Router Corporativo Teldat-M1 Series

Declaración de Seguridad

ST Version 1.6

22/09/2022

Índice

1 Introducción

1.1 Información del Patrocinador, TOE y Evaluación

Datos del patrocinador	Teldat, S.A. Parque Tecnológico de Madrid c/ Isaac Newton, 10 28760, Tres Cantos - Madrid (Spain)
Datos del desarrollador	Teldat, S.A. Parque Tecnológico de Madrid c/ Isaac Newton, 10 28760, Tres Cantos - Madrid (Spain)
Datos de contacto del desarrollador	Vanesa Gil Sánchez secteam@teldat.com
Nombre del TOE	Teldat-M1 Series
Versión del TOE	Software 11.01.09.90.01
Tipo de evaluación	LINCE + MEC
Manuales de uso del producto y su versión	La información detallada sobre cada guía incluyendo su versión se puede encontrar en la sección **2.2. Identificación de las Guías de Uso, Instalación y Configuración Seguras del TOE** en el presente documento.
Taxonomía del producto según CCN-STIC-140	Anexo D.1-M: Enrutadores Anexo D.2-M: Switches

1.2 Metodología y Criterios de Evaluación

CCN-STIC-2001	CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad, v2.0
CCN-STIC-2002	CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad, v2.0

2 Descripción del TOE

2.1 Descripción Funcional 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.

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.

2.2 Identificación de las Guías de Uso, Instalación y Configuración Seguras del TOE.

La siguiente tabla identifica las guías de uso, instalación y configuración que permiten operar al TOE en su configuración evaluada y certificada:

Nombre del Documento	Versión	Fecha
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

3 Entorno de Ejecución

La instalación y configuración segura del entorno se describe en las guías de instalación y configuración definidas en la sección **2.2. Identificación de las Guías de Uso, Instalación y Configuración Seguras del TOE** de este mismo documento.

3.1 Descripción del Entorno de Ejecución

El TOE se entrega en forma de equipo dedicado o *appliance,* que es capaz de operar por sí mismo de forma independiente debido a su naturaleza.

El appliance dispone de un puerto de expansión y de varios conectores internos que incluyen la posibilidad de incorporar al mismo un módulo celular (3G/4G), Wi-Fi, expandir los puertos del Switch o incorporar puertos de fibra óptica o VSDL. 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. Todos estos elementos opcionales se encuentran fuera del alcance de la evaluación, quedando dentro de la evaluación solamente el *appliance* base, que incluye un Switch de 4 puertos y un puerto WAN destinado a la funcionalidad de *routing*.

El dispositivo está diseñado para proporcionar funcionalidades de encaminamiento y conmutación de tráfico a los dispositivos que se le conectan. El entorno de ejecución evaluado presenta un caso de uso en el que el TOE se usará como dispositivo frontera, protegiendo una red interna frente a una red externa (típicamente “Internet”).

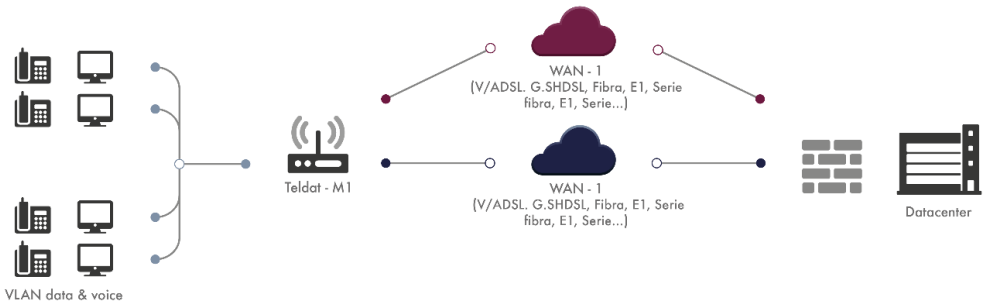

ILUSTRACIÓN 1–EJEMPLO DE ENTORNO DE EJECUCIÓN

En este contexto, el TOE se encontrará conectado a una red externa mediante su puerto WAN y a los dispositivos de la red interna a través de los puertos LAN del mismo.

