

Guía de Seguridad de las TIC

CCN-STIC 1235

Procedimiento de Empleo Seguro NetinDS



Octubre 2025



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO: 083-26-123-9

Fecha de Edición: Octubre de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1	INTRODUCCIÓN	3
2	OBJETO Y ALCANCE	4
3	ORGANIZACIÓN DEL DOCUMENTO	5
4	FASE PREVIA A LA INSTALACIÓN	6
4.1	ENTREGA SEGURA DEL PRODUCTO	6
4.2	ENTORNO DE INSTALACIÓN SEGURO	6
4.3	CONSIDERACIONES PREVIAS.....	6
4.4	COMPONENTES DEL ENTORNO DE OPERACIÓN	6
5	FASE DE INSTALACIÓN.....	8
6	FASE DE CONFIGURACIÓN	9
6.1	MODO DE OPERACIÓN SEGURO	9
6.2	AUTENTICACIÓN	9
6.3	ADMINISTRACIÓN DEL PRODUCTO.....	9
6.3.1	ADMINISTRACIÓN LOCAL Y REMOTA	9
6.3.2	CONFIGURACIÓN DE ADMINISTRADORES.....	9
6.4	CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	9
6.5	GESTIÓN DE CERTIFICADOS	10
6.6	ACTUALIZACIONES	10
6.7	AUDITORÍA	10
6.7.1	REGISTRO DE EVENTOS.....	10
6.7.2	ALMACENAMIENTO LOCAL.....	10
7	REFERENCIAS	12
8	ABREVIATURAS.....	13

1 INTRODUCCIÓN

1. El software Netin Diagnostic System, o también conocido como **NetinDS**, es un sistema de monitorización para entornos industriales, capaz de realizar una diagnosis de las instalaciones e infraestructuras OT de estos entornos.
2. Gracias a esta herramienta, se crea un ecosistema donde tener gran cantidad de información disponible para poder gestionar grandes instalaciones IIoT (Industrial Internet of Things). Gracias al análisis de toda esta información, NetinDS es capaz de reconocer situaciones que estén fuera de lo esperado gracias a reglas de filtrado.
3. Por otra parte, ofrece la generación de alarmas de modo que se notifique a los operarios del entorno industrial cuando algún evento no esperado es detectado, con el objetivo de poder ponerle solución lo antes posible.

2 OBJETO Y ALCANCE

4. El presente documento tiene como objetivo detallar las configuraciones de seguridad del software **NetinDS** en su versión **2.0.2**, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.
5. Bajo el alcance de NetinDS encontramos los siguientes componentes:
 - NetinDS Agent: Captura la información de los dispositivos del entorno gestionados, y la envía a NetinDS Server. Para ello, hace uso de bloques de código que permiten a los dispositivos IT gestionados conectarse al agente.
 - NetinDS Server: Coordina el agente desplegado guardando la información recogida e interpretando los datos recopilados. Para ello, ofrece una interfaz web accesible para los usuarios a través de un navegador.
6. La versión 2.0.2 de NetinDS es la cualificada e incluida en el Catálogo de Productos y Servicios STIC (CPSTIC), en la familia *‘Herramientas de gestión de red’*.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado 5. En este apartado se recogen recomendaciones 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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Al tratarse de una solución *software*, **NetinDS** es entregado mediante un archivo ejecutable (.exe), el cual instalará todas las dependencias necesarias. Para ello, el fabricante deberá conceder acceso vía e-mail a un servidor FTPS propio para poder descargar el archivo instalador de la solución.
8. Una vez descargado el archivo de instalación, se debe de comprobar el hash y la firma del archivo descargado. Este archivo estará firmado con un certificado RSA-4096 con SHA-256 por parte de Mytra Control S.L. Además, se proporcionará otro fichero con el hash SHA-512 del archivo ejecutable. Si tanto el certificado como el hash son correctos, se podrá iniciar la instalación del software.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. NetinDS deberá de ser instalado en un ordenador cuyo sistema operativo sea Windows 10 Pro o Windows 11. Tanto el propio ordenador como las personas autorizadas a utilizarlo deben de ser confiables, y deben de darle un uso legítimo a este producto.
10. Las personas autorizadas a acceder al ordenador deben de seguir las guías de instalación segura ([REF1] y [REF2]) y cumplir con la política de seguridad de Mytra Control S.L.

4.3 CONSIDERACIONES PREVIAS

11. El archivo de instalación provisto por el fabricante instalará todos los componentes de NetinDS descrito.
12. Previo a la instalación, las personas autorizadas administradoras con acceso al ordenador sobre el que se va a llevar a cabo la instalación deben de asegurar el sistema operativo. Para ello, el sistema Windows 10 Pro donde el producto es instalado, debe de ser desplegado junto a las herramientas “*Microsoft Security Compliance Toolkit*”. Este conjunto de herramientas puede ser descargado en [REF3] ayuda a aumentar la seguridad del Sistema Operativo. El proceso para desplegar estas herramientas queda descrito en la sección 3.1 de la guía [REF1].
13. De igual forma, se deberá de activar el servicio Bitlocker ofrecido por el Sistema Operativo Windows 10 Pro, el cual se encarga de realizar un cifrado al disco de memoria interna del ordenador donde NetinDS es desplegado. De esta forma, se consigue proteger mediante control de acceso a los datos contenidos en este. Para ello se deberá de seguir la sección 3.2 de la guía [REF1].

