

Referencia: 2022-10-INF-3986-v1
Difusión: Pública
Fecha: 12.05.2023

Creado por: I006
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente # **2022-10**

TOE **Teldat-M1 Series, Software 11.01.09.90.01**

Solicitante **A28877579 - Teldat, S.A.**

Referencias

[EXT-7575] Solicitud de certificación

[EXT-8111] Informe Técnico de Evaluación

Informe de Certificación del producto Teldat-M1 Series, Software 11.01.09.90.01, según la solicitud de referencia [EXT-7575], de fecha 03/02/2022, evaluado por el laboratorio Applus Laboratories, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-8111], recibido el pasado 28/10/2022.

CONTENIDOS

RESUMEN.....	3
RESUMEN DEL TOE.....	3
ACTIVIDADES DE EVALUACIÓN.....	5
IDENTIFICACIÓN DEL TOE.....	6
HIPÓTESIS Y ENTORNO DE USO	6
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS	6
FUNCIONES DE SEGURIDAD	6
PRUEBAS DEL PRODUCTO	7
CONFIGURACIÓN EVALUADA.....	8
RESULTADOS DE LA EVALUACIÓN	8
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES	8
RECOMENDACIONES DEL CERTIFICADOR.....	8
VALIDEZ DEL CERTIFICADO.....	9
GLOSARIO DE TÉRMINOS	9
BIBLIOGRAFÍA	9
DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)	10

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Teldat-M1 Series, Software 11.01.09.90.01.

El Teldat-M1 Series es un router compacto para oficinas medianas y pequeñas que requieren conexiones de alta velocidad.

Solicitante:	Teldat, S.A..
Organismo de Certificación:	Centro Criptológico Nacional (CCN).
Laboratorio de Evaluación:	Applus Laboratories.
Tipo de Evaluación:	LINCE + MEC - Certificación Nacional Esencial de Seguridad, versión 2.0
Taxonomía según CCN-STIC-140:	Anexo D.1-M: Enrutadores Anexo D.2-M: Switches
Fecha de término de la evaluación:	03/01/2023
Fecha de validez recomendada¹:	25/04/2025

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE + MEC presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Applus Laboratories asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para LINCE + MEC, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Teldat-M1 Series, Software 11.01.09.90.01, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es la plataforma de encaminamiento y conmutación de tráfico (Router y Switch) Router Corporativo Teldat-M1 Series con la versión Software 11.01.09.90.01.

El dispositivo se distribuye en forma de equipo dedicado o *appliance* que incluye el software y el hardware necesarios para su operación segura.

¹ Ver sección VALIDEZ DEL CERTIFICADO

El Teldat-M1 Series es un router compacto para oficinas medianas y pequeñas que requieren conexiones de alta velocidad.

Posee una potente arquitectura hardware que permite velocidades de 600 Mbps simétricos con servicios habilitados. Muy versátil y escalable, además de la conectividad Ethernet, incluye un puerto de expansión que permite adaptarse a un amplio abanico de escenarios: Fibra + Ethernet, Fibra + Ethernet + VDSL, Ethernet + Serie, conmutador local de hasta 12 puertos, y opción 3G/4G. Las funcionalidades añadidas a través del puerto de expansión o sus conexiones internas (Conexión Celular 3G/4G, Wi-Fi, VDSL o Fibra Óptica) quedarán fuera del alcance del TOE. El dispositivo se distribuye con o sin dichos elementos en función de la elección del cliente, no teniendo efecto la presencia de los mismos en el software del TOE ni en la funcionalidad básica del mismo.

Adicionalmente, el producto proporciona conectividad hacia la red local mediante un switch de 4 puertos con velocidad Gigabit así como con un puerto WAN para la funcionalidad de routing que sí se encuentran dentro del alcance de la evaluación.

Las principales funciones de seguridad que implementa Teldat-M1 Series son las siguientes:

- **Auditoría:** Se generan, almacenan y protegen los registros de auditoría de los eventos relativos al TOE.
- **Identificación y Autenticación:** El acceso al TOE se encuentra restringido por cada una de sus interfaces de administración remota (SSH) mediante usuario y contraseña o autenticación mediante certificados. El acceso mediante su interfaz local también estará restringido hasta que el usuario introduzca un usuario y contraseña correctos.
- **Administración Confiable:** El TOE ofrece la capacidad de ser gestionado y configurado por usuarios autorizados mediante SSH y conexión local (puerto de consola local). El producto bloquea las cuentas de los usuarios cuando se produce un número elevado de intentos incorrectos de autenticación, de manera que se protege contra ataques de fuerza bruta.
- **Canales Seguros:** El TOE establece canales seguros para el intercambio de información sensible a través de SSH, TLS o IPsec empleados para sus sesiones de administración, túneles entre dispositivos o como soporte para proteger las comunicaciones de otros protocolos.
- **Instalación y Actualización Confiables:** El producto permite la consulta de su versión actual, así como la posibilidad de actualizar su firmware de forma segura. Los ficheros de actualización se encuentran firmados utilizando ECDSA y su instalación no se lleva a cabo hasta que se comprueba la veracidad de su firma.
- **Protección Contra Fallos:** El producto tiene la capacidad de realizar pruebas para verificar el correcto funcionamiento de las funciones criptográficas y de la integridad del firmware. Estas pruebas se realizan de forma automática durante el arranque del producto y pueden ser configuradas de manera que se realicen periódicamente o manualmente a petición de los usuarios autorizados.