Adicionalmente, el TOE proveerá funcionalidad de conmutación de tráfico sobre la red interna. Los diferentes dispositivos de la red interna conectados a los puertos internos del TOE se encontrarán interconectados mediante la funcionalidad de *switching* del producto, existiendo dos posibles casos de uso en este ámbito:

- **Unión de segmentos de red**: El TOE interconectará todos los dispositivos que se encuentren dentro del segmento de la red interna.
- **VLAN**: El TOE separará de forma lógica los dispositivos conectados a cada uno de los puertos de la red interna en distintos segmentos virtuales que solo serán capaces de alcanzarse entre sí mismos.

4 Problema de Seguridad

4.1 Hipótesis sobre el Entorno de Ejecución

En esta sección se incluyen las hipótesis sobre el entorno en el que se ejecutará el producto.

Hipótesis	Descripción
Protección física	El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
Funcionalidad limitada	El producto deberá utilizarse para el enrutamiento, filtrado de red y conmutación de redes como su función básica y no proporcionar ninguna otra funcionalidad, salvo aquellas determinadas compatibles orientadas a la protección de las comunicaciones.
Administración confiable	El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina.
Actualizaciones periódicas	El producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
Protección de las credenciales	Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
Política de seguridad de la información	Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

4.2 Activos Sensibles a Proteger

En esta sección se describen los activos que las funciones de seguridad del TOE protegen.

Activo	Descripción
AC.Administración	Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos. Se protegerá la integridad y la confidencialidad de este activo.
AC.Datos	Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red. Se protegerá la integridad, confidencialidad y disponibilidad de este activo.
AC.Actualizaciones	Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad. Se protegerá su autenticidad e integridad.

4.3 Descripción de las Amenazas

En esta sección se describen las amenazas mitigadas por las funciones de seguridad del TOE.

Amenaza	Descripción
A.NOAUT	**Acceso no autorizado de administrador**: Un atacante puede obtener un acceso como administrador del producto haciéndose pasar por un administrador ante el producto, por el producto ante un administrador, reproduciendo una sesión de administración, realizando ataques del hombre en medio.
A.CIFRA	**Cifrado débil**: Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
A.COM	**Canales de comunicación no confiables**: Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
A.AUT	**Autenticación débil de los nodos**: Un producto puede utilizar protocolos de autenticación seguros que utilicen métodos de autenticación débiles (contraseñas no robustas, contraseñas como texto en claro, contraseñas precompartidas) para hacerse pasar por un usuario administrador u otro nodo para realizar un ataque de hombre en el medio.
A.ACT	**Actualización maliciosa:** Un atacante puede realizar una actualización maliciosa que debilite las funcionalidades de seguridad del producto.
A.AUD	**Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
A.CRED	**Funcionalidades de seguridad comprometidas:** Un atacante puede comprometer las credenciales o información del producto permitiendo un acceso continuado al producto y a su información sensible.
A.CON	**Contraseñas débiles:** Un atacante puede aprovecharse del uso de contraseñas débiles para acceder con acceso privilegiado al dispositivo.
A.FUN	**Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.

5 Funciones de Seguridad

Las siguientes secciones describen las funciones de seguridad que implementa el TOE. Cada una de estas funciones de seguridad está a su vez subdividida en requisitos de seguridad. Estos requisitos corresponden con los requisitos establecidos por las taxonomías de *Enrutadores* y *Switches* para *ENS Media* según los documentos **[CCN-STIC-140-D.1-M]** y **[CCN-STIC-140-D.2-M].**

5.1 FS. Administración

Esta función de seguridad mitiga la amenaza **A.NOAUT**.

El TOE requiere que los usuarios con permisos de administración sean autenticados correctamente en el sistema antes de permitirles realizar ninguna acción.

Requisitos Cubiertos:

- **ADM.1:** El TOE define los roles en base a diferentes niveles de acceso. De esta forma, cada usuario registrado en el sistema tendrá asignado un determinado nivel de acceso, que puede variar entre 0 y 15 y un modo de acceso (*default* o *strict*). En el modo *default*, el usuario podrá ejecutar cualquier comando con un nivel de acceso igual o inferior al que tiene asignado dicho usuario. En el modo *strict*, el usuario solo podrá ejecutar los comandos que tienen el mismo nivel de acceso que el propio usuario.

