Guía de Seguridad de las TIC
CCN-STIC 1471

Procedimiento de Empleo Seguro
Teldat Router

Julio 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.07.28 09:22:47 +02'00'

ÍNDICE

1 INTRODUCCIÓN

1. **Teldat Router** es un dispositivo de red diseñado para proporcionar conectividad en entornos altamente complejos y exigentes. Basado en una arquitectura ARM, este producto es parte de una gama de soluciones que optimizan el rendimiento de las operaciones de **enrutamiento y conmutación entre múltiples redes como LAN, VLAN y WAN, así como funciones de cortafuegos para el control y filtrado del tráfico.**
2. La configuración y gestión de sus funcionalidades se realiza de forma intuitiva mediante una consola de línea de comandos (CLI) o a través de una interfaz web. Estas interfaces permiten acceder y administrar el dispositivo tanto localmente como de manera remota, mediante protocolos seguros como SSHv2 y HTTP sobre TLS 1.2 y TLS 1.3, garantizando así el cumplimiento de los estándares de seguridad establecidos por la normativa LINCE para la categoría Alta del ENS.
3. Teldat Router ofrece distintas funcionalidades destacables en relación con la gestión de la red:
    - Aplicación de reglas: Este producto permite emplear políticas avanzadas de calidad de servicio y control de acceso sobre los flujos de tráfico.
    - Asignación de prioridades: Los administradores pueden determinar prioridades a las tramas entrantes, categorizándolas en colas de prioridad *Urgente*, *Alta*, *Normal* o *Baja* para una mejor gestión del tráfico de red.
    - Capacidad de segmentación VLAN.
    - Creación de *banners*.

2 OBJETO Y ALCANCE

El producto Teldat Router ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF13].

El presente documento tiene como objeto detallar la integración segura del producto Teldat Router en la infraestructura del cliente. Asimismo, especifica las configuraciones necesarias para que el dispositivo cumpla con los estándares establecidos por las taxonomías bajo las cuales se ha cualificado este producto, que incluyen la familia de enrutadores [REF1], familia de switches [REF2] y familia de cortafuegos [REF3].

El alcance del producto evaluado comprende:

- La versión 11.02.04.85.02 del *firmware.*
- Los siguientes modelos *hardware:*
    - Atlas-840, M10-Smart Series, M2 Series, 4GePlus Series, Teldat-5Ge Series, 5Ge-Rail Series, Connect-4GePlus Series, Connect-5Ge Series, Connect-FW Series, Regesta SmartV2 Series, H5 Rail Series.
- Las siguientes interfaces para gestionar su funcionalidad:
    - CLI. Permite tanto acceso local (cable) como remoto mediante el protocolo SSH.
    - Interfaz web. Accesible remotamente a través del protocolo HTTPS.

El dispositivo se conecta a la red externa a través del puerto WAN y a la red interna mediante los puertos LAN. Para información más detallada sobre el método de despliegue y las

especificaciones del entorno seguro, consultar las secciones 4.2 ENTORNO DE INSTALACIÓN SEGURO y 4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN.

3 ORGANIZACIÓN DEL DOCUMENTO

- Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- Apartado 5. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de instalación del producto.
- Apartado 6. En este apartado se recogen las recomendaciones para 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

Las organizaciones interesadas en **Teldat Router** pueden adquirir el dispositivo de red a través de la página web de TELDAT [REF11], acudiendo al apartado "CONTACT US".

Tras la gestión contractual entre la parte interesada y TELDAT, el equipo de TELDAT hará efectivo el envío del producto a la dirección especificada por la parte interesada, aportando el número de seguimiento correspondiente al envío.

En su recepción, la parte interesada deberá poner atención al empaquetado verificando que este no ha sido manipulado durante su transporte. El receptor deberá comprobar que el contenido del paquete se corresponde con lo indicado en la etiqueta de la caja. Si se observa que la etiqueta está rota o no está presente, contacte con el proveedor del producto.

Una vez el producto se ha desempaquetado, compruebe que el modelo y número de serie que aparece en el propio producto coinciden con el modelo y número de serie declarados en el albarán incluido en el paquete.

El producto que se entrega incluye el hardware y el firmware que compone el producto. Junto con el dispositivo, se incluye un impreso con la guía de seguridad y el listado de embalaje. En este último, se proporciona un código QR que da acceso a las guías de instalación y configuración.

Además, es posible acceder a los manuales y documentación técnica a través de la página web oficial de TELDAT visitando la sección de *Support* [REF12].

TELDAT mantendrá la comunicación con las partes interesadas empleando direcciones de correo electrónico bajo el domino @teldat.com asegurando una comunicación directa y eficaz.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Teldat Router debe instalarse en una ubicación física segura, cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa. Se espera que el producto se instale en un rack protegido, dentro de una sala de comunicaciones accesible solo a personal autorizado.

4.3 REGISTRO Y LICENCIAS

Las licencias para Teldat Router se proporcionan de dos formas distintas:

- El cliente recibirá un correo electrónico con las licencias necesarias, estas se encuentran asignadas al número de serie del equipo en específico. Para dar de alta la licencia, el cliente debe cargar el archivo en la memoria flash del router. Una vez finalizada la carga, es necesario reiniciar el dispositivo para aplicar los cambios.
- El cliente recibirá el producto con las licencias ya embebidas, siguiendo la orden del pedido, esta forma de entrega se denomina "*from-factory*".

