se indica a continuación:

    # config admin users add <nombre de usuario> <rol>.

    Indicando en el campo *<rol> administrator* o *crypto* según si se trata de un usuario de rol administrador u oficial de criptografía, respectivamente.

49. Adicionalmente, se deberán configurar los siguientes parámetros de sesión y políticas de contraseña para los usuarios administradores:

    a) **Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:

        i. Longitud mínima de la contraseña: doce (12) caracteres:

            # config admin authentication local password minlength 12

        ii. Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Debe utilizarse al menos un carácter de los cuatro (4) grupos. El usuario que establece la contraseña es responsable de usar esta composición segura de la contraseña de forma procedural.

        iii. Número de contraseñas anteriores que no se permite utilizar: al menos, diez (10). Esta configuración viene dada por defecto.

        iv. Tiempo de validez en días de las contraseñas tras el cual expiran: aproximadamente dos meses (60 días). Se debe aplicar individualmente para cada usuario:

 # config admin users edit <nombre de usuario> *pwdaging 60*

b) **Configuración de los parámetros de sesión,** mediante el comando *'config admin session'***.** Deberá cumplir con los siguientes requisitos mínimos:

i. Tiempo de inactivid*ad de las sesiones: cinco (5) minutos.*

 # config admin session timeout 5

ii. Número de intentos fallidos de inicio de sesión: tres (3) intentos.

 # config admin session maxfailedlogins 3

iii. Tiempo de bloqueo tras los intentos fallidos: un (1) minuto.

 # config admin session minwaitlogin 60

50. Se deberá realizar un reinicio para que los cambios efectuados se apliquen mediante el siguiente comando:

 # config admin resetne warm

51. Consultar el apartado *"3 System administration commands"* de [REF2] para más detalle sobre los comandos de configuración mencionados.

52. El acceso a la administración y funciones de cifrado únicamente es posible tras la autenticación como usuario administrador. Para más información sobre los roles de usuario, consultar el apartado *"Roles, services and authentication"* de [REF1]. Para un ejemplo de configuración de roles, ver el apartado *"Procedure 1.4 Provision user roles"* de [REF1].

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

53. El dispositivo en su modo de operación seguro consta de las siguientes interfaces lógicas:

a) **Interfaces de datos:** interfaces de la tarjeta 11QPEN4. Se usan para la conexión con equipos cliente externos al producto. Estos equipos se deben localizar en una red interna fiable y segura.

b) **Interfaces de fibra óptica:** interfaces de la tarjeta 11QPEN4. Se usan para la conexión con otros equipos Nokia 1830 PSS o equipamiento similar. El protocolo OTU2 está cifrado por el producto, por lo que las fibras entre los sistemas pueden extenderse a través de redes públicas.

c) **Interfaces de Administración:** interfaces del controlador. Se usan para la configuración y administración del producto. Consultar el apartado 5.3 ADMINISTRACIÓN DEL PRODUCTO para los detalles de los sistemas conectados a las interfaces. Los nombres de las interfaces físicas en el controlador son:

i. CRAFT: administración local por puerto serie.

ii. CIT (*Craft Interface Terminal*): administración local a través de SSH.

iii. OAMP (*Operation, Administration, Management Port*): administración remota.

54. Para reducir la superficie de ataque contra el producto, cualquier otra interfaz de administración no mencionada se encuentra deshabilitada, al igual que las funciones de depurado y otros servicios subyacentes del sistema operativo. Las interfaces de administración *In-band* y las funciones del plano de control DWDM están bloqueadas por defecto y no deben utilizarse.

