centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1455

Procedimiento de empleo seguro
Teldat M1 Series

Agosto de 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-285-5.
Fecha de Edición: agosto de 2023.

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.15 12:03:08 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

ILUSTRACIONES

1. INTRODUCCIÓN

1. El dispositivo **Teldat M1 Series** es una plataforma de encaminamiento (*routing*) y conmutación (*switching*) de paquetes que provee conectividad entre diversas redes y entre dispositivos pertenecientes a la misma subred.
2. El producto provee capacidades de administración local mediante puerto serie y administración remota a través del protocolo seguro SSH.
3. 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 + Ehternet, Fibra + Ethernet + VDSL, Ethernet + Serie, conmutador local de hasta 12 puertos, y opción 3G/4G.
4. El producto proporciona un control de la conectividad entre dos o más entornos de red, siendo capaz de enrutar el tráfico entre las distintas redes y de aplicar distintas reglas de calidad de servicio y control de acceso sobre los flujos de tráfico que se generan entre las mismas.

2. OBJETO Y ALCANCE

5. En la presente guía se recoge el procedimiento de empleo seguro de la plataforma de encaminamiento y conmutación de tráfico **Teldat-M1 Series,** versión **software 11.01.x**.

6. Dicha plataforma ha sido **cualificada e incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional**, en las familias de “Enrutadores” y “Switches”. Se debe consultar el CPSTIC para saber la versión de *software* cualificada en cada momento.

3. ORGANIZACIÓN DEL DOCUMENTO

7. El presente documento se divide en tres partes fundamentales, de acuerdo a las distintas fases que componen el ciclo de vida del producto:

   a) **Apartado 4**. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación física** del producto.

   b) **Apartado 5**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

   c) **Apartado 6**. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **operación y mantenimiento**.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Para asegurar una correcta recepción del producto será necesario revisar que no ha sido manipulado durante su transporte. Para ello, se llevarán a cabo los siguientes pasos:

    a) Comprobar que la caja tiene una etiqueta blanca con un código de barras, número de serie y modelo y otra información relacionada con el contenido de la caja. El objetivo de esta etiqueta es evitar la alteración del interior del paquete. Si se observa que la etiqueta está rota o no está, se debe contactar con el proveedor del producto.

    b) Comprobar que el contenido del paquete se corresponde con lo indicado en la etiqueta de la caja.

    c) Una vez el producto se ha desempaquetado, inspeccionar la unidad. Se debe Comprobar que el número de serie que aparece en el propio producto coincide con el número de serie de la caja.

4.2 INSTALACIÓN SEGURA

9. El producto se entrega con una imagen del *firmware* y *software* precargada. Sin embargo, la imagen puede no encontrarse en su versión evaluada (**Software 11.01.x**).

10. Con el objetivo de comprobar si la versión instalada es la correcta y de instalar la versión correcta en caso contrario se deben seguir los pasos indicados en las siguientes subsecciones.

4.2.1 CONEXIÓN MEDIANTE LA CONSOLA LOCAL

11. En primera instancia, se deberá examinar el manual Teldat Router M1/M1L Installation Manual (**1**) con el objetivo de ensamblar correctamente las piezas incluidas en la caja del producto.

12. Opcionalmente se instalarán las antenas de WIFI o 3G incluidas en el paquete en los conectores indicados en la guía mencionada anteriormente y se conectará la fuente de alimentación.

13. Tras ello, se debe asegurar que el botón de encendido se encuentra en la posición I (encendido).

14. Finalmente, el usuario debe conectarse a la consola local siguiendo los pasos en la sección A.3 Connecting to the device de la guía Teldat Router M1/M1L Installation Manual (**1**).

4.2.2 COMPROBACIÓN DE LA VERSIÓN DEL PRODUCTO

15. Una vez se haya iniciado la conexión a través de la consola local, el usuario deberá comprobar la versión del producto.

16. Para ello, se deberá entrar en el modo de monitorización mediante el comando `monitor`, tras lo que se mostrará la versión usando el comando `version`.

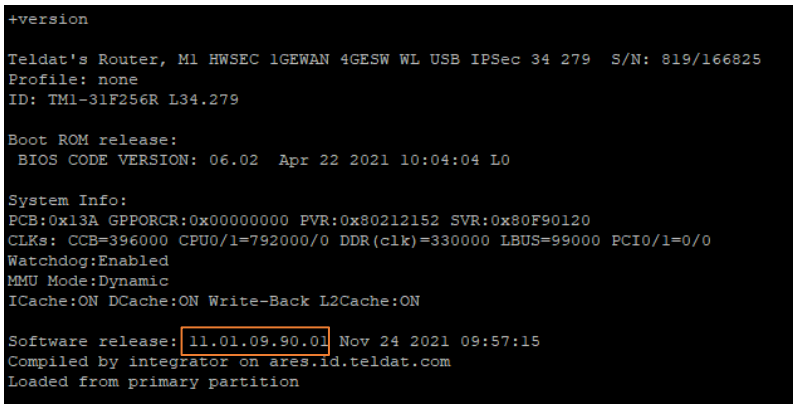

Ilustración 1 - Versión del producto

17. Una vez el producto muestre por pantalla las versiones de sus componentes, el usuario deberá verificar que la versión de los mismos coincide con la siguiente:

    - *Software release*: **11.01.09.90.01**

18. Si la versión del producto es la correcta se deberán omitir los siguientes pasos en la sección **4.2.3 ACTUALIZACIÓN DEL PRODUCTO** y el dispositivo estará listo para ser configurado.

19. En caso de que la versión sea incorrecta, se seguirán los pasos en la siguiente sección para instalar la versión correcta del mismo.

4.2.3 ACTUALIZACIÓN DEL PRODUCTO

20. Se obtendrá el paquete de actualización para la versión correcta poniéndose en contacto con el desarrollador a través del correo mailto:secteam@teldat.com.