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

A continuación, se detalla la arquitectura recomendada y los componentes esenciales que deben estar presentes en el entorno de operación de Teldat Router:

- **VLAN y WAN:** Una o más redes VLAN y WAN configuradas para la correcta segmentación y comunicación de la red.
- **Servidor Syslog:** Es indispensable para el almacenamiento de los registros de auditoría, permitiendo el seguimiento y control de eventos.
- **Servidor NTP:** Necesario para proporcionar al dispositivo una sincronización precisa de la hora en tiempo real.

El diagrama presentado proporciona un modelo orientativo para la implementación de la infraestructura del cliente:

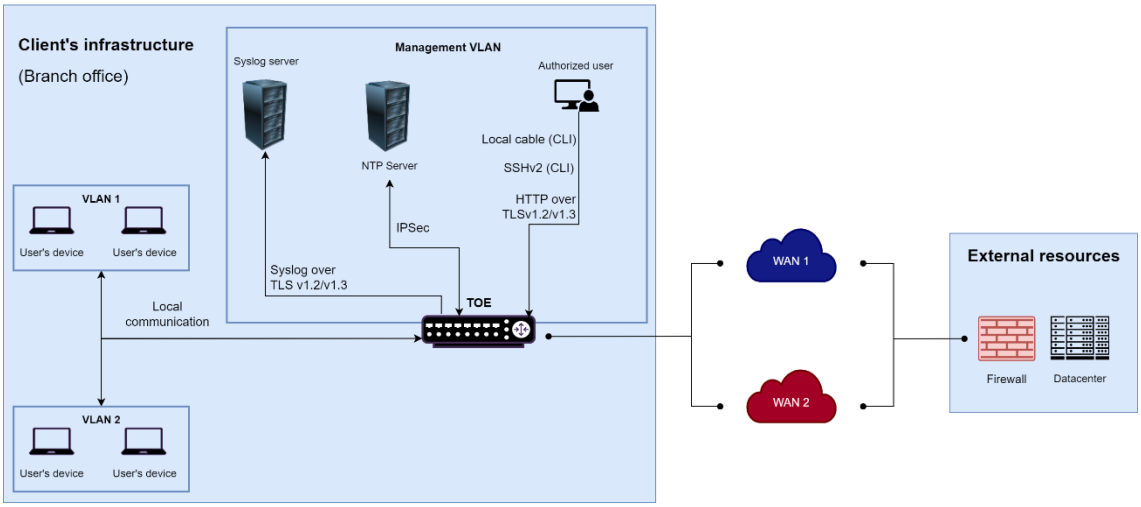

Ilustración 1. Infraestructura del cliente

Teldat Router (TOE en el diagrama), se despliega como router y firewall perimetral, actuando como punto de interconexión entre la red interna del cliente y las redes externas. Los dispositivos de la red interna se conectan al TOE a través de sus puertos físicos LAN, organizados en distintas VLANs para separar lógicamente el tráfico de usuario y el tráfico de gestión. La ubicación específica de estos puertos se detalla en la sección “3.1 Components” de la guía de instalación de Teldat Router [REF4].

El TOE permite que la red interna del cliente se encuentre segmentada en distintas VLANs para organizar el tráfico de usuario y facilitar la separación lógica de los distintos dominios de red. Además, el TOE aplica funciones de control y filtrado del tráfico, proporcionando protección perimetral básica en el acceso a redes externas.

El diagrama representa un escenario empresarial típico, en el que el TOE se despliega en una sede remota, integrándose con una infraestructura central o datacenter corporativo. Este modelo es habitual en entornos con múltiples sedes, donde cada emplazamiento dispone de su propio punto de acceso perimetral. En este caso de uso, la conectividad externa se realiza mediante dos interfaces WAN (WAN 1 y WAN 2), que dota al despliegue de redundancia y alta disponibilidad.

Aunque el diagrama ilustre un escenario corporativo con conexión a un datacenter, la misma arquitectura es igualmente válida para acceso redundante a Internet, manteniendo al TOE

como único punto de salida y entrada de la red interna y garantizando un acceso controlado y resiliente.

4.5 CONSIDERACIONES PREVIAS

Para que las configuraciones descritas en las secciones 5 FASE DE INSTALACIÓN y 6 FASE DE CONFIGURACIÓN se implementen es necesario seguir los siguientes pasos:

- Salvar la configuración ejecutando el comando `save` desde el proceso CONFIG.
- Regresar al modo inicial, mediante el comando `root` o presionando las teclas "*Ctrl + P*".
- Reiniciar el dispositivo empleando el comando `restart`.

5 FASE DE INSTALACIÓN

5.1 INSTALACIÓN DEL PRODUCTO

Teldat Router será instalado físicamente conforme las indicaciones que se describen en la guía de instalación [REF4] que TELDAT facilita junto al producto.

Nota: Durante este paso se deberá realizar el conexionado necesario para el correcto funcionamiento del producto; sin embargo, deberá evitarse su conexión a Internet hasta que se completen los pasos descritos en la sección 5.3 MODO DE OPERACIÓN SEGURO de este documento.

5.2 COMPROBACIÓN DE LA VERSIÓN

Con el objetivo de comprobar la versión instalada y asegurar el uso de la versión cualificada, se deberán seguir los siguientes pasos:

El administrador deberá acceder al dispositivo mediante la consola local, siguiendo los pasos indicados en la sección "*A.3.1 Connecting using the local console (AUX connector)"* de la guía de instalación [REF4].