  Cada comando del sistema tendrá asignado un nivel de acceso, de manera que solo los usuarios con un nivel de acceso igual o superior (dependiendo de su modo) podrán ejecutar dicho comando.

  Por defecto, existen los siguientes niveles de acceso, que son equiparables a los roles del sistema:

  - **NONE [0]:** No permite al usuario acceder al sistema.
  - **EVENTS [1]:** El usuario puede acceder a la consola de administración y al proceso de eventos, pero no puede acceder a la funcionalidad de ping, reinicio o carga desde la Flash.
  - **MONITOR [5]:** Un usuario con este nivel de acceso puede acceder a la consola de administración, al proceso de eventos, al proceso de monitorización, al comando de ping y puede iniciar una conexión SSH. Sin embargo, no tendrá acceso a la función de reinicio y carga desde la Flash.
  - **CONFIG [10]:** Este nivel de privilegio otorga acceso a todos los procesos y comandos estándar con la excepción de los comandos de administración de usuarios.
  - **ROOT [15]:** Acceso a todos los procesos y comandos del sistema. Este nivel de privilegio se puede equiparar con el rol de administrador.
- **ADM.2:** El producto asocia un nivel de privilegios a cada usuario del sistema. Los usuarios tendrán acceso a diversas funciones del producto en función del nivel de privilegio que tengan asignado.
- **ADM.3:** El producto puede ser gestionado de forma local a través del puerto de consola local que incorpora y de forma remota empleando SSH.

Existe la posibilidad de configurar el tiempo de terminación de sesión al detectar inactividad para las interfaces SSH y el puerto de consola local mediante el comando *set inactivity-timer* dentro del menú *Config*. El tiempo de terminación de sesión podrá ser configurado entre 1 minuto y 10 horas.

Adicionalmente, el TOE permite la gestión y configuración de los siguientes elementos:

- Usuarios y privilegios del sistema.
- Gestión de red y puertos del producto.
- Administración de los diferentes protocolos soportados por el sistema.
- Tiempo del sistema.
- Gestión de las funciones de encaminamiento y conmutación de tráfico.

5.2 FS. Identificación y Autenticación

Esta función de seguridad mitiga las amenazas **A.NOAUT, A.CON** y **A.CRED, A.AUT.**

El TOE puede ser administrado de forma remota a través de SSH y de forma local utilizando el puerto de consola local del que dispone el producto.

Requisitos Cubiertos:

- **IAU.1**: Todos los usuarios deben ser autenticados antes de tener acceso al TOE y a sus funciones de administración. El producto requerirá la introducción de las credenciales de usuario (nombre de usuario y contraseña) cuando se realice cualquier intento de acceso a través de las interfaces de administración. Adicionalmente, la interfaz de SSH permite que los usuarios se autentiquen utilizando mecanismos de clave pública.
- **IAU.2:** El producto permite configurar un número máximo de intentos de autenticación entre 1 y 100 para su interfaz de administración local a través del puerto de consola local. Una vez se ha producido ese número de intentos, la consola local queda bloqueada temporalmente para los accesos a través de dicha interfaz. El tiempo durante el cual la consola queda bloqueada también puede ser configurado entre 0 segundos y 1 día.

  En el caso de la interfaz de SSH, el producto introduce un retardo entre cada intento de conexión, impidiendo que se establezcan numerosas conexiones simultáneamente. El retardo introducido entre conexiones es de un segundo, lo que hace inviable la realización de ataques de fuerza bruta. Adicionalmente, se puede restringir el número de intentos de autenticación por sesión y el número máximo de conexiones SSH simultáneas. También existe la posibilidad de cambiar el puerto utilizado para SSH de forma que no se utilice el puerto estándar.