21. Una vez se disponga de las versiones correctas del paquete de actualización se deberán seguir los pasos en la sección **5.15 PROCESO DE ACTUALIZACIÓN** para actualizar el dispositivo**.**

22. Se podrá emplear cualquiera de los métodos de actualización del *software* de aplicación (C.I.T) que se indican en dicha sección para actualizar el producto a la versión evaluada. Se deberá tener en cuenta que en este punto el producto no se deberá encontrar conectado a internet y que por tanto aún no se habrán deshabilitado los protocolos inseguros que serán deshabilitados durante el proceso de configuración.

23. Una vez se haya actualizado el dispositivo, se volverá a comprobar su versión siguiendo los pasos en la sección **4.2.2 COMPROBACIÓN DE LA VERSIÓN DEL PRODUCTO** de este mismo documento.

24. Una vez la versión instalada sea la correcta se procederá a configurar el producto.

25. En caso de que la versión siga sin ser la adecuada, se deberá repetir el proceso de actualización.

4.2.4 CONFIGURACIÓN INICIAL Y MODO LINCE

26. Antes de conectar el producto a una red con acceso a internet y de proceder a realizar el resto de la configuración necesaria se deberá activar el modo LINCE.

27. El modo LINCE restringirá el uso de protocolos y canales seguros a los que se incluyen en la evaluación.

28. Por tanto, una vez activado este modo y configurado un usuario inicial, el producto podrá ser conectado a internet a través de su interfaz WAN y se podrá proceder con el resto de pasos de la instalación y configuración del mismo.

29. Para activar el modo LINCE se accederá de nuevo al producto a través de la consola local siguiendo los pasos en la sección **4.2.1 CONEXIÓN MEDIANTE LA CONSOLA LOCAL**.

30. Una vez en la consola local, se accederá al modo de configuración mediante el comando `config`. En dicho modo, se activará el modo LINCE usando el comando `set configuration-mode lince`.

31. Tras ello, en el mismo modo de configuración, se deberá crear un usuario nuevo. Para crear un usuario se empleará el comando `user <usuario> password <contraseña>`, sustituyendo usuario y contraseña por los valores deseados. La contraseña deberá cumplir los requisitos descritos en la sección **6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN**.

32. Finalmente, se guardará la configuración utilizando el comando `save`. Dicho comando pedirá confirmación, por lo que habrá que introducir la palabra *"yes"* como respuesta al comando. Una vez guardada la configuración se deberá volver al modo inicial de la consola usando el comando `root` o pulsando las teclas *ctrl + p*. En dicho modo, se reiniciará el producto utilizando el comando `restart` y nuevamente se confirmará dicho reinicio con *"yes"*.

```
*config


Config>sa
Config>save
Save configuration (Yes/No)? yes

Warning: Running-config has been changed
Building configuration as text... OK
Writing configuration... OK on Flash
Config>re
Config>res
Config>


*resta
*restart
Are you sure to restart the system(Yes/No)? yes
```

Ilustración 2 – Guardar configuración

33. Una vez realizados estos pasos el producto podrá ser conectado a su entorno operacional, donde se realizarán el resto de pasos de configuración necesarios para alcanzar la operación segura del mismo.

4.2.5 ENTORNO DE OPERACIÓN

34. El entorno de operación del TOE será similar y equivalente al que se presenta en la siguiente imagen:

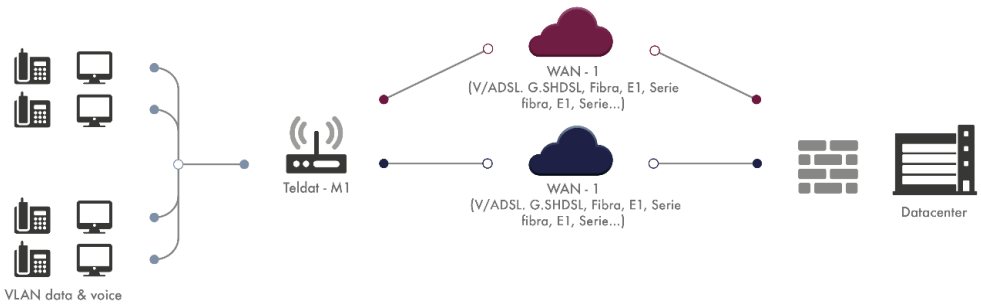

Ilustración 3 - Entorno operacional

35. El producto se usará como dispositivo frontera, protegiendo una red interna (izquierda) frente a una red externa (derecha). 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. Dichos puertos se encuentran físicamente marcados con las etiquetas "*WAN*" y "*LAN*" en la carcasa del dispositivo.

36. El usuario deberá conectar el producto a una red externa en el puerto WAN y a al menos un dispositivo en la red interna a través de cualquiera de los puertos LAN.

5. FASE DE CONFIGURACIÓN

5.1 PROCESOS DE LA CONSOLA

37. Para operar el producto será necesario entender cómo funciona la consola de administración del producto. Tras acceder al dispositivo mediante puerto serie se le pedirá al usuario que introduzca el nombre de usuario y contraseña. De igual manera, al acceder mediante SSH, el usuario deberá identificarse con su usuario y contraseña.

38. Una vez se hayan introducido unas credenciales correctas, el producto presentará al usuario el proceso GESTCON.

39. El router Teldat-M1 Series contiene los siguientes procesos:

    - P 1 (GESTCON): Será el punto de partida de la consola de administración. Permite acceder al resto de procesos.
    - P 2 (VISEVEN): Este proceso permite monitorizar los eventos que ocurren en el sistema. Dichos eventos deben ser programados previamente usando los otros procesos.
    - P 3 (MONITOR): Permite acceder a los comandos de monitorización, estado y estadísticas recogidas por el dispositivo.
    - P 4 (CONFIG): Este proceso permite modificar todos los parámetros de configuración. Desde este proceso se puede crear una nueva configuración del producto sin alterar su modo de operación actual. Será necesario guardar la configuración con el comando `save` y reiniciar el dispositivo para que se aplique la nueva configuración.
    - P 5 (RUNNING-CONFIG): Este proceso permite cambiar la configuración del producto en tiempo real. Los cambios que se realicen en este proceso tendrán un efecto inmediato, pero será necesario guardar los cambios con el comando `save` para que perduren después de un reinicio.