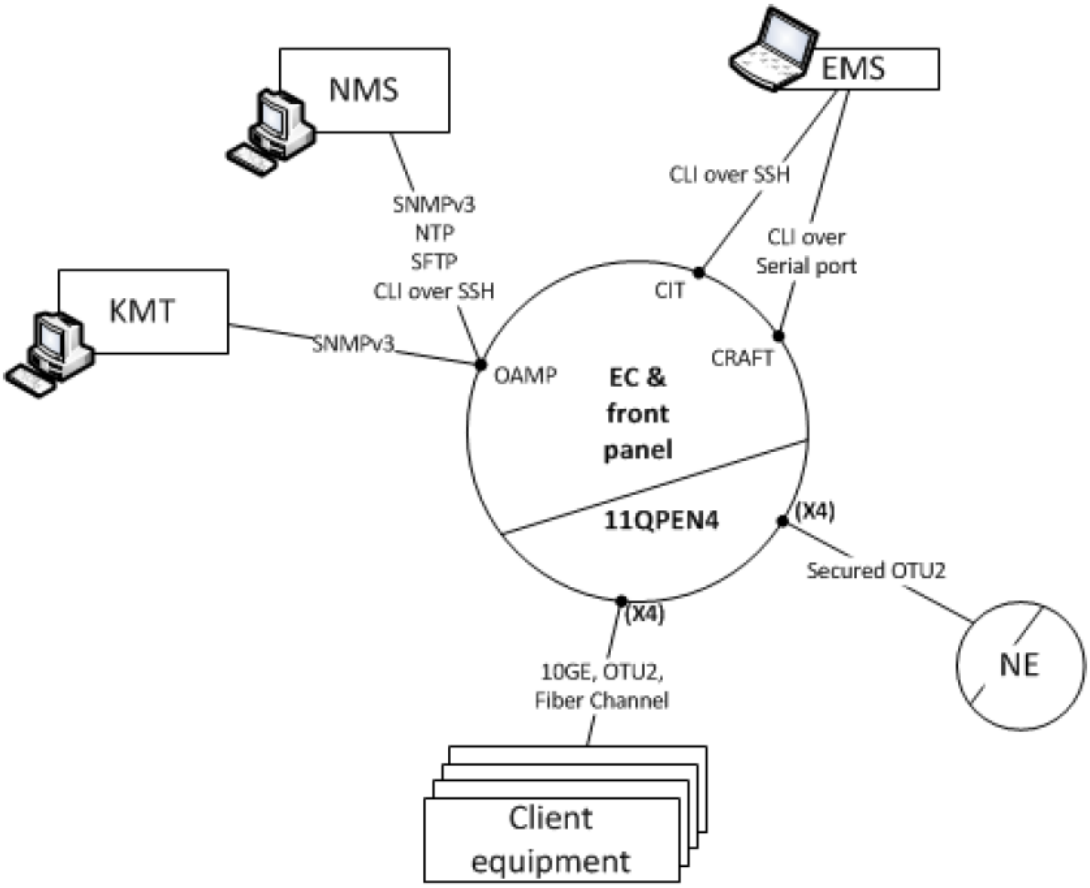

Ilustración 2 – Arquitectura de Interfaces del appliance.

55. Los puertos nombrados como AUX, ES1 y ES2 están deshabilitados y no deben utilizarse. El intento de uso de dichos puertos generará una alarma (Para más información sobre las alarmas, consultar el apartado "*Alarm and Condition Details"* de [REF5]).

56. Para la conexión con las interfaces, se debe seguir el procedimiento descrito en los apartados *"Procedure 1.1: Connect to the NE using CIT port"* para administración local *y "Procedure 1.3: Connect to the NE using OAMP port"* para administración remota de [REF1].

57. Para la configuración de direcciones IP de los sistemas debe consultarse el apartado *"1.2 Provision IP addresses and date/time"* de [REF1]. Adicionalmente, seguir también los siguientes pasos:

5.4.1 CONFIGURACIÓN DE LOS PUERTOS DE LAS TARJETAS 11QPEN4 Y 11DPM12

58. Para configurar los puertos, se debe iniciar sesión en el NE de administración utilizando CLI con el rol de usuario Administrador. A continuación, se indica un ejemplo de configuración de interfaces para una tarjeta 11QPEN4 instalada en el *slot* 3 con un puerto de línea L1 y puerto cliente C1 y una tarjeta 11DPM12 instalada en el *slot* 4 con un puerto de línea L1 y un puerto cliente C1-1GbE:

    a) Configurar el puerto de línea de la 11QPEN4:

        # config interface 11qpen4 1/3/l1 ty otu2

    b) Configurar el puerto cliente de la 11QPEN4:

        # config interface 11qpen4 1/3/c1 ty tenGig

    c) Activar el servicio tanto el puerto de línea como el puerto cliente:

        # config interface 11qpen4 1/3/l1 st up

        # config interface 11qpen4 1/3/c1 st up

    d) Configurar el puerto de línea de la 11DPM12:

        # config interface 11dpm12 1/4/l1 ty otu2

        # config otu 1/4/l1 fec rsfec

    e) Configurar el puerto cliente de la 11DPM12:

        # config interface 11dpm12 1/4/c1 ty 1GbE

    f) Crear la conexión cruzada interna en la 11DPM12 para pasar el cliente C1-1GbE al puerto de línea L1:

        # config interface 11dpm12 1/4/c1 1GbE container odu0

        # config oduptf odu2 1/4/l1 odustruct odu0#1-1

        # config odukxc odu0-1/4/c1 odu2odu0-1/4/l1/1 create odu0 bi

    g) Activar el servicio del puerto cliente y el de línea para la tarjeta 11DPM12:

        # config interface 11dpm12 1/4/c1 st up

        # config interface 11dpm12 1/4/l1 st up

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

59. La clave de cifrado de sesión 11QPEN4 es una clave cifrada mediante AES-256 la cual se importa mediante un canal cifrado SNMPv3 desde el KMT. Dicha clave es utilizada por el producto y los NE para cifrar el tráfico de las comunicaciones OTU2. Para habilitar el cifrado y configurar la clave, se deben ejecutar los comandos indicados a continuación mediante un ejemplo a través de CLI local:

    a) **Configuración de la clave WKAT** (*Well Known Answer Test*). Esta clave se utiliza para comprobar el correcto funcionamiento del cifrado/descifrado entre dos extremos.

El parámetro <clave hexadecimal_32> debe ser introducido por el administrador, siendo esta una cadena de 32 caracteres en Hexadecimal.

 # config interface 11qpen4 1/3/L1 encrypt wkat <clave hexadecimal_32>

b) **Configuración de la clave de cifrado**, donde el parámetro <clave hexadecimal_64> a introducir por el administrador debe ser una cadena de 64 caracteres en Hexadecimal.

 # config interface 11qpen4 1/3/l1 encrypt nextkey <clave hexadecimal_64>

c) **Habilitar el cifrado en el puerto correspondiente,** en este caso el puerto de línea L1 (indicado en el comando de la forma <*shelf*>/<*slot*>/Puerto L{1-4}). Es importante también habilitar el cifrado en el otro extremo del enlace, donde se encontrará un NE similar al 1830 PSS.

 # config interface 11qpen4 1/3/L1 encrypt encryptstate enable

d) En caso de que se quiera modificar la clave, volver a ejecutar el comando en ambos nodos y rotarla con '*switchkey*':

 # config interface 11qpen4 1/3/l1 encrypt nextkey <clave hexadecimal_64>

 # config interface 11qpen4 1/3/L1 encrypt switchkey

60. SSH cumple con el nivel 2 de FIPS. Esto se garantiza mediante una autocomprobación de los algoritmos de cifrado (ver apartado 7.9 AUTO-CHEQUEOS). Esta conformidad con el nivel 2 de FIPS también se aplica a SFTP, que se basa en SSH. SSH y SFTP admiten diferentes subconjuntos de algoritmos ya configurados por defecto en la versión ECE 9.1. Para el uso de administración SSH o SFTP, se deben proteger los canales de comunicación tal y como se indica en el apartado 7.3.1 ADMINISTRACIÓN LOCAL Y REMOTA. En caso de no poder garantizarse dicho bastionado, se recomienda el uso de administración local.

61. Los siguientes protocolos no seguros para la administración están deshabilitados por defecto en la versión software ECE 9.1:

a) No se admite la gestión a través de TL1. Todo el acceso TL1 está bloqueado, incluido TL1 sobre SSH, TL1 15 Telnet y *"tools tl1"* (CLI).

5.5.1 INICIALIZACION DE LAS CLAVES CRIPTOGRAFICAS

62. Los armazones del 1830 PSS utilizan claves de estándar de cifrado AES-256 para cifrar el tráfico de clientes sobre la red WAN.