Una vez se haya iniciado la conexión a través de la consola local, el usuario deberá comprobar la versión del producto. Para ello, se deberá consultar la sección "*3.2.31 VERSION"* de la guía de configuración y monitorización del producto [REF5]. En esta, se encuentra toda la información necesaria para ejecutar el comando que muestra la versión del producto.

El administrador a cargo de la instalación debe comprobar que la versión mostrada en la CLI se corresponda con la versión cualificada para el *firmware*.

Las distintas versiones se encuentran disponibles en el portal de soporte [REF12], previo registro del cliente. Si la versión instalada en el dispositivo no coincide con la cualificada y fuera anterior a esta, el administrador deberá descargar la versión cualificada desde el portal de soporte.

Una vez descargado el paquete de actualización, se deberán seguir los pasos indicados en la sección 6.6 ACTUALIZACIONES de este documento para proceder con la instalación del nuevo firmware.

5.3 MODO DE OPERACIÓN SEGURO

Antes de conectar el producto a una red con acceso a internet, es imprescindible activar el **modo ENS-HIGH** para garantizar el cumplimiento con los estándares de seguridad exigidos por la normativa LINCE para categoría Alta del ENS.

5.3.1 ACTIVACIÓN DEL MODO ENS-HIGH

Una vez dentro del dispositivo (a través de la interfaz CLI), el administrador deberá ingresar al modo de configuración utilizando el comando `config`.

Para activar el modo ENS-HIGH, se deberá ejecutar el siguiente comando: `set configuration-mode ens-high`. Una vez aplicado, es necesario guardar los cambios utilizando el comando `save`.

Tras el primer acceso y para salvar los cambios, será necesario crear un usuario, para ello el administrador debe seguir la sección "*2.4.40 USER"* de la guía de configuración y monitorización del producto [REF5]. La contraseña deberá cumplir los requisitos descritos en la sección 6.1.3 CONFIGURACIÓN DE ADMINISTRADORES.

Finalmente, para que la configuración del modo ENS-HIGH quede activada en el dispositivo, se debe regresar al modo inicial de la consola mediante el comando `root` o presionando las teclas "*Ctrl + P*". Posteriormente, será necesario reiniciar el dispositivo empleando el comando `restart`.

Activado el modo ENS-HIGH, el producto estará listo para conectarse a internet a través de su interfaz WAN. A partir de este punto, se podrá continuar con el proceso de instalación y configuración restante, garantizando una operación segura del dispositivo.

6 FASE DE CONFIGURACIÓN

6.1 ADMINISTRACIÓN DEL PRODUCTO

6.1.1 ADMINISTRACIÓN DE LA INTERFAZ DE USUARIO

La consola de administración de Teldat Router presenta varios procesos:

- **Proceso GESTCON**. Es la primera consola que se muestra al administrador al iniciar sesión. A través de esta, se puede acceder a los demás procesos del sistema, sirviendo como el punto de partida para la administración del dispositivo.
- **Proceso MONITOR**. Permite al usuario monitorizar, supervisar el estado y las estadísticas del dispositivo.
- **Proceso CONFIG**. Desde esta consola se permite modificar todos los parámetros de configuración del dispositivo, sin aplicarse en tiempo real, incluyendo la asignación de direcciones de red, creación de *banners* y la gestión de eventos. Para que se apliquen los cambios es necesario guardar la configuración con el comando `save` y reiniciar el dispositivo.
- **Proceso RUNNING-CONFIG**. Permite modificar la configuración del dispositivo en tiempo real. Los cambios realizados a través de este proceso se aplican de inmediato, pero deben guardarse con el comando `save` para que persistan después del reinicio.
- **Proceso VISEVEN**. Permite monitorizar los eventos que ocurren en el sistema. Dichos eventos deben estar previamente configurados desde otros procesos para que puedan ser visualizados aquí.

Para más información acudir a la sección "*1.3.3 User Interface Processes*" y siguientes de la guía de configuración y monitorización del producto [REF5].

6.1.2 CANALES DE ADMINISTRACIÓN LOCAL Y REMOTA

En la administración local de Teldat Router se emplea una consola (CLI), el acceso es mediante un puerto físico que permite a los administradores interactuar con el producto sin necesidad de una red o conexión remota.

En el caso de la administración remota del producto es posible mediante dos canales:

- Acceso remoto mediante CLI. Para configurar que el protocolo empleado en esta comunicación es SSHv2, un mecanismo seguro, debe accederse al proceso CONFIG y configurarse lo siguiente: `feature ssh > server > enable`.
- Acceso remoto mediante interfaz web vía HTTPS. El protocolo que debemos configurar para esta comunicación es HTTP sobre TLS v1.2 y/o superior. Por lo que, tras acceder al proceso CONFIG, se ejecuta el siguiente comando: `feature http > secure-server enable > secure-server dont-verify`.

Los mecanismos criptográficos se encuentran aceptados siguiendo el criterio de la guía CCN-STIC-807 [REF6], por lo que no será necesario ajustar los mecanismos por parte del cliente.

6.1.3 CONFIGURACIÓN DE ADMINISTRADORES

La configuración de los roles de usuario que permite el producto se encuentra detallado en la sección "*2.4.40 USER*" de la guía de configuración y monitorización [REF5]. La descripción de los roles se encuentra en la sección 6.2.1 NIVELES DE ACCESO del presente documento.