  De esta forma se impiden los ataques de fuerza bruta al dispositivo.
- **IAU.3:** Por defecto, solo los usuarios con el máximo nivel de privilegios (15) serán capaces de modificar las credenciales de autenticación de los usuarios, mientras que ningún usuario será capaz de tener acceso de lectura a dichas credenciales en claro. Las contraseñas de acceso se almacenan usando PBKDF2-SHA256 y solo los usuarios con el máximo nivel de privilegios (15) podrán acceder a

ellas. En el caso de las claves privadas utilizadas para el servidor de SSH y otro tipo de claves como las contraseñas usadas para las conexiones de IPsec o el PIN de la tarjeta SIM, todas ellas son almacenadas cifradas en el dispositivo y solo los usuarios con capacidad de configurar dichas claves (a partir del nivel 10 de privilegios) podrán acceder a ver el valor cifrado de las mismas.

- **IAU.4**: Es posible establecer contraseñas con longitudes mayores o iguales a 9 caracteres y que contengan, al menos, los siguientes caracteres:
    - Letras minúsculas y mayúsculas.
    - Números.
    - Al menos los siguientes caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “)”].
- **IAU.5:** El producto es capaz de cerrar las sesiones de administración de los usuarios cuando pasa un determinado periodo de tiempo. Existe la posibilidad de configurar el tiempo de terminación de sesión de las sesiones administrativas a través de SSH y consola local al detectar inactividad mediante el comando *set inactivity-timer* dentro del menú *Config*. El tiempo de terminación de sesión podrá ser configurado entre 1 minuto y 10 horas para estas interfaces.

5.3 FS. Canales de Comunicación Confiables

Esta función de seguridad mitiga las amenazas **A.NOAUT, A.CIFRA**y**A.COM, A.AUT.**

Requisitos Cubiertos:

- **COM.1:** El producto emplea SSH, IPsec y TLS como canales seguros para el intercambio de información sensible con otras entidades a través de cualquiera de los canales que quedan expuestos al exterior. Estos canales se encuentran protegidos empleando funciones, algoritmos y protocolos que están de acuerdo a lo establecido en la guía CCN-STIC-807.

  Se empleará el protocolo SSH para iniciar canales seguros de administración desde los que los usuarios autorizados podrán cambiar la configuración del TOE o acceder a su información de auditoría.

  El protocolo TLS será empleado en caso de que se habilite el servidor web del producto (que permitirá actualizarlo previa autenticación del usuario) o en conjunto con otros protocolos soportados por el producto, como por ejemplo HTTPS, SIP, .1X, NETFLOW, Hotspot, DNS-overHTTPS, MNGP o CWMP.

  IPsec será empleado cuando se configure el establecimiento de túneles IPsec entre el TOE y otros dispositivos.
- **COM.2:** El producto permite el inicio de canales SSH, IPsec y TLS desde entidades externas, solo permitiendo el acceso a la funcionalidad disponible a través de dichos canales si las entidades externas se autentican utilizando las credenciales correctas. A su vez, el producto permite iniciar conexiones SSH, IPsec y TLS hacia entidades externas.
- **COM.3:** Al iniciar las conexiones descritas en los requisitos anteriores, el TOE comprueba el certificado que le presentan las entidades externas y solo permite la conexión si confía en dicho

certificado (con la excepción del servidor SSH). En el caso de las conexiones en las que el TOE actúa como cliente SSH, el dispositivo permite al usuario que inicia la conexión elegir qué acción tomar (conectarse o rechazar la conexión) si el certificado del servidor externo es desconocido. En otros casos la conexión será rechazada si el TOE no confía en el certificado que le presenta la entidad externa.

En el caso en el que el producto actúa como servidor SSH, los clientes tendrán la posibilidad de autenticarse empleando certificados o usuario y contraseña. Si se decide usar el método de usuario y contraseña, el TOE no requerirá que los usuarios presenten un certificado para autenticarse. El TOE empleará certificados digitales para autenticar su propia identidad cuando actúe como servidor SSH.

5.4 FS. Criptografía

Esta función de seguridad mitiga las amenazas **A.CIFRA** y **A.COM**.

