centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1306

Procedimiento de Empleo Seguro
N2OS

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-127-0

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:24:21 +02'00'

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 producto Network Appliance Platform, modelo NS1, con sistema operativo N2OS (Nozomi Networks Operating System), es una solución IDS distribuida en modo appliance que permite detectar amenazas dentro de una red en tiempo real.
2. El producto cuenta con un software propio (N2OS) que permite la gestión y administración del TOE. Su función principal es analizar el tráfico de red en tiempo real e identificar cualquier irregularidad. Para ello, profundiza en los paquetes utilizando su conocimiento de los protocolos.
3. Dicho análisis de red puede realizarse sobre redes que usan protocolos comunes, así como en redes OT que utilicen el protocolo SCADA.
4. Para la instalación, configuración y operación del producto, esté dispone de una consola que permite realizar las operaciones necesarias y que serán descritas a lo largo de este manual. El usuario podrá interactuar con dicha consola de las siguientes maneras:
    - De manera local, a través de la conexión de un cable serie al sensor.
    - De manera remota, a través de los siguientes canales de comunicación:
        - Una terminal de comandos vía SSHv2.
        - Una interfaz gráfica a través de una consola web vía HTTPS.
5. La arquitectura del producto se presenta a continuación, quedando resaltado en rojo el propio producto con los canales de comunicación posibles.

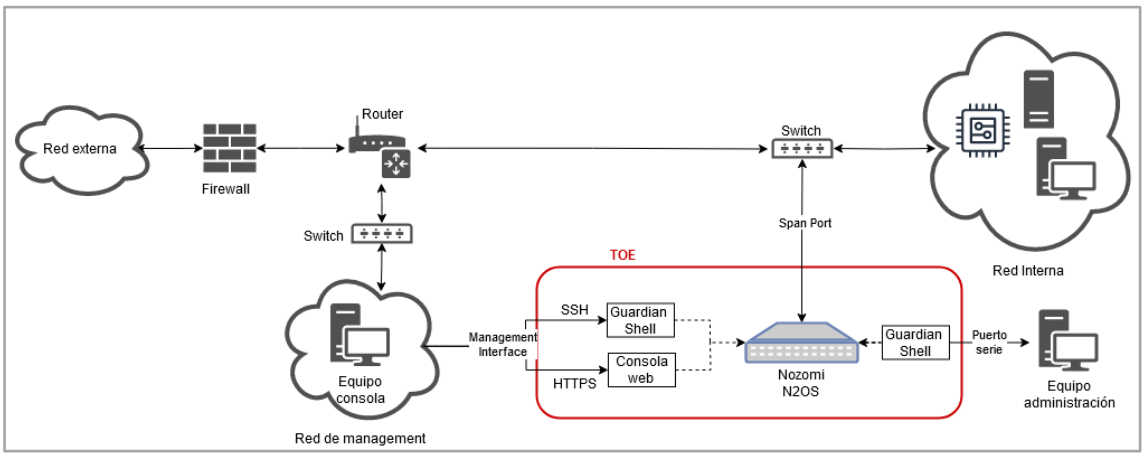

Ilustración 1: Arquitectura del TOE

2 OBJETO Y ALCANCE

6. El objetivo de este documento es servir como guía de configuración y empleo seguro del producto N2OS de Nozomi Networks, en su versión 24.2.0.

7. El despliegue de este producto viene proporcionado por su sensor físico NS1 que cuenta con las siguientes especificaciones técnicas:

TITULOS	TITULOS
Máximo rendimiento	500 Mbps
Máximos colectores remotos	20
Puertos de monitorización	7x 1000BASE-T
Puertos de gestión	1x 1000BASE-T
Ranuras de expansión	1 ranura disponible: 4x 1000Base-T ó 4x SFP
Almacenamiento	128GB para OS y datos
Formato	1 unidad de *rack*
Máximo consumo de energía	220W
Fuente de alimentación	Sencillo 100-240V AC
Rango de temperatura en funcionamiento (ºC)	0 - 40
Dimensiones (Alto x Ancho x Largo) (mm)	44 x 438 x 321
Peso (kg)	8.8
Certificaciones	CE, FCC, UL, CB

Tabla 1: Especificaciones técnicas dispositivo NS1

8. Adicionalmente, el dispositivo permite dos licencias distintas, en función del tamaño de la red que quiera monitorizarse, pero no influye en la funcionalidad ofrecida.

9. Respecto al equipo usado para la conexión y gestión de la consola, se puede utilizar cualquier versión de las distribuciones de Windows, Linux o MacOS. En caso de que se quiera acceder a la interfaz web de la consola, será necesario alguno de los siguientes navegadores en sus últimas versiones:

    - Google Chrome.
    - Chromium.
    - Safari (para macOS).
    - Firefox.
    - Microsoft Edge.