Para garantizar que Teldat Router cumple con los requisitos establecidos por la normativa, es esencial que el administrador tenga en cuenta los siguientes aspectos:

- Configuración de **contraseñas** seguras. Para cumplir con los estándares de seguridad del CCN, las contraseñas deben seguir la siguiente política:
  - Longitud mínima: La contraseña debe tener al menos doce caracteres.
  - Composición: La contraseña debe incluir una combinación de mayúsculas, minúsculas, números y símbolos especiales.

  El producto sigue esta política al activarse el **modo ENS-HIGH**.
- Configuración del **tiempo de inactividad**. Para proteger el acceso no autorizado, se debe configurar el tiempo máximo de inactividad de la sesión en cinco minutos.
  - En la CLI se establece con el siguiente comando desde el proceso CONFIG: `set inactivity-timer 5`
  - En la interfaz web, el periodo de inactividad predeterminado es de cinco minutos.
- Configuración de **intentos fallidos de autenticación.** Para prevenir ataques de fuerza bruta, el número máximo de intentos fallidos de autenticación debe limitarse a tres intentos.
  - Para la consola local se configura con el comando desde el proceso CONFIG: `set console > login attempts 3`
  - En el servidor SSHv2 debe configurar el número máximo de sesiones para evitar ataques de fuerza bruta. Para ello, se deben ejecutar los siguientes comandos:

    ```
    feature ssh
        server
            max-connections 1
        exit
    exit
    ```

  - En segundo lugar, se establece el número de intentos fallidos empleando el comando desde el proceso CONFIG: `feature ssh > server > max-auth-tries 3`
  - En la interfaz web, el sistema predeterminado permite tres intentos de autenticación antes de bloquear el acceso.

6.2 AUTENTICACIÓN

En esta sección se detallan los mecanismos de autenticación que implementa Teldat Router para garantizar que únicamente los usuarios autorizados pueden acceder a la gestión y monitorización del dispositivo:

- **Autenticación de usuarios**: El acceso a Teldat Router se gestiona a través de credenciales almacenadas localmente en el dispositivo. Cada usuario debe autenticarse utilizando su nombre de usuario y contraseña, cumpliendo con las políticas de seguridad configuradas en la sección anterior.

- **Autenticación entre comunicaciones:** El producto utiliza certificados digitales para autenticar las comunicaciones establecidas con los componentes del entorno. Estos certificados se gestionan en la sección 6.4 GESTIÓN DE CERTIFICADOS.
- **Autenticación de sesiones SSHv2:** Para las conexiones remotas, el dispositivo soporta la autenticación basada tanto en clave pública, como haciendo uso de contraseña. Para obtener más información sobre como configurar la autenticación por clave pública para el protocolo SSH, acudir a la guía *SSH protocol* [REF10].
  La clave pública que se establezca debe estar en conformidad con la guía 807 de CCN [REF6].

6.2.1 NIVELES DE ACCESO

Teldat Router establece por defecto un valor de 0 a 15 para indicar el nivel de acceso del usuario. Los niveles superiores tienen permisos adicionales a los niveles inferiores, existen cinco niveles de acceso predefinidos que resultan equiparables al rol de los usuarios:

- **NONE [0]:** No permite al usuario acceder al sistema.
- **EVENTS [1]:** El usuario únicamente puede acceder a la consola de administración y a la vista de eventos, pero no tiene permisos de administración.
- **MONITOR [5]:** Acceso a la consola de administración, vista de eventos y monitorización. No tendrá acceso a la función de reinicio y carga.
- **CONFIG [10]:** Este nivel de privilegio otorga acceso a todos los procesos y comandos estándar a través de la CLI y la interfaz web, a excepción de los comandos de administración de usuarios.
- **ROOT [15]:** Acceso a todos los procesos y comandos del sistema, además tiene acceso a la gestión de usuarios a través de la CLI y la interfaz web.

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Para garantizar el uso seguro del producto es necesario configurar correctamente las interfaces, puertos y servicios que soportan la comunicación y la administración del dispositivo.

6.3.1 CONTROL DE ACCESO A PUERTOS

Para prevenir ataques de inundación MAC, es necesario definir un control de acceso a todos los puertos abiertos siguiendo los comandos:

```
Config > network <interfaz_ethernet_1> repeater-switch

port <num> access-control > maximum 200
```

6.3.2 CONFIGURACIÓN CALIDAD DE SERVICIO

El sistema de calidad de servicio (QoS) de Teldat Router gestiona el tráfico basado en un esquema de colas que clasifica el tráfico en cuatro categorías: Urgente, Alta, Normal y Baja.

Este sistema se puede configurar siguiendo la guía de administración de interfaces LAN del producto [REF7].

6.3.3 CONFIGURACIÓN DE TERMINACIÓN DE SESIÓN TCP

Para garantizar que el TOE no acepte paquetes pertenecientes a una sesión TCP finalizada, es necesario ejecutar los siguientes comandos desde el proceso CONFIG, una vez conectado vía SSH con el TOE:

```
feature afs

time-out tcp time-wait 5s
```

6.3.4 PROTECCIÓN DE LA RED INTERNA

Para que Teldat Router funcione como router y firewall perimetral, será necesario activar el sistema AFS (Advanced Firewall System) y configurar las interfaces WAN estableciendo las siguientes reglas de NAT:

- Activación de AFS:

```
feature afs > enable
```

- Configuración de WAN 1:

```
network <interfaz_WAN_1>
ip afs firewall in

protocolo ip
nat
rule 1 out <interfaz_WAN_1> dynamic overload
rule 1 translation source interface <interfaz_WAN_1>
```

- Configuración de WAN 2:

```
network <interfaz_WAN_2>
ip afs firewall in
```

```
protocolo ip
nat
rule 2 out <interfaz_WAN_2> dynamic overload
rule 2 translation source interface <interfaz_WAN_2>
```

6.3.5 VLAN DE GESTIÓN

Se recomienda la creación de una VLAN dedicada al tráfico de gestión del Teldat Router con el objetivo de aislar las comunicaciones de administración del resto de redes. En el entorno cualificado, la segmentación se implementa mediante la creación de una VLAN 25 asociada a la interfaz ethernet0/0, así como la correspondiente subinterfaz ethernet0/0.25.