- **Criptografía:** El TOE implementa funciones y algoritmos criptográficos de acuerdo con lo establecido en la guía [CCN-STIC-807] e impide el acceso en claro a los parámetros de seguridad del sistema. Las claves y contraseñas empleadas por el producto se encuentran cifradas o en forma de hashes en el almacenamiento del mismo.
- **Enrutador:**
 - Administración de puertos, permitiendo habilitarlos o deshabilitarlos, así como asignarles prioridades.
 - Encaminamiento de paquetes y filtrado de tráfico en base a dirección IP, MAC y puerto interconectando las distintas subredes existentes.
- **Switch:**
 - Administración de puertos, permitiendo habilitarlos o deshabilitarlos, así como asignarles prioridades.
 - Conmutación de paquetes en la red local e interconexión de segmentos físicos de red.
 - Creación de redes VLAN.
 - Control de acceso mediante filtrado por MAC.

La interfaz WAN-Ethernet y la funcionalidad de punto de acceso Wi-Fi son opcionales y activables en remoto. Incluye todas las funcionalidades demandadas a un router profesional, como routing (RIP, OSPF, BGP, VRF, PolicyRouting), seguridad (ACLs, Firewall, IPsec, 802.1X), calidad de servicio (CBWFQ, PQ, perfilado), o gestión (CLI, SNMPv3, RADIUS, TACACS+, Syslog, Netflow, Mirroring). Conectividad fija usando dos (o tres) accesos distintos (Ethernet, Fibra, ADSL/VDSL, G.SHDSL, E1/T1), como acceso principal y backup, o ambos activos para balanceo.

ACTIVIDADES DE EVALUACIÓN

El producto se evaluó con todas las evidencias necesarias para la satisfacción del tipo de evaluación LINCE + MEC, más las requeridas para el componente adicional MEC, según la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

Las actividades de evaluación realizadas en el transcurso de la evaluación han sido:

- ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD
- INSTALACIÓN DEL PRODUCTO
- ANÁLISIS DE CONFORMIDAD – ANÁLISIS DE LA DOCUMENTACIÓN
- ANÁLISIS DE CONFORMIDAD –PRUEBAS FUNCIONALES
- ANÁLISIS DE VULNERABILIDADES
- PRUEBAS DE PENETRACIÓN DEL TOE
- EVALUACIÓN CRIPTOGRÁFICA (MEC)

IDENTIFICACIÓN DEL TOE

Objeto de evaluación (TOE): Teldat-M1 Series, Software 11.01.09.90.01.

Declaración de Seguridad: Router Corporativo Teldat-M1 Series-Declaración de Seguridad V1.6, 22/09/2022.

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Dichas hipótesis, se relacionan en el apartado 4.1 de la declaración de seguridad [ST].

Estas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las hipótesis declaradas para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las amenazas detalladas en el apartado 4.3 de la declaración de seguridad [ST], no suponen un riesgo explotable para el producto Teldat-M1 Series, Software 11.01.09.90.01, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a moderado según lo definido en LINCE, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

FUNCIONES DE SEGURIDAD

El TOE declara en el apartado 5 de la declaración de seguridad [ST] las funciones de seguridad que han sido verificadas por el CCN respecto a su cumplimiento con la Taxonomía de productos declarada con respecto de la guía CCN-STIC-140 y han sido evaluadas por el laboratorio para verificar su efectividad en el entorno operacional definido.