10. Por último, destacar que Nozomi Networks proporciona varias guías que recogen gran cantidad de información relativa a la fase operacional y de configuración del producto, y que van a ser referenciadas a lo largo de este procedimiento para los detalles.

    - N2OS Configuration-Reference Guide (v24.2.0) [Configuration].
    - N2OS-Software Development Kit (v24.2.0) [Development].
    - Guardian-User Guide (v24.2.0) [UserGuide].

- Guardian-Installation Guide (v24.2.0) [InstallationGuide].
- Guardian-Administrator Guide (v24.2.0) [AdminGuide].
- Guardian and Central Management Console-Maintenance Guide (v24.2.0) [Maintenance].

11. El producto N2OS en su versión 24.2.0 ha sido cualificado en el catálogo CPSTIC para categoría MEDIA en la familia “IDS, IPS y AntiDDoS”.

3 ORGANIZACIÓN DEL DOCUMENTO

12. Este documento se compone de los siguientes apartados:

a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

13. El producto se entrega en un paquete con remitente Nozomi Networks, que contiene la siguiente información:
    - MODEL NO.: Hace referencia al modelo del dispositivo físico.
    - S/N FROM: Número de serie del dispositivo.
    - SW Version: Versión del software instalada en el dispositivo.
14. Dentro de este paquete se encuentra: el dispositivo, cable de alimentación con clavija tipo A, cable de alimentación con clavija tipo C, cable ethernet y cable de consola a USB.
15. Al recibir el paquete, se debe comprobar que:
    - El paquete se encuentra debidamente precintado y no muestra indicios de haber sido alterado.
    - El modelo recibido es NS1.
    - El número de serie del producto recibido corresponde con el indicado en el albarán de compra.
    - La versión del software es la 24.2.0 o que se pueda posteriormente actualizar a la misma.
16. Es posible descargar la documentación del producto ([InstallationGuide], [AdminGuide], [Maintenance], [UserGuide], [Configuration], [Development]) desde la página “Product Releases” de [Support].

4.2 ENTORNO DE INSTALACIÓN SEGURO

17. Es recomendable que el producto sea instalado en un *rack,* ubicado en un espacio seguro que sea accesible únicamente por personal autorizado.

4.3 REGISTRO Y LICENCIAS

18. Una vez comprado el producto, se recibirá un correo electrónico que incluirá un código de activación de N2OS. Para obtener la clave de licencia, es necesario introducir dicho código en el portal de licencias de Nozomi Networks [Licenses].
19. Para el registro de la licencia dentro del sensor, consultar el punto 6.2.1 de este mismo documento, tras haber realizado la configuración inicial (puntos 6.1 y 6.2 respectivamente).

4.4 CONSIDERACIONES PREVIAS

20. El producto ha de instalarse teniendo en cuenta las siguientes consideraciones:
    - No usar equipamiento dañado, incluyendo cables dañados o deteriorados.
    - No usar el sensor sin las cubiertas.
    - Instalar el sensor en un área bien ventilada limpia y libre de polvo. Evitar zonas que generen calor, ruido eléctrico y campos electromagnéticos. Proteger el sensor de

zonas húmedas. Proteger el sensor de la intrusión de líquidos. En caso de que el sensor se moje, desconectarlo inmediatamente.

- Utilizar un Sistema de Alimentación Ininterrumpida (SAI). Este mantiene el sensor activo en caso de corte de corriente y lo protege de subidas y picos de tensión.
- Mantener toma de tierra fiable todo el tiempo. Conectar el *rack* en el que se encuentre el sensor y el chasis del sensor a tierra a través del cable de conexión a tierra del sensor.
- Montar el sensor en un *rack* o en una zona con suficiente flujo de aire.
- Evitar cargas mecánicas desiguales en el *rack* en el que se encuentre el sensor.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

21. Para la operación de la consola del sensor, se necesitará lo siguiente:

    - Equipo con sistema operativo Windows, Linux o macOS que contenga emuladores de terminal capaces de comunicarse por una línea serie.
    - Para acceder a la interfaz web de la consola, se ha de contar con alguno de los siguientes navegadores en sus últimas versiones: Google Chrome, Chromium, Safari (para macOS), Firefox o Microsoft Edge.