Adicionalmente, se deberá configurar un mecanismo que permita identificar y filtrar el tráfico asociado a la VLAN de gestión mediante una política de clasificación y una lista de control de acceso aplicada al sistema, de forma que únicamente el tráfico procedente de dicha VLAN pueda acceder a los servicios de administración del dispositivo. En consecuencia, los servicios de gestión, como SSH y HTTPS, así como las comunicaciones de Syslog y NTP que se encuentren configuradas, deberán desplegarse o ser accesibles exclusivamente a

través de esta VLAN de gestión, garantizando así el aislamiento del tráfico administrativo respecto al resto de redes. Dichas configuraciones se describen en las secciones 6.1.2, 6.3.7 y 6.5.2 de este documento.

Las configuraciones mencionadas se realizarán aplicando los siguientes comandos en el módulo de configuración del producto:

```
config
  feature vlan
    enable
  vlan 25 ethernet0/0 port <port_number>
  vlan 25 ethernet0/0 port internal
  exit
add device eth-subinterface ethernet0/0 25
feature access-lists
  access-list 200
    entry 1 default
    entry 1 permit
    entry 1 label 25
    entry 2 default
    entry 2 permit
    entry 2 source port-range 53 53
    entry 2 protocol udp
    entry 3 default
    entry 3 permit
    entry 3 destination port-range 53 53
    entry 3 protocol udp
  exit
exit
network ethernet0/0
  ip address <ip_local> <netmask>
exit
network ethernet0/0.25
  ip address <ip_vlan_management> <netmask>
  ip policy route-map VLAN_MANAGEMENT
  encapsulation dot1q 25
exit
feature route-map
  route-map "VLAN_MANAGEMENT"
```

```
    entry 1 default
    entry 1 permit
    entry 1 set label 25
  exit
exit
protocol ip
  local access-group 200 in
exit
```

6.3.6 LISTAS DE CONTROL DE ACCESO

Con el fin de que todas las reglas IPv4 sean verdaderamente "stateful" y se descarten automáticamente los paquetes malformados, así como cualquier paquete cuyo origen pertenezca a rangos de broadcast, multicast o loopback; paquetes con direcciones de origen o destino en rangos de enlace local o reservados para uso futuro; y paquetes que contengan opciones IP como "Loose Source Routing", "Strict Source Routing" o "Record Route", las listas de control de acceso IPv4 creadas deben incluir obligatoriamente las siguientes entradas:

```
entry 1 permit
entry 1 session state established
entry 2 deny
entry 2 source address <IP-NETWORK-BROADCAST>
entry 3 deny
entry 3 source address range 224.0.0.0 239.255.255.255
entry 4 deny
entry 4 source address range 127.0.0.0 127.255.255.255
entry 5 deny
entry 5 source address range 169.254.0.0 169.254.255.255
entry 6 deny
entry 6 destination address range 169.254.0.0 169.254.255.255
entry 7 deny
entry 7 source address 0.0.0.0
entry 8 deny
entry 8 destination address 0.0.0.0
entry 9 deny
```

```
entry 9 source address range 240.0.0.0 255.255.255.254
entry 10 deny
entry 10 destination address range 240.0.0.0 255.255.255.254
entry 11 deny
entry 11 opts-field lsr
entry 12 deny
entry 12 opts-field rr
entry 13 deny
entry 13 opts-field ssr
…
```

De forma similar, de cara que todas las reglas IPv6 sean stateful, también es necesario permitir los paquetes ICMPv6 utilizados para "Neighbor Discovery", de modo que el protocolo pueda funcionar correctamente. Para descartar los paquetes cuya dirección de origen y destino se definen como una dirección no especificada o local de enlace, las listas de acceso IPv6 deben incluir obligatoriamente las siguientes entradas:

```
entry 1 permit
entry 1 session state established
entry 2 permit
entry 2 protocol ipv6-icmp 135 0
entry 3 permit
entry 3 protocol ipv6-icmp 136 0
entry 4 deny
entry 4 source address ::/128
entry 5 deny
entry 5 destination address ::/128
entry 6 deny
entry 6 source address 4000::/3
entry 7 deny
entry 7 destination address 4000::/3
entry 8 deny
entry 8 source address 0100::/8
entry 9 deny
entry 9 destination address 0100::/8
```

```
entry 10 deny
entry 10 source address 0200::/7
entry 11 deny
entry 11 destination address 0200::/7
entry 12 deny
entry 12 source address 0400::/6
entry 13 deny
entry 13 destination address 0400::/6
entry 14 deny
entry 14 source address 0800::/5
entry 15 deny
entry 15 destination address 0800::/5
entry 16 deny
entry 16 source address 1000::/4
entry 17 deny
entry 17 destination address 1000::/4
entry 18 deny
entry 18 source address 6000::/3
entry 19 deny
entry 19 destination address 6000::/3
entry 20 deny
entry 20 source address 8000::/3
entry 21 deny
entry 21 destination address 8000::/3
entry 22 deny
entry 22 source address A000::/3
entry 23 deny
entry 23 destination address A000::/3
entry 24 deny
entry 24 source address C000::/3
entry 25 deny
```

```
entry 25 destination address C000::/3
entry 26 deny
entry 26 source address E000::/4
entry 27 deny
entry 27 destination address E000::/4
entry 28 deny
entry 28 source address F000::/5
entry 29 deny
entry 29 destination address F000::/5
entry 30 deny
entry 30 source address F800::/6
entry 31 deny
entry 31 destination address F800::/6
entry 32 deny
entry 32 source address FE00::/9
entry 33 deny
entry 33 destination address FE00::/9
entry 34 deny
entry 34 source address FEC0::/10
entry 35 deny
entry 35 destination address FEC0::/10
entry 36 deny
entry 36 source address fe80::/10
entry 37 deny
entry 37 destination address fe80::/10
…
```