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. El software NetinDS debe de ser instalado junto al siguiente entorno operacional:
 - Plataforma con Windows 10 Pro instalado.
 - Navegador Web: Navegador desde el que se accede a la interfaz gráfica de NetinDS. El navegador a utilizar deberá de soportar la versión 5 de HTML y la versión 3 de CSS, como mínimo, para conseguir un correcto funcionamiento con NetinDS.

- Dispositivos y entidades IIoT: Estos son los dispositivos que serán analizados por el Agente NetinDS, capturando todos los datos que sean necesarios para analizarlos, consiguiendo así un correcto funcionamiento y gestión de estos. El Agente NetinDS configurará protocolos como SNMP o MQTT capaces de automatizar el proceso de recolección de datos de estos dispositivos.

5 FASE DE INSTALACIÓN

15. La instalación deberá de realizarse en un entorno Windows 10 Pro, y tal y como se describe en la sección 4.2 de la guía [REF1]. Para la instalación del producto habrá que seguir las indicaciones del wizard que aparece al ejecutar el archivo de instalación (.exe) de NetinDS, tal y como se describe en la referencia anterior. El producto se instala en modo *standalone* (opción *NetinDS Standalone Agent* en la ventana *Installation type* mostrado en el wizard de instalación), englobando todos los componentes de este en un único paquete.
16. Una vez instalado el software, se deberán de tener en cuenta todas las consideraciones descritas en la sección 4.3 de la guía [REF1]. Esta sección incluye las siguientes configuraciones necesarias a realizar una vez las dependencias de NetinDS han sido instaladas, y necesarias para finalizar con la fase de instalación.
17. Una vez finalizada la instalación de las dependencias, se deberá de comprobar la versión de NetinDS instalada como se describe en la sección 4.3.1 de la guía [REF1]. Si el proceso de instalación del software se ha realizado correctamente, la versión que se debería mostrar sería la 2.0.2. En caso contrario, se deberá de realizar el proceso de nuevo.
18. Habiendo comprobado que la versión es correcta, la administración confiable deberá de eliminar todos los usuarios y sus contraseñas que vengan instaladas por defecto en el software como se describe en la sección 4.3.2 de [REF1]. Seguidamente, todos los nuevos usuarios se crearán utilizando una política de contraseñas segura.
19. Para que la administración confiable y los usuarios puedan acceder a los servicios de NetinDS, deben de generarse las claves privadas y los certificados firmados para todos los canales de comunicación establecidos como se describe en la sección 4.3.3 de la guía [REF1].
20. El canal de comunicación entre NetinDS Server y el navegador web debe de estar protegido mediante el protocolo HTTPS, el cual debe de ser configurado como se describe en la sección 4.3.4 de la guía [REF1].
21. Por último, se debe de configurar el servicio MQTT, para que el agente sea capaz de recibir datos desde los dispositivos IIoT como se describe en la sección 4.3.6 de la guía [REF1].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

22. Para utilizar el producto de un modo seguro, se deberá de seguir la sección 4 de la guía [REF2]. En esta guía se detallan todas las acciones posibles y cómo llevarlas a cabo manteniendo el producto en un estado seguro.

6.2 AUTENTICACIÓN

23. Para poder acceder a la interfaz web de NetinDS, se utiliza un navegador web estableciendo un canal HTTPS como se indica en la sección 4.3 de [REF2].
24. Una vez se accede a la interfaz web, el producto ofrece una pantalla de login donde se debe de introducir un usuario y una contraseña. Esta contraseña es creada por el administrador para cada nuevo usuario y debe de cumplir con un cierto nivel de complejidad para que sea segura, tal y como se describe en la sección 4.3.3.4 de la guía [REF2].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

25. La administración de NetinDS se realiza exclusivamente de forma remota mediante la interfaz web que el servidor NetinDS ofrece. Esta comunicación a la interfaz web se realiza mediante HTTPS.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

26. Para conocer las funcionalidades que pueden realizar los roles del producto, se debe de seguir la sección 4.3.1 de la guía [REF2]. En esta se especifican los roles con permisos para realizar funciones de administración, y aquellos roles que solo tienen como finalidad la propia utilización del producto, sin funciones de administración.
27. Por un lado, el producto ofrece el rol *User Administrator*. Este se trata del rol encargado de gestionar los usuarios exclusivamente, sin capacidad de realizar configuraciones de administración.
28. Por otro lado, el rol *Configuration Administrator* tiene acceso completo a todas las funcionalidades de NetinDS, excepto las funciones del rol *User Administrator* mencionado anteriormente.
29. Por último, existe un rol llamado *User* que se corresponde a las funciones básicas para poder utilizar NetinDS, sin ningún tipo de funcionalidad de administración disponible.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