5 FASE DE INSTALACIÓN

22. El sensor se debe conectar al equipo que servirá como controlador de la consola mediante su cable de consola correspondiente.
23. Una vez conectado, se debe abrir en el equipo un emulador de consola y ajustaremos la velocidad a 9600 baudios sin ningún bit de paridad.
24. Se conectará a través de SSH utilizando la siguiente configuración para el sensor físico:
    - Dirección IP: 192.168.1.254
    - Máscara de red: 255.255.255.0
    - Puerta de acceso: 192.168.1.1
25. Finalmente, el sensor mostrará un formulario de login.
26. Para continuar con la configuración, consultar la siguiente sección.

6 FASE DE CONFIGURACIÓN

6.1 CONFIGURACIÓN INICIAL FASE 1 (CONFIGURACIÓN BÁSICA)

27. A continuación, se describe el proceso que se ha de seguir para aplicar la configuración mediante el uso de la consola del sensor:

    a) Introducir las siguientes credenciales en el formulario de login que aparece en la consola:

        b) Usuario: admin

        c) Contraseña: nozominetworks

    d) Introducir el comando **enable-me** para elevar privilegios al usuario **admin**.

    e) Introducir el comando **setup** para iniciar el asistente de configuración inicial.

    f) Cambiar la contraseña de ***admin*** a una que cumpla con los siguientes requisitos mínimos, establecidos por la guía [CCN-STIC-807]:

        i. Longitud mínima de 12 caracteres.

        ii. Mínimo tres tipos de los siguientes: mayúsculas, minúsculas, números y caracteres especiales.

        iii. No usar patrones comunes de caracteres.

        iv. El uso de mayúsculas al inicio y números al final de la contraseña no cuenta para el cumplimiento de los requisitos.

        v. Entre caracteres del mismo tipo, debe haber suficiente diferencia entre ellos. Por ejemplo, no usar "a" seguido de "b".

    g) Acceder y configurar la IP del sensor correspondiente a la interfaz de *management*. Para ello, acceder a la ventana **Network Interfaces** del menú mostrado.

    h) Seleccionar la interfaz de *management*, identificada como **em0** o **mgmt**.

    i) Elegir la dirección IP deseada para el sensor dentro de la interfaz de *management*.

    j) Seleccionar ***Default Router/Gateway*** para asignar automáticamente la dirección del router.

    k) Seleccionar ***DNS Nameserver*** para configurar las direcciones DNS deseadas.

    l) Guardar y salir.

    NOTA: Si se desea información más detallada, consultar la sección *"Do the basic configuration"* del manual [InstallationGuide].

6.2 CONFIGURACIÓN INICIAL FASE 2 (CONFIGURACIÓN INTERFAZ WEB)

28. En este punto se muestra el proceso de configuración de la interfaz web de la consola:

    a) En primer lugar, se accede a la consola web introduciendo la siguiente información: **https://<IP_sensor>**, donde IP_sensor es la IP asignada en la interfaz de *management*.

b) En la ventana de login, se introducen las credenciales establecidas en el apartado 27.f) de este documento. Tras el inicio de sesión será necesario restablecer la contraseña por motivos de seguridad, siguiendo los requisitos descritos en el apartado anterior.

c) Acceder a **"⚙ > General"** y cambiar el nombre del host.

d) Acceder a **"⚙ > System > Date and time"** y seleccionar la franja horaria correspondiente.

29. **NOTA:** Si se desea información más detallada, consultar sección *"Do the web console configuration"* del manual [InstallationGuide].

6.2.1 AÑADIR NUEVA LICENCIA

30. A continuación, se muestra el proceso a seguir para configurar una nueva licencia:

a) Dentro de la interfaz web, acceder a **"⚙ > Updates & Licenses".**

b) Introducir una clave de licencia válida, compuesta por el ID de la máquina en conjunto con el código de activación de Nozomi Networks.

c) Para más información, consultar sección *"Install a License"* del [InstallationGuide] y sección *"Updates and licenses"* del [InstallationGuide].

6.2.2 INSTALACIÓN DE CERTIFICADOS SSL (HTTPS)

31. Este punto describe el proceso necesario para la configuración e importación de un certificado SSL para la autenticación del sensor mediante HTTPS, aunque durante la instalación inicial, el sensor genera un certificado auto firmado con validez de 1 año, el cual debe ser cambiado por un **certificado digital emitido por una CA y que cumpla los requisitos marcados por la guía [CCN-STIC-807].**

32. El procedimiento para la instalación del certificado digital es el siguiente:

a) Cargar el certificado digital y los archivos de clave en el sensor mediante el cliente SSH, almacenando estos en el directorio **/data/tmp**. Para esto, se puede utilizar el siguiente comando:

NOTA: Se toman como ejemplo los siguientes nombres de archivo: https_certificado.crt y https_clave.key.

```
scp <https_*> admin@<IP_sensor>:/data/tmp
```

b) Iniciar sesión en la consola, ya sea directamente o a través de SSH. A continuación, usar el siguiente comando para elevar privilegios de usuario:

```
enable-me
```

c) **En caso de que el certificado esté protegido por contraseña,** usar el siguiente comando para desprotegerlo para evitar que esta se solicite después de cada reinicio del servidor:

```
openssl rsa -in <https_clave.key> -out <https_clave_nopass.key>
```

```
mv <https_clave_nopass.key> <https_clave.key>
```

d) Ejecutar el siguiente comando para activar el certificado.