Requisitos Cubiertos:

- **CIF.1**: El TOE implementa exclusivamente operaciones criptográficas de acuerdo con lo establecido en la guía [CCN-STIC-807] para establecer sus canales seguros. Se emplean los siguientes algoritmos para el establecimiento de canales SSH, TLS e IPsec:
    - **SSH**: Solo se emplea SSH 2.0 para establecer conexiones empleando los siguientes algoritmos:
        - **Key Exchange Algorithms:**
            - diffie-hellman-group-exchange-sha256
        - **Host-key algorithms:**
            - rsa-sha2-256
            - rsa-sha2-512
        - **Encryption Algorithms:**
            - aes128-cbc
            - aes192-cbc
            - aes256-cbc
            - aes128-ctr
            - aes192-ctr
            - aes256-ctr
        - **MAC Algorithms**
            - hmac-sha1

- hmac-sha2-256
- hmac-sha2-512

- **IPsec**: Solo se utilizará IKEv2 empleando los siguientes algoritmos:
  - Key Exchange Algorithms:
    - MODP group 15
  - **Encryption Algorithms:**
    - aes128
    - aes192
    - aes256
  - **MAC Algorithms**
    - hmac-sha1
    - hmac-sha2-256
    - hmac-sha2-384
    - hmac-sha2-512
- **TLS:** Solo se permite el uso de TLS1.2 y TLS1.3 empleando las siguientes ciphersuites (En formato OpenSSL):
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_256_CCM
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_128_CCM
  - TLS_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_128_CBC_SHA

La lista de ciphersuites muestra el conjunto de ciphersuites que pueden ser configuradas en el conjunto de los servicios del producto que usan TLS, como por ejemplo HTTPS, SIP, .1X, NETFLOW, Hotspot, DNS-overHTTPS, MNGP o CWMP. Por defecto, estos servicios se encuentran deshabilitados y el usuario deberá habilitarlos si quiere usar dicha funcionalidad.

- **CIF.2**: El producto no permite el acceso en claro a parámetros de seguridad del sistema como contraseñas de usuarios o claves privadas. Las contraseñas de acceso se almacenan usando PBKDF2-SHA256 y solo los usuarios con el máximo nivel de privilegios (15) podrán acceder a ellas. En el caso de las claves privadas utilizadas para el servidor de SSH y otro tipo de claves como las contraseñas usadas para las conexiones de IPsec o el PIN de la tarjeta SIM, todas ellas son almacenadas cifradas en el dispositivo y solo los usuarios con capacidad de configurar dichas claves (a partir del nivel 10 de privilegios) podrán acceder a ver el valor cifrado de las mismas. Los usuarios con ese nivel de privilegios (10 o mayor) pueden acceder a los valores cifrados de dichas claves ya que esos mismos usuarios tiene la capacidad de crear nuevas claves y sustituir o borrar las claves existentes.
- **CIF.3**: El producto emplea **CTR_DRBG(AES)** como método para la generación de números aleatorios determinísticos.
- **CIF.4**: Teldat M1 utiliza un acelerador hardware para la generación de números aleatorios de acuerdo a la ISO/IEC 18031:2011. Este módulo implementa un PRNG alimentado por un TRNG con dos fuentes de entropía que en conjunto generan 2 bits de entropía cada 100 ciclos de reloj. El algoritmo PRNG se ejecuta haciendo un muestreo del TRNG para crear semillas iniciales de 512 bits de datos aleatorios. Adicionalmente, el TRNG realiza pruebas estadísticas periódicas en su salida.

5.5 FS. Instalación y Actualización Confiables

Esta función de seguridad mitiga las amenazas **A.ACT** y **A.NOAUT**.

Requisitos Cubiertos:

- **ACT.1:** El TOE ofrece la posibilidad de consultar su versión cuando se accede a través de sus interfaces de administración (SSH, consola local).
- **ACT.2:** El producto verifica la autenticidad e integridad de las actualizaciones utilizando ECDSA (NIST P-256, SHA-256). Los servicios de actualización del producto verifican dichas firmas antes de instalar las actualizaciones. El producto puede ser actualizado a través de SFTP, HTTPS y a través de la BIOS solo en los casos en los que el producto no pueda ser actualizado usando los otros medios. La interfaz de actualización HTTPS debe habilitarse expresamente para este cometido siguiendo las recomendaciones incluidas en las guías de usuario, manteniendo el TOE en una red aislada durante el proceso de actualización.
- **ACT.3:** Solo los usuarios con el máximo nivel de privilegios (15) pueden iniciar el proceso de actualización manual a través de SFTP o HTTPS. El resto de usuarios no tendrán la posibilidad de ejecutar los comandos o realizar las acciones necesarias para realizar el proceso de actualización.