40. Cada uno de los procesos permitirá la introducción de una serie de comandos diferentes. Para navegar entre distintos procesos se tendrán en cuenta las siguientes reglas:

    - Cualquiera de los procesos puede ser accedido desde el proceso GESTCON escribiendo P 2, P 3, P 4 y P 5 respectivamente en la consola.
    - Para volver al proceso P 1 desde cualquiera de los otros procesos se podrá usar el comando `root` o presionar las teclas *ctrl + p*.

41. A lo largo de este documento se especificará el proceso en el que deberán lanzarse cada uno de los comandos de configuración.

5.2 ASIGNACIÓN DE DIRECCIONES IP

42. El producto dispone de 4 puertos físicos LAN asignados a un *switch* interno que se encuentra conectado al puerto interno ethernet0/0 del *router* y un puerto físico WAN que se encuentra conectado al puerto ethernet0/1 del mismo.

43. Por defecto, el producto realizará conmutación de paquetes a nivel de capa de enlace entre todos los puertos del *switch* y realizará encaminamiento del tráfico entre la red LAN y WAN, sin embargo, no se aplicará ninguna regla de NAT hasta que dicha configuración sea aplicada específicamente. Dicha configuración se encuentra incluida en este documento.

44. Tras iniciar el *router* en modo LINCE, la interfaz del dispositivo correspondiente al *switch* (ethernet0/0) tendrá asignada la dirección IP 192.168.1.1 con máscara 255.255.255.0. Por tanto, cualquier dispositivo conectado al *switch* podrá alcanzar al producto utilizando dicha dirección IP.

45. Habrá que tener en cuenta que el dispositivo no dispondrá de un servidor DHCP por defecto, y por tanto no se asignarán direcciones IP a los dispositivos conectados al *switch* hasta que dicha configuración sea aplicada, como se describe en secciones posteriores en esta misma guía.

46. Con el objetivo de administrar el producto y configurarlo será necesario aplicar las direcciones IP deseadas a las interfaces externa e interna del *router* (ethernet0/1 y ethernet0/0).

47. Para ello, se deberá acceder al proceso CONFIG o RUNNING-CONFIG y ejecutar los siguientes comandos:

    - `network <interfaz>`: Donde interfaz deberá ser sustituido por ethernet0/1 o ethernet0/0 en función de la interfaz que se quiera configurar. Tras ejecutar este comando aparecerá el modo de edición de la interfaz.
    - Dentro de dicho menú se debe elegir si se le asignará una dirección IP estática a esa interfaz o si se utilizará DHCP para que el servidor DHCP externo le asigne la dirección. Para ello se usarán los siguientes comandos dentro del modo de edición de la interfaz:
        - `ip address <a.b.c.d> <a.b.c.d>`: Se deberá sustituir el primer parámetro por la dirección IP deseada y el segundo por la máscara de red utilizada en dicha subred. Este comando le asignará una dirección IP estática a la interfaz.
        - `ip address dhcp-negotiated:` Este comando le indicará a la interfaz que debe obtener su dirección IP usando DHCP.

```
Config$net
Config$network ethe
Config$network ethernet0/1

-- Ethernet Interface User Configuration --
ethernet0/1 config$ip addr
ethernet0/1 config$ip address dhc
ethernet0/1 config$ip address dhcp-negotiated
```

Ilustración 4 - Configuración DHCP en Interfaz WAN

48. Usando el método anteriormente descrito, el usuario deberá asignar las direcciones IP deseadas a las interfaces externa e interna del *router* antes de proseguir con la configuración.

49. Una vez asignadas, las direcciones IP asignadas a cada interfaz pueden ser consultadas en el modo de consola **MONITOR** tal y como se muestra en la siguiente imagen:

```
+protocol ip

-- IP protocol monitor --

IP+inter
IP+interface-addresses
Interface IP Addresses:
-----------------------
ethernet0/0         192.168.1.1/24
ethernet0/1         dhcp-negotiated -

Special IP Addresses:
---------------------
internal-address     0.0.0.0
management-address   0.0.0.0
router-id            0.0.0.0
global-address       192.168.1.1
```

Ilustración 5 - Mostrar Direcciones IP

5.3 SSH

5.3.1 SERVIDOR

50. Una vez las interfaces tengan asignada una dirección IP, se podrá habilitar el servidor de SSH del *router*.

51. Tras habilitar dicho servidor el producto podrá ser administrado a través de esta interfaz, por lo que a partir de este momento el usuario podrá elegir si proseguirá configurando el *router* a través de la interfaz de consola o la interfaz SSH.

52. Para habilitar el servidor de SSH se deberá acceder al proceso **CONFIG** o **RUNNING-CONFIG** de la consola y se ejecutarán los siguientes comandos:

- `feature ssh`
- `server`
- `enable`

```
Config$feature ss
Config$feature ssh

-- SSH protocol configuration --

SSH Config$server

-- SSH Server --
SSHS$enab
SSHS$enable
```

Ilustración 6 - Habilitación del Servidor SSH

53. Tras ejecutar estos pasos el servidor SSH quedará habilitado en la configuración.

54. El usuario podrá seguir los pasos en la guía SSH Protocol (**2**) para configurar el resto de las características de SSH, como habilitar la autenticación mediante clave pública o modificar parámetros como el tiempo de autenticación, cuentas de usuario o la gestión de permisos a través de la consola de SSH.

55. No se deberán modificar parámetros relativos a los algoritmos criptográficos utilizados para el establecimiento del canal SSH.

5.3.2 CLIENTE

56. El producto dispone de un cliente SSH que puede ser empleado por los usuarios para conectarse a un servidor SSH externo.