63. Las claves de cifrado se ponen a cero por cualquiera de las siguientes acciones, lo que resulta en una pérdida de tráfico:

a) **Deshabilitar el cifrado para un puerto de línea de la 11QPEN4.** Esta acción pone a cero la clave de cifrado del puerto. A continuación, se incluye un comando por CLI como ejemplo (11QPEN4 en slot 3, puerto L1):

 # config interface 11qpen4 1/3/L1 encrypt encryptstate disable.

b) **Desmantelamiento del sistema.** Esta acción pone a cero todas las claves de cifrado en el sistema.

c) **Restauración de datos de aprovisionamiento**. Esta acción pone a cero todas las claves de cifrado en el sistema.

d) **Desaprovisionamiento (eliminación) de la tarjeta 11QPEN4.** Esta acción pone a cero todas las claves de cifrado en la 11QPEN4.

e) **Reiniciar el sistema o la tarjeta 11QPEN4 cuando haya claves de cifrado caducadas.** Esta acción pone a cero todas las claves caducadas en el sistema o la tarjeta 11QPEN4.

64. Adicionalmente, se destaca que deshabilitar el estado administrativo de un puerto no inicializa la clave de cifrado del puerto.

65. **Puesta a cero (*zeroization*):** las claves de sesión de cifrado se pueden poner a cero extrayendo físicamente la tarjeta 11QPEN4 o reseteándola a través de CLI con este comando, utilizando privilegios de administrador:

 # config card 11QPEN4 shelf/slot reset cold

5.6 SERVIDORES DE AUTENTICACIÓN

66. Para una configuración segura del producto no se debe utilizar la autenticación a través de RADIUS. La autenticación de los usuarios debe realizarse únicamente mediante la base de datos local de usuarios del sistema.

5.7 SINCRONIZACIÓN HORARIA

67. Para la sincronización horaria se debe inicialmente establecer una fecha y hora siguiendo el procedimiento indicado en el apartado *"Procedure 1.2: Provision IP addresses and date/time"* de [REF1].

68. 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 equipos del sistema. En caso de que no se pueda garantizar el bastionado del entorno, no se recomienda el uso de servidor NTP para una configuración segura de la sincronización de tiempo.

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

a) Siendo, como ejemplo, 1 el índice del servidor, con un máximo de 3 Servidores NTP posibles, añadir el Servidor NTP:

 # config general ntp add 1 <IP del Servidor NTP>

b) Habilitar el Servidor NTP:

 # config general ntp client enable

c) Para ver los detalles del Servidor NTP configurado:

 # config general ntp detail

5.8 ACTUALIZACIONES

5.8.1 DESCARGA SEGURA DEL SOFTWARE

70. El software 1830 PSS 9.1 ECE está disponible para descarga electrónica a través del portal de formación y soporte de NOKIA (https://networks.nokia.com/support):

    a) Se debe iniciar sesión en el Portal de soporte de Nokia y seleccionar "Atención al cliente en línea (OLCS)".

    b) En el apartado "Mis productos" determine el software del producto que desea descargar (según sea el producto 1830 PSS-8 o 1830 PSS-32).

    c) En "*Product Downloads*", se debe seleccionar "*Downloads: Electronic Delivery*". Dentro del apartado "*Release 9.X*" se debe descargar, utilizando la opción "*Downloadplus*", la versión "*Release 9.1.0_ECE 3KC69624AAAA"*.

71. La página de descarga muestra el hash SHA-256 del *software* para confirmar su integridad tras la descarga.

Ilustración 3 – Página de descarga del software del producto.

72. Cuando aparezca el mensaje "*Download finished*", se debe comparar el valor del hash SHA-256 del fichero descargado con el indicado por NOKIA en La web de descarga. En caso de que no coincida, no se considera seguro utilizar dicho *software* y se deberá repetir el procedimiento de descarga segura. Si el mensaje no aparece, se debe contactar con el soporte técnico de NOKIA (http://www.nokia.com/en_int/contact-us).

5.8.2 ACTUALIZACION DEL SOFTWARE DEL PRODUCTO

73. Las actualizaciones de *software* se realizan de forma segura (de forma manual por un usuario administrador) a través de un servidor SFTP que contenga la versión *software* descargada del apartado anterior.

74. Para proceder con la instalación, se debe acceder como usuario administrador al interfaz CLI del producto y seguir los pasos indicados en la sección *"Upgrade to 1830PSSECE-9.1-0 software (CLI)"* en el apartado *"3 Software Upgrades"* de la documentación oficial [REF6]. Se debe consultar el apartado en su totalidad para más detalle sobre el proceso de actualización.