En el caso de la actualización mediante BIOS, es posible iniciar el proceso de actualización sin autenticación, sin embargo, la actualización mediante BIOS requiere una conexión física con el producto, que se encuentra protegido por la hipótesis **Protección física**, por lo que solo los usuarios autorizados tendrán acceso físico al mismo y a realizar la actualización.

- **ACT.4:** El producto permite a los usuarios autorizados iniciar el proceso de actualización de forma manual. Adicionalmente, el TOE permite comprobar la existencia de nuevas actualizaciones utilizando el comando *check-update*, lo que le permite conectarse a un servidor de Teldat que le informa de si hay actualizaciones pendientes o no. Una vez se ha comprobado que existen actualizaciones disponibles, el administrador podrá obtener dichas actualizaciones desde la página de soporte de Teldat.

5.6 FS. Auditoría

Esta función de seguridad mitiga la amenaza **A.AUD**.

Requisitos cubiertos:

- **AUD.1:** El producto genera información de auditoría cuando se inician y finalizan las funciones de auditoría. Los siguientes eventos son generados por el TOE:
  a) Login y logout de usuarios registrados: El TOE registra cualquier evento de login y logout de los usuarios en el sistema, incluyendo eventos relativos a la caducidad de sesiones activas debido al cumplimiento del timeout configurado en el sistema.
  b) Cambios en las credenciales de usuarios: El TOE almacenará eventos relativos a la modificación de las credenciales de los usuarios locales del sistema.
  c) Cambios en la configuración del producto: Se almacenarán en los registros de auditoría todas las acciones llevadas a cabo por parte de los usuarios que impliquen un cambio en la funcionalidad del producto:
     - Gestión de los roles de usuario y acciones que afecten a la autenticación de los usuarios del sistema.
     - Cambios en el reloj del sistema y la configuración del mismo.
     - Modificaciones en las interfaces de red.
     - Cambio de configuración de cualquiera de los protocolos y servicios soportados por el sistema.
  d) Eventos relativos a la funcionalidad del producto: Se generará un evento de auditoría cada vez que un usuario, política o evento cause la ejecución de alguna de las funciones proporcionadas por el TOE:
     - Cambios de estado de las interfaces de red.
     - Actualizaciones del sistema.
     - Inicio y finalización de los auto-tests realizados por el TOE.

- Errores y alarmas producidas durante la ejecución de las funciones y servicios proporcionados por el TOE.

e) Generación, importación, cambio o eliminación de claves criptográficas.

- **AUD.2**: Los eventos de auditoría contienen la fecha y hora del evento, el tipo de evento, su resultado y, en caso de que el evento haya sido producido por parte de un usuario, la identidad de dicho usuario. El resultado del evento está contenido de forma implícita en la descripción del mismo. Por ejemplo, los eventos que indiquen que se ha levantado una interfaz indicarán de manera implícita que la operación se ha realizado de forma correcta si no se especifica ningún fallo, mientras que se especificará que la operación ha fallado si la descripción del evento indica un fallo al levantar la interfaz.
- **AUD.3**: Los registros de auditoría solo son accesibles a través de los comandos designados para la visualización de los mismos. No existe ningún comando que permita la modificación de los mismos a ningún usuario. Por defecto, solo los usuarios con el máximo nivel de privilegios (15) tendrán acceso a los comandos de visualización y borrado de los registros de auditoría. De manera adicional, el producto permite la configuración de una serie de eventos que serán mostrados a través de la consola de monitorización de eventos (VISEVEN) a los usuarios autorizados cada vez que se produzcan. Estos eventos serán eventos especiales del sistema y no los registros de auditoría del mismo.
- **AUD.4**: El producto almacena los registros de auditoría en su memoria Flash oculta a los usuarios, de forma que los usuarios autorizados puedan acceder a dicha información a través de los comandos designados para mostrar los registros de auditoría. Ningún usuario podrá acceder al sistema de archivos donde se encuentran almacenados dichos ficheros.
- **AUD.5**: Existe un tamaño máximo de memoria no volátil asignada a los registros de auditoría. Cuando los ficheros de auditoría alcanzan un determinado tamaño se realiza una rotación de ficheros, generando un fichero nuevo y almacenando los más antiguos. Una vez se alcanza el límite de ficheros o el tamaño máximo de la memoria no volátil asignada a los registros de auditoría, se eliminarán los ficheros más antiguos dejando así espacio para los nuevos. Los límites de tamaño de dichos ficheros no son configurables.