57. Los usuarios autorizados pueden utilizar dicha funcionalidad a través del siguiente comando:

    - `ssh <a.b.c.d> login <user> port <port>`:
        - <a.b.c.d>: Dirección IP del servidor con el que se desea establecer la conexión.
        - <user>: El usuario con el que el producto intentará iniciar sesión en el servidor de SSH.
        - <port>: El puerto en el que está escuchando el servidor.

58. Si es la primera vez que se establece una conexión con ese servidor, el producto pedirá al usuario que confirme que confía en la firma de la clave pública presentada por el servidor.

59. Tras ejecutar el comando, el producto requerirá que el usuario introduzca la contraseña necesaria para iniciar sesión en el servidor y la sesión quedará establecida.

5.4 NAT

60. El producto no realiza funcionalidad de NAT por defecto. Por lo que si uno de los hosts de la red LAN intenta alcanzar un host que se encuentra en la red WAN, el *router* no traducirá su dirección IP y el host externo recibirá un paquete con la dirección IP de la LAN interna.

61. Con el objetivo de permitir que el producto actúe con una configuración de NAT en la que se enmascaren las direcciones IP de la red LAN usando la dirección IP externa del producto se deberán seguir los siguientes pasos desde el proceso **CONFIG** o **RUNNING-CONFIG**:

    - `feature afs`
    - `enable`
    - `exit`
    - `protocol ip`
    - `nat`
    - `rule 1 out ethernet0/1 dynamic overload`
    - `rule 1 translation source interface ethernet0/1`

62. Adicionalmente, el producto permite realizar más operaciones de NAT. Si se requiere, el usuario podrá consultar la guía New NAT (**3**) y seguir los pasos allí descritos.

5.5 DHCP

63. Como parte de la funcionalidad básica del *router*, el administrador podrá habilitar opcionalmente un servidor DHCP en el mismo, de manera que los dispositivos que se conecten a cualquiera de los puertos de la red LAN reciban una dirección IP de forma automática.

64. Con el objetivo de realizar una configuración básica del servidor DHCP se deberán llevar a cabo los siguientes pasos:

    - Desde el proceso **CONFIG** o **RUNNING-CONFIG** de la consola se accederá al menú del servidor DHCP mediante los siguientes comandos:
        - `protocol dhcp`
        - `server`
    - Se deberá habilitar el servidor DHCP y se establecerá el nombre del servidor:
        - `enable`
        - `global server-name <nombre>`
            - <name>: El nombre que se le quiera asignar al servidor.
    - Tras ello, se deberá crear una red compartida:
        - `shared 1`
    - Finalmente, se asignará la subred y el rango de direcciones IP que servirá el servidor DHCP en la interfaz ethernet0/0:
        - `subnet <nombre> <id> range <ip_inicio> <ip_fin>`
            - <nombre>: El nombre que se le asignará a la subred.

- <id>: El ID de la red compartida creada con anterioridad. En este ejemplo 1.
- <ip_inicio>: La dirección IP que marcará el inicio de direcciones IP que asignará el servidor.
- <ip_fin>: La dirección IP que marcará el final de direcciones IP que asignará el servidor.

- `subnet <nombre> <id> router <ip>`
  - <nombre>: El nombre que se le asignará a la subred.
  - <id>: El ID de la red compartida creada con anterioridad. En este ejemplo 1.
  - <ip>: La dirección IP del servidor de DHCP. Deberá coincidir con la dirección asignada en la interfaz ethernet0/0.

65. Para realizar una configuración avanzada del servidor de DHCP, como asignación de direcciones de los servidores de DNS o la asignación de direcciones IP estáticas a cada host se deberán seguir los pasos en la guía DHCP Protocol (**4**).

5.6 HTTPS

66. El producto ofrece la posibilidad de habilitar un servidor HTTPS que, previa autenticación, permitirá a los usuarios con nivel de acceso 15 aplicar actualizaciones sobre el dispositivo.

67. **El servidor HTTPS se encuentra deshabilitado por defecto y así debe mantenerse dado que dicho canal no aporta la fortaleza criptológica suficiente exigida por la guía CCN-STIC-807 Criptología de empleo en el ENS.**

5.7 IPSEC

68. Opcionalmente, existe la posibilidad de establecer túneles IPSec con otros productos que soporten el protocolo. De esta manera, se encaminarán los paquetes que se configuren en las reglas de la SPD de IPSec a través del túnel.

69. Durante la fase de configuración se deberá tener en cuenta que solo se podrán emplear los siguientes algoritmos al establecer túneles IPSec para estar dentro de la configuración evaluada:

- Intercambio de claves: *MODP group 15*
- Cifrado: *AES128, AES192, AES256 (opción recomendada).*
- Autenticación: *HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 (opción recomendada).*

70. Adicionalmente, solo se podrá emplear el modo IKEv2 para el establecimiento de las asociaciones de seguridad si éstas no se configuran de manera estática.

71. A continuación, se muestra un ejemplo indicando cómo configurar el canal de IPSec utilizando IKEv2, clave precompartida y los algoritmos aceptados. Para ello se deberán seguir los siguientes pasos desde el proceso CONFIG o RUNNING-CONFIG de la consola:

- Configuración de la lista de control de acceso: La lista de control de acceso determinará qué paquetes con un origen y destino determinado serán enviados a través del túnel:
  - `feature access-lists`
  - `access-list <id>`
    - <id>: El número de identificación de la lista de acceso entre 100 y 1999.
  - `entry 1 default`
  - `entry 1 permit`
  - entry 1 source address <source_address> <máscara>
    - <source_address>: La dirección IP del host o red de origen.
    - <máscara>: Máscara de red.
  - `entry 1 destination address <destination address> <máscara>`
    - <destination address>: La dirección IP del host o red de destino.
    - <máscara>: Máscara de red.
- Configuración de las plantillas de IPSec. Se deberán configurar dos plantillas de IPSec y habilitar el servicio IPSec:
  - `protocol ip`
  - `ipsec`
  - `enable`
  - `assign-access-list 100`
    - Donde 100 es el identificador de la lista de control de acceso.
  - `template 1 dynamic esp aes128 sha256`
    - Dentro de la configuración segura **no se podrán elegir los algoritmos de cifrado *des* y *tdes* ni los algoritmos de resumen *md5* y *sha1*.**
  - `template 1 negotiation-protocol ikev2`
  - `template 1 source-address <ip_origen>`
    - <ip_origen>: La dirección IP de la interfaz del producto desde la que se establecerá el túnel.