Para asignar dichas listas de acceso a una interfaz, se podrá hacer uso de los siguientes comandos:

```
network ethernet<interface>
ip access-group <IPv4-access-list> <in/out>
ipv6 access-group <IPv6-access-list> <in/out>
```

6.3.7 SERVIDOR NTP

Para asegurar la comunicación entre Teldat Router y el servidor NTP utilizando IPSec, se debe sincronizar la fecha y hora manualmente desde el módulo de configuración de la CLI como paso inicial: `Config > time set <mes> <día> <año> <día_de_la_semana> <hora> <minuto> <segundos>.`

De forma similar, para sincronizar el horario de verano será necesario aplicar el siguiente comando, desde la misma interfaz: `time summer-time recurring <start week number> sun mar 02:00 <final week number> sun oct 03:00.`

Tras ello, será necesario establecer la siguiente política:

```
config
   feature access-lists
      access-list 100
         entry 1 default
         entry 1 permit
         entry   1   source   address   <ip_vlan_management>
255.255.255.255
         entry  1  destination  address  <ip_vlan_server_ntp>
255.255.255.255
         entry 1 destination port-range 123 123
         entry 1 protocol udp
;
      exit
   exit
   protocol ip
;
      ipsec
         enable
         assign-access-list 100
;
         template 2 dynamic esp aes256 sha512
         template 2 negotiation-protocol ikev2
         template 2 source-address <ip_vlan_management>
         template 2 destination-address <ip_vlan_server_ntp>
;
         template 3 ikev2 encryption aes256
         template 3 ikev2 authentication sha512
         template 3 ikev2 prf sha512
         template 3 ikev2 group fifteen
         template 3 destination-address <ip_vlan_server_ntp>
         template 3 ike natt-version rfc
         template 3 ike method local rsa
         template 3 ike method remote rsa
         template 3 ike rsa-sign-hash prf
        template 3 ike idtype asn-dn
         template 3 keepalive dpd
         template 3 ike ca <certificate_ca_filename>
         template 3 ike fragmentation disable
;
         map-template 100 2
```

```
; -- In order to accept self-signed certificates, the
following command is required --
 advanced self-signed-cert accepted
      exit
;
   exit
;
   feature ntp
      protocol
      poll-interval 16
      peer address 1 <ip_vlan_server_ntp>
   exit
       ;

   feature dns
      servers-checking
   exit
```

Tras estos pasos el producto se sincronizará automáticamente con el servidor NTP.

6.4 GESTIÓN DE CERTIFICADOS

Teldat Router permite la gestión de certificados personalizados para las comunicaciones: HTTPS, Syslog sobre TLS e IPSec. Estos certificados se deben cargar en el dispositivo a través de SFTP en el directorio `/DSK/`.

El administrador empleará la CLI para importar los certificados, soporta tanto el formato PKCS12 como el PEM. Estos se importan desde el módulo de configuración (`config`), ejecutando los siguientes pasos:

- Importación de certificados en PKCS12:

```
protocol ip > ipsec > cert > certificate
<nombre_del_fichero> pkcs12 import > certificate
<nombre_del_fichero> load
```

- Importación de certificados en PEM:

```
protocol ip > ipsec > cert > certificate
<nombre_del_fichero> load
```

También es posible cargar un certificado en formato PEM a través de la interfaz web, para este caso el administrador deberá seguir los siguientes pasos:

- Acceder al panel de configuración.
- Navegar al panel de VPN.
- Acceder al panel de certificados.
- Subir el archivo del certificado.

Para que el TOE pueda verificar el estado de revocación de los certificados, es necesario proporcionarle una CRL. El producto permite dos formas de hacerlo:

- Aplicar una CRL de forma remota mediante una URL HTTP incluida en el certificado: Una vez conectado a través de SSH con el TOE, es necesario ejecutar los siguientes comandos desde el proceso CONFIG:

```
feature syslog
crl mode strict
```

Cabe destacar que para la evaluación del producto se ha llevado a cabo la opción remota.