5.9 AUTO-CHEQUEOS

75. El producto realiza los siguientes auto-chequeos durante su fase de arranque:

    a) Integridad de archivo (*File integrity check):* utiliza firma hash SHA256 incluida con el *software*.

    b) AES256/HMAC KAT: chequeo para cifrado SNMP AES256/HMAC

    c) Algoritmo SSH KAT: chequeo de los algoritmos de cifrado SSH.

    d) AES FPGA KAT (11QPEN4): chequeo de cifrado AES-256 CTR/ECB en la tarjeta 11QPEN4.

76. El 1830PSS realiza auto-chequeos continuos de integridad del Software y de operación de funciones criptográficas, para ello es capaz de detectar posibles fallos indicando al usuario determinadas alarmas al respecto.

77. Se debe habilitar habilitar el modo '*fips-squelching*'. Este modo establece una política de seguridad que, en caso de detección de fallo en los auto-chequeos periódicos de criptografía (*FIPS selftests*), paralizará el envío de tráfico cifrado.

    # config general fips-squelching enable

78. El sistema es capaz de detectar y notificar estos problemas mediante alarmas, ya tengan su origen en la integridad *software:*

    a) FIPS Software version mismatch

79. O ya sea mediante alarmas relacionadas directamente con las funciones criptográficas:

    a) AES FIPS Failure

    b) FIPS Selftest Squelch

    c) Card failure - crypto

    d) Current Key Mismatch

    e) Next Key Mismatch

80. El documento oficial de Nokia [REF5] cuenta con un listado y detalle de las alarmas mencionadas, así como de todas las alarmas posibles que puede notificar el sistema, en su apartado "*2 Alarm and Condition Details*". También se incluyen los procedimientos

correspondientes a cada alarma para solucionar los fallos causantes, que se pueden consultar en el apartado *"3 Trouble- clearing procedures".*

5.10 SNMP

81. El sistema 1830 PSS es configurable como servidor y cliente SNMP. El producto implementa SNMPv3 con cifrado AES-256 y autenticación HMAC-SHA1.
82. Para la configuración segura, se recomienda el uso de autenticación HMAC-SHA256. Se considera inseguro en cualquier caso el uso de MD5.
83. Para agregar un usuario, se deben usar el siguiente comando:

    # config admin snmpusers add <usuario> *admin aes256sha1*
84. Se deben modificar las credenciales de usuario mediante los comandos:

    # config admin snmpusers edit <usuario> *authpasswd*

    # config admin snmpusers edit <usuario> *privpasswd*
85. Para deshabilitar los suarios por defecto, se deben introducir los siguientes comandos:

    # config admin snmpusers edit v3DefaultUser status disable

    # config admin snmpusers edit v3DftAdvUser status disable
86. Consultar los puntos 8, 9 y 10 del apartado *"Procedure 1.4: Provision user roles"* de [REF1] para la configuración de los usuarios de administración SNMP (Administrador y Oficial de Criptografía). Para más información sobre los comandos utilizados, consultar *"config admin snmpusers"* en la documentación [REF2].
87. El servidor SNMP del Nokia 1830 **PSS deberá configurarse para el envío de logs a un servidor externo de almacenamiento**. Para la configuración de esta comunicación, se debe consultar el apartado 7.12.3 ALMACENAMIENTO REMOTO de este documento.
88. El uso de **administración remota mediante SNMPv3 no se considera dentro de la configuración segura y no se recomienda su uso** salvo que se utilicen medidas adicionales de bastionado del canal de operación, tal y como se indica en el apartado 5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA.
89. Para más información sobre el protocolo SNMP en el producto, consultar el apartado *"SNMP interface"* de [REF1].

5.11 ALTA DISPONIBILIDAD

90. Los modelos 1830 PSS-8 y 1830 PSS-32 contienen una controladora activa y, opcionalmente, la capacidad de añadir una segunda controladora en *standby* para proporcionar redundancia.
91. Para verificar el estado de sincronización de la base de datos del NE y el estado de las dos controladoras (activa y *standby*):

    # show redundancy

92. Se puede realizar una conmutación de controladoras mediante el comando:

    # config redundancy switch ec <identificador_controlador>

93. Se deben consultar los apartados "1830 PSS-8 Equipment Controller (8EC2E)" y "1830 PSS-32 high-performance Equipment Controller (32EC2E)" de [REF1] para más información sobre la configuración de controladoras de redundancia.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

94. El dispositivo registra diferentes tipos de eventos. Los principales son:

    a) **Registros generales (General Log):** registro de eventos de naturaleza general, tales como los referentes a la administración de tarjetas y demás componentes, eventos de canales DWDM o los distintos servicios del producto.

    b) **Registros de seguridad (Security Log):** registro de eventos de seguridad, tales como cambios de cifrado y criptografía, alarmas, SNMP, intrusión o intentos de acceso a la administración.

    c) **Registros de acciones de usuario**: registro de eventos realizados por usuarios administradores, tales como cambios en políticas de contraseñas, cambio de credenciales, sesiones de administración o cambios de configuración.