- `template 1 destination-address <ip_destino>`
  - <ip_destino>: La dirección IP de la interfaz del dispositivo con el que se establecerá el túnel.
- `template 2 ikev2 encryption aes128 aes256`
- `template 2 ikev2 authentication sha256 sha512`
- `template 2 ikev2 prf sha256 sha384 sha512`
- `template 2 ikev2 group fifteen`
- `template 2 destination-address <ip_destino>`
  - <ip_destino>: La dirección IP de la interfaz del *peer* IPSec con el que se establecerá el túnel.
- `template 2 ike natt-version rfc`
- `template 2 ike method local preshared`
- `template 2 ike method remote preshared`
- `map-template 100 1`
  - Donde 100 y 1 son el identificador de la lista de control de acceso y el identificador de la plantilla dinámica.
- `key preshared ip <ip_destino> plain <pre-shared>`
  - <ip_destino>: La dirección IP de la interfaz del *peer* IPSec con el que se establecerá el túnel.
  - <pre-shared>: La clave precompartida.

72. Una vez realizada la configuración del ejemplo el producto será capaz de conectarse con un *peer* IPSec compatible con la configuración establecida.

73. Para realizar configuraciones avanzadas del protocolo IPSec como autenticación mediante certificados se podrá consultar la guía IPSec (**5**) y seguir los pasos.

5.8 CALIDAD DE SERVICIO

74. El dispositivo permite configurar mecanismos de calidad de servicio asignando diferentes prioridades al tráfico. Estos mecanismos son aplicables al tráfico del *switch* a nivel de puerto o al tráfico que se encamina a través del producto.

5.8.1 CALIDAD DE SERVICIO EN LAS INTERFACES DEL SWITCH

75. Es posible configurar diferentes opciones para controlar la prioridad que se les asigna a los puertos del *switch* así como la prioridad que se asigna al tipo de tráfico que pasa por el mismo. Todas las opciones de configuración permitidas están descritas en las secciones *7.4 Quality of Service, 7.5 Accessing the Switch Configuration, 7.6 Switch Configuration Commands* y 7.6.8.12 QoS de la guía LAN Interfaces (**6**).

5.8.2 CALIDAD DE SERVICIO EN EL TRÁFICO QUE SE ENRUTA

76. Adicionalmente, el producto ofrece la posibilidad de configurar diferentes mecanismos que permiten gestionar las prioridades del tráfico que procesa el *router* en base a diferentes parámetros, como el tipo de protocolo, el ancho de banda asignado a las interfaces o la clasificación que ha recibido el tráfico (*Access-list* en IPv4 e IPv6).

77. Para configurar las opciones de calidad de servicio y de gestión de prioridades del tráfico se deberán seguir los pasos descritos en la guía *Bandwidth Reservation System* (**7**).

5.9 CONFIGURACIÓN DE LAS INTERFACES

78. El dispositivo permite habilitar o deshabilitar las interfaces físicas del mismo. De esta manera, si los puertos se encuentran deshabilitados el producto no enviará ningún paquete de red ni establecerá el canal de capa física en ninguno de esos puertos.

79. El puerto físico WAN (ethernet0/1) puede ser deshabilitado desde el modo CONFIG o RUNNING-CONFIG utilizando los siguientes comandos:

    - `network ethernet0/1`
    - `phy-shutdown`

80. La interfaz puede ser habilitada nuevamente desde el mismo menú utilizando el comando `no phy-shutdown`.

81. En el caso de los puertos LAN del switch interno asociados a la interfaz ethernet0/0, dichos puertos podrán deshabilitarse utilizando los siguientes comandos:

    - `network ethernet0/0`
    - `repeater-switch`
    - `port <port-number> disable`
        - <port-numbet>: En número del puerto que será deshabilitado.

82. El puerto podrá ser habilitado nuevamente desde el mismo menú utilizando el comando `port <port-number> enable`.

83. Adicionalmente, el usuario podrá seguir los pasos de la guía LAN Interfaces (**6**) para administrar el resto de parámetros asignados a cada interfaz, incluyendo la administración de las direcciones MAC, la negociación del canal ethernet y las opciones de control de acceso.

5.10 VLAN

84. Los usuarios autorizados podrán definir una serie de VLANs en las interfaces LAN asignadas al switch interno del producto.

85. Para configurar las VLANs en los puertos del *switch* se deben seguir los pasos indicados en la guía VLAN (8).

5.11 AUTENTICACIÓN

5.11.1 ROLES DE USUARIO

86. El producto define los roles de usuario 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.

87. 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.

88. 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 a la vista de eventos, pero no puede acceder a la funcionalidad de Ping, reinicio o carga desde la Flash.
    - MONITOR [5]: Acceso a la consola de administración, vista de eventos y de monitorización, comando de Ping e iniciar una conexión SSH. 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 niveles de privilegio y comandos del sistema. Este nivel de privilegio se puede equiparar con el rol de administrador.

89. Para crear un nuevo usuario se empleará el comando `user` en el modo P 4 o P 5. Dicho comando recibirá como argumentos el nombre de usuario y la contraseña de la siguiente forma:

```
user <Usuario> password <Contraseña>
```

90. Tras ejecutar el comando, el usuario quedará creado y habilitado con el nivel de privilegios 15 (root) y el modo *default*. El mismo comando podrá ser usado en cualquier momento para modificar la contraseña de los usuarios ya existentes.

91. Los privilegios de dicho usuario podrán ser modificados mediante el siguiente comando:

```
user <Usuario> access-level <nivel de acceso>
```

92. Donde el nivel de acceso será un valor entre 0 y 15 que determinará los permisos que el usuario tendrá en el sistema.