- Uso de una CRL local: Para llevar a cabo el procedimiento de forma manual y cargar la CRL localmente, es preciso seguir los siguientes pasos:
  - Cargar el fichero de la CRL en el dispositivo a través de SFTP en el directorio /DSK/.
  - Cargar la CRL en el almacén local de CRLs del equipo. Para ello, desde el proceso CONFIG es necesario ejecutar los siguientes comandos:

```
protocol ip
ipsec
cert
crl
load <nombre_del_fichero>
```

  - Asociar la CRL a la funcionalidad syslog. Para ello desde el proceso CONFIG ejecutar los siguientes comandos:

```
feature syslog
crl mode strict
crl name <nombre_crl>
```

Por último, los mecanismos criptográficos importados deben cumplir con las especificaciones de la guía CCN-STIC-807 siendo únicamente validos los siguientes mecanismos criptográficos:

- ECDSA con curvas P-256 o superior.
- Funciones Hash SHA-256 o superior.

6.5 AUDITORÍA

6.5.1 REGISTRO DE EVENTOS

Teldat Router es un producto capaz de generar, almacenar y transmitir la información de aquellos eventos que tienen lugar durante la operación del dispositivo.

El acceso a los registros de eventos del producto se encuentra limitado, por lo que sólo los usuarios con el nivel de acceso ROOT [15] podrán visualizar y eliminar la información guardada en los registros de auditoría a través de la CLI. Para visualizarlos, será necesario ejecutar el siguiente comando:

```
p 3 > event > security-traces show
```

6.5.2 ALMACENAMIENTO

Para garantizar el almacenamiento de los registros, el producto sobrescribe aquellos más antiguos para evitar que el almacenamiento interno llegue a su máxima capacidad.

Teldat Router almacena los detalles de auditoría tanto internamente, en su memoria flash, como en un servidor Syslog externo. Para asegurar la transmisión de esa información, el canal empleará TLS v1.2/v1.3 como protección, por lo que será necesario ejecutar los siguientes comandos en el lado del dispositivo:

```
config
feature syslog
      enable
      server <ip_vlan_server_syslog> port 6514 protocol tcp
tcp-secure-enable
     ca ca-name <certificate_ca>
 ;
     severity debug
 exit
 ;
```

Para más información sobre la integración de Teldat Router y el servidor de registros, acudir a la guía *Syslog Client* del producto [REF8].

6.5.3 CONFIGURACIÓN DE LOS PARÁMETROS DE LOGGING

Para recuperar todos los registros necesarios al examinar el registro en el TOE, ejecute los siguientes comandos desde el proceso CONFIG para configurarlo:

```
event
enable security-traces default
enable trace subsystem IKE ALL
enable trace subsystem NTP ALL
enable trace subsystem SMGT ALL
enable trace subsystem SYSLOG ALL
disable trace subsystem SSH ALL
disable trace subsystem TCP ALL
disable trace subsystem IP ALL
enable trace event AFS.002
enable trace event AFS.004
enable trace event AFS.013
```

```
enable trace event AFS.014
enable trace event AFS.015
enable trace event AFS.020
enable trace event AFS.022
enable trace event AFS.031
enable trace event AFS.032
enable trace event AFS.033
enable trace event AFS.038
enable trace event AFS.039
enable trace event AFS.040
enable trace event AFS.041
enable trace event AFS.046
enable trace event AFS.055
enable trace event AFS.072
enable trace event AFS.078
enable trace event AFS.106
enable trace event AFS.118
enable trace event AFS.119
enable trace event AFS.120
enable trace event AFS.121
enable trace event AFS.123
enable trace event IP6.071
enable trace event IP6.084
enable syslog event SSL.002
enable syslog event SSH.006
enable syslog event SSH.007
enable syslog event SSH.008
enable syslog event SSH.015
enable syslog event SSH.016
enable syslog event SSH.017
enable syslog event SSH.018
```

```
enable syslog event SSH.033
enable syslog event SSH.035
enable syslog event SSH.043
enable syslog event SSH.044
enable syslog event SSH.046
enable syslog event SSH.078
enable syslog event SSH.081
enable syslog event SSH.082
enable syslog event SSH.083
enable syslog event SSH.084
enable syslog event SSH.085
enable syslog event SSH.086
enable syslog event SFTP.001
enable syslog event ETH.050
enable syslog event ETH.051
enable syslog event NTP.003
enable syslog event NTP.016
enable syslog event NTP.027
enable syslog event NTP.029
enable syslog event NTP.030
enable syslog event NTP.031
enable syslog event NTP.040
enable syslog event NTP.042
enable syslog event NTP.043
enable syslog event NTP.044
enable syslog event NTP.045
enable syslog event NTP.047
enable syslog event NTP.048
enable syslog event NTP.068
enable syslog event NTP.070
enable syslog event NTP.071
```

```
enable syslog event NTP.072
enable syslog event NTP.076
enable syslog event NTP.077
enable syslog event NTP.079
enable syslog event IPSEC.020
enable syslog event IPSEC.021
enable syslog event IPSEC.039
enable syslog event IPSEC.050
enable syslog event IPSEC.051
enable syslog event IPSEC.052
enable syslog event IPSEC.053
enable syslog event IKE.011
enable syslog event IKE.012
enable syslog event IKE.036
enable syslog event IKE.037
enable syslog event IKE.038
enable syslog event IKE.039
enable syslog event IKE.040
enable syslog event IKE.041
enable syslog event IKE.048
enable syslog event IKE.049
enable syslog event IKE.083
enable syslog event IKE.085
enable syslog event GW.052
enable syslog event GW.053
enable syslog event GW.081
enable syslog event GW.082
enable syslog event GW.083
enable syslog event GW.084
enable syslog event GW.085
enable syslog event GW.086
```

```
enable syslog event CNSL.019
enable syslog event CNSL.020
enable syslog event HTTP.026
enable syslog event HTTP.027
enable syslog event HTTP.028
enable syslog event HTTP.029
enable syslog event SYSLOG.009
enable syslog event SYSLOG.010
enable syslog event SYSLOG.011
enable syslog event SYSLOG.012
enable syslog event SYSLOG.013
enable syslog event SYSLOG.014
enable syslog event SYSLOG.015
enable syslog event SYSLOG.016
enable syslog event SYSLOG.017
enable syslog event SYSLOG.018
```

6.6 ACTUALIZACIONES

Las actualizaciones se realizan mediante la carga del archivo de firmware actualizado en el sistema, y sólo los usuarios con nivel de acceso CONFIG [10] o ROOT [15] pueden realizar estas actualizaciones.