NOTA: Si se ha desprotegido el certificado, usar ese archivo en el segundo parámetro del comando, quedando así:

```
n2os-addtlscert <https_certificado.crt> <https_clave_nopass.key>
```

e) Reiniciar el servidor web para que se apliquen los cambios con el siguiente comando:

```
service nginx stop
```

f) Comprobar si los cambios han sido efectuados accediendo desde el navegador a la dirección **https://<IP_sensor>/** verificando si el certificado es reconocido como válido.

NOTA: En caso de que detecte que la CA emisora de certificados no es confiable, consultar sección 6.8.1 INSTALACIÓN DE CERTIFICADOS DE CA.

6.3 ACTUALIZACIÓN DE LA VERSIÓN DEL DISPOSITIVO

33. El primer paso que ha de realizarse tras la configuración inicial es actualizar el software del dispositivo a la versión 24.2.0 si este no trae dicha versión. Para ello, se hará lo siguiente:

- Acceder al Portal de Soporte de Nozomi Networks e iniciar sesión.
- Dentro de la ventana "Product Releases", seleccionar la versión indicada.
- Una vez dentro, seleccionaremos la descarga "*Update Package with Smart Polling addon*".
- Comprobar que el hash SHA256 del archivo descargado se corresponde con el hash publicado junto con el archivo en el Portal de Soporte.
- Una vez tengamos el archivo *"VERSION-update.bundle"*, consultar sección *"Do a software update from the web UI"* del manual [Maintenance].

6.4 MODO DE OPERACIÓN SEGURO

34. Para cumplir con los requisitos establecidos por [CCN-STIC-807] y, por lo tanto, operar el TOE de acuerdo con la certificación *LINCE*, se debe aplicar la configuración descrita en las siguientes subsecciones.

6.4.1 CONFIGURACIÓN PERFIL CCN PARA SSHV2

35. Con el objetivo de proteger las comunicaciones a través del protocolo SSHv2, según lo establecido en la guía [CCN-STIC-807], es necesario aplicar el perfil CCN para las comunicaciones SSH del producto. Para ello:

a) Conectarse a la consola del producto (SSH o por cable serie).

b) Introducir el siguiente comando para elevar privilegios de la sesión:

```
enable-me
```

c) Introducir el siguiente comando para cambiar el perfil de SSH:

```
sysrc n2osssh_profile=ccn
```

d) Guardar los cambios realizados:

```
n2os-save
```

e) Reiniciar el servicio para aplicar los cambios:

```
shutdown -r now
```

6.4.2 CONFIGURACIÓN HASH PBKDF2-SHA512

36. El TOE ofrece la posibilidad de usar el algoritmo PBKDF2-SHA512 para el cálculo de hashes de las contraseñas locales. Dicha opción ha de activarse para cumplir con los requisitos criptográficos establecidos por la guía [CCN-STIC-807]. El proceso para la activación de este es el siguiente:

    a) Acceder a la ventana **"⚙ > Settings > CLI"** desde la interfaz web.

    b) Introducir el siguiente comando:

```
conf.user configure password_policy hashing_pbkdf2 true
```

6.4.3 CONFIGURACIÓN DE REGLAS ADICIONALES

37. De forma adicional a la funcionalidad por defecto, es necesario añadir reglas de detección adicionales. Para ello, se acecde a "⚙ **> Threat Intellingence > Packet rules**" y se crean las siguientes reglas, haciendo click en "+ Add":

38. Nombre: `TCP SYN RST`

39. Contenido:

```
alert tcp any any -> any any (sid:1633668; msg:"Invalid SYN/RST Packet";
tcp.flag.syn:1; tcp.flag.rst:1;)
```

40. Nombre: `ICMP Fragment`

41. Contenido:

```
alert icmp any any -> any any (sid: 1633669; msg:"ICMP fragment";
fragbits=1;)
```

6.5 AUTENTICACIÓN

42. El sensor solicita la autenticación de los usuarios como paso previo a realizar cualquier otra acción. Todas las interfaces (interfaz web, conexión por puerto serie y SSH) permiten autenticación mediante usuario y contraseña. Además, en el caso de SSH también se permite autenticación mediante clave pública. Dichas credenciales se almacenan de manera local en el propio sensor.