5.11.2 TIEMPO DE FINALIZACIÓN DE SESIÓN

93. Los usuarios podrán configurar el tiempo máximo de inactividad que deberá transcurrir antes de que el producto finalice las sesiones de administración. Por defecto, este tiempo de inactividad está configurado en 10 minutos.

94. Una vez se alcance dicho tiempo sin que el usuario emita ningún comando a través de esa sesión de administración, el producto cerrará la sesión y el usuario deberá volver a autenticarse si quiere seguir administrando el dispositivo.

95. Para configurar el tiempo de finalización de sesión se debe emplear el siguiente comando en los procesos CONFIG o RUNNING-CONFIG de la consola:

    - `set inactivity-timer <time>`: Donde el parámetro deberá ser el tiempo de finalización de sesión en minutos (entre 1 minuto y 10 horas).

96. El tiempo de finalización de sesión afectará tanto a las sesiones establecidas mediante la consola local como a las sesiones SSH.

5.11.3 MÁXIMO NÚMERO DE INTENTOS DE AUTENTICACIÓN (CONSOLA LOCAL)

97. **Se debe configurar un número máximo de intentos de autenticación tras el cual el acceso mediante consola local queda bloqueado temporalmente**. Este mecanismo servirá para prevenir ataques de fuerza bruta a través de esta interfaz.

98. Para configurar este parámetro se deberá acceder al modo de consola CONFIG o RUNNING-CONFIG y ejecutar los siguientes comandos:

    - `set console`
    - `login blocking <blocking_time>`:
        - <blocking_time>: Tiempo que la consola permanecerá bloqueada. El tiempo deberá establecerse indicando la unidad temporal (s, m, h, d) y podrá ser establecido entre 0s y 1d.
    - `login attempts <max_attempts>`:
        - <max_attempts>: El número máximo de intentos de autenticación. Podrá variar entre 1 y 100.

```
Config$set console

-- Console configuration --
Con config$login blo
Con config$login blocking 30m
Con config$login attem
Con config$login attempts 4
Con config$exit
```

Ilustración 7 - Máximo Número de Intentos de Autenticación

99. El usuario deberá configurar este parámetro de forma obligatoria estableciendo un número máximo de intentos de autenticación que se encuentre dentro de los

márgenes permitidos por el producto. **Se recomienda establecer un número máximo de intentos de autenticación de 4 intentos y un tiempo de bloqueo de la consola no superior a 30 minutos.**

5.12 SELF-TESTS

100. El producto realiza pruebas durante el arranque para verificar la integridad de los ficheros del *firmware* y el correcto funcionamiento de las funciones criptográficas.

101. Los usuarios autorizados podrán configurar la ejecución periódica de dichas pruebas, de forma que el dispositivo las lanzará cuando pase el periodo estipulado de tiempo.

102. Para configurar las pruebas periódicas se deberán utilizar los siguientes comandos en el proceso **CONFIG** o **RUNNING-CONFIG**:

- `set crypto self-test periodic <Time-Period>`
  - <Time-Period>: El tiempo que deberá transcurrir entre la ejecución de los *self-tests*. El tiempo deberá ser introducido indicando la unidad temporal (h, d, w) y podrá ser configurado entre 1 hora (1h) y 4 semanas y 2 días (4w2d).

```
Config$set crypto self-test periodic ?
  <1h..4w2d>    Time period
Config$set crypto self-test periodic 4w2d
Warning: This functionality will affect the perfomance of the system when the self-tests are running
Config$set crypto self-test periodic 4w
Warning: This functionality will affect the perfomance of the system when the self-tests are running
Config$set crypto self-test periodic 2d
Warning: This functionality will affect the perfomance of the system when the self-tests are running
```

Ilustración 8 - Configuración de *Self-Tests* Periódicos

103. De manera adicional, los usuarios autorizados podrán realizar estas pruebas de forma manual en cualquier momento utilizando el comando `crypto self-test` desde el proceso **MONITOR**:

```
+crypto ?
  self-test    Execute a set of self tests to verify the OpenSSL cryptographic
               algorithms and the integrity of the software
+crypto se
+crypto self-test
The following test will affect the perfomance of the system while it is running
Are you sure to run the test?(Yes/No)? yes

OpenSSL self-tests
----------------------------------
RAND     ...Pass

Digest tests:
------------------
SHA1     ...Pass
SHA2     ...Pass
SHA3     ...Pass

HMAC tests:
------------------
HMAC     ...Pass

CMAC tests:
------------------
CMAC     ...Pass

Cipher tests:
------------------
3DES     ...Pass
AES      ...Pass
AES-CCM  ...Pass
AES-GCM  ...Pass

Signature tests:
------------------
RSA      ...Pass
ECDSA    ...Pass
DSA      ...Pass

DH/ECDH tests:
------------------
DH       ...Pass
ECDH     ...Pass

KDF tests:
------------------
PBKDF2   ...Pass
KBKDF    ...Pass

Firmware integrity test
----------------------------------
BIOS Integrity  ...Pass
APP Integrity   ...Pass
FW Integrity    ...Pass

20 test(s) run in 15450 ms. 0 test(s) failed.
```

Ilustración 9 - Ejecución Manual de los *Self-Tests*

5.13 REGISTROS DE AUDITORÍA

104. Por defecto, solo los usuarios con el nivel de acceso 15 podrán acceder a la información guardada en los registros de auditoría.