El protocolo SFTP es el que emplea Teldat Router para garantizar la seguridad de los paquetes de actualización, la configuración para este protocolo se encuentra descrita en la sección "*1.7 SFTP clients*" de la guía de actualización que facilita TELDAT [REF9].

Los pasos para realizar la actualización del producto son los siguientes:

- El administrador con nivel de acceso ROOT [15] podrá subir el nuevo firmware al dispositivo empleando el siguiente comando:

```
put <firmware filename> /MEM/cit.bin

rename /MEM/cit.bin /DSK/APPCODE1.BIN
```

- Desde la CLI, tanto un usuario con nivel de acceso ROOT [15] como con nivel de acceso CONFIG [10], podrá ejecutar la actualización con el comando: `load immediate yes`

Antes de instalar el nuevo firmware, el producto autentica la actualización utilizando una firma digital ECDSA-SHA256. Si la firma no es válida, el dispositivo rechazará la actualización y no sobrescribirá el firmware existente.

Por último, se recomienda realizar actualizaciones periódicas de firmware a versiones posteriores a la cualificada, siempre que dichas actualizaciones no afecten a las funcionalidades de seguridad del producto y prestando especial atención a aquellas versiones que corrijan nuevas vulnerabilidades.

6.7 AUTO-CHEQUEOS

Teldat Router es un producto que es capaz de realizar auto-chequeos (*self-test*) durante su proceso de arranque. Estos permiten verificar la integridad del firmware, asegurando que no han sido alterados y que el sistema se inicia en un estado confiable.

En caso de que durante estos auto-chequeos se detecte una anomalía o corrupción del firmware, el equipo entrará en un estado de error e impedirá su uso. Para recuperarlo, será necesario cargar un firmware válido directamente desde la BIOS a través de una conexión serie con el equipo. Este método de carga de firmware solo deberá utilizarse en este caso excepcional.

6.8 BACKUP

Teldat Router permite la realización de copias de seguridad del firmware almacenado en la memoria flash del dispositivo. El equipo admite la coexistencia de múltiples imágenes de firmware en dicha memoria. Como procedimiento de respaldo, el administrador podrá copiar la imagen de firmware activa asignándole un nombre diferente mediante el comando “file copy”, conservarla como versión de recuperación y, posteriormente, proceder a la carga de una nueva versión de firmware y al reinicio del dispositivo.

En caso de que, tras el proceso de arranque, se detecte un funcionamiento anómalo de la nueva versión instalada, la BIOS del equipo realizará automáticamente la búsqueda de otras imágenes de firmware disponibles en memoria e intentará el arranque con ellas. Este mecanismo permite la recuperación del servicio mediante la ejecución de una versión previamente validada y almacenada como respaldo.

Nota: Cuando el equipo opere en modo ENS Alta y el fallo detectado durante el arranque esté relacionado con la verificación de integridad del firmware, se aplicará el comportamiento descrito en el apartado 6.7 AUTO-CHEQUEOS. En tal circunstancia, el dispositivo entrará en estado de error y no procederá al arranque automático con la imagen de respaldo.

7 REFERENCIAS

[REF1] Enrutadores (CCN-STIC-140-D1)

[REF2] Switches (CCN-STIC-140-D2)

[REF3] Cortafuegos (CCN-STIC-140-D3)

[REF4] Teldat Installation Manual

[REF5] Teldat Configuration and Monitoring

[REF6] Criptología de empleo en el Esquema Nacional de Seguridad (CCN-STIC-807)

[REF7] LAN interfaces - Teldat Dm709-I

[REF8] Syslog Client-Teldat-Dm 753-I

[REF9] Software Updating Quick Guide – Teldat-Dm 835-I

[REF10] SSH Protocol – Teldat-Dm 787-I

[REF11] Teldat – Official Website

[REF12] Teldat - Customer Global Support Portal

[REF13] CPSTIC

8 ABREVIATURAS

ARM	Advanced RISC Machine
CCN	Centro Criptológico Nacional
CLI	Command-Line Interface
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
LAN	Local Area Network
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
MAC	Media Access Control
NAT	Network Address Translation
NTP	Network Time Protocol
PEM	Privacy-Enhanced Mail
PKCS12	Public Key Cryptography Standards #12
QoS	Quality of Service
QR	Quick Response
RSA	Rivest–Shamir–Adleman
SFTP	Secure File Transfer Protocol
SFTP	SSH File Transfer Protocol
SHA	*Secure Hash Algorithm*

SSH	Secure Shell
STIC	Sistema de Tecnologías de la Información y las Comunicaciones
TLS	Transport Layer Security
TOE	Target of Evaluation
VLAN	Virtual Local Area Networks
VPN	Virtual Private Network
WAN	Wide Area Network