5.7 FS. Protección Contra Fallos

Esta función de seguridad mitiga la amenaza **A.FUN**.

Requisitos Cubiertos:

- **PRO.1:** El producto realiza pruebas durante el arranque del mismo para verificar su correcto funcionamiento y para comprobar la integridad del firmware. Dichas pruebas también pueden ser configuradas de manera que se realicen de forma periódica o ejecutadas de manera manual por parte de los usuarios autorizados.

  Dichas pruebas consisten en la verificación del correcto funcionamiento de las funciones criptográficas, incluyendo cifrado simétrico, funciones resumen, generación de números aleatorios,

HMAC, generación de claves RSA y curva elíptica, firmas digitales, intercambio de claves y derivación de claves.

Las pruebas también incluyen la verificación de la integridad del firmware del dispositivo, la BIOS y el software de aplicación.

5.8 FS. Enrutador

Esta función de seguridad mitiga la amenaza **A.FUN**.

El producto proporciona funcionalidad de encaminamiento de tráfico entre los puertos físicos pertenecientes a la red interna (LAN) y el puerto físico perteneciente a la red externa (WAN). El puerto externo se encuentra identificado en la carcasa del dispositivo mediante la etiqueta *"Eth WAN"*.

Requisitos Cubiertos:

- **ROU.1:** El producto permite la administración de sus puertos, habilitando o deshabilitando su uso y configurando diferentes protocolos de calidad de servicio. El producto ofrece la posibilidad de asignar diferentes prioridades al tráfico en base al tipo de tráfico y clasificarlo para asignarle diferentes prioridades que el TOE tendrá en cuenta a la hora de transmitir los paquetes. Adicionalmente, se pueden configurar limitaciones de ancho de banda en cada uno de los puertos del router.
- **ROU.2:** El producto es capaz de reenviar el tráfico y encaminarlo a través de sus puertos a nivel de capa de red (capa 3) del modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) en función de sus tablas de encaminamiento. El TOE soporta protocolos de capa de red como ICMP, IGMP, IPsec, IPv4, IPv6, OSPF y RIP.

5.9 FS. Switch

Esta función de seguridad mitiga la amenaza **A.FUN**.

El dispositivo proporciona funcionalidad de conmutación de tráfico o *switching* en los puertos físicos pertenecientes a la red interna (LAN) del mismo. Dichos puertos se encuentran identificados en la carcasa del dispositivo con la etiqueta *"LAN"* seguida del número de puerto.

Requisitos Cubiertos:

- **SWI.1:** El producto permite la administración de sus puertos, habilitando o deshabilitando su uso y configurando diferentes protocolos de calidad de servicio, de forma que se les pueden asignar diferentes prioridades que el TOE tendrá en cuenta a la hora de transmitir los paquetes.
- **SWI.2**: El producto es capaz de conmutar el tráfico de red a través de los puertos de la red interna a nivel de capa de enlace (capa 2) del modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) según direccionamiento físico o Media Access Control (MAC) utilizando el protocolo Ethernet.
- **SWI.3**: El TOE es capaz de segmentar la red interna en diferentes redes VLAN asignadas a cada puerto, de manera que el tráfico transmitido a través de una de las redes virtuales no puede llegar

a alcanzar a las subredes de las interfaces que no están asignadas a dicha VLAN. El producto soporta la inserción de etiquetas por defecto al tráfico entrante o saliente por los diferentes puertos configurados como parte de una VLAN o la eliminación de dichas etiquetas a través de los puertos de salida. De esta manera, los paquetes etiquetados para una determinada VLAN solo son conmutados a través de los puertos que pertenecen a dicha VLAN. Adicionalmente, el TOE permite configurar un filtro de entrada (*ingress-filter*) que hará que se descarten los paquetes etiquetados con una etiqueta de VLAN a la que no pertenezca el puerto por el que se reciben dichos paquetes.