105. Los registros de auditoría se pueden activar utilizando los siguientes comandos desde los modos CONFIG y RUNNING-CONFIG:

    - `event`
    - `enable security-traces default`

106. Para desactivar los registros se usarán los siguientes comandos (esta funcionalidad no puede ser desactivada en el modo LINCE, por lo que el comando retornará un error si se está dicho modo):

    - `event`

- `no enable security-traces default`

107. Para visualizar dicha información se deberá acceder al proceso MONITOR y utilizar los siguientes comandos:
    - `event`
    - `security-traces show`
108. Tras ejecutar dichos comandos se mostrará el contenido de los registros de auditoría.
109. Los usuarios con el máximo nivel de privilegios también tendrán la capacidad de borrar los registros de auditoría utilizando los siguientes comandos:
    - `event`
    - `security-traces clear`

5.14 TIEMPO DEL SISTEMA

110. El usuario con privilegios adecuados podrá cambiar la fecha y la hora del sistema a través del proceso **CONFIG** de la consola mediante el siguiente comando:
    - `time set <month> <day> <year> <week day> <hour> <minute> <second>`:
        - < month > el mes del año.
        - < day > el día del mes.
        - < year > el año (últimos dos dígitos).
        - < week day > número del día de la semana.
        - < hour > hora.
        - < minute > minuto.
        - < seconds > segundo.

5.14.1 NTP

111. Durante el proceso de configuración **se deberá configurar la comunicación del producto con un servidor NTP de forma que el producto sincronice la hora del sistema** de forma periódica con la información proporcionada por dicho servidor.
112. Para llevar a cabo esta configuración se deberán seguir los pasos establecidos en la guía NTP Protocol (9).
113. El servidor NTP deberá ser conectado directamente en uno de los puertos del *switch* del producto, que se empleará exclusivamente para dicha conexión. De esta manera, el TOE y el servidor NTP se encontrarán dentro de una subred aislada del resto de puertos del *switch*, de forma que solo podrán comunicarse entre sí sin intervención de ningún agente externo. Con el objetivo de aislar lógicamente el

puerto del *switch* en el que se conectará el NTP, se deberán seguir los siguientes pasos desde el proceso CONFIG de la consola:

- `feature vrf`
- `vrf vrf-ntp`
- `exit`
- `add device eth-subinterface ethernet0/0 <Puerto>`
  - <Puerto>: El número de puerto que se aislará del resto de puertos del switch, donde se conectará el servidor NTP. Podrá ser un valor de 1 a 4.
- `network ethernet0/0.<Puerto>`
  - <Puerto>: El número de puerto escogido en el paso anterior.
- `port-tag <Puerto>`
  - <Puerto>: El número de puerto escogido anteriormente.
- `vrf forwarding vrf-ntp`
- `ip address <IP_ADDRESS> <MASK>`
  - <IP_ADDRESS>: La dirección IP de la interfaz.
  - <MASK> La máscara de subred.
- `exit`
- `feature ntp`
- `poll-interval 16`
- `peer address 1 <IP_ADDRESS> use-vrf vrf-ntp`
  - <IP_ADDRESS>: La dirección IP del servidor NTP. Se deberá tener en cuenta que el servidor NTP deberá tener una interfaz conectada al puerto del switch seleccionado con una dirección IP dentro del rango de la misma subred.

114. Tras la configuración del servidor NTP, el usuario deberá seguir los pasos en la sección 2.2.9 PERSISTENT-SAVE de esa misma guía con el objetivo de permitir que el producto mantenga la hora tras ser reiniciado. Para ello se deberá ejecutar el siguiente comando desde el proceso CONFIG o RUNNING-CONFIG de la consola:

- `feature ntp`
- `persistent-save 1`

115. Se debe tener en cuenta que el producto solo comenzará a tener una hora fiable tras establecer una conexión con el servidor NTP y obtener el tiempo del mismo. Por lo tanto, tras el primer inicio del producto, solo se tendrá una hora precisa una vez se ha establecido la conexión con el servidor NTP. La misma situación se dará cuando el TOE se apague y encienda, el tiempo del producto solo será fiable y

preciso una vez se haya obtenido la hora del servidor NTP, lo que será llevado a cabo por parte del TOE automáticamente tras su arranque.

5.15 PROCESO DE ACTUALIZACIÓN

116. **El producto debe estar actualizado.** La actualización puede hacerse a través del servidor SFTP o adicionalmente, existe la posibilidad de actualizar el dispositivo directamente desde la BIOS a través de una conexión mediante el puerto serie. El método de actualización mediante BIOS no deberá ser llevado a cabo excepto en el caso excepcional de que el dispositivo no arranque y no pueda actualizarse de otra manera.

5.15.1 COMPROBACIÓN DE ACTUALIZACIONES DISPONIBLES

117. El dispositivo permite comprobar si existen actualizaciones disponibles utilizando el comando `check-update` desde el proceso MONITOR. Tras ejecutar el comando, el producto se conectará a uno de los servidores de Teldat y mostrará por pantalla un aviso indicando si existen actualizaciones disponibles o si el producto se encuentra actualizado a la última versión existente. Este proceso utiliza el puerto 4661, por lo que habrá que asegurarse de que ningún elemento bloquea dicho puerto.
118. Se obtendrá el paquete de actualización para la versión correcta poniéndose en contacto con el desarrollador a través del correo secteam@teldat.com.

5.15.2 ACTUALIZACIÓN MEDIANTE SFTP

119. Si se elige el método de SFTP, se deberá acceder al TOE utilizando el protocolo SFTP con el mismo usuario y contraseña establecidos para acceder a través de SSH. Solo un usuario con el nivel de acceso 15 podrá realizar el proceso de actualización.
120. Una vez se ha accedido a través de SFTP, se seguirán los siguientes pasos para actualizar el software CIT:

- CIT:
    - Desde SFTP se accederá a la carpeta /MEM y se subirá el fichero de actualización de la aplicación CIT utilizando el comando `put <update>`, donde <update> será el nombre del fichero de actualización.
    - Una vez subido el fichero, se renombrará el mismo de la siguiente manera:

      ```
      rename <update> ../DSK/APPCODE1.BIN
      ```

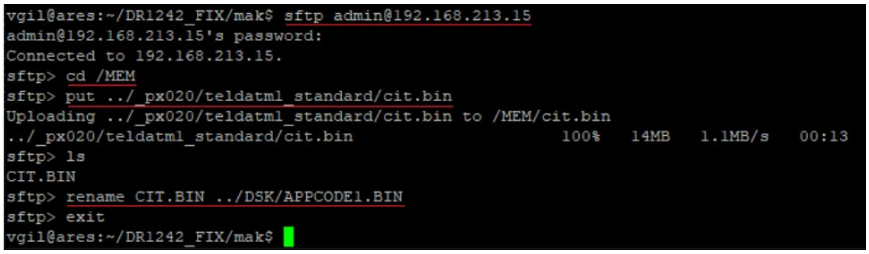

Ilustración 10 - Actualización de CIT SFTP

- Tras la aplicación de la actualización se deberá reiniciar el dispositivo accediendo a él a través de la consola local o mediante SSH.