43. Para la creación y gestión de usuarios/grupos, y gestión de políticas de contraseñas, ver apartados 6.6.2 CONFIGURACIÓN DE ADMINISTRADORES y 6.6.3 POLÍTICA DE CONTRASEÑAS, respectivamente.

6.6 ADMINISTRACIÓN DEL PRODUCTO

6.6.1 ADMINISTRACIÓN LOCAL Y REMOTA

44. El producto permite su administración de manera local y remota.
45. La **administración local** se realiza mediante la conexión con el sensor Guardian a través de un cable serie.
46. La **administración remota**, que se realiza a través de un cable ethernet y el puerto *management*, se puede realizar de las siguientes maneras:
    - A través de un terminal mediante una conexión SSHv2. Para la configuración relativa a la seguridad del protocolo SSHv2, consultar apartado 6.4.1 CONFIGURACIÓN PERFIL CCN PARA SSHV2.
    - A través de una interfaz web mediante una conexión HTTPS con TLS v1.2 o superior. Esta será accesible desde https://<IP_del_sensor>/. La debida configuración de este protocolo, en concreto, el uso de certificados SSL, se encuentra descrita anteriormente en el apartado 6.2.2 INSTALACIÓN DE CERTIFICADOS SSL (HTTPS).

6.6.2 CONFIGURACIÓN DE ADMINISTRADORES

47. El TOE por defecto cuenta con dos grupos de usuarios, con distintas políticas:
    - **Administradores**: Cuenta con acceso a todas las funcionalidades. En este grupo se encuentra el usuario *"admin"*, usado durante la instalación.
    - ***Authentication Only***: Únicamente puede autenticarse en la consola, sin poder alterar configuraciones de esta.
48. Adicionalmente, se pueden crear nuevos usuarios. Para ello, desde la interfaz web, se accederá a **" ⚙ > Settings > Users > +Add"**.
49. De igual manera, desde la interfaz web, se pueden crear nuevos grupos, pudiendo personalizar las políticas asociadas a cada uno de ellos, de la siguiente manera: **" ⚙ > Settings > Users > Groups"**.
50. Para obtener información más detallada acerca de la gestión de usuarios y grupos, consultar sección *"Users management"* del manual [AdminGuide].

6.6.3 POLÍTICA DE CONTRASEÑAS

51. Dentro de la interfaz web, acceder a la ventana **" ⚙ > Settings > CLI"**. Esto otorgará acceso mediante una CLI (*Command Line Interface*).
52. Aplicar los siguientes comandos:
    a) Mínimo 1 número requeridos:

```
conf.user configure password_policy digit 1
```

    b) Mínimo 1 minúscula requerida:

```
conf.user configure password_policy lower 1
```

    c) Mínimo 1 mayúscula requerida:

```
conf.user configure password_policy upper 1
```

d) Mínimo 1 carácter especial requerido:

```
conf.user configure password_policy symbol 1
```

e) Prohibición de reutilizar 10 contraseñas anteriores:

```
conf.user configure password_policy history 10
```

f) Activar expiración de contraseñas:

```
conf.user configure password_policy password_expire_enable true
```

53. Con esto ya se cumplirían los siguientes requisitos mínimos de composición de contraseñas, impuestos por la guía [CCN-STIC-807] para nivel MEDIO de ENS:

- Longitud mínima de 12 caracteres.
- Mínimo 3 tipos de caracteres diferentes.
- Periodo de renovación máximo de 2 años (por defecto el producto establece 90 días).
- Máximo 5 intentos de autenticación fallidos (por defecto el producto establece 3).
- Prohibición de reutilizar 10 contraseñas anteriores.

6.6.4 BANNER DE ACCESO

54. Es necesario configurar el mensaje de aviso previo a la autenticación en el producto. Para ello:

a) Acceder a la interfaz web. Una vez ahí, navegar hasta la ventana **“ > System > General”.** Se mostrará lo siguiente:

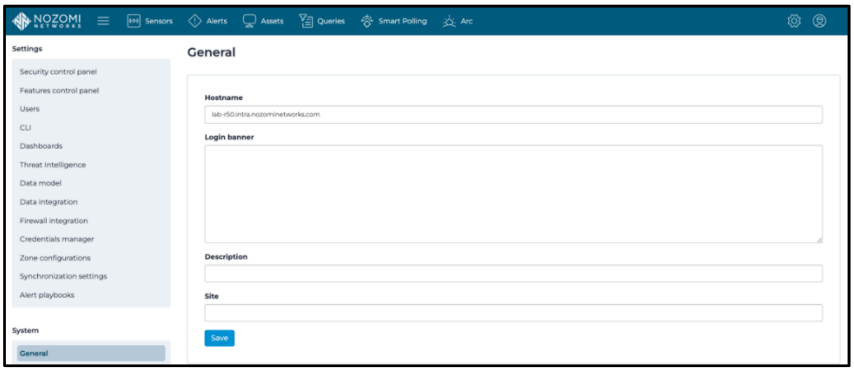

Ilustración 2: Banner

b) Introducir el mensaje que se desea mostrar.

6.7 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

55. Este producto solo permite su gestión y administración desde la interfaz de management. Esta ya se configuró durante la instalación inicial (consultar sección 6.1 CONFIGURACIÓN INICIAL FASE 1 (CONFIGURACIÓN BÁSICA)).

6.8 GESTIÓN DE CERTIFICADOS

56. El TOE permite la importación de un certificado para el servidor de N2OS. Consultar el punto 6.2.2 INSTALACIÓN DE CERTIFICADOS SSL (HTTPS) de este mismo documento para visualizar este proceso de importación. Se debe tener en cuenta que los certificados digitales empleados deben cumplir los requisitos marcados por la guía [CCN-STIC-807].

6.8.1 INSTALACIÓN DE CERTIFICADOS DE CA

57. En esta sección se describe el proceso a realizar para la instalación de certificados de CA. Este proceso se ha de realizar cuando la CA que emite el certificado no es reconocida como de confianza.

    NOTA: Si los certificados de la CA intermedia y CA raíz están en archivos separados, se han de combinar de la siguiente manera:

```
cat <cert_CA_inter> <cer_CA_raiz> > cert.crt
```

    NOTA: El certificado debe estar en formato PEM (*Privacy Enhanced Mail*). No se admiten formatos DER (*Distinguished Encoding Rules*) o PKCS#12.

58. Para instalar certificados de CA, se han de seguir las siguientes instrucciones:

    a) Subir el certificado de CA al sensor al directorio **/data/tmp** usando el cliente SSH:

```
scp cert.crt admin@<IP_sensor>:/data/tmp
```

    b) Acceder a la consola (directamente o a través de SSH). Una vez conectados, elevar privilegios de usuario usando el siguiente comando:

```
enable-me
```

Usar el siguiente comando para añadir el certificado de CA al almacén de certificados:`n2os-addcacert cert.crt`

6.9 CREACIÓN DE LISTAS NEGRAS DE DIRECCIONES IP

59. Para crear una lista negra, o una lista de direcciones IP sospechosas, en primer lugar se debe crear un script Python con el siguiente contenido:

```
text="""
{
    "type": "bundle",
    "id": "bundle--e957e77f-e463-43a9-9fc1-a0afa3065044",
    "objects": [
        {
            "type": "identity",
            "spec_version": "2.1",
            "id": "identity--7247edc2-e889-4624-9b89-ef90f9202d06",
            "created": "2023-02-03T10:13:15.932645Z",
            "modified": "2023-02-03T10:13:15.932645Z",
            "name": "LEV",
            "identity_class": "organization"
        },
        {
            "type": "marking-definition",
            "spec_version": "2.1",
```

```
            "id":         "marking-definition--f88d31f6-486f-44da-b317-
01333bde0b81",
            "created": "2017-01-20T00:00:00.000Z",
            "definition_type": "tlp",
            "name": "TLP:AMBER",
            "definition": {
                "tlp": "amber"
            }
        },
        {
            "type": "threat-actor",
            "spec_version": "2.1",
            "id": "malware--6b28f795-a98b-43f9-b272-13a2aa7b30b0",
            "created": "2020-02-10T16:02:08.654857Z",
            "modified": "2020-02-10T16:02:08.654857Z",
            "name": "Blacklist",
          "description":"Fake malware used for testing",
            "is_family": false
        },
        {
            "type": "relationship",
            "spec_version": "2.1",
            "id": "relationship--6cd290fe-6398-404f-8a21-f72643926bc4",
            "created": "2020-02-10T16:02:08.654857Z",
            "modified": "2020-02-10T16:02:08.654857Z",
            "relationship_type": "indicates",
            "source_ref":          "indicator--921d65de-13fb-4f42-a242-
75e5d1a5dbae",
            "target_ref":            "malware--6b28f795-a98b-43f9-b272-
13a2aa7b30b0"
        }
"""
indicator="""
,{{
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--921d65de-13fb-4f42-a242-75e5d1a5dbae",
            "created_by_ref":       "identity--7247edc2-e889-4624-9b89-
ef90f9202d06",
            "created": "2020-02-10T16:02:08.654857Z",
            "modified": "2020-02-10T16:02:08.654857Z",
            "name": "Malicious SHA256",
            "description": "SHA256 of file",
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[ipv4-addr:value =  '{}' ]",
            "pattern_type": "stix",
            "pattern_version": "2.1",
            "valid_from": "2020-02-10T16:02:08.654857Z",
            "object_marking_refs": [
                "marking-definition--f88d31f6-486f-44da-b317-
01333bde0b81"
            ]
        }}
"""
last="""    ]
}
"""
```

```
with open('blacklist') as f:
    ips = [l.strip('\n') for l in f.readlines()]
with open('/data/contents/stix_indicators_v2/blacklist.content','w') as
f:
    f.write(text)
    for ip in ips:
        f.write(indicator.format(ip))
    f.write(last)
```