GUÍAS DE OPERACIÓN E INSTALACIÓN DEL TOE

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Router Corporativo Teldat-M1 Series-Declaración de Seguridad V1.6, 22/09/2022
- Teldat Router M1/M1L Installation Manual, Teldat Dm569-I Versión 9.1 09/10/2020

- Configuration and Monitoring, Teldat Dm704-I Versión 12.0G 27/09/2021
- LAN Interfaces, Teldat Dm709-I Versión 11.0J 20/04/2021
- Bandwidth Reservation System, Teldat-Dm 715 Versión 11.0A 02/09/2020
- NAT Feature, Teldat-Dm 720-I Versión 11.01 06/06/2017
- DNS, Teldat-Dm 723-I Versión 11.09 13/01/2021
- FTP/sFTP Protocol, Teldat-Dm 724-I Versión 11.07 25/04/2018
- NTP Protocol, Teldat-Dm 728-I Versión 11.08 19/11/2020
- DHCP Protocol, Teldat Dm730-I Versión 11.0A 28/01/2020
- NAPT Facility, Teldat-Dm 735-I Versión 11.00 07/06/2017
- HTTP Protocol, Teldat Dm737-I Versión 11.08 03/12/2020
- IPsec, Teldat Dm739-I Versión 11.0H 19/02/2021
- Software Updating, Teldat-Dm 748-I Versión 11.05 26/06/2020
- Ethernet Subinterface, Teldat Dm750-I Versión 11.09 07/06/2017
- VLAN, Teldat-Dm 751-I Versión 11.05 13/05/2020
- Access Control, Teldat Dm752-I Versión 11.0A 08/03/2021
- DYNAMIC NAT, Teldat-Dm 755-I Versión 10.71 08/06/2017
- Common Configuration for Interfaces, Teldat Dm772-I Versión 11.0B 05/05/2020
- AFS, Teldat-Dm 786-I Versión 11.0I 12/04/2021
- SSH Protocol, Teldat-Dm 787-I Versión 11.06 06/09/2021
- New NAT, Teldat Dm788-I Versión 11.04 20/03/2019
- Procedimiento de empleo seguro Router Corporativo Teldat-M1 Versión 1.2 Mayo 2022

PRUEBAS DEL PRODUCTO

Para verificar la funcionalidad de seguridad declarada, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con lo declarado en la Declaración de Seguridad [ST].

Adicionalmente, el laboratorio ha realizado un análisis de vulnerabilidades teniendo en cuenta las funcionalidades de seguridad declaradas en la [ST] y el nivel de resistencia a atacantes con potencial de ataque moderado tal y como se define en CCN-STIC-2002. Teniendo en cuenta las potenciales vulnerabilidades extraídas de dicho análisis, el laboratorio evaluador ha realizado pruebas de penetración para verificar la explotabilidad de las mismas en el entorno de operación declarado en [ST].

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde al entorno de operación, identificado en la Declaración de Seguridad [ST].

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no supone una merma en la capacidad funcional del producto conforme a lo declarado en su Declaración de Seguridad [ST].

CONFIGURACIÓN EVALUADA

Para el funcionamiento del producto conforme a la evaluación evaluada del TOE Teldat-M1 Series, Software 11.01.09.90.01 es necesario disponer de los componentes software que se indican en la sección 3.1 de la declaración de seguridad [ST].

RESULTADOS DE LA EVALUACIÓN

El producto Teldat-M1 Series, Software 11.01.09.90.01 ha sido evaluado en base a la Declaración de Seguridad Router Corporativo Teldat-M1 Series-Declaración de Seguridad V1.6, 22/09/2022.

Todas las actividades de evaluación requeridas por el tipo de evaluación LINCE+MEC presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Applus Laboratories asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 2.0 para el tipo de evaluación LINCE + MEC.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- El evaluador no ha proporcionado recomendaciones o comentarios.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Teldat-M1 Series, Software 11.01.09.90.01, se propone la resolución estimatoria de la misma.

El certificador adicionalmente recomienda a los usuarios finales del TOE que tengan en cuenta las siguientes recomendaciones:

- El presente certificado cubre la funcionalidad declarada en la [ST] del TOE en su versión especificada en la sección Identificación del TOE de este informe, concretamente:

- Teldat-M1 Series, Software 11.01.09.90.01
- Los usuarios finales del TOE deben comprobar que las hipótesis sobre el entorno de ejecución definidas en el apartado 4.1 de la declaración de seguridad [ST] son aceptables para el caso de uso esperado del TOE.

VALIDEZ DEL CERTIFICADO

Un certificado LINCE se emite indicando la versión específica del producto que fue evaluada. Si este producto evoluciona, sus nuevas versiones no serán certificadas por defecto. El proceso de “Assurance Continuity” o continuidad de la garantía [AC] se usa para facilitar el mantenimiento del certificado en versiones nuevas del producto. Este proceso es aplicable a la certificación LINCE.

Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. En todo momento el desarrollador podrá optar al proceso de renovación del certificado o re-certificación del mismo, según lo establecido en el procedimiento de certificación PO-005.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Enero 2020. Centro Criptológico Nacional.
[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.
[CCN-STIC-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial

de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.

[ST] Router Corporativo Teldat-M1 Series-Declaración de Seguridad V1.6, 22/09/2022

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- Router Corporativo Teldat-M1 Series-Declaración de Seguridad V1.6, 22/09/2022