5.16 GESTIÓN DE CERTIFICADOS

121. El dispositivo permite gestionar, generar e importar claves privadas, públicas y certificados que serán utilizados por el producto tanto para autenticar su identidad como para verificar la autenticidad de las entidades externas que se le conectan.

5.16.1 CERTIFICADOS EN SSH

122. Se podrán seguir los pasos en la sección 2.2.2 HOST-KEY de la guía SSH Protocol **(2)** para modificar el certificado que utilizará el producto para autenticar su identidad frente a entidades externas**. Este certificado deberá ser siempre un certificado que use RSA con un tamaño de clave 3072 bits o mayor.**

123. Adicionalmente, se podrán seguir los pasos en la sección 2.3.3.2 AUTHENTICATION PUBLIC KEY de esa misma guía para configurar la autenticación de los clientes que se conectan al servidor utilizando criptografía de clave pública.

5.16.2 CERTIFICADOS EN IPSEC

124. Se podrán seguir los pasos en la sección 2.5 Certificates de la guía IPSec (**5**) para configurar el uso de certificados como método de autenticación cuando se establezcan túneles IPSec.

6. FASE DE OPERACIÓN Y MANTENIMIENTO

6.1 RECOMENDACIONES PARA LA FASE DE OPERACIÓN

125. El correcto funcionamiento del producto requiere de características que deben estar presentes en el entorno. Es responsabilidad del administrador autorizado asegurar que el entorno operacional cumple con los requisitos enumerados a continuación:

    a) **El producto estará instalado y será mantenido en un entorno físico seguro**. Esto incluye una sala con control de acceso o un entorno móvil controlado por el administrador.

    b) El producto **no contendrá ninguna aplicación de uso general** como compiladores o aplicaciones de usuario.

    c) Se realizarán **comprobaciones periódicas del *hardware* del dispositivo** para asegurar que no ha sido manipulado.

    d) Los administradores deben estar correctamente **entrenados en el uso y la correcta operación del producto**, así como en las características del entorno seguro en que está presente. Al mismo tiempo, los administradores seguirán las guías e indicaciones presentes.

    e) Los administradores se asegurarán de que el producto cuenta con las **últimas actualizaciones de *software*** para preservar al mismo de amenazas y vulnerabilidades conocidas. Las actualizaciones serán llevadas a cabo a través de las interfaces HTTPS o SFTP, evitando el uso de la actualización mediante BIOS. El proceso de actualización mediante BIOS solo se llevará a cabo si el producto queda dañado y no es posible arrancarlo sin actualizar el firmware del mismo.

    f) Los administradores mantendrán sus **credenciales** de acceso al producto **seguras y protegidas**.

    g) Los administradores deben **eliminar** toda la información residual sensible que pudiera quedar resultante de operar con el producto después de terminar la vida útil de este.

    h) Los auditores se encargarán de **examinar de forma periódica los registros de auditoría** buscando eventos específicos relacionados con los cambios de la configuración del sistema y que puedan indicar que éste ha sido comprometido.

126. Con el fin de prevenir que los administradores escojan contraseñas inseguras, estas deben de cumplir con los siguientes requisitos:

    - Deberán observarse y tenerse en cuenta las recomendaciones expuestas en la guía *CCN-STIC 821, Apéndice V: Normas de Creación y Uso de Contraseñas NP40* [2].

- Las contraseñas deben de tener una longitud recomendada de 12 o más caracteres.
- Deben de estar compuestas por una combinación de caracteres pertenecientes, al menos, a 3 o 4 de los siguientes grupos de caracteres: letras en minúscula, letras en mayúscula, números y los caracteres especiales: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")"*.
- No se deben reutilizar las últimas 5 contraseñas.
- La validez de las contraseñas no debería superar los 60 días.
- Se debería establecer un tiempo mínimo antes de permitir un nuevo cambio de contraseña: 10 días.

7. REFERENCIAS

1. Teldat**.** *Teldat Router M1/M1L Installation Manual, DM569-I, Versión 9.1.* 2019.

2. *SSH Protocol, Teldat-Dm 787-I, Version 11.06.*

3. *New NAT, Teldat-Dm 788-I, Version 11.04.*

4. *DHCP Protocol Teldat Dm730-I, Versión 11.0A.*

5. *IPSec, Teldat DM 739-I, version 11.0H.*

6. *LAN Interfaces, Teldat DM709-I, Version 11.0J.*

7. *Bandwidth Reservation System, Teldat-Dm 715, Versión 11.0A.*

8. *VLAN, Teldat-Dm 751-I, version 11.05.*

9. *NTP Protocol, Teldat-Dm 728-I, Versión 11.08.*

10. *Software Updating, Teldat -Dm 748-I, Version 11.05.*

8. ABREVIATURAS

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de productos de Seguridad TIC
CSR	Certificate Signing Request
CRL	Certificate Revocation List
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENS	Esquema Nacional de Seguridad
FTP	File Transport Protocol
GCM	Galois/Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IKE	Internet key Exchange
IPSec	Internet Protocol Security
LAN	Local Area Network
NAT	Network Address Translation
NTP	Network Time Protocol
RSA	Rivest, Shamir y Adleman Algorithm
SHA	Secure Hash Algorithm
SPD	Security Policy Database
SSH	Secure Shell Protocol
STIC	Seguridad de Tecnologías de Información y Comunciación
TLS	Transport Layer Security Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network

PUBLICACIONES DE DEFENSA

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