60. Posteriormente, se debe crear un fichero llamado "blacklist" en el que se incluyan las direcciones IP que se deseen incluir en la lista negra, una por línea.

61. A continuación, se debe acceder a la interfaz web, y desde ahí, a "⚙ **> Threat Intelligence > STIX Indicators".**

62. Desde este apartado, se crea una nueva regla haciendo click en "+ Add". Se le da el nombre "blacklist" y se le añade el contenido mínimo para que quede vacía:

```
{}
```

63. Finalmente, se copia el script y el fichero con la lista negra de IPs al directorio /data/tmp de n2os y se ejecuta el script.

```
Python nombre_scrypt.py
```

6.10 SINCRONIZACIÓN

64. **Se recomienda la integración del servicio NTP.** Para ello, seguir las siguientes instrucciones:

    - Acceder a la interfaz web de la consola.
    - Acceder a la ventana "⚙ > System > Date and Time".
    - En la sección NTP, marcar la casilla **Enabled** e introducir la dirección de los servidores NTP deseados (separados por comas en caso de que se introduzcan varios).

6.11 ACTUALIZACIONES

65. Se puede consultar la versión actual del producto en la barra superior en la interfaz web y en el mensaje de login en la interfaz ssh, así como ejecutando el comando `n2os-version`.

66. La actualización del producto se puede realizar desde la interfaz web o desde la línea de comandos.

67. Antes de seguir los siguientes pasos, es necesario haber descargado el *Update bundle* correspondiente a la versión a la que se desea actualizar. Esto se puede encontrar desde el Portal de Soporte de Nozomi Networks [Support].

68. En el caso de la interfaz web, el proceso de actualización del software es el siguiente:

    a) Acceder a la ventana "⚙ > System > Operations".

    b) Hacer click sobre **"Software Updates"** y seleccionar el archivo con extensión ".bundle" de la versión deseada.

    c) Pulsar el botón **"Proceed".**

69. Para obtener más información sobre estos procesos de actualización, consultar la sección *"Software update and rollback"* del manual [Maintenance].

6.12 AUTO-CHEQUEOS

70. Las imágenes del firmware operan en modo solo-lectura, por lo que son inmutables si no se tiene acceso físico a los discos del dispositivo. Aunque no se soporta el arranque seguro, un HIDS interno escanea continuamente el sistema para verificar su integridad.

6.13 AUDITORÍA

6.13.1 REGISTRO DE EVENTOS

71. El sensor genera registros de auditoría para: cambios en la configuración del producto y funcionamiento normal del mismo.

72. Estos registros de auditoría se pueden consultar desde la interfaz web, accediendo a **" > System > Audit"**. El formato de estos registros es el mostrado a continuación:

Ilustración 3: Registro de auditoría

73. Como se observa en la figura anterior, los registros incluyen: hora de evento, dirección IP, usuario, y evento en cuestión.

6.13.2 ALMACENAMIENTO LOCAL

74. El producto almacena los registros de auditoría de forma local. Cuando se alcance el límite de almacenamiento configurado, estos se sobrescribirán por encima de los eventos más antiguos. Dicho límite se puede configurar siguiendo las instrucciones que se pueden encontrar en el capítulo "Chapter 17. Retention" del manual [Configuration].

6.14 BACKUP

75. El producto ofrece la posibilidad de crear copias de seguridad, entre las que se distinguen dos tipos: *Full Backup*, que contiene toda la información del sistema; *Environment Backup*, usado para restaurar la parte más importante del sistema en otro sensor para su análisis o como *backup* delta para un *full backup*.