5.10 Librerías de Terceros

Las siguientes librerías de terceros son empleadas en el TOE para implementar funcionalidad de seguridad:

- OpenSSL 1.1.1.g: Establecimiento de canales seguros (FS. Canales de Comunicación Confiables, FS. Criptografía).
- OpenSSH 4.6p1: Establecimiento de canales seguros para sesiones de administración mediante SSH (FS. Canales de Comunicación Confiables, FS. Criptografía).
- Zlib 1.1.4: Establecimiento de canales seguros para sesiones de administración mediante SSH (FS. Canales de Comunicación Confiables, FS. Criptografía).

6 Evaluaciones con Módulos Opcionales

6.1 (MEC) Listado de Mecanismos Criptográficos

Los algoritmos y funciones criptográficas descritas en esta sección están exclusivamente orientados al establecimiento de canales seguros mediante TLS e IPsec entre el producto y otras entidades para el intercambio de información sensible, a la verificación de la integridad y autenticidad de las actualizaciones, a la protección del almacenamiento de las contraseñas y a la autenticación mediante certificados con entidades de confianza.

Funciones criptográficas proporcionadas:

- Cifrado de la información transmitida a través de los canales seguros.
- Funciones resumen (Hash):
  - Verificación de la integridad de las actualizaciones.
  - Establecimiento de canales seguros.
  - Almacenamiento de contraseñas en el TOE.
- Funciones de derivación de claves:
  - Almacenamiento de contraseñas en el TOE.
- Mensajes de Autenticación en los canales seguros.
- Generación de Claves destinadas al establecimiento de canales seguros y a la autenticación.
- Establecimiento de claves entre el TOE y otras entidades.
- Generación y Verificación de Firmas de los certificados intercambiados durante el establecimiento de canales seguros.
- Verificación de firmas de los ficheros de actualización y del firmware del producto.

Algoritmos empleados:

Operación	Algoritmo	Tamaño de Clave / Longitud de Salida	Estándar
Cifrado Simétrico	AES-CCM AES-GCM AES-CBC AES-CTR	128/256 bits 128/192/256 bits 128/192/256 bits 128/192/256 bits	NIST SP 800-38C SPC8000-38D FIPS PUB 197
Función resumen	SHA-256 SHA-384 SHA-512	256 bits 384 bits 512 bits	FIPS PUB 180-4
Derivación de Claves	PBKDF2-SHA256	256bits	NIST SP 800-132
Mensajes de Autenticación	hmac-sha1 hmac-sha2-256 hmac-sha2-384 hmac-sha2-512	256 bits 512 bits	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”
Generación de Claves	RSA EC (P-256, P-384, P-521)	2048 bits 256, 384, 521	FIPS PUB 186-4

Establecimiento de Claves	ECDHE RSA 3072-bit MODP group 15 (IKEv2) diffie-hellman-group-exchange-sha256 (MODP group 14)	256, 384, 521 bits 2048 bits 3072 bits 2048 bits	NIST PUB 800-56-A REV 3 NIST PUB 800-56-B REV 2 SP 800-135 RFC 3526
Generación y Verificación de Firma Digital	RSA ECDSA	2048 bits 256, 384, 521 bits	FIPS PUB 186-4
Generación de números pseudo-aleatorios	CTR_DRBG(AES)	128/192/256 bits	SP 800-90A

7 Referencias

[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), v2.0 – Marzo 2022
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), v2.0 – Marzo 2022
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC
[CCN-STIC-140-D.1-M]	Taxonomía de productos STIC-Anexo D.1-M: Enrutadores, Enero 2020
[CCN-STIC-140-D.2-M]	Taxonomía de productos STIC-Anexo D.2-M: Switches, Enero 2020
[CCN-STIC-807]	Criptología de empleo en el Esquema Nacional de Seguridad, Abril 2017

8 Acrónimos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema nacional de Seguridad
IPsec	Internet Protocol Security
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEC	Módulo de Evaluación Criptográfica
ST	Security Target- Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	Target of Evaluation – Objeto a Evaluar