30. Toda la configuración segura de las interfaces, puertos y servicios de NetinDS puede seguirse según la sección 4 de la guía [REF2].
31. Siguiendo esta guía, se configurarán las siguientes interfaces:

- Interfaz SNMP, para la comunicación con dispositivos IIoT del entorno operacional, donde le enviarán información de su estado de funcionamiento. Esta configuración se lleva a cabo a través de la interfaz web de NetinDS. La configuración por realizar en cada dispositivo IIoT se debe de realizar siguiendo la sección 4.3.4.5 de la guía [REF2].
- Interfaz MQTT, para la comunicación con dispositivos IIoT del entorno operacional. La configuración por realizar en cada dispositivo IIoT se debe de realizar siguiendo la sección 4.3.4.6 de la guía [REF2].
- Interfaz web de NetinDS, a través de la cual se puede gestionar el producto de forma remota por medio de un canal HTTPS como se describe en la sección 4.3 de la guía [REF2].

6.5 GESTIÓN DE CERTIFICADOS

32. El certificado digital utilizado por NetinDS para las comunicaciones HTTPS y MQTT debe de ser creado siguiendo la sección 4.3.3 de la guía [REF1] con RSA-3072. Además, el producto se debe configurar para usar este certificado como indica la sección 4.3.4 de la guía [REF1].

6.6 ACTUALIZACIONES

33. Tal y como se describe en la sección 3 de la guía [REF2], Mytra Control S.L. deberá de notificar a sus clientes cuando exista una nueva actualización de software, a través de un e-mail. En este e-mail, se especificará la nueva versión disponible, y se concederá acceso a un servidor FTPS mediante unas credenciales temporales
34. En este servidor FTPS estará alojada la nueva actualización de producto, que será descargada por un usuario administrador. Una vez descargada, se debe comprobar el hash SHA-512 y la firma del archivo.

6.7 AUDITORÍA

6.7.1 REGISTRO DE EVENTOS

35. NetinDS genera registros de auditoría para los siguientes eventos:
 - Intento de acceso de un usuario mediante credenciales a través de la interfaz web, incluyendo si el intento de acceso es exitoso o no.
 - Cambios en la configuración del producto.
 - Cambios en las credenciales de los usuarios.
 - Recepción de datos desde los dispositivos IIoT a través de MQTT y SNMP.
36. Los registros de auditoría incluyen la fecha, el usuario asociado (si aplica) y un nombre indicador del evento al que corresponde.

6.7.2 ALMACENAMIENTO LOCAL

37. Los registros de auditoría de NetinDS se almacenan de forma local en el ordenador donde este es instalado.

38. La ruta donde los registros de auditoría son almacenados en el Sistema Operativo es la siguiente: *C:\ProgramData\Netin\NDS-Datasource\logs\netin-ds-datasource-audit.log.gz*

7 REFERENCIAS

- [REF1] *NetinDS Preparational Guidance v0.12, 2024-04-24*
- [REF2] *NetinDS Operational User Guidance v0.12, 2024-04-24*
- [REF3] <https://www.microsoft.com/en-us/download/details.aspx?id=55319>

8 ABREVIATURAS

AES	<i>Advanced Encryption Standard (Estándar de Cifrado Avanzado)</i>
CPSTIC	<i>Catálogo de Productos STIC</i>
CSS	<i>Cascading Style Sheets (Hojas de Estilo en Cascada)</i>
ECDHE	<i>Elliptic Curve Diffie-Hellman Ephemeral (Intercambio de Claves de Diffie-Hellman Efímero de Curva Elíptica)</i>
ENS	<i>Esquema Nacional de Seguridad.</i>
GCM	<i>Galois/Counter Mode (Modo Galois/Contador)</i>
HTML	<i>HyperText Markup Language (Lenguaje de Marcado de Hipertexto)</i>
HTTP	<i>HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto)</i>
HTTPS	<i>HTTP over TLS (HTTP sobre TLS)</i>
IIoT	<i>Industrial Internet of Things (Internet Industrial de las Cosas)</i>
IT	<i>Information Technology (Tecnologías de la Información)</i>
MQTT	<i>Message Queuing Telemetry Transport (Transporte de Telemetría de Cola de Mensajes)</i>
OT	<i>Operational Technology (Tecnología Operacional)</i>
RSA	<i>Rivest–Shamir–Adleman</i>
SFTP	<i>Secure File Transfer Protocol (Protocolo de Transferencia de Archivos Seguro)</i>
SHA	<i>Secure Hash Algorithm (Algoritmo de Hash Seguro)</i>
SNMP	<i>Simple Network Management Protocol (Protocolo Simple de Gestión de Redes)</i>
STIC	<i>Servicio de Tecnologías de la Información y Comunicaciones</i>
TLS	<i>Transport Layer Security (Seguridad de la Capa de Transporte)</i>