76. Consultar la sección *"Backup and restore"* del manual [Maintenance] para el proceso de *backup*, recomendándose realizar la configuración de backups periódicos.

6.15 FUNCIONES DE SEGURIDAD

77. El sensor proporciona un amplio abanico de funciones que son utilizadas para la gestión de detecciones de incidencias y de posibles soluciones ante estas:

    - Cuenta con un control de acceso basado en roles, que permiten determinar qué acciones puede realizar cada usuario autenticado.
    - Presentación del entorno que está monitorizando, mostrando una vista de todos los activos y nodos de la red, así como las comunicaciones entre ellos. El sensor también permite gestionar cualquier actor dentro de la red.
    - Los usuarios pueden acceder a los resultados a través de una GUI disponible en navegador web. El sensor recoge los datos y los presenta en forma de gráficos y tablas. La autenticación a esta GUI es gestionada a partir de una base de datos local de usuarios.
    - Monitorización y detección de vulnerabilidades presentes en la red, gracias al análisis constante de la red contra un repositorio de vulnerabilidades de ICS.
    - Uso de querys gracias a N2QL (Nozomi Networks Query Language) que permite crear complejos patrones de procesamiento de información, a través de la concatenación de operaciones simples.
    - Detección de anomalías y generación de alertas de eventos sospechosos en la red. Dichas alertas, pueden ser de cuatro tipos:
        - Validación de protocolo: Guardian monitoriza cada paquete y lo compara con anomalías con el respectivo protocolo de transporte y aplicación.
        - Comportamiento aprendido: El TOE observa el comportamiento de la red, de modo de cualquier desviación de comportamiento resultará en una anomalía.
        - Comprobaciones integradas: El TOE comprueba en tiempo real las anomalías conocidas.
        - Comprobaciones personalizadas: Permite personalizar la detección de anomalías y la generación de alertas personalizadas.
    - Permite la descarga de paquetes de red en formato Packet Capture (PCAP) para su posterior análisis.
    - Gestión de las detecciones basadas en anomalías, pudiendo elegir entre: a) aprendizaje adaptativo, mediante el cual la red monitorizada es aprendida por el sensor y generará alertas en base a anomalías de comportamiento típico detectadas; b) estricto, el cual permite definir una referencia detallada para la detección de anomalías.

78. La configuración de estas funcionalidades se describe a lo largo de los manuales [UserGuide], [Configuration] y [AdminGuide].

7 FASE DE OPERACIÓN

79. La operación y mantenimiento correcto del sensor debe incluir los procedimientos necesarios para realizar las siguientes tareas

- Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido hardware o software no autorizado.
- *Firmware* activo y su integridad, deberán verificarse periódicamente para comprobar que está libre de software malicioso.
- Aplicación regular de los parches de seguridad, con objeto de mantener una configuración segura.
- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.
- Se deben gestionar correctamente los certificados utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben realizar copias de seguridad de manera periódica.

8 REFERENCIAS

[CCN-STIC-807]	Criptografía de empleo en el Esquema Nacional de Seguridad. Marzo 2022
[InstallationGuide]	Guardian-Installation Guide (v24.2.0)
[AdminGuide]	Guardian-Administrator Guide (v24.2.0)
[Maintenance]	Guardian and Central Management Console-Maintenance (v24.2.0)
[UserGuide]	Guardian-User Guide (v24.2.0)
[Configuration]	N2OS Configuration-Reference Guide (v24.2.0)
[Development]	N2OS-Software Development Kit (v24.2.0).
[Licenses]	https://licenses.nozominetworks.com
[Support]	https://www.nozominetworks.com/support
[Portal]	https://nozominetworks.my.site.com/support

9 ABREVIATURAS

CA	Autoridad de Certificación
CB	Certification Body
CE	Conformité Européene
CLI	Command Line Interface
ENS	Esquema Nacional de Seguridad.
FCC	Federal Communications Commission
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HTTPS	Hypertext Transfer Protocol Secure
ICS	Industrial Control System
IDS	Intrusion Detection System
LINCE	Certificación Nacional Esencial de Seguridad
N2OS	Nozomi Networks Operating System
N2QL	Nozomi Networks Query Language
NTP	Network Time Protocol
OT	Operational Technology
PBKDF2-SHA512	Password-Based Key Derivation Function 2 con SHA-512
PCAP	Package Capture
SAI	Sistema de Alimentación Ininterrumpida
SCADA	Supervisory Control and Data Acquisition
SSH	Secure Shell
SSHv2	Secure Shell version 2
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
UL	Underwriters Laboratories

PUBLICACIONES DE DEFENSA

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