5.12.2 ALMACENAMIENTO LOCAL

95. Los registros de auditoría se almacenan permanentemente en las controladoras de los equipos 1830 PSS. Los eventos de seguridad auditables se registran en:

    a) SNMP log

    b) Security event log

    c) User Activities Log (UAL)

96. Se puede acceder a los registros de seguridad registrándose como usuario administrador y ejecutando el siguiente comando:

    # show logs all

```
NODE1# show logs all

8221       2021/09/03 09:24:03  Security                                    11.11.15.3
Type      : Log View
Desc      : View security log
Condition : CONTCOM
Changed   :
Data      : admin #97

8220       2021/09/03 09:23:59  Security                                    10.150.24.34
Type      : Login
Desc      : Login
Condition : CONTCOM
Changed   :
Data      : admin #97 CLI SSH

8219       2021/09/03 09:23:58  Security                                    11.11.15.3
Type      : Exceeded Login
Desc      : Excessive invalid login attempts
Condition : INTRUSIONEVT
Changed   :
Data      : admin CLI SSH
```

Ilustración 4 – Ejemplo de formato de los registros del sistema.

97. Los registros de auditoría usan el mecanismo *round-robin*: sobreescribe los registros más antiguos por los nuevos que se van almacenando una vez se ha llenado el espacio de almacenamiento. Cada uno de los log indicados previamente se maneja independientemente, y permite almacenar hasta 500 registros. Se puede comprobar el nivel de almacenamiento con el comando:

    # show logs summary

```
NODE1# show logs summary

Log History Summary
Total           :   1881

Critical Alarms:    169
Major Alarms    :     68
Minor Alarms    :     43
Not Alarmed     :     69
Warning Alarms  :      0

Not Reported    :    344
General Events  :    500
State Changes   :     23
User Actions    :    210

Security        :    455
```

Ilustración 5 – Ejemplo de llenado de los registros generales.

98. Se puede observar en el ejemplo mostrado que los registros generales están llenos, se podrá acceder al registro de los logs generales de la siguiente forma:

    # show logs general

99. A partir de este número, se podrá observar cómo se van reemplazando los registros de mayor antigüedad. Se puede consultar el apartado "*show logs*" de [REF2] para más información de los comandos utilizados y las opciones de visualización de los logs registrados.

5.12.3 ALMACENAMIENTO REMOTO

100. Los registros de auditoría se deben enviar a un servidor remoto mediante SNMPv3. En este caso existen dos ficheros de ´log´ que se pueden transferir:

a) **SNMP log:** se registran todas las acciones que se han realizado en los NEs a través de comandos SNMPv3.

b) **UAL log:** se registran todos los accesos y actividades de los usuarios a los equipos

101. Para la transferencia de registros al servidor externo se deben seguir los siguientes pasos:

a) Acceder al dispositivo como usuario administrador y configurar el servidor SNMv3 mediante el siguiente comando:

 # config snmpserver trapdest add <Destino_ID> <Destino IP [: puerto]> <*timeout*> <Reintentos> <Versión SNMP> <NMS ID> <Usuario SNMP>

b) Donde se deben indicar los siguientes parámetros:

i. <Destino_ID>: Identificador del servidor SNMP remoto, máximo 32 caracteres

ii. <Destino IP [: puerto]>: dirección IP del servidor SNMP, seguido del puerto (162 por defecto).

iii. <*timeout*>: tiempo en el que termina la conexión si no se recibe respuesta, valores de 1 a 2147483647 (en centésimas de segundo).

iv. <Reintentos>: número de intentos que se realizaran para realizar la conexión una vez agotado el *timeout* (entre 0 y 255)

v. <versión SNMP>: Versión SNMP. Deberá elegirse la v3.

vi. <NMS ID>: Identificador del equipo para el envío del destino de las SNMP traps (0 para servidores de terceros).

vii. <Usuario SNMP>: usuario SNMPv3 que se conectará al servidor.

c) Se puede comprobar la configuración de los servidores SNMP configurados en el equipo:

 # config snmpserver trapdest brief

102. Para más información sobre los pasos de configuración del servidor SNMP, se puede consultar el apartado "*config snmpserver*" de [REF2].

103. Consultar los apartados *"auditing"* y *"start and stopping auditing"* de [REF1] para más información sobre auditoría y registros.

5.13 COPIAS DE SEGURIDAD

104. Para realizar una copia de seguridad o *backup* de la base de datos del sistema, la cual incluye todos los datos y configuraciones del dispositivo, se debe consultar el apartado "*Backup database (CLI)*" de la documentación oficial de referencia [REF6]. Para la realización y almacenamiento de las copias de seguridad se utiliza el protocolo SFTP.

6. FASE DE OPERACIÓN

105. Durante la fase de operación y mantenimiento del producto se deberán de llevar a cabo los siguientes procedimientos operativos:

a) Comprobaciones periódicas de la existencia de alarmas en el sistema y establecer protocolos de resolución de incidentes.

b) Comprobaciones periódicas del correcto almacenamiento de los registros de auditoría, tanto local como los transferidos al servidor externo de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.

c) Comprobar periódicamente el estado de las etiquetas de evidencia de manipulación en los equipos 1830 PSS-8 y/o 1830 PSS-32. Se recomienda llevar un registro del cambio de etiquetado mediante un *logbook* tal y como se muestra en el apartado "*Logbook*" de [REF1].

d) Realizar copias de seguridad periódicas. Asegurar su almacenamiento en un lugar seguro y planificar procesos de automatización.

e) Planificar y aplicar parches de seguridad y/o realizar actualizaciones requeridas en el producto en caso de ser necesarias por motivos de seguridad.

7. CHECKLIST

106. Incluir un *checklist* que contenga todas las recomendaciones sobre la configuración de cada apartado. Como ejemplo:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto.	☐	☐	
Instalación física del producto en un entorno seguro.	☐	☐	
Comprobación del etiquetado seguro.	☐	☐	
Instalación de los equipos de administración.	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURA			
Configuración de las políticas de credenciales.	☐	☐	
Configuración y bastionado de red de administración remota (en caso de su uso)	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración de los usuarios administradores.	☐	☐	
Configuración de las interfaces.	☐	☐	
Configuración de claves y protocolos seguros.	☐	☐	
Configuración de la sincronización horaria.	☐	☐	
Configurar usuarios y servidor SNMP.	☐	☐	
Configuración de auditoría local y envío a servidor externo.	☐	☐	
Configuración de redundancia (opcional).	☐	☐	
Realización de copias de seguridad.	☐	☐	

8. REFERENCIAS

107. Todos los documentos oficiales referenciados en el documento requieren de registro como usuario en la web oficial de NOKIA, para lo cual se debe haber contratado un servicio u adquirido alguno de sus productos.

108. En la tabla se muestran los diferentes documentos de referencia mencionados en alguno de los puntos del documento.

REF1 *1830 Photonic Service Switch (PSS) Release 9.1.0 Common Criteria User Guide*

REF2 *1830 Photonic Service Switch (PSS) Release 9.1 Command Line Interface Guide*

REF3 *1830 Photonic Service Switch 8 (PSS-8) Release 9.1 Installation and System Turn-up Guide*

REF4 *1830 Photonic Service Switch 16/32 (1830 PSS-16/PSS-3232) Release 9.1 Installation and System Turn-up Guide*

REF5 *1830 Photonic Service Switch (PSS) Release 9.1 Maintenance and Trouble-Clearing Guide*

REF6 *1830 Photonic Service Switch 8/32 (PSS-8/PSS-32) Release 9.1.0 ECE Customer Release Notes*

9. ABREVIATURAS

DDR	Double Data Rate
DWDM	Dense Wavelength Division Multiplexing
NMS	Network Management System
OTDR	Optical Time Domain Reflectometer
OTU	Optical Transport Unit
SMS	Security Management System
TL1	Transaction Language 1

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL