IS101

DECLARACIÓN DE SEGURIDAD

PREPARADO: DPTO. ING. SISTEMAS	**REVISADO:** DIR. CALIDAD	**APROBADO:** RESP. DPTO. ING. SISTEMAS
Fecha y Firma:	Fecha y Firma:	Fecha y Firma:

REGISTRO DE EDICIONES Y MODIFICACIONES

ED.	FECHA (dd/mm/aa)	MODIFICACIÓN REALIZADA (Incluir breve descripción y/o capítulos o apartados modificados)	REALIZADO POR	NOTA DE CAMBIO
1	25/10/16	Se edita nuevo.	Ing. Sistemas	N/P
2	19/12/16	Se corrigen erratas. Se revisa el contenido completo del documento.	Ing. Sistemas	--
3	10/02/17	Se incorporan cambios para subsanar ORs recibidas del evaluador. Se corrigen erratas.	Ing. Sistemas	--
4	22/03/17	Se incorporan cambios para subsanar ORs recibidas del evaluador. Se corrigen erratas.	Ing. Sistemas	--
5	05/05/17	Se incorporan cambios para subsanar ORs recibidas del evaluador.	Ing. Sistemas	--
6	21/09/17	Se incorporan cambios para aclarar alcance de la evaluación.	Ing. Sistemas	--
7	02/11/17	Se incorporan nuevos cambios para aclarar el alcance de la evaluación.	Ing. Sistemas	--
8	20/11/17	Se añaden aclaraciones en el activo USER_DATA y en algunos SFRs. Se actualiza la versión del TOE.	Ing. Sistemas	--
9	25/01/18	Se realizan pequeños ajustes en la definición del problema de seguridad.	Ing. Sistemas	--
10	23/04/18	Se realizan correcciones de formato en la nomenclatura de algunos SFRs. Se actualiza descripción en apartado “Entrega y Guías de Instalación y Operación”.	Ing. Sistemas	--

N/P = NO PROCEDE

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. OBJETO

1.1. CONTENIDO DEL DOCUMENTO

1 En este documento se recoge la declaración de seguridad aplicable al IS101, de acuerdo a la normativa de certificación Common Criteria, versión 3.1 revisión 4.

1.2. ÁMBITO DE APLICACIÓN

2 Este documento es aplicable al IS101 en versión y revisión especificadas en el apartado 3.2.

2. DOCUMENTOS Y NORMAS APLICABLES

2.1. REFERENCIAS GENERALES

CÓDIGO	TÍTULO UNIFORME	TÍTULO DEL DOCUMENTO	ED	FECHA
-	NORMATIVA	Common Criteria for Information Technology Security Evaluation	3.1R4	Sep. 2012

2.2. REFERENCIAS ESPECÍFICAS

CÓDIGO	TÍTULO UNIFORME	TÍTULO DEL DOCUMENTO	ED	FECHA
IS240101ZZ01	240	IS101. Manual de Usuario	*	*

* Última versión y revisión en vigor.

3. INTRODUCCIÓN

3.1. TÉRMINOS Y DEFINICIONES

CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTP	Trusted Third Party

Tabla 1. Acrónimos de la Norma CC

A	Amperio
AES	Advanced Encryption Standard
CdG	Centro de Gestión
CPLD	Complex Programmable Logic Device
FPGA	Field Programmable Gate Array
FW	Firmware
Gbps	Gigabit per second
GCM	Galois Counter Mode
HW	Hardware

Hz	Hertzios
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IP*XY*	Ingress Protection *XY*
IT	Information Technology
LED	Light Emitting Diode
MP	Módulo Principal
MT	Módulo Tamper
OR	Observation Report
OSI	Open Systems Interconnection
PC	Personal Computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSS	Pre-Shared Secrets
PSU	Power Supply Unit
RAM	Random Access Memory
RF	Radiofrecuencia
RTC	Real Time Clock
SNMP	Simple Network Management Protocol
SW	Software
USB	Universal Serial Bus
Vac	Voltaje de Corriente Alterna
Vcc	Voltaje de Corriente Continua
VPN	Virtual Private Network
W	Watt

Tabla 2. Definiciones y Acrónimos del TOE

3.2. REFERENCIAS DE LA DECLARACIÓN DE SEGURIDAD Y DEL TOE

3.2.1. Referencia de la Declaración de Seguridad

Título	IS101. Declaración de Seguridad (IS251101ZZ01)
Versión	ED10 / Rev. 27
Autor	Istria Soluciones de Criptografía, S.A.
Fecha de publicación	23/04/18

Tabla 3. Referencia de la Declaración de Seguridad

3.2.2. Referencia del TOE

Nombre	IS101
Versión	v1.01
Desarrollador	Istria Soluciones de Criptografía, S.A.

Tabla 4. Referencia del TOE

3.3. DESCRIPCIÓN DEL PRODUCTO

3 El IS101 es un dispositivo de altas prestaciones que integra una plataforma hardware segura con un FW/SW específico y permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada).

4 Opera sobre el nivel 3 del modelo OSI y emplea el protocolo IPsec para permitir llevar a cabo el procesamiento, filtrado y manejo de forma controlada del tráfico de datos de usuario que lo atraviesa en base a las políticas de seguridad IPsec previamente configuradas en el mismo y, en caso necesario, proteger la comunicación entre distintas redes locales geográficamente distantes (redes rojas) mediante el establecimiento de

túneles VPN con otros dispositivos remotos compatibles conforme a los parámetros negociados entre extremos y las correspondientes credenciales de cada uno. Gracias a ello, la información sensible intercambiada (incluidas cabeceras IP) queda protegida frente a modificación durante su tránsito por la red no confiable (red negra) y se impide el acceso a la misma desde ubicaciones diferentes a las redes rojas expresamente especificadas como conexiones permitidas en la configuración de los IS101 involucrados.

5 Para el establecimiento de conexiones cifradas (túneles VPN) utiliza el protocolo IPSec en modo túnel con encapsulado ESP y el protocolo IKEv2 para la identificación y autenticación mutua entre extremos y la negociación y renovación de claves y algoritmos para la correspondiente asociación de seguridad (mediante certificados X.509 y/o claves secretas pre-compartidas (PSS)). Para el posterior cifrado del tráfico de datos de usuario a través de una asociación de seguridad ya establecida, el IS101 implementa y permite ejecutar, de forma simultánea, dos algoritmos criptográficos independientes: uno estándar (AES256-GCM) y un segundo que, partiendo de un algoritmo de las mismas características del anterior, puede ser personalizado según las necesidades del cliente.

6 De acuerdo con la especificación del estándar IPsec, el IS101 permite también: 1) realizar comunicaciones en claro que facilitan el intercambio de información desde / hacia dispositivos localizados en una red roja (para facilitar la integración del equipo en redes ya existentes o en aquellas en las que se maneja información de ambos tipos: información sensible, que debe ser protegida, y otra no sensible o que debe ser intercambiada en claro) y 2) establecer reglas específicas de descarte, para prohibir expresamente determinado tipo de tráfico en base a sus características (direcciones, puertos, protocolo...) y/o definir excepciones sobre las conexiones permitidas a través de otras políticas de seguridad.

7 El IS101 alcanza velocidades de transferencia de hasta un máximo de 2Gbps agregados y permite establecer y gestionar hasta un máximo de 4096 asociaciones de seguridad simultáneas.

8 El IS101 soporta y es capaz de gestionar tráfico tanto IPv4 como IPv6, unicast y multicast, e incorpora un conjunto completo de protocolos de red para facilitar su integración en redes IP, incluyendo, tanto para IPv4 como para IPv6, protocolos de asignación dinámica de direccionamiento DHCP, rutado dinámico RIP y OSPF, mecanismos de redundancia mediante VRRP para incrementar la disponibilidad, soporte VLAN, etc.

9 Asimismo, dispone de mecanismos y auto-tests específicos para arranque seguro y protección de los componentes y datos internos sensibles que almacena.

10 El equipo está diseñado de forma que se garantizan los niveles necesarios de seguridad para el personal de operación y mantenimiento (evitando especialmente los peligros de contacto eléctrico) y permitiendo un manejo y configuración del mismo sencillo e intuitivo, minimizando las acciones requeridas por parte del usuario.

11 Adicionalmente, su diseño completo está orientado a minimizar las emisiones radiadas y conducidas para evitar la extracción de información sensible manejada por el equipo a través de este tipo de canales laterales.

12 Para asegurar que la funcionalidad del IS101 se proporciona con el nivel de confiabilidad y protecciones requeridas, éste implementa un conjunto de servicios que permiten garantizar que la operación y aplicación del control de flujo y el manejo, configuración y gestión del propio equipo se llevan a cabo de forma segura, incluyendo para ello, los servicios de seguridad ofrecidos por el TOE, listados en el apartado 3.4.2. El alcance de la evaluación Common Criteria a la que hace referencia este documento y, por tanto, las garantías de seguridad derivadas de la misma, se refieren sólo a la funcionalidad de seguridad del TOE declarada en dicho apartado.

3.4. RESUMEN DEL TOE

3.4.1. Tipo de TOE

13 El objeto a evaluar (TOE) es el conjunto de elementos HW y SW/FW del IS101 que permiten garantizar que la operación y aplicación del control de

flujo de datos de usuario y el manejo, configuración y gestión del propio equipo se llevan a cabo de forma segura.

3.4.2. Uso del TOE

14 Los principales servicios y características de seguridad ofrecidos por el TOE incluyen:

- Control robusto del procesamiento y manejo del tráfico de datos de usuario, limitando el tráfico que está permitido que atraviese el equipo a aquellos flujos determinados por las políticas de seguridad IPsec configuradas en cada momento.
- Identificación y Autenticación de usuarios y establecimiento de canales seguros para aquellos usuarios conectados de forma remota.
- Control de acceso a las operaciones de administración, gestión y configuración mediante perfiles de usuario y esquemas de permisos.
- Protecciones físicas y lógicas (activas y pasivas).
- Almacenamiento seguro de ciertos datos sensibles en el supervisor de seguridad (necesarios para el arranque del equipo), permitiendo verificar su integridad en cada arranque, y chequeos periódicos (auto-tests) del estado de los sensores y mecanismos anti-tamper.
- Trazabilidad de los eventos más relevantes desde el punto de vista de seguridad.

3.4.3. Software y Hardware Requerido por el TOE

15 El entorno operacional empleado por el TOE para operar consta de los siguientes elementos necesarios, que quedan fuera del alcance de la certificación:

- Inyector IS101K.

  Empleado para realizar ciertas operaciones de administración en el equipo (como llevar a cabo el proceso de instalación, habilitar el acceso a través del interfaz de consola o del interfaz web...) y, si fuera necesario, para realizar la carga / actualización off-line de ciertos parámetros de configuración.

  Este dispositivo de transporte compatible, denominado inyector, funciona como token de seguridad y se encarga de aportar los permisos necesarios para llevar a cabo las operaciones de administración y/o de almacenar la información que se ha de cargar en el equipo.

Figura 1. Inyector

  El contenido del inyector se programa desde el Centro de Gestión correspondiente y está protegido por un código de acceso (código PIN), de forma que, al insertar el inyector en el IS101, su contenido sólo es accesible desde el equipo una vez que el dispositivo se ha validado, es decir, una vez que se ha introducido correctamente su código PIN.

  Este dispositivo se considera un dispositivo IT confiable externo al TOE.

- Fuente de alimentación.

  La alimentación del IS101 para su arranque y para su operativa normal se debe proporcionar mediante una fuente externa de 12Vcc, 30W (rango aproximado de entrada admitido 10,5-17Vcc).

No obstante, ISTRIA como fabricante suministra el equipo junto con una fuente externa para su alimentación desde la red AC estándar.

- Cables de conexionado externo del equipo, PCs, switches, routers y/o resto de equipamiento de red que componen la(s) red(es) roja(s) y la red negra.

  Para la integración del equipo entre la red o redes locales que ha de proteger (redes rojas) y la red no confiable (red negra), éste dispone de dos interfaces de red independientes, que se han de conectar por medio de sendos cables Ethernet a la red roja y a la red negra, respectivamente. Nótese que, a nivel físico, el equipo podrá estar equipado con interfaces Gigabit en cobre (10/100/1000BaseT con conectores RJ45) (configuración evaluada) o en fibra óptica (1000BaseSX con conectores LC), por lo que los cables Ethernet empleados deberán ser acordes con el tipo de interfaz del equipo.

  Así mismo, para la gestión del equipo a través del interfaz de consola, será necesaria la conexión a un PC que disponga de un emulador de terminal compatible (Minicom, PuTTY…) mediante un cable USB-miniUSB_B.

  Los PCs, switches, routers y/o resto de equipamiento de red que componen la(s) red(es) roja(s) y la red negra no forman parte del TOE. Dentro de este conjunto, se encuentran también los dispositivos IT genéricos externos empleados para el manejo y gestión de la configuración del TOE (PCs, navegadores, interfaz serie...). Para éstos últimos, será responsabilidad del entorno operacional establecer las políticas de uso y procedimientos necesarios para contribuir a la inicialización y gestión segura del equipo.

16 Si bien necesarios para operar con el IS101, estos dispositivos no forman parte del TOE.

17 Por otro lado, de forma opcional (no necesario obligatoriamente para operar normalmente con el equipo), se puede emplear el dispositivo Centro de Gestión IS101M (fabricado y distribuido únicamente por ISTRIA). Este dispositivo se considera un dispositivo IT confiable externo al TOE. La operativa o gestión del IS101 desde el dispositivo Centro de Gestión IS101M queda fuera del alcance de la evaluación CC del IS101. Es por ello que en los SFRs incluidos en el presente documento, a través de los que se expresa la funcionalidad de seguridad evaluada dentro del alcance de la certificación CC, no se incluye el "Centro de Gestión" como rol independiente, no se especifican las acciones de gestión derivadas de su uso, ni se incluye la selección de los eventos auditables cuyo origen es dicho dispositivo (origen "manager").

3.5. DESCRIPCIÓN DEL TOE

3.5.1. Ámbito Físico del TOE

3.5.1.1. Entrega y Guías de Instalación y Operación

18 El TOE se suministra como un único equipo ya programado (HW + SW/FW embebido), empaquetado y etiquetado conforme a los procedimientos de entrega establecidos para el equipo. La fuente de alimentación del equipo así como el cable de consola estándar, son elementos auxiliares que, aunque no forman parte del TOE, se suministran junto con el mismo.

19 También forman parte del TOE (y se entregan con el mismo) las siguientes guías:

- IS101. Manual de Usuario (IS240101ZZ01), donde se describen los procedimientos para instalación y operación del mismo. Esta guía se entrega en formato electrónico (PDF) junto con el TOE.

20 Conforme a los procedimientos estándar de entrega establecidos, el manual de usuario referido se entrega en formato electrónico (PDF) grabado en un dispositivo USB estándar. Este dispositivo USB, aunque por

sí mismo no forma parte del TOE, se suministra junto con el mismo en el interior del embalaje del equipo e incluirá también una copia del certificado raíz cargado en el equipo, de forma que la Organización usuaria pueda disponer de él para su distribución a los usuarios autorizados que deban acceder al equipo a través del interfaz de configuración web seguro.

3.5.1.2. Descripción Mecánica

21 Desde el punto de vista físico, el IS101 tiene un tamaño y peso reducidos (Alto: 45 mm, Ancho: 220 mm, Largo: 280 mm y Peso: 3,6 Kg), apto para montaje en rack 19", altura 1U y cuyo ancho reducido permite instalar dos unidades en paralelo en una misma U de un rack de 19" mediante un soporte mecánico especialmente diseñado para ello). Así mismo, tiene un diseño mecánico muy robusto apto para operar en ambientes agresivos (diseñado para proporcionar características de estanqueidad y reducir emisiones, posibilidad de anclaje en plataforma anti-vibratoria…).

22 Esto le proporciona una gran versatilidad, pudiendo ser instalado en diversos tipos de entorno (sobremesa, rack de 19" o en entornos más hostiles), a la vez que facilita su transporte y despliegue en entornos móviles.

23 La mecánica está formada por tres piezas principales (*cuna o base*, *tapa* y *frontal*) fabricadas en aluminio. Estas piezas reciben los tratamientos adecuados para proporcionar al equipo una alta resistencia en entornos agresivos (humedad, temperatura, vibración, polvo,…) y, además, están específicamente diseñadas para facilitar la instalación del equipo sobre una plataforma anti-vibratoria, si fuese necesario.

24 El diseño incluye un radiador situado en el panel trasero que permite realizar la disipación de calor mediante conducción térmica, convección natural y radiación térmica sin necesidad de orificios o ranuras de ventilación, ni ventiladores integrados.

25 Además, el diseño de las piezas mecánicas, sus uniones (con gaskets RF) y la selección de conectores empleados permiten dotar al equipo de características de estanqueidad (IP67) y del aislamiento electromagnético

adecuado para minimizar las emisiones radiadas y conducidas. Así mismo, el diseño mecánico proporciona barreras físicas que dificultan la introducción de sondas y el acceso a los componentes internos críticos evitando así su alteración y la extracción de la información sensible almacenada en el equipo.

26 El acceso a la batería de respaldo del equipo, situada en el panel frontal, se puede realizar desde el exterior simplemente retirando su correspondiente tapa sin necesidad de abrir el equipo para ello y simplificando así el proceso de sustitución de la misma cuando sea necesario.

27 Cualquier otro intento de apertura estándar del equipo diferente a éste será considerado un potencial ataque y se activarán los correspondientes mecanismos anti-tamper.

3.5.1.3. Descripción de Interfaces Externos

28 La conectividad física del IS101 y su interacción con el usuario se basa en un conjunto de interfaces externos repartidos entre el panel frontal del equipo y el panel trasero, tal y como se describe a continuación:

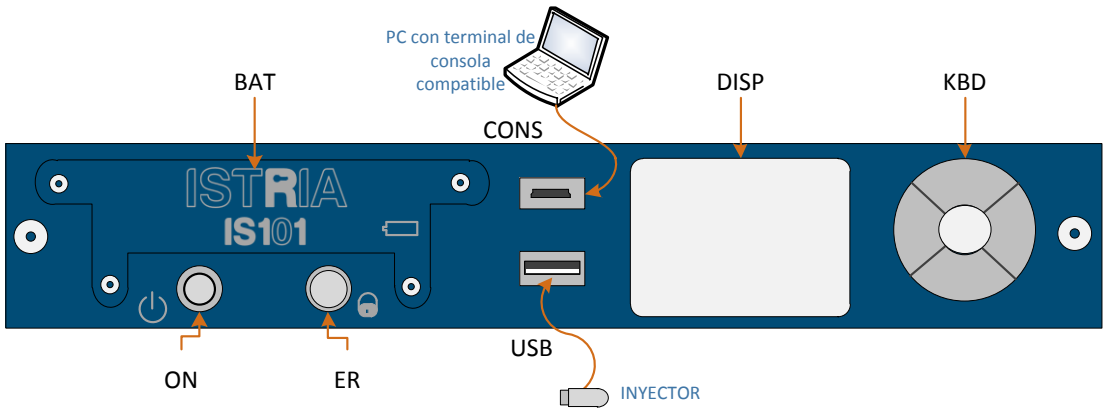

Figura 2. Interfaces Externos IS101 (Panel Frontal)

- En el panel frontal se localizan (ver también *Figura 2*):
    - **DISP:** Display a color de 1,8” del equipo para facilitar la autenticación de inyectores, la notificación de las operaciones en curso y eventos y ciertas tareas básicas de configuración.
    - **KBD:** Teclado de navegación del equipo compuesto por cinco teclas ( ARRIBA,  ABAJO,  IZQUIERDA,  DERECHA y  CENTRAL) para facilitar la autenticación de inyectores y ciertas tareas básicas de configuración. Cada una de las teclas incluidas en el mismo dispone además de un led integrado. Estos leds se utilizan para llamar la atención sobre el usuario respecto al estado del equipo (por ejemplo, en situaciones de tamper), reforzando así la información al respecto que se muestra en el display del equipo.
    - **CONS:** Interfaz mini-USB para configuración y manejo local del equipo mediante la conexión de un PC con un emulador de consola compatible.
    - **USB:** Interfaz USB para conexión de los inyectores compatibles con el equipo.
    - **BAT:** Alojamiento para la batería de respaldo del equipo que permite mantener activa la monitorización de seguridad y las claves del equipo en ausencia de alimentación externa.
    - **ER:** Pulsador de emergencia del equipo. Incluye un indicador LED para notificación de información de estado. Se activa con pulsación larga.
    - **ON:** Botón de encendido / apagado del equipo. Incluye un indicador LED para notificación de información de estado.

Se activa con pulsación corta o larga según operación a realizar.

Figura 3. Interfaces Externos IS101 (Panel Trasero)

- En el panel trasero (ver también *Figura 3*):
  - **PWR:** Entrada de alimentación para la conexión de una fuente externa compatible con el equipo.
  - **RED:** Interfaz Gigabit Ethernet (nivel de enlace Ethernet IEEE 802.3) para conexión del equipo a la red roja (información en claro). A nivel físico, se proporciona por defecto como interfaz eléctrico (10/100/1000 BaseT con conector RJ45) (configuración evaluada). No obstante, opcionalmente, se podrá suministrar (bajo demanda) como interfaz óptico (1000 BaseSX con conectores LC) en vez de interfaz eléctrico.
  - **BLACK:** Interfaz Gigabit Ethernet (nivel de enlace Ethernet IEEE 802.3) para conexión del equipo a la red negra (información en cifrado). A nivel físico, se proporciona por defecto como interfaz eléctrico (10/100/1000 BaseT con conector RJ45) (configuración evaluada). No obstante, opcionalmente, se podrá suministrar (bajo demanda) como interfaz óptico (1000 BaseSX con conectores LC) en vez de interfaz eléctrico.

- Conexión de tierra: el equipo dispone de dos tornillos para realizar la conexión a tierra, para que el usuario emplee aquél que se ajuste mejor a su instalación. Ambos tornillos están conectados al mismo potencial, por lo que se recomienda emplear únicamente una conexión.

3.5.2. Ámbito Lógico del TOE

29 Para garantizar que la funcionalidad del IS101 se proporciona con el nivel de confiabilidad y protecciones requeridas, el TOE incluye e integra los componentes HW y SW/FW necesarios para proveer los servicios y características de seguridad relacionados en el apartado 3.4.2.

30 Para ello, el TOE implementa los siguientes protocolos, funcionalidades y mecanismos:

- **Implementación de un control y filtrado robusto del tráfico** gestionado a través de sus interfaces de red, de forma que el tráfico de datos de usuario que atraviesa el equipo desde el lado rojo al lado negro y viceversa, está limitado a los flujos de datos expresamente permitidos por alguna de las políticas de seguridad IPsec configuradas (de forma autorizada). Nótese que, por defecto, el TOE implementa un control restrictivo del tráfico permitido a través del mismo, es decir, todo el tráfico que no esté expresamente permitido a través de las correspondientes políticas de seguridad IPsec configuradas, está, por defecto, prohibido.

- Definición de un **sistema de control de acceso** para la gestión del IS101, de acuerdo a una serie de perfiles de usuario:

  - Usuario con perfil “Administrador de Seguridad”.

  - Usuario con perfil “Administrador de Configuración”.

  - Usuario con perfil “Operador”.

Para cada perfil de usuario se implementa un mecanismo específico de autenticación y, para algunos perfiles, también un esquema de permisos. El tipo de perfil de usuario y el esquema de permisos (cuando aplique) determinan qué operaciones puede realizar el usuario autorizado sobre el equipo.

- **Mecanismos anti-tamper pasivos**, tales como precintos de seguridad, para evidenciar los intentos de acceso no autorizado al equipo.

- **Mecanismos anti-tamper activos**, que permiten detectar diferentes intentos de manipulación o comportamientos anómalos, considerados como ataques (eventos de tamper), tanto en presencia como en ausencia de alimentación externa, protegiendo al equipo frente a posibles ataques físicos o situaciones que puedan suponer un riesgo para su funcionamiento, llevándolo a un estado seguro (NO operativo). El equipo es capaz de detectar dos niveles de tamper (Tamper ALTO y Tamper BAJO) según la gravedad del evento detectado.

- Almacenamiento seguro de ciertos datos sensibles en el supervisor de seguridad (necesarios para el arranque del equipo), permitiendo verificar implícitamente su integridad en cada arranque, y chequeos periódicos (auto-tests) del estado de los sensores y mecanismos anti-tamper, tanto en presencia como en ausencia de alimentación externa.

- Monitorización de los eventos más relevantes que se producen en el equipo, desde el punto de vista de la seguridad, y almacenamiento de los mismos en el **registro de auditoría** (memoria no volátil), siendo posible, además, su envío a un gestor externo como **traps SNMP** conforme al protocolo SNMPv3.

- **Establecimiento de canales seguros** para la comunicación **con dispositivos IT confiables externos al TOE**, principalmente

empleados para para operaciones de inicialización, gestión / configuración y/o monitorización.

4. DECLARACIONES DE CONFORMIDAD

4.1. CONFORMIDAD RESPECTO A LA NORMA COMMON CRITERIA

31 Esta Declaración de Seguridad cumple con lo indicado en la norma Common Criteria versión 3.1:

- Parte 1: CCMB-2012-09-001, “Part 1: Introduction and general model”, rev.4.
- Parte 2: CCMB-2012-09-002, “Part 2: Security functional components”, rev.4.
- Parte 3: CCMB-2012-09-003, “Part 3: Security assurance components”, rev.4.

32 La conformidad respecto a la segunda parte de CC es extendida, mientras que para la parte tres la conformidad es estricta. El nivel de garantía para esta evaluación es EAL4+ (aumentado con el componente ALC_FLR.1).

4.2. CONFORMIDAD RESPECTO A PERFILES DE PROTECCIÓN

33 Esta Declaración de Seguridad no declara cumplimiento de ningún Perfil de Protección.

5. DEFINICIÓN DEL PROBLEMA DE SEGURIDAD

5.1. ACTIVOS

34 Para definir el problema de seguridad se tienen en cuenta los activos que se definen en los siguientes apartados.

5.1.1. Activos a Proteger por el TOE

USER_DATA Flujos de datos de usuario (paquetes IP) que se transmiten entre una red local (red roja) conectada al lado rojo del IS101 y la red negra conectada al lado negro del mismo a través de los elementos activos del TOE[1], para los cuales se proporciona confidencialidad (mediante la aplicación de funciones de control y filtrado para impedir que atraviesen el TOE a aquellos datos que no satisfagan los criterios de filtrado de tráfico configurados en el equipo, independientemente de si sobre dichos datos se aplica cifrado o no)[2].

5.1.2. Activos del Propio TOE

CONFIG Parámetros sensibles de configuración del equipo, para los cuales se proporciona confidencialidad e integridad.

AUDIT Registro de auditoría del equipo, para el cual se proporciona confidencialidad e integridad.

[1] Quedan excluidos de este conjunto, aquellos flujos de datos de usuario que pudieran, por cualquier motivo, transmitirse entre una red local (red roja) y la red negra por caminos físicos o lógicos diferentes a los elementos activos del TOE.

[2] La disponibilidad de los flujos de datos de usuario es posible mantenerla sólo en condiciones normales de operación (equipo correctamente conectado y en estado operativo, resto de elementos de la red a la que se conecta operando correctamente y capacidad disponible del canal adecuada para el flujo de datos de usuario que se desea transmitir / recibir).

5.2. AMENAZAS

35 De acuerdo a los activos anteriormente definidos, se determinan una serie de amenazas que pueden comprometer la seguridad del TOE o los servicios de seguridad ofrecidos por éste.

T.UNAUT_TRAF Un agente modifica de forma no autorizada e inadvertida el comportamiento del TOE o bien su configuración TSF para transmitir o permitir la recepción de datos de usuario no autorizados[3] con objeto de que éstos atraviesen el TOE, violando así las políticas de control de flujo establecidas.

El agente es un atacante (usuario no autorizado[4]) con acceso físico y/o lógico al TOE desde la red negra o desde una red roja, local o remota, que posea amplios conocimientos sobre el protocolo IPsec.

T.UNAUT_MNG Un agente logra violar el sistema de control de acceso del TOE para acceder de forma no autorizada a su gestión y, de esta forma, violar el acceso a la configuración del TOE y/o al registro de auditoría o realizar operaciones de gestión (pudiendo incluir la actualización del SW principal) o configuración no autorizadas.

[3] Un flujo de datos de usuario se considera autorizado cuando sus características encajan de forma no ambigua en alguna de las reglas de filtrado determinadas por las correspondientes políticas de seguridad IPsec configuradas por un usuario autorizado en el TOE. Cualquier otro flujo de datos de usuario se considera no autorizado.

[4] Se considera “usuario no autorizado” a cualquier usuario no autenticado frente al equipo (incluidos todos aquellos que no dispongan de credenciales válidas para ello) o bien a un usuario autenticado frente al equipo que intenta acceder a funcionalidad que no le está autorizada (para la cual no tiene permisos habilitados).

El agente es un atacante (usuario no autorizado[5]) con acceso físico y/o lógico al TOE desde la red negra o desde una red roja, local o remota.

T.UNAUTH_SW Un atacante logra, mediante la manipulación física del TOE, dentro de su entorno operativo y de forma inadvertida, modificar el comportamiento lógico del equipo cargando un SW fraudulento que sea aceptado como válido por el equipo y pueda, por tanto, ser ejecutado en su entorno operacional, permitiendo, en consecuencia, violar el acceso a la configuración del TOE y/o al registro de auditoría o realizar operaciones de gestión (pudiendo incluir la actualización del SW principal) o configuración no autorizadas.

El agente es un atacante (usuario no autorizado[6]) con acceso físico al TOE.

36 En la siguiente tabla se indica, a modo resumen, qué activos se verían afectados por cada una de las amenazas detalladas anteriormente:

ACTIVOS / AMENAZAS	USER_DATA	CONFIG	AUDIT
T.UNAUT_TRAF	X	X	X
T.UNAUT_MNG		X	X
T.UNAUTH_SW		X	X

Tabla 5. Matriz de Trazabilidad: Amenazas vs. Activos

[5] Ver nota al pie 4.

[6] Ver nota al pie 4.

5.3. POLÍTICAS ORGANIZATIVAS DE SEGURIDAD

37 Se consideran las siguientes políticas organizativas de seguridad que podrían llegar a estar impuestas por una organización que vaya a hacer uso del TOE:

OSP.AUDIT El TOE debe mantener un registro de auditoría que permita monitorizar los eventos relevantes desde el punto de vista de la seguridad.

Los eventos ocurridos en el equipo deben poder ser enviados a un gestor externo para su supervisión mediante un mecanismo basado en traps SNMPv3.

OSP.TRAF_MNG El TOE debe ser capaz de controlar y filtrar el tráfico entrante a través de sus interfaces de red en base a la configuración de las correspondientes políticas de seguridad y resto de parámetros IPsec y, en función de ellas, decidir qué flujos de datos de usuario están permitidos y cuáles no y, para aquellos flujos permitidos, si deben ser protegidos a través de túneles IPsec.

OSP.SEC_OP El TOE debe disponer de mecanismos que posibiliten el manejo y gestión de sus principales parámetros de configuración, en local o en remoto, de forma segura.

OSP.TAMP_MEC El TOE debe disponer de mecanismos anti-tamper y chequeos periódicos sobre los mismos que le permitan detectar determinados intentos de manipulación física, ataque o condiciones de operación anómalas (sobre-tensión en entrada de alimentación o batería, temperatura fuera de rango, ausencia total de alimentación, apertura estándar del equipo[7] o manipulación física de determinados componentes

[7] Entendida como la apertura del equipo mediante la retirada de los correspondientes tornillos y piezas mecánicas.

sensibles), tanto en presencia como en ausencia de la alimentación externa, y considerarlos como eventos de tamper. La finalidad de estos mecanismos es contribuir a mejorar la seguridad del equipo, permitiéndole auto-protegerse frente a condiciones de operación anómalas (intencionadas o fortuitas) y frente a determinados intentos de manipulación física y/o ataque al comportamiento lógico del equipo (incluso aunque se disponga de acceso físico autorizado al equipo).

5.4. HIPÓTESIS

38 Los servicios de seguridad proporcionados por el TOE se pueden ver comprometidos ante ciertas condiciones, por lo que es necesario contemplar las siguientes hipótesis para el entorno operacional:

A.TRUSTED_USR Todos los usuarios autorizados[8] a través del sistema de control de acceso del TOE son no hostiles, confiables y competentes, reciben la formación adecuada y disponen de los medios necesarios para llevar a cabo sus tareas asignadas de forma correcta, responsable y siguiendo las directrices y recomendaciones estipuladas para la conexión, inicialización y manejo seguro del TOE.

A.CRYPTO La PKI utilizada (o dispositivo equivalente) para la generación o firma de los certificados de comunicaciones IPsec o del dispositivo empleado para la generación de las claves secretas pre-compartidas está gestionada por personal confiable. En consecuencia, sólo se generan y distribuyen a los IS101 parámetros criptográficos para un uso final conocido

[8] Se considera “usuario autorizado” a un usuario autenticado frente al equipo (en posesión de credenciales válidas para ello) que dispone de autorización (permisos necesarios habilitados) para llevar a cabo las operaciones gestión y/o configuración consideradas en cada caso.

y aceptado y dichos parámetros criptográficos NO se distribuyen a dispositivos no autorizados. De esta forma, se puede asegurar que los parámetros criptográficos involucrados en el establecimiento de las asociaciones de seguridad cargados en el TOE son confiables y que los dispositivos no autorizados NO están en posesión de dichos parámetros criptográficos.

A.SEC_OP Se dispone de los medios materiales adecuados, políticas de uso y procedimientos necesarios para conectar, configurar y operar de forma segura los componentes IT genéricos externos (PCs, navegadores, interfaz serie, cables, switches y/u otros elementos de red) empleados para la conexión, manejo y gestión del TOE y su configuración.

A.PHY_ACC El entorno de explotación implementa medidas físicas y organizativas adecuadas para que el acceso físico al equipo quede restringido a los usuarios autorizados para su conexión, configuración y manejo en local.

6. OBJETIVOS DE SEGURIDAD

39 Los objetivos de seguridad que se incluyen en este apartado representan, en alto nivel, la solución propuesta frente al problema de seguridad definido en el apartado 5. Estos objetivos se dividen en dos grupos, los que deben ser proporcionados por el propio TOE o los que se deben facilitar desde el entorno operacional (entorno de uso del producto).

6.1. OBJETIVOS DE SEGURIDAD DEL TOE

O.TRAFFIC El TOE será capaz de procesar y manejar el tráfico de datos de usuario que circula entre sus interfaces rojo y negro en base a las reglas determinadas por las políticas de seguridad IPsec configuradas y, en función de ello, descartar o permitir el flujo de información (a través del correspondiente túnel IPsec, cuando corresponda). La regla a aplicar por defecto en el TOE, cuando el tráfico de datos de usuario no encaje en ninguna de las determinadas por las políticas de seguridad IPsec configuradas, deberá ser descartar.

O.SEC_MNG El TOE establecerá un sistema de control de acceso que defina diferentes roles de usuario para acceder a la gestión y configuración del mismo o a la invocación de los mecanismos seguros dispuestos para actualizar el SW principal que almacena, limitando las operaciones a realizar por cada uno de ellos en base a las políticas de control de acceso definidas en el equipo (según perfil y/o permisos habilitados en cada caso) y garantizando que las operaciones relevantes desde el punto de vista de seguridad sólo se pueda llevar a cabo por determinados roles de usuario una vez completado con éxito el correspondiente proceso de autenticación y siempre que se tenga habilitado/s el/los permiso/s correspondiente/s.

O.TAMPER_DET El TOE implementará una serie de mecanismos anti-tamper y chequeos periódicos sobre los mismos que le permitan detectar determinados intentos de manipulación física, ataque

	o condiciones de operación anómalas (sobre-tensión en entrada de alimentación o batería, temperatura fuera de rango, ausencia total de alimentación, apertura estándar del equipo o manipulación física de determinados componentes sensibles), tanto en presencia como en ausencia de la alimentación externa, y considerarlos como eventos de tamper. La finalidad de estos mecanismos es contribuir a mejorar la seguridad del equipo, permitiéndole auto-protegerse frente a condiciones de operación anómalas (intencionadas o fortuitas) y frente a determinados intentos de manipulación física y/o ataque al comportamiento lógico del equipo (incluso aunque se disponga de acceso físico autorizado al equipo).
O.SEC_STATE	El TOE entrará en un estado seguro (NO operativo) al detectar cualquiera de los eventos de tamper definidos para el mismo (ataque físico o comportamiento anómalo en su operativa habitual), de forma que, para devolver el equipo al estado operativo sea necesario al menos, la intervención de un Administrador de Seguridad.
O.AUDIT_REG	El TOE mantendrá un registro de auditoría, en memoria no volátil, de los eventos relevantes desde el punto de vista de la seguridad acontecidos. El conjunto de eventos relevantes a registrar de entre todos los posibles debe ser configurable.
O.AUDIT_SNMP	El TOE permitirá enviar las alarmas generadas a un supervisor externo (ubicado en una localización alcanzable por el equipo a través de alguna de sus políticas de seguridad IPsec configuradas) mediante el protocolo SNMPv3, aunque no contestará a sondeos. El conjunto de alarmas a enviar al supervisor externo de entre todas las posibles debe ser configurable. Esta funcionalidad podrá ser habilitada / deshabilitada por determinados roles de usuario.

6.2. OBJETIVOS DE SEGURIDAD DEL ENTORNO OPERACIONAL

OE.TRUSTED_USR El entorno operacional debe garantizar que los usuarios autorizados[9] a través del sistema de control de acceso del TOE son no hostiles, confiables y competentes y que reciben la formación adecuada y disponen de los medios necesarios para llevar a cabo sus tareas asignadas de forma correcta, responsable, y siguiendo las directrices y recomendaciones estipuladas para la conexión, inicialización y manejo seguro del TOE. Este objetivo contribuye a garantizar que la configuración del TOE se realiza de forma segura, conforme a las políticas establecidas por la Organización para su inicialización y manejo seguro y a evitar errores en su gestión, configuración y/o monitorización siempre que se haga de forma autorizada.

OE.CRYPTO El entorno operacional debe garantizar que la PKI utilizada (o dispositivo equivalente) para la generación o firma de los certificados de comunicaciones IPsec o el dispositivo empleado para la generación de las claves secretas pre-compartidas está gestionada por personal confiable. En consecuencia, sólo se generan y distribuyen a los IS101 parámetros criptográficos para un uso final conocido y aceptado y dichos parámetros criptográficos NO se distribuyen a dispositivos no autorizados. De esta forma, se puede asegurar que los parámetros criptográficos involucrados en el establecimiento de las asociaciones de seguridad cargados en el TOE son confiables y que los dispositivos no autorizados NO están en posesión de dichos parámetros criptográficos.

OE.SEC_OP El entorno operacional debe garantizar que se proveen los medios materiales adecuados, políticas de uso y

[9] Ver nota al pie 8.

procedimientos necesarios para conectar, configurar y operar de forma segura los componentes IT genéricos externos (PCs, navegadores, interfaz serie, cables, switches y/u otros elementos de red) empleados para la conexión, manejo y gestión del TOE y su configuración.

OE.PHY_ACC El entorno operacional debe garantizar que se proveen las medidas físicas y organizativas adecuadas para que el acceso físico al equipo quede restringido a los usuarios autorizados para su conexión, configuración y manejo en local.

6.3. JUSTIFICACIÓN DE LOS OBJETIVOS DE SEGURIDAD

6.3.1. Cobertura

40 La siguiente tabla muestra el modo en que los objetivos del TOE y del entorno operacional colaboran para solucionar el problema de seguridad definido:

PROBLEMA DE SEGURIDAD / OBJETIVOS DE SEGURIDAD	T.UNAUT_TRAF	T.UNAUT_MNG	T.UNAUTH_SW	OSP.AUDIT	OSP.TRAF_MNG	OSP.SEC_OP	OSP.TAMP_MEC	A.TRUSTED_USR	A.CRYPTO	A.SEC_OP	A.PHY_ACC
O.TRAFFIC	X				X						
O.SEC_MNG	X	X			X	X					
O.TAMPER_DET			X				X				
O.SEC_STATE			X				X				
O.AUDIT_REG		X		X							
O.AUDIT_SNMP		X		X							
OE.TRUSTED_USR	X	X	X	X	X	X		X			
OE.CRYPTO					X				X		
OE.SEC_OP	X	X		X	X	X				X	
OE.PHY_ACC	X	X	X								X

Tabla 6. Matriz de Trazabilidad: Objetivos de Seguridad vs. Problema de Seguridad

6.3.2. Suficiencia

41 Justificación de suficiencia para las amenazas:

T.UNAUT_TRAF	El procesamiento y manejo de los flujos de datos de usuario que atraviesan el TOE se realiza en base a las reglas determinadas por las políticas de seguridad IPsec configuradas, permitiendo, en función de ellas, descartar o permitir el flujo de información y, para aquellos permitidos, cuando aplique, encaminarlos a través del correspondiente túnel IPsec previamente establecido. La regla que aplica por defecto el TOE, cuando el tráfico de datos de usuario no encaja en ninguna de las determinadas por las políticas de seguridad IPsec configuradas, es descartar (filtrado de tráfico de tipo “lista blanca”), impidiendo que circulen a través del TOE flujos de datos de usuario no autorizados debido a una configuración incompleta de las políticas de seguridad aplicables (O.TRAFFIC). El sistema de acceso establecido por el TOE impide que personal no autorizado pueda acceder a la gestión y configuración del mismo o realizar operaciones de actualización de SW, con el objetivo de modificar de forma no autorizada las políticas de seguridad configuradas para permitir que atraviesen el TOE flujos de datos de usuario no contemplados en la configuración autorizada del TOE, de modificar el comportamiento del TOE (versión SW) para que no aplique dichas reglas de procesamiento y manejo de flujos conforme a las políticas de seguridad IPsec configuradas de forma autorizada o bien para eliminar o impedir que se anoten los registros de auditoría que evidenciarían cambios en las políticas de seguridad configuradas o en los componentes SW encargados de aplicarlas (O.SEC_MNG). El entorno operacional debe garantizar que se proporcionan los medios (IT y humanos), políticas de uso y procedimientos adecuados, y que éstos se aplican debidamente, para garantizar que la configuración, por parte de un usuario autorizado, de las políticas de seguridad IPsec se realiza de forma correcta, contribuyendo a evitar que un flujo de datos no autorizado por la Organización usuaria del TOE pueda ser permitido debido a una conexión o configuración incorrecta, insegura o ambigua (OE.TRUSTED_USR, OE.SEC_OP). De forma complementaria el entorno operacional debe implementar las medidas físicas y/u organizativas adecuadas para asegurar que el acceso físico al TOE en su entorno de explotación se restringe a los usuarios debidamente autorizados para su conexión, configuración y manejo en local y que éstos son no hostiles, confiables y competentes, contribuyendo a evitar manipulaciones indebidas del equipo y/o sus conexiones o su sustracción con fines de análisis de ingeniería inversa (OE.PHY_ACC, OE.TRUSTED_USR).

T.UNAUT_MNG	El sistema de acceso establecido por el TOE impide que personal no autorizado pueda acceder a la gestión y configuración del mismo, violando el acceso a su configuración y/o al registro de auditoría o invocando operaciones de gestión no autorizadas (pudiendo incluir la actualización del SW principal) (O.SEC_MNG, O.AUDIT_REG, O.AUDIT_SNMP). El entorno operacional debe garantizar que se proporcionan los medios (IT y humanos), políticas de uso y procedimientos adecuados, y que éstos se aplican debidamente, para garantizar que la configuración del TOE, por parte de un usuario autorizado, en los referente al control de acceso se realiza de forma correcta, contribuyendo a evitar que el acceso a la configuración del TOE y/o al registro de auditoría pueda quedar desprotegido debido a una configuración incorrecta o insegura y a evitar que se cargue en el equipo un SW malicioso debido a un manejo incorrecto o inseguro de los privilegios e información necesarios para ello (OE.TRUSTED_USR, OE.SEC_OP). De forma complementaria el entorno operacional debe implementar las medidas físicas y/u organizativas adecuadas para asegurar que el acceso físico al TOE en su entorno de explotación se restringe a los usuarios debidamente autorizados para su conexión, configuración y manejo en local y que éstos son no hostiles, confiables y competentes, contribuyendo a evitar manipulaciones indebidas del equipo y/o sus conexiones o su sustracción con fines de análisis de ingeniería inversa (OE.PHY_ACC, OE.TRUSTED_USR).
T.UNAUTH_SW	El entorno operacional debe implementar las medidas físicas y/u organizativas adecuadas para asegurar que el acceso físico al TOE en su entorno de explotación se restringe a los usuarios debidamente autorizados para su conexión, configuración y manejo en local y que éstos son no hostiles, confiables y competentes, contribuyendo a evitar manipulaciones indebidas del equipo cuyo objetivo final pudiera ser modificar su comportamiento lógico mediante la carga de un SW fraudulento en el mismo (OE.PHY_ACC, OE_TRUSTED_USR). Aunque acorde a lo explicado anteriormente la amenaza quedaría mitigada, la inclusión de los mecanismos anti-tamper activos implementados y la transición del equipo a un estado seguro (NO operativo) en caso de detección por parte del TOE de cualquiera de los eventos de tamper definidos para el mismo (O.TAMPER_DET, O.SEC_STATE) ayudan también a mejorar la seguridad física del equipo (mecanismos de auto-protección) frente a condiciones anómalas de operación o entorno, cuyo objetivo final pudiera ser manipular el comportamiento lógico del equipo mediante la carga de un SW fraudulento en el mismo.

Tabla 7. Justificación de Suficiencia para las Amenazas

42 Justificación de suficiencia para las políticas organizativas de seguridad:

OSP.AUDIT	El TOE mantiene un registro de auditoría para almacenar los eventos relevantes desde el punto de vista de la seguridad acontecidos, de acuerdo a un filtro configurado por un usuario autorizado (O.AUDIT_REG). Asimismo, la funcionalidad de envío de alarmas como “traps” a un supervisor externo mediante el protocolo SNMPv3 (configurado por un usuario autorizado), permite que el las alarmas generadas por el TOE puedan ser monitorizadas de forma remota (O.AUDIT_SNMP). El entorno operacional debe garantizar que se proporcionan los medios (IT y humanos), políticas de uso y procedimientos adecuados, y que éstos se aplican debidamente, para garantizar que la configuración y monitorización del registro de auditoría, por parte de un usuario autorizado, se realiza de forma que los eventos relevantes de seguridad ocurridos en el equipo se anotan, se revisan con la periodicidad adecuada y que se toman las acciones oportunas en cada caso, contribuyendo a evitar que un posible ataque, intento de acceso no autorizado o comportamiento anómalo detectado pasen de forma inadvertida (OE.TRUSTED_USR, OE.SEC_OP).
OSP.TRAF_MNG	El sistema de acceso establecido por el TOE define los roles de usuario que pueden llevar a cabo su configuración, incluyendo la definición de políticas de seguridad y resto de parámetros IPsec que especifiquen qué flujos de datos de usuario están permitidos y cuáles no y, para aquellos flujos permitidos, si deben ser protegidos a través de túneles IPsec (O.SEC_MNG). El sistema de control de flujo implementado en el TOE se encarga de aplicar las reglas determinadas por la configuración autorizada de políticas de seguridad y resto de parámetros IPsec al tráfico de datos de usuario manejado por el equipo (O.TRAFFIC). El entorno operacional debe garantizar que se proporcionan los medios (IT y humanos), políticas de uso y procedimientos adecuados, y que éstos se aplican debidamente, para garantizar que la configuración, por parte de un usuario autorizado, de las políticas de seguridad y resto de parámetros IPsec se realiza de forma correcta y que las credenciales empleadas son confiables, contribuyendo a evitar un manejo inadecuado de los flujos de datos de usuario debido a una configuración incorrecta, insegura o ambigua de los mismos o a una conexión incorrecta que pudiera permitir la circulación de éstos por caminos diferentes al TOE (OE.TRUSTED_USR, OE.CRYPTO, OE.SEC_OP).

OSP.SEC_OP	El sistema de acceso establecido por el TOE impide que personal no autorizado pueda acceder a la gestión del mismo (O.SEC_MNG), mientras que el establecimiento de canales seguros con los dispositivos IT externos que acceden a la configuración en remoto permite proteger la confidencialidad e integridad de los datos durante su tránsito. El entorno operacional debe garantizar que se proporcionan los medios (IT y humanos), políticas de uso y procedimientos adecuados, y que éstos se aplican debidamente, para garantizar que la conexión y configuración, por parte de un usuario autorizado, se realiza de forma correcta, contribuyendo a evitar una operación inadecuada del equipo debido a la gestión negligente de los usuarios autorizados en el mismo, sus credenciales y permisos asignados, a una configuración incorrecta o insegura o a una conexión incorrecta que pudiera permitir la circulación de datos de usuario por caminos diferentes al TOE (OE.TRUSTED_USR, OE.SEC_OP).
OSP.TAMP_MEC	El TOE es capaz de detectar determinados intentos de manipulación física, ataque o condiciones anómalas de operación y considerarlos como eventos de tamper. Para ello, el TOE ejecuta durante toda su operación chequeos automáticos del estado (integridad) de los sensores y mecanismos anti-tamper activos dispuestos para ello. La detección por parte del TOE de cualquiera de los eventos de tamper definidos para el mismo (manipulación física o comportamiento anómalo en su operativa habitual) provoca su entrada en un estado seguro (NO operativo), para cuya recuperación se requiere, al menos, la intervención de un Administrador de Seguridad, protegiendo de esa forma el acceso a los datos sensibles que almacena y contribuyendo a que dichos intentos no pasen de forma inadvertida (O.TAMPER_DET, O.SEC_STATE).

Tabla 8. Justificación de Suficiencia para las Políticas Organizativas de Seguridad

43 Justificación de suficiencia para las hipótesis:

A.TRUSTED_USR	Esta hipótesis queda totalmente cubierta con el objetivo del entorno operacional (OE.TRUSTED_USR).
A.CRYPTO	Esta hipótesis queda totalmente cubierta con el objetivo del entorno operacional (OE.CRYPTO).
A.SEC_OP	Esta hipótesis queda totalmente cubierta con el objetivo del entorno operacional (OE.SEC_OP).
A.PHY_ACC	Esta hipótesis queda totalmente cubierta con el objetivo del entorno operacional (OE.PHY_ACC).

Tabla 9. Justificación de Suficiencia para las Hipótesis

7. DEFINICIÓN DE COMPONENTES EXTENDIDOS

7.1. COMPONENTE EXTENDIDO: "IMPORT OF TSF DATA FROM OUTSIDE OF THE TOE (FPT_ITK)"

Justificación

44 Para ciertos procesos llevados a cabo por el TOE, es necesario realizar previamente la importación de datos sensibles o no sensibles (TSF Data) desde otro dispositivo externo al TOE, de forma que éste pueda hacer uso de ellos. Este tipo de operaciones constituyen una importación de TSF Data desde fuera del TOE, bajo determinadas reglas de control, dependientes del tipo de TSF Data.

45 La clase estándar FPT (Protection of the TSF), bajo la que se recogen los requisitos que definen las protecciones en referencia a la TSF y los TSF Data, no dispone de ninguna familia estándar que permita definir las condiciones o reglas a cumplir en caso de requerir la importación de TSF Data.

46 Se considera necesario, por tanto, definir una nueva familia, dentro de la clase FPT (Protection of the TSF), que permite establecer las condiciones y reglas para importación de TSF Data desde el exterior del TOE. Se denomina a esta nueva familia "FPT_ITK Import of TSF Data from outside of the TOE", siendo su definición la siguiente:

Family Behaviour

47 This family defines the mechanisms for importing of TSF data into the TOE such that it is appropriately controlled and/or protected. It is concerned with limitations on importation and determination of importation control rules to be applied.

Component levelling

FPT_ITK Import of TSF Data from outside of the TOE	→	1

48 FDP_ITK.1 Import of TSF data from outside of the TOE, provides the ability to define the types of TSF data that can be imported together with the importation control rules to be applied in order to make sure that the importation operation is allowed.

Management: FPT_ITK.1

49 There are no management activities foreseen.

Audit: FPT_ITK.1

50 There are no auditable events foreseen.

7.1.1. FPT_ITK Import of TSF Data from outside of the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITK.1.1 The TSF shall provide the ability to import the following TSF data from outside of the TOE: [assignment: list of TSF data to be imported].

FPT_ITK.1.2 The TSF shall enforce the following rules when importing TSF data controlled under the TSF from outside the TOE: [assignment: importation control rules to be applied].

8. REQUISITOS DE SEGURIDAD

8.1. REQUISITOS FUNCIONALES DE SEGURIDAD (SFRS)

51 De acuerdo con la implementación del TOE, y en base a las limitaciones e instrucciones proporcionadas para ello en la normativa CC aplicada (ver apartado 4.1), algunos de los requisitos funcionales de seguridad (SFRs) incluidos a continuación han sido "refinados" ("refinement operation") con el objetivo de restringir su aplicación a determinados objetos, sujetos o atributos o de especificar con mayor detalle o claridad la forma en que se cumple o aplica el requisito. Para facilitar su identificación, las pequeñas alteraciones realizadas para ello, se marcan en el texto utilizando fuente ~~tachada~~ (eliminaciones) y *cursiva* (añadidos).

52 Del mismo modo, en algunos casos, el cumplimiento (para todos los objetos, sujetos o atributos o para parte de ellos) de la dependencia de un SFR respecto a otro, se alcanza mediante la inclusión de un SFR jerárquicamente superior al explícitamente indicado en la dependencia, cumpliendo de este modo implícitamente la dependencia mínima requerida. Para facilitar su identificación, dichos casos se marcarán con el símbolo (*) junto a la dependencia afectada.

8.1.1. FAU_ARP.1 Security Alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [the following actions:

- Equipment STATUS modification to "NO INSTALADO" or "DESPROGRAMADO", according to detected tamper event level.
- Make unavailable access to certain keys and/or secrets stored in the security supervisor, according to detected tamper event level.

- Equipment reboot.
- The corresponding audit event(s) registering, according to audit registering filter configuration.]

upon detection of a potential security violation.

8.1.2. FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [alarm events defined for the TOE].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [level of severity of event].

8.1.3. FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification (*)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

8.1.4. FAU_SAA.1 Potential Violation Analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [audit events whose source is “anti-tamper”] known to indicate a potential security violation;

b) [none].

8.1.5. FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [those users whose roles are “Administrador de Configuración” or “Operador” (depending on the assigned set of

rights)] with the capability to read [all the information associated to each event] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

8.1.6. FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide *authorized users whose roles are "Administrador de Configuración" or "Operador" (depending on the assigned set of rights)* the ability to apply [filter criteria for visualization] of audit data based on [type(s), level of severity and source of the events; and additionally based on:

a) Either date and time range and/or text contained in the short description of the event and/or user identity (when applicable according to source selected), provided that they are visualized through the web interface,

b) Or index of the event in the audit record, provided that they are visualized through the console interface].

8.1.7. FAU_SEL.1(AR) Selective Audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1(AR) The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [event type,]

b) [minimum level of severity and/or source(s).]

Application Note: event source “antitamper” is not selectable, as events coming from this source are always registered, so this source is out of the scope of this SFR.

Application Note: selection of the event source “manager” is out of the scope of this SFR, as it refers to events derived from operation / management of the IS101 from the compatible associated Management Center IS101M, which is out of the scope of the CC evaluation for the IS101 according to this security target.

8.1.8. FAU_SEL.1(SNMP) Selective Audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

FAU_SEL.1.1(SNMP) The TSF shall be able to select the set of events to be *sent to an external SNMP supervisor as traps SNMPv3 so that they can be* audited from the set of all auditable events based on the following attributes:

a) [event type,]

b) [minimum level of severity and/or source(s).]

8.1.9. FAU_STG.2 Guarantees of Audit Data Availability

Hierarchical to: FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [a minimum number of 6.800] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion, failure or attack].

8.1.10. FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage (*)

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [register the corresponding audit event, according to audit registering filter configuration] if the audit trail is full.

8.1.11. FDP_ACC.1(INY) Subset Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1*(INY)* Security attribute based access control

FDP_ACC.1.1(INY) The TSF shall enforce the [FillDev_Access_Control_SFP] on: [

- Subjects: Users whose role corresponds to “Administrador de Seguridad”,
- Objects: TOE configuration parameters and information available through the display menu,
- Operations: access and/or execution of administration operations available through the display menu].

8.1.12. FDP_ACC.1(USR) Subset Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1*(USR)* Security attribute based access control

FDP_ACC.1.1(USR) The TSF shall enforce the [User_Access_Control_SFP] on: [

- Subjects: Users whose role corresponds to “Administrador de Configuración” or “Operador”,
- Objects: TOE configuration parameters (including the ones associated to “Operador” role users) and audit record,
- Operations: creation, query, modification and/or deletion of objects indicated, depending on their assigned set of rights available through the console interface or the secure web configuration interface].

8.1.13. FDP_ACF.1(INY) Security Attribute Based Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1*(INY)* Subset access control

FDP_MSA.3*(INY)* Static attribute initialization

FDP_ACF.1.1(INY) The TSF shall enforce the [FillDev_Access_Control_SFP] to objects based on the following: [

- Subjects: Users whose role corresponds to “Administrador de Seguridad”,
- Subjects named groups of SFP-relevant security attributes: set of rights enabled for the authorized user and fill device assigned authentication PIN,

- Objects: TOE configuration parameters and information available through the display menu,
- Objects SFP-relevant security attributes: none].

FDP_ACF.1.2(INY) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [FillDev_Access_Control_SFP operations of subjects over controlled objects are allowed only if the associated right is activated for the authorized user].

FDP_ACF.1.3(INY) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [the authorized user whose role corresponds to “Administrador de Seguridad” can perform the following actions through the display menu, with no need to have a specific right enabled for this:

- Operations allowed before user identification and authentication (see FIA_UID.1(INY) and/or FIA_UAU.1(INY) requirement(s));
- Operations requiring previous authentication but no specific rights for its access or execution, such as access (read only) to basic red and black network interfaces configuration (MAC and IP addresses) and statistics, and to visualization of the set of rights programmed in the validated fill device or uploading of configuration parameters (network parameters and/or IPsec parameters) stored in the associated fill device].

FDP_ACF.1.4(INY) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [authentication failure or associated fill device not detected or in blocked status].

8.1.14. FDP_ACF.1(USR) Security Attribute Based Access Control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1*(USR)* Subset access control

FDP_MSA.3*(USR1)* Static attribute initialization

FDP_MSA.3*(USR2)* Static attribute initialisation

FDP_ACF.1.1(USR) The TSF shall enforce the [User_Access_Control_SFP] to objects based on the following: [

- Subjects: Users whose role corresponds to “Administrador de Configuración” or “Operador”,
- Subjects named groups of SFP-relevant security attributes: set of rights enabled for the authorized user and users assigned authentication password,
- Objects: TOE configuration parameters (including the ones associated to “Operador” role users) and audit record,
- Objects SFP-relevant security attributes: none].

FDP_ACF.1.2(USR) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [User_Access_Control_SFP operations of subjects over controlled objects are allowed only if the associated right is activated for the authorized user].

FDP_ACF.1.3(USR) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [the authorized user whose role corresponds to “Administrador de Configuración” or “Operador” can perform the following actions through the console interface and/or the secure web interface, with no need to have a specific right enabled for this:

- Operations allowed before user identification and authentication (see FIA_UID.1(USR) and/or FIA_UAU.1(USR) requirement(s));
- Operations requiring previous authentication but no specific rights for its access or execution, such as modification of its own full name and password and, only for users trying to access through console interface (what requires physical access), visualization of available commands help and local management of files temporary storage].

FDP_ACF.1.4(USR) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [authentication failure or maximum number of simultaneous active sessions met for the corresponding access method: maximum 1 active session for access through the console interface and maximum 8 active sessions for access through the secure web interface)].

8.1.15. FDP_IFC.1 Subset Information Flow Control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [UserData_Flow_Control_SFP] on [

- Subjects: instances of the TOE,
- Information: **USER_DATA** packet flows,

- Operations: information flows management to perform, according to rules determined through FDP_IFF.1 requirement, one of the following actions:
  - IP packet processing (including or not encryption/decryption), depending on its attributes and the TOE configuration) and forwarding to the black network (through the secure IPsec tunnel previously established, when applicable) or to the corresponding entity in the red network, depending on flow bound, or
  - IP packet discarding].

8.1.16. FDP_IFF.1 Simple Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3*(IFC)* Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [UserData_Flow_Control_SFP] based on the following types of subject and information security attributes: [

- Subject (TOE instance) Security Attributes:
  - TOE configured security policy settings
  - TOE identity credentials (when applicable)
- Information Security Attributes:
  - Source / destination IP address
  - Source / destination port number
  - Protocol].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the

following rules hold: [all the information security attribute values of the corresponding IP packet are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the configured security policy settings (“protect” type or “bypass” type security policies) and associated information flow security attributes, created by the authorized users for that TOE].

FDP_IFF.1.3 The TSF shall enforce the [forwarding of specific (sensitive) user data information flows through the corresponding IPsec Security Association (control security association + child security association) previously established when the security attribute values of the corresponding IP packet are unambiguously permitted (see element FDP_IFF1.2 above) and shall be managed under the rules determined by a “protect” type configured security policy].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [

- information security attribute values of the corresponding IP packet are either not matching any of the rules that explicitly permit information flows or are unambiguously denied by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the configured security policy settings (“discard” type security policies) and associated information flow security attributes, created by the authorized users for that TOE].

8.1.17. FIA_AFL.1(INY) Authentication Failure Handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1*(INY)* Timing of authentication.

FIA_AFL.1.1(INY) The TSF shall detect when [five (5)] unsuccessful authentication attempts occur related to [fill device PIN code validation involved within authentication process for the user to which it has been assigned, whose user role corresponds to "Administrador de Seguridad"].

FIA_AFL.1.2(INY) When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [

- Not allowing new authentication attempts for that user; while the associated fill device keeps in blocked status and
- Notify the corresponding status error for the inserted fill device through the integrated display].

8.1.18. FIA_AFL.1(USR) Authentication Failure Handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1*(USR)* Timing of authentication.

FIA_UAU.2 User authentication before any action. (*)

FIA_AFL.1.1(USR) The TSF shall detect when [one (1)] unsuccessful authentication attempts occur related to ["Administrador de Configuración" or "Operador" role user authentication].

FIA_AFL.1.2(USR) When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [

- Wait 1 second before allowing a new authentication attempt and
- Register the corresponding audit event, according to audit registering filter configuration].

8.1.19. FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users, *whose user role corresponds to "Administrador de Configuración" or "Operador"*: [username and associated password].

8.1.20. FIA_SOS.1(INY) Verification of Secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1(INY) The TSF shall provide a mechanism to verify that secrets *used as PIN for fill devices assigned to individual users whose user role corresponds to "Administrador de Seguridad"* meet [the following conditions: size from 8 to 16 decimal digits].

8.1.21. FIA_SOS.1(USR) Verification of Secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1(USR) The TSF shall provide a mechanism to verify that secrets *used as passwords for individual users whose user role corresponds to "Administrador de Configuración" or "Operador"* meet [the following conditions: secret size from 8 to 16 alphanumeric characters].

8.1.22. FIA_UAU.1(INY) Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1*(INY)* Timing of identification

FIA_UAU.1.1(INY) The TSF shall allow [*a user, with physical access to the TOE, to perform the following actions through the display menu:*

- Same actions included in FIA_UID.1(INY) requirement;

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(INY) The TSF shall require each user*, with physical access to the TOE,* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.1.23. FIA_UAU.1(USR) Timing of Authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1*(USR)* Timing of identification

FIA_UAU.1.1(USR) The TSF shall allow [*a user, trying to access through secure web interface, to perform the following actions:*

- Same actions included in FIA_UID.1(USR) requirement;

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(USR) The TSF shall require each user*, trying to access through secure web interface,* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.1.24. FIA_UAU.2 User Authentication Before any Action

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.2 User Identification Before Any Action (*)

FIA_UAU.2.1 The TSF shall require each user*, trying to access through console interface (what requires physical access to the TOE)*, to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.1.25. FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [a fill device together with its corresponding PIN code or the combination of username and password] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [associated authentication mechanism, dependent on access method, as follows:

- For users with physical access, trying to access to display menú: authentication is based on insertion of a compatible key fill device and validation using its associated PIN code.
- For users trying to access through console interface (what requires physical access) or through secure web interface: authentication is based username and password insertion].

8.1.26. FIA_UID.1(INY) Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1(INY) The TSF shall allow [*a user, with physical access to the TOE, to perform the following actions through the display menu:*

- Display menu language selection;
- Visualization of display menu home window containing information about equipment general status, network interfaces status and configured date/time;
- Visualization of basic equipment information: model, serial number and software version and
- Visualization of essential information for maintenance purposes: battery charge status and internal components temperature;]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(INY) The TSF shall require each user*, with physical access to the TOE,* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

8.1.27. FIA_UID.1(USR) Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1(USR) The TSF shall allow [*a user, trying to access through secure web interface, to perform the following actions:*

- Web interface language selection;

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(USR) The TSF shall require each user*, trying to access through secure web interface,* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

8.1.28. FIA_UID.2 User Identification Before Any Action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user*, trying to access through console interface (what requires physical access to the TOE),* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

8.1.29. FMT_MSA.1(IFC) Management of Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(IFC) The TSF shall enforce the [UserData_Flow_Control_SFP] to restrict the ability to [create, query, modify and/or delete] the security attributes [security policy settings and/or TOE identity credentials] to [the authorized users whose user role corresponds to: “Administrador de Configuración” or “Operador” (depending on their assigned set of rights)].

8.1.30. FMT_MSA.1(INY) Management of Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1*(INY)* Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(INY) The TSF shall enforce the [FillDev_Access_Control_SFP] to restrict the ability to [modify] the security attributes [PIN code of the fill device assigned to the user whose role corresponds to "Administrador de Seguridad"] to [himself once authenticated ("Administrador de Seguridad" user role) and provided that the corresponding right is enabled in the associated fill device].

8.1.31. FMT_MSA.1(USR1) Management of Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1*(USR)* Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(USR1) The TSF shall enforce the [User_Access_Control_SFP] to restrict the ability to [modify] the security attributes [user password, applicable to user whose role corresponds to "Administrador de Configuración"] to [himself once authenticated ("Administrador de Configuración" user role) or to a previously authenticated user with role "Administrador de Seguridad" and the appropriate right enabled in the associated fill device].

8.1.32. FMT_MSA.1(USR2) Management of Security Attributes

Hierarchical to: No other components.

Dependencies: FDP_ACC.1*(USR)* Subset access control

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(USR2) The TSF shall enforce the [User_Access_Control_SFP] to restrict the ability to [query, modify and/or assign initial values] the security attributes [user password and/or set of rights assigned to a specific user whose role corresponds to "Operador"] to [himself once authenticated (only applicable for own password modification) or to the following user roles: "Administrador de Configuración" or other "Operador" with the appropriate right enabled].

8.1.33. FMT_MSA.3(IFC) Static Attribute Initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1*(IFC)* Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [UserData_Flow_Control_SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [following user roles: "Administrador de Configuración" or "Operador" (depending on their assigned set of rights)] to specify alternative initial values to override the default values when an object or information is created.

8.1.34. FMT_MSA.3(INY) Static Attribute Initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1*(INY)* Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(INY) The TSF shall enforce the [FillDev_Access_Control_SFP] to provide [minimum 8 decimal digits length] default values for *the following* security attributes*: PIN code of the fill device assigned to the user whose role corresponds to "Administrador de Seguridad",* that are used to enforce the SFP.

FMT_MSA.3.2(INY) The TSF shall allow the [himself once authenticated ("Administrador de Seguridad" user role) and provided that the corresponding right is enabled in the associated fill device] to specify alternative initial values to override the default values when an object or information is created.

8.1.35. FMT_MSA.3(USR1) Static Attribute Initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1*(USR1)* Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(USR1) The TSF shall enforce the [User_Access_Control_SFP] to provide [not specified] default values for *the following* security attributes*: user password, applicable to user whose role corresponds to "Administrador de Configuración",* that are used to enforce the SFP.

FMT_MSA.3.2(USR1) The TSF shall allow the [a previously authenticated user with role "Administrador de Seguridad" and the appropriate right enabled in

the associated fill device] to specify alternative initial values to override the default values when an object or information is created.

8.1.36. FMT_MSA.3(USR2) Static Attribute Initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1*(USR2)* Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1(USR2) The TSF shall enforce the [User_Access_Control_SFP] to provide [restrictive] default values for *the following* security attributes*: user password and/or set of rights assigned to users whose role corresponds to "Operador",* that are used to enforce the SFP.

FMT_MSA.3.2(USR2) The TSF shall allow the [following user roles: either "Administrador de Configuración" or "Operador" with the appropriate right enabled] to specify alternative initial values to override the default values when an object or information is created.

8.1.37. FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify and/or delete] the [TSF configuration parameters] to [the authorized users, whose user role corresponds to "Administrador de Seguridad" (depending on their assigned set of rights), "Administrador de Configuración" or "Operador" (depending on their assigned set of rights), according to

operations available for each role as defined in FMT_SMF.1 requirement].

8.1.38. FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- Users whose role corresponds to “Administrador de Configuración”, “Operador” (depending on their assigned set of rights):
  - Visualization and configuration of the audit record (including filters associated) and SNMPv3 traps sending functionality (including filter associated and supervisor parameters);
  - Creation, query, modification and/or deletion of TSF configuration parameters (i.e. network configuration, IPsec configuration…) and its security attributes;
  - Configuration of system time and/or timezone attributes;
  - Operations allowed before user identification and authentication, when accessing through the secure web interface (see FIA_UID.1(USR) and/or FIA_UAU.1(USR) requirement(s));
  - Download, restore and deletion of current TOE configuration and TOE rebooting invocation;

- Invocation of utilities for testing other equipments reachability / routability from red / black interface.
- Creation, query, deletion and/or modification of users with user role “Operador” and its security attributes;
- Modification of own associated password and full name;
- Only for users trying to access through console interface (what requires physical access), visualization of available commands help and local management of files temporary storage;

o Users whose role corresponds to “Administrador de Seguridad”: administration operations performed through the display menu, including:

- Operations allowed before user identification and authentication (see FIA_UID.1(INY) and/or FIA_UAU.1(INY) requirement(s));
- Visualization of network interfaces addresses configured and statistics;
- Visualization of the set of rights programmed in the validated fill device;
- Uploading of configuration parameters (network parameters and/or IPsec parameters) stored in the associated fill device;
- Other security-enforced operations such as installation, security options configuration, “Administrador de Configuración” password configuration, fill device PIN code modification,

main software version update and web access certificates management].

8.1.39. FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1*(INY)* Timing of identification

FIA_UID.1*(USR)* Timing of identification

FIA_UID.2 User Identification Before Any Action (*)

FMT_SMR.1.1 The TSF shall maintain the roles [

- User role “Administrador de Seguridad”;
- User role “Administrador de Configuración”;
- User role “Operador”].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

8.1.40. FPT_FLS.1 Failure with Preservation of Secure State

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- Physical attacks declared in FPT_PHP.3 requirement;
- Emergency button activation;
- Internal security supervisor reset or self-tests failure].

8.1.41. FPT_ITK.1 Import of TSF Data from Outside of the TOE

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITK.1.1 The TSF shall provide the ability to import the following TSF data from outside of the TOE: [encrypted file containing a new software (signed) version for the main processor].

FPT_ITK.1.2 The TSF shall enforce the following rules when importing TSF data controlled under the TSF from outside the TOE: [

- In order to allow importation process to start, an "Administrador de Seguridad" role user must be authenticated against the TOE, using a fill device with the data required to be allowed to invoke software updating process.
- In order to succeed, the mentioned data (contained in the fill device used for authentication) must be the same used in origin for encryption of the updating file provided to the equipment within the process].

8.1.42. FPT_PHP.3 Resistance to Physical Attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [the following potentially hazardous situations (considered as physical attacks):

- External power supply overvoltage;
- Battery overvoltage;
- High temperature;

- Low temperature;
- Standard case opening;
- Total absence of power supply;
- Hardware manipulation of specific sensitive components].

to the [TSF] by responding automatically such that the SFRs are always enforced.

Application Note: standard case opening referred in this SFR means opening the IS101 by screwing up the corresponding screws and mechanical pieces.

8.1.43. FPT_RCV.1 Manual Recovery

Hierarchical to: No other components.

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.1.1 After [a tamper event] the TSF shall enter a ~~maintenance mode~~ *tamper state* where the ability to return to a secure state is provided.

8.1.44. FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

8.1.45. FPT_TST.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self-tests [periodically during operation] to demonstrate the correct operation of the [TSF anti-tamper mechanisms].

FPT_TST.1.2 The TSF shall provide authorised users, *whose user role corresponds to "Administrador de Configuración" or "Operador" (depending on their assigned set of rights),* with the capability to verify the integrity of [specific sensitive data (required for allowing equipment successful start-up), by means of rebooting the equipment].

FPT_TST.1.3. The TSF shall provide authorised users, *with physical access to the TOE,* with the capability to verify the integrity of [TSF anti-tamper mechanisms].

8.1.46. FTA_SSL.3 TSF-Initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session *of the following user roles: "Administrador de Configuración" or "Operador"* after a [pre-defined maximum time of inactivity: 10 minutes, for access through secure web interface, and 5 minutes, for access through console interface].

8.1.47. FTA_SSL.4 User-Initiated Termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

8.1.48. FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [another trusted IT product] to initiate communication via the trusted channel *for at least the following management functions:*

- *Remote initialization / management from the corresponding secure web interface;*

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [no additional management functions foreseen].

8.2. REQUISITOS DE GARANTÍA DE SEGURIDAD (SARS)

53 A continuación, a modo de resumen, se incluye un listado de los requisitos de garantía de seguridad (SARs) aplicables al TOE, de acuerdo con la declaración de conformidad referida en el apartado 4.1. Los componentes resaltados en negrita se corresponden con los componentes aumentados.

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete Functional Specification
	ADV_IMP.1	Representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and Automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.1	**Basic Flaw Remediation**
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample

Assurance Class	Assurance Components	
Vulnerability Assessment	AVA_VAN.3	Focused Vulnerability Analysis

Tabla 10. Listado SARs

8.2.1. Justificación

54 La elección del nivel de evaluación referido en el apartado 4.1 y, en consecuencia, del conjunto de SARs aplicables (presentado en la Tabla 10), se ha realizado en consonancia con el entorno de amenazas experimentado por los consumidores típicos del TOE.

8.3. CONCLUSIÓN DE REQUISITOS DE SEGURIDAD

55 En la siguiente tabla se muestra la relación entre los objetivos de seguridad que debe proporcionar el TOE y los diferentes requisitos de seguridad (SFRs) que debe cumplir para alcanzar dichos objetivos, de forma que quede de manifiesto que todos los SFRs quedan trazados con al menos un objetivo de seguridad y viceversa.

OBJETIVOS DE SEGURIDAD / SFRs	O.TRAFFIC	O.SEC_MNG	O.TAMPER_DET	O.SEC_STATE	O.AUDIT_REG	O.AUDIT_SNMP
FAU_ARP.1				X	X	
FAU_GEN.1					X	X
FAU_GEN.2					X	X
FAU_SAA.1					X	
FAU_SAR.1					X	
FAU_SAR.3					X	

OBJETIVOS DE SEGURIDAD / SFRs	O.TRAFFIC	O.SEC_MNG	O.TAMPER_DET	O.SEC_STATE	O.AUDIT_REG	O.AUDIT_SNMP
FAU_SEL.1(AR)					X	
FAU_SEL.1(SNMP)						X
FAU_STG.2					X	
FAU_STG.4					X	
FDP_ACC.1(INY)		X				
FDP_ACC.1(USR)		X				
FDP_ACF.1(INY)		X				
FDP_ACF.1(USR)		X				
FDP_IFC.1	X					
FDP_IFF.1	X					
FIA_AFL.1(INY)		X				
FIA_AFL.1(USR)		X				
FIA_ATD.1		X				
FIA_SOS.1(INY)		X				
FIA_SOS.1(USR)		X				
FIA_UAU.1(INY)		X				
FIA_UAU.1(USR)		X				
FIA_UAU.2		X				
FIA_UAU.5		X				
FIA_UID.1(INY)		X				
FIA_UID.1(USR)		X				

OBJETIVOS DE SEGURIDAD / SFRs	O.TRAFFIC	O.SEC_MNG	O.TAMPER_DET	O.SEC_STATE	O.AUDIT_REG	O.AUDIT_SNMP
FIA_UID.2		X				
FMT_MSA.1(IFC)	X					
FMT_MSA.1(INY)		X				
FMT_MSA.1(USR1)		X				
FMT_MSA.1(USR2)		X				
FMT_MSA.3(IFC)	X					
FMT_MSA.3(INY)		X				
FMT_MSA.3(USR1)		X				
FMT_MSA.3(USR2)		X				
FMT_MTD.1	X	X			X	X
FMT_SMF.1	X	X			X	X
FMT_SMR.1	X	X			X	X
FPT_FLS.1				X		
FPT_ITK.1		X				
FPT_PHP.3			X			
FPT_RCV.1				X		
FPT_STM.1					X	X
FPT_TST.1			X	X		
FTA_SSL.3		X				
FTA_SSL.4		X				
FTP_ITC.1	X	X				

Tabla 11. Matriz de Trazabilidad: SRFs vs. Objetivos de Seguridad del TOE

8.3.1. Justificación

56 En la siguiente tabla se recoge la justificación que permite demostrar que la trazabilidad proporcionada entre los requisitos de seguridad (SFRs) y los objetivos de seguridad del TOE es consistente y completa.

OBJETIVO	SFRs	Justificación
O.TRAFFIC	FDP_IFC.1 FDP_IFF.1 FMT_MSA.1(IFC) FMT_MSA.3(IFC) FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FTP_ITC.1	El TOE es capaz de procesar y manejar el tráfico de datos de usuario que circula entre sus interfaces rojo y negro en base a las reglas determinadas por las políticas de seguridad IPsec configuradas y, en función de ello, descartar o permitir el flujo de información y, para aquellos permitidos, cuando aplique, encaminarlos a través del correspondiente túnel IPsec previamente establecido. Las reglas que determinan qué paquetes de tráfico IP se permiten (a través de una asociación de seguridad de usuario o no, según aplique) y cuáles se descartan, vienen impuestas por la política de control de flujo implementada en el TOE (FDP_IFC.1, FDP_IFF.1). Dichas reglas son resultado de la configuración TSF del TOE en lo referente a políticas de seguridad IPsec (incluyendo tipo de política, selectores de tráfico y, en su caso, las credenciales IPsec, algoritmos permitidos para la negociación...). Los valores por defecto para los parámetros asociados a dicha configuración TSF del TOE son restrictivos (FMT_MSA.3(IFC)) y su gestión únicamente pueden realizarla determinados roles de usuario, una vez autenticados y siempre que tengan permitida la operación correspondiente y/o dispongan de los permisos adecuados para ello (FMT_MSA.1(IFC), FMT_MSA.3(IFC), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). Así mismo, para el acceso a la configuración del TOE a través de ciertos interfaces, el TOE emplea canales seguros (FTP_ITC.1).
O.SEC_MNG	FDP_ACC.1(INY) FDP_ACC.1(USR) FDP_ACF.1(INY) FDP_ACF.1(USR) FIA_AFL.1(INY) FIA_AFL.1(USR) FIA_ATD.1 FIA_SOS.1(INY)	El TOE establece un sistema de control de acceso que define diferentes roles de usuario (FMT_SMR.1) para acceder a la gestión del equipo, limitando las operaciones a realizar por cada uno de ellos, en base a las políticas de control de acceso definidas en el equipo, según perfil y/o permisos habilitados en cada caso (FDP_ACC.1(INY), FDP_ACC.1(USR), FDP_ACF.1(INY), FDP_ACF.1(USR)). Asimismo, para la implementación de dichas políticas de control de acceso, se incluyen los SFRs que permiten definir:

OBJETIVO	SFRs	Justificación
	FIA_SOS.1(USR) FIA_UAU.1(INY) FIA_UAU.1(USR) FIA_UAU.2 FIA_UAU.5 FIA_UID.1(INY) FIA_UID.1(USR) FIA_UID.2 FMT_MSA.1(INY) FMT_MSA.1(USR1) FMT_MSA.1(USR2) FMT_MSA.3(INY) FMT_MSA.3(USR1) FMT_MSA.3(USR2) FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FPT_ITK.1 FTA_SSL.3 FTA_SSL.4 FTP_ITC.1	○ Los mecanismos de identificación y autenticación de los diferentes usuarios, en función de su método de acceso, así como, cuando procede, las acciones permitidas previamente (FIA_UAU.1(INY), FIA_UAU.1(USR), FIA_UAU.2, FIA_UAU.5, FIA_UID.1(INY), FIA_UID.1(USR), FIA_UID.2). ○ Los atributos de seguridad y/o secretos empleados para el proceso de identificación / autenticación de los distintos usuarios y sus características necesarias (cuando se especifiquen/verifiquen a través del equipo), según aplique en cada caso (FIA_ATD.1, FIA_SOS.1(INY), FIA_SOS.1(USR),). ○ La gestión y, en su caso, valores por defecto seguros para los atributos de seguridad en cada caso (FMT_MSA.1(INY), FMT_MSA.1(USR1), FMT_MSA.1(USR2), FMT_MSA.3(INY), (FMT_MSA.3(USR1), FMT_MSA.3(USR2)). ○ Las operaciones de configuración y gestión (pudiendo incluir la invocación de los mecanismos seguros dispuestos para actualizar el SW principal que almacena) permitidas para cada rol de usuario y el manejo de datos TSF asociados (FMT_SMF.1, FMT_MTD.1, FPT_ITK.1. ○ Los límites y acciones derivadas a ejecutar en caso de fallos de autenticación (FIA_AFL.1(INY), FIA_AFL.1(USR)). ○ Las opciones disponibles para el cierre de sesiones abiertas y acciones a ejecutar en caso de inactivada en las sesiones abiertas (FTA_SSL.3, FTA_SSL.4). ○ Los requisitos respecto a la necesidad de establecer canales seguros para interacción de los usuarios con el equipo según el método de acceso (FTP_ITC.1).
O.TAMPER_DET	FPT_PHP.3 FPT_TST.1	El TOE implementa mecanismos que le permiten chequear periódicamente, la integridad de los sensores y mecanismos anti-tamper incluidos en el mismo y, de esta forma, detectar determinados intentos de manipulación física, ataque o condiciones anómalas de operación, tanto en presencia como en ausencia de la alimentación externa, y considerarlos como eventos de tamper (FPT_PHP.3, FPT_TST.1).

OBJETIVO	SFRs	Justificación
O.SEC_STATE	FAU_ARP.1 FPT_FLS.1 FPT_RCV.1 FPT_TST.1	El TOE entra en un estado seguro (NO operativo) al detectar cualquiera de los eventos de tamper definidos para el mismo: ataque físico, activación del pulsador de emergencia o comportamiento anómalo del supervisor de seguridad (FPT_FLS.1, FPT_TST.1). Esto provoca, asimismo, que el equipo desencadene acciones orientadas a proteger el acceso a los activos que almacena y situarse en un estado seguro (FAU_ARP.1). Para devolver el equipo al estado operativo es necesario al menos, la intervención de un Administrador de Seguridad (FPT_RCV.1).
O.AUDIT_REG	FAU_ARP.1 FAU_GEN.1 FAU_GEN.2 FAU_SAA.1 FAU_SAR.1 FAU_SAR.3 FAU_SEL.1(AR) FAU_STG.2 FAU_STG.4 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FPT_STM.1	El TOE mantiene un registro de auditoría, en memoria no volátil, de los eventos relevantes desde el punto de vista de la seguridad. Para cada alarma se anotan su marca temporal, tipo (categoría(s)), nivel de gravedad, fuente y, cuando aplique, la identidad del usuario/inyector asociado (FAU_GEN.1, FAU_GEN.2, FPT_STM.1). Cuando estos eventos proceden de la fuente denominada “antitamper”, se consideran potenciales violaciones de la seguridad (ataques) y el equipo desencadena acciones orientadas a proteger los activos que almacena y situarse en un estado seguro (FAU_ARP.1, FAU_SAA.1). La visualización de los eventos registrados, y toda su información asociada, está disponible para determinados roles de usuario (una vez autenticados y conforme a su esquema de permisos), pudiendo establecer, en función del método de acceso, criterios adicionales para el filtro de visualización en vía a facilitar su revisión (FAU_SAR.1, FAU_SAR.3). El conjunto de eventos relevantes a registrar de entre todos los posibles es configurable, en base a diferentes criterios fijados por determinados roles de usuario (una vez autenticados y conforme a su esquema de permisos) a través de la configuración del filtro de alarmas a registrar (FAU_SEL.1(AR), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). El registro de auditoría está protegido frente a modificación, se garantiza espacio suficiente para un mínimo número de alarmas, incluso en caso de llenado del registro, ataque o fallo (FAU_STG.2) y es cíclico, de forma que cuando el registro se llena se sobre-escriben por bloques las alarmas más antiguas (FAU_STG.4).

OBJETIVO	SFRs	Justificación
O.AUDIT_SNMP	FAU_GEN.1	El TOE permite enviar las alarmas generadas (FAU_GEN.1, FAU_GEN.2, FPT_STM.1) a un supervisor externo mediante el protocolo SNMPv3.
	FAU_GEN.2 FAU_SEL.1(SNMP) FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	El conjunto de alarmas a enviar al supervisor externo de entre todas las posibles es configurable, en base a diferentes criterios fijados por determinados roles de usuario (una vez autenticados y conforme a su esquema de permisos) a través de la configuración del filtro de alarmas SNMP (FAU_SEL.1(SNMP), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1).
	FPT_STM.1	Esta funcionalidad puede ser habilitada / deshabilitada por determinados roles de usuario (FMT_MTD.1, FMT_SMF.1).

Tabla 12. Justificación Trazabilidad: Objetivos de Seguridad del TOE - SFRs

9. ESPECIFICACIÓN RESUMIDA DEL TOE (TSS)

57 A continuación, a modo de resumen de la especificación del TOE, se proporciona una breve descripción de cómo éste satisfice los diferentes requisitos funcionales de seguridad incluidos en el apartado 6.1.

CLASE FAU: SECURITY AUDIT	
FAU_ARP.1	Ante la detección de una potencial violación de su seguridad (cualquier evento de tamper), el TOE lleva a cabo las siguientes acciones para protegerse: ○ Modificación del STATUS del TOE y, según el nivel del evento de tamper detectado, cambio del mismo a estado “NO INSTALADO” o “DESPROGRAMADO”. ○ Hacer inaccesibles ciertas claves y/o parámetros sensibles almacenados en el supervisor de seguridad, según el nivel del evento de tamper detectado. ○ Reinicio del equipo, provocando el reset de los componentes principales, incluyendo el procesador principal, su memoria volátil y la FPGA (provocando así su desconfiguración). ○ Registro de las correspondientes alarmas en el registro de auditoría, según la configuración vigente del filtro de alarmas a registrar.
FAU_GEN.1	El TOE almacena un registro de auditoría que permite registrar los eventos más relevantes que se producen en el equipo, desde el punto de vista de la seguridad (alarmas). Por cada evento (alarma) registrado, el TOE almacena: ○ Su marca temporal (fecha y hora), ○ la(s) categoría(s) en la(s) que se engloba (tipo de evento), ○ la fuente que ha generado el evento y, cuando aplique, la identificación del usuario/inyector correspondiente (identidad del sujeto), ○ la descripción del evento acontecido (que incluye implícitamente el resultado) y ○ su nivel de gravedad.

FAU_GEN.2	Por cada evento registrado, el TOE almacena la identidad de la fuente que lo ha generado. En el caso de que se trate de una fuente de tipo “usuario”, incluye, adicionalmente, el nombre del usuario (con perfil “Administrador de Configuración” u “Operador”) correspondiente. En el caso de que se trate de una fuente de tipo “inyector”, incluye, adicionalmente, el nombre del inyector asignado al usuario (con perfil “Administrador de Seguridad”) correspondiente.
FAU_SAA.1	El TOE considera los eventos de tamper como potenciales violaciones de su seguridad (ataques o comportamientos anómalos). Por ello, el registro de cualquier alarma cuya fuente de origen sea “antitamper” se considera una potencial violación de la seguridad del TOE, situándolo, en consecuencia, en un estado seguro (NO operativo). Para reforzar el registro de estas alarmas, la fuente “antitamper” NO es configurable a través del filtro de alarmas que se han de almacenar (definido por el requisito FAU_SEL.1(AR)), estando siempre seleccionada y, por tanto, las alarmas cuya fuente sea “antitamper” se registran siempre con independencia de la configuración establecida por dicho filtro.
FAU_SAR.1	El usuario con perfil “Administrador de Configuración” podrá siempre acceder a la visualización y gestión del registro de auditoría. Los usuarios con perfil “Operador” podrán acceder a la visualización y gestión del registro de auditoría sólo si tienen los permisos correspondientes habilitados.
FAU_SAR.3	El TOE proporciona mecanismos para filtrar los eventos a visualizar (de entre los almacenados en el registro de auditoría) de acuerdo a uno o varios de los siguientes atributos: ○ Categoría(s) del evento (tipo(s) de evento). ○ Nivel de gravedad del evento. ○ Fuente que ha generado el evento. Adicionalmente: ○ Cuando el registro de auditoría se visualiza a través del interfaz web, es posible también filtrar los eventos de acuerdo a uno o varios de los siguientes atributos: ▪ Fecha / hora (o rango de las mismas) del evento. ▪ Texto contenido en la descripción del evento. ▪ Cuando aplique (según fuente seleccionada), identificación del usuario/inyector asociado. ○ Cuando el registro de auditoría se visualiza a través del interfaz de consola, es posible también filtrar los eventos de acuerdo a su índice (posición) en el listado de eventos.

FAU_SEL.1(AR)	El TOE permite configurar un filtro que define el conjunto de eventos que se han de almacenar en el registro de auditoría, de acuerdo a uno o varios de los siguientes atributos: ○ Categoría(s) de los eventos a registrar (tipo de evento). ○ Nivel mínimo de gravedad de los eventos a registrar. ○ Fuente(s) de los eventos a registrar[10].
FAU_SEL.1(SNMP)	El TOE permite configurar un filtro que define el conjunto de eventos que se han de enviar a un supervisor SNMP externo como traps SNMPv3, de acuerdo a uno o varios de los siguientes atributos: ○ Categoría(s) de los eventos a enviar como trap SNMPv3 (tipo de evento). ○ Nivel mínimo de gravedad de los eventos a enviar como trap SNMPv3. ○ Fuente(s) de los eventos a enviar como trap SNMPv3. La configuración y aplicación de este filtro de eventos es independiente del filtro configurado para su almacenamiento en el registro de auditoría (definido en el requisito FAU_SEL.1(AR)), lo que permite emplear conjuntos de criterios independientes para el filtro de eventos a registrar en el TOE y para el filtro de eventos a enviar como trap SNMPv3 al gestor SNMP configurado.
FAU_STG.2	El número de eventos que puede llegar a contener el registro de auditoria depende del tamaño que requiera cada uno de ellos (campos “descripción”, “fuente”…). Se garantiza espacio suficiente para un mínimo de 6800 eventos. Ningún usuario autorizado (independientemente de su perfil y esquema de permisos asignado) puede modificar o borrar individualmente las entradas (alarmas) del registro de auditoría almacenado en el equipo. El borrado del registro de auditoría almacenado en el equipo sólo puede realizarse de forma completa, pudiendo esta operación llevarla a cabo un usuario autorizado: ○ con perfil “Administrador de Configuración”, o ○ con perfil “Operador”, si tiene los permisos correspondientes habilitados. Ante un fallo o evento de tamper (ataque) el registro de auditoría almacenado en el equipo persiste.

[10] Teniendo en cuenta las notas de aplicación incluidas en la definición de este SFR (ver apartado 8.1.7 del presente documento).

FAU_STG.4	Cuando el registro de auditoría alcanza su límite máximo de almacenamiento, se sobrescriben los eventos más antiguos. Dicha sobre-escritura se realiza por bloques de 128KB. Cuando se alcanza el límite máximo de almacenamiento, la siguiente alarma que deba registrarse, según la configuración vigente del filtro de alarmas a registrar, provoca que se borre el bloque (128KB) del registro de auditoría más antiguo en ese momento y se sobre-escriba la nueva alarma y las subsiguientes sobre el bloque previamente borrado. Así mismo, el borrado automático de un bloque de alarmas por sobre-escritura se anota en el registro de auditoría del equipo, según la configuración del filtro de alarmas a registrar.
CLASE FDP: USER DATA PROTECTION	
FDP_ACC.1(INY)	El TOE define una política de función de seguridad (SFP) denominada “FillDev_Access_Control_SFP” para el control de acceso de los usuarios con perfil “Administrador de Seguridad”. Para dicha política se definen a través de este requisito los sujetos (usuarios con perfil “Administrador de Seguridad”) y objetos (parámetros de configuración del TOE e información disponible a través del menú display) sobre los que se aplica, así como las posibles acciones a realizar (operaciones de administración disponibles a través del menú display); mientras que las reglas aplicables para dicho control se especifican a través del requisito FDP_ACF.1(INY).
FDP_ACC.1(USR)	El TOE define una política de función de seguridad (SFP) denominada “User_Access_Control_SFP” para el control de acceso de los usuarios con perfil “Administrador de Configuración” u “Operador”. Para dicha política se definen a través de este requisito los sujetos (usuarios con perfil “Administrador de Configuración” u “Operador”) y objetos (parámetros de configuración del TOE, incluidos los asociados a la configuración de usuarios con perfil “Operador”, y registro de auditoría) sobre los que se aplica, así como las posibles acciones a realizar (operaciones de gestión y configuración (para creación, consulta, modificación y/o borrado de los mismos) disponibles a través de los interfaces de consola y acceso web seguro); mientras que las reglas aplicables para dicho control se especifican a través del requisito FDP_ACF.1(INY). Nótese que la lista de usuarios con perfil “Operador” dados de alta en el TOE forma parte también de la configuración del mismo y, por tanto, las operaciones de creación, consulta, modificación y/o borrado de los mismos, están también cubiertas por la política de control de acceso descrita, existiendo un permiso específico asociado a las operaciones de manejo de la configuración de usuarios con perfil “Operador”.

FDP_ACF.1(INY)	En el TOE, la SFP "FillDev_Access_Control_SFP" se implementa por medio del sistema de control de acceso aplicable a los usuarios con perfil "Administrador de Seguridad", donde se establece que las operaciones de administración disponibles a través del menú display están permitidas, como normal general, una vez autenticado el usuario frente al TOE y siempre que el inyector empleado por dicho usuario disponga de el/los permiso/s correspondiente/s habilitado/s. Así mismo, en este requisito se definen: ○ Las excepciones a dicha política restrictiva de control de acceso: operaciones explícitamente permitidas de forma previa al proceso de identificación/autenticación del usuario o que no requieren disponer de ningún permiso específico en el inyector. ○ Las situaciones bajo las cuales se deniega explícitamente el acceso: fallo de autenticación del usuario, desconexión del inyector o inyector bloqueado. .
FDP_ACF.1(USR)	En el TOE, la SFP "User_Access_Control_SFP" se implementa por medio del sistema de control de acceso implementado para los usuarios con perfil "Administrador de Configuración" y "Operador", donde se establece que las operaciones de gestión y configuración disponibles a través del interfaz de consola o el interfaz web seguro están permitidas, como normal general, una vez autenticado el usuario frente al TOE y siempre que dicho usuario disponga de el/los permiso/s correspondiente/s habilitado/s. Así mismo, en este requisito se definen: ○ Las excepciones a dicha política restrictiva de control de acceso: operaciones explícitamente permitidas de forma previa al proceso de identificación/autenticación del usuario o que no requieren disponer de ningún permiso específico para el usuario. ○ Las situaciones bajo las cuales se deniega explícitamente el acceso: fallo de autenticación del usuario o alcance del máximo número de sesiones simultáneas a través del interfaz correspondiente (1 sesión activa máximo para el interfaz de consola y 8 sesiones activas máximo para el interfaz de configuración web seguro).
FDP_IFC.1	El TOE define una política de función de seguridad (SFP) denominada "User_Data_Flow_Control_SFP" para el control por parte del mismo de los flujos de datos de usuario **USER_DATA**. Para dicha política se definen a través de este requisito los sujetos (instancias del TOE) y flujos de información (datos de usuario) sobre los que se aplica, así como las posibles acciones a realizar (proteger, dejar pasar o descartar); mientras que las reglas aplicables para dicho control se especifican a través del requisito FDP_IFF.1.
FDP_IFF.1	En el TOE, la SFP "User_Data_Flow_Control_SFP" se implementa por medio de la aplicación de las políticas de seguridad IPsec configuradas en el equipo, que definen los requisitos que debe cumplir un flujo de paquetes para ser permitido o no y, para aquellos permitidos, bajo qué

	circunstancias deben ser enviados a través del correspondiente túnel IPsec previamente establecido. Las reglas de control a aplicar sobre los flujos de datos de usuario que atraviesan el TOE se determinan en base a los atributos de seguridad de los sujetos (parámetros de las políticas de seguridad IPsec configuradas - principalmente la acción a realizar y, cuando aplique, la suite(s) de algoritmos a ofrecer para el establecimiento del correspondiente túnel IPsec - y las credenciales para autenticación) y a los atributos de seguridad del propio flujo (paquete IP) (direcciones origen/destino, a puertos origen/destino o protocolo). De esta forma, un flujo de datos de usuario estará permitido únicamente si sus atributos de seguridad coinciden de forma no ambigua con las reglas inferidas de la configuración de conexiones expresamente permitidas para una política de seguridad de tipo “Protect” o “Bypass”. Adicionalmente, la política de control de flujo establece que, cuando un flujo permitido deba manejarse bajo las reglas inferidas de la configuración de conexiones expresamente permitidas para una política de tipo “Protect, se deberá transmitir a través de un túnel IPsec (asociación de seguridad de usuario) previamente establecido entre los extremos. No se establecen, reglas adicionales por las que un flujo de datos de usuario deba ser permitido, en base a sus atributos. Así mismo, establece las condiciones bajo las cuales se rechazarán (descartarán) explícitamente los flujos de datos usuario, cuando: ○ Cuando, en base a sus atributos, el tráfico no cumpla con ninguna de las reglas que explícitamente autorizan flujos de información o cumpla de forma no ambigua con alguna de las reglas inferidas de la configuración de conexiones expresamente prohibidas por una política de tipo “Discard” configurada en el equipo.

CLASE FIA: IDENTIFICATION AND AUTHENTICATION	
FIA_AFL.1(INY)	Los inyectores compatibles con el TOE, asociados a los usuarios con perfil “Administrador de Seguridad”, se programan en el centro de gestión correspondiente con un máximo de 5 intentos fallidos de inserción del código PIN asociado. Cuando se inserta el inyector en un IS101 y se solicita el PIN, cada vez que el usuario intenta validar el inyector empleando un código PIN de longitud adecuada (entre 8 y 16 dígitos) pero erróneo, el número máximo de intentos fallidos restantes se decrementa Así mismo, esta situación se notifica al usuario a través del display integrado en el equipo mediante el correspondiente mensaje de error. Cuando se valida el inyector con éxito empleando el código PIN correcto, el número máximo de intentos restantes se restaura a su valor original. Si se agota el número máximo de intentos fallidos sin éxito el inyector se bloquea. Si se introduce un inyector bloqueado en un IS101, éste lo detecta, y no se solicita el código PIN asociado no permitiendo, por tanto, la autenticación de dicho usuario mientras el inyector permanezca en estado bloqueado. Así mismo, esta situación se notifica al usuario a través del display integrado en el equipo mediante el correspondiente mensaje de error.
FIA_AFL.1(USR)	Los usuarios con perfil “Administrador de Configuración” u “Operador” deben autenticarse frente al TOE introduciendo su correspondiente nombre de usuario y contraseña asociada. Tanto a través del interfaz de consola como a través del interfaz web seguro, el TOE detecta cuando se realiza un intento fallido de autenticación (usuario desconocido o contraseña errónea), siendo necesario en ese caso, esperar 1 segundo antes poder volver a realizar un nuevo intento de autenticación. Así mismo, cada intento fallido de autenticación se anota en el registro de auditoría del equipo, según la configuración del filtro de alarmas a registrar.
FIA_ATD.1	El usuario con perfil “Administrador de Configuración” y cada usuario con perfil “Operador” dado de alta en la configuración del equipo tiene asociado un nombre de usuario y una contraseña independiente, para su acceso al sistema.
FIA_SOS.1(INY)	El TOE restringe los códigos PIN posibles de los inyectores asignados a los usuarios con perfil “Administrador de Seguridad” para que estén comprendidos entre 8 y 16 dígitos decimales.
FIA_SOS.1(USR)	El TOE restringe las contraseñas posibles de los usuarios con perfil “Administrador de Configuración” y “Operador” para que estén comprendidas entre 8 y 16 caracteres alfanuméricos.

FIA_UAU.1(INY)	El TOE implementa un control de accesos para asegurar que un usuario con acceso físico al TOE únicamente podrá realizar las siguientes operaciones a través del menú display antes de acceder al sistema autenticándose frente a él: ○ Mismas operaciones incluidas en la descripción del requisito FIA_UID.1(INY). Para realizar cualquier otra operación disponible a través del menú display, deberá autenticarse previamente frente al equipo mediante el uso del correspondiente inyector y PIN asociado, asumiendo de este modo el perfil de “Administrador de Seguridad”
FIA_UAU.1(USR)	El TOE implementa un control de accesos para asegurar que un usuario, accediendo a través del interfaz web seguro, únicamente podrá realizar las siguientes operaciones a través del mismo antes de acceder al sistema autenticándose frente a él: ○ Mismas operaciones incluidas en la descripción del requisito FIA_UID.1(USR). Para realizar cualquier otra operación disponible a través del interfaz web seguro, deberá autenticarse previamente frente al equipo mediante el uso del correspondiente nombre de usuario y contraseña asociada, asumiendo de este modo el perfil de “Administrador de Configuración” u “Operador”, según corresponda.
FIA_UAU.2	El TOE implementa un control de accesos para asegurar que un usuario, accediendo a través del interfaz de consola (lo cual requiere acceso físico al TOE), no podrá realizar ninguna operación antes de acceder al sistema autenticándose frente a él, asumiendo de este modo el perfil de “Administrador de Configuración” u “Operador”, según corresponda.
FIA_UAU.5	El TOE proporciona diferentes mecanismos de autenticación, dependiendo del método de acceso empleado por el usuario que intenta autenticarse frente a él, lo que determina, una vez realizada la autenticación, el perfil de dicho usuario: ○ Usuario con acceso físico al TOE intentando acceder al menú display (perfil “Administrador de Seguridad”): inyector compatible y su PIN asociado. Para completar la validación del inyector es necesario, adicionalmente, el establecimiento previo de un canal seguro (cifrado y autenticado) con autenticación mutua de los extremos. ○ Usuario intentando acceder a través de interfaz de consola (lo que requiere acceso físico) o a través del interfaz de configuración web (perfil “Administrador de Configuración” u “Operador”): combinación de nombre de usuario y contraseña. Si la autenticación se lleva a cabo a través del interfaz web seguro es necesario, adicionalmente, el establecimiento previo de un canal cifrado con autenticación mutua de los extremos, conforme al protocolo TLS v1.2.

FIA_UID.1(INY)	El TOE implementa un control de accesos para asegurar que un usuario con acceso físico al TOE únicamente podrá realizar las siguientes operaciones a través del menú display antes de acceder al sistema identificándose frente a él: ○ Seleccionar el idioma de presentación del menú display. ○ Visualizar la pantalla principal del menú display, con información sobre el estado general del equipo, el estado de sus interfaces de red y la fecha/hora configuradas. ○ Visualizar información básica sobre el equipo: modelo, número de serie y versión de software cargada. ○ Visualizar información básica necesaria para tareas de mantenimiento: nivel de carga de la batería y temperatura de componentes internos. Para realizar cualquier otra operación disponible a través del menú display, deberá identificarse previamente frente al equipo mediante el uso del correspondiente inyector y PIN asociado, asumiendo de este modo el perfil de “Administrador de Seguridad”.
FIA_UID.1(USR)	El TOE implementa un control de accesos para asegurar que un usuario, accediendo a través del interfaz web seguro, únicamente podrá realizar las siguientes operaciones a través del mismo antes de acceder al sistema identificándose frente a él: ○ Seleccionar el idioma de presentación del interfaz web seguro. Para realizar cualquier otra operación disponible a través del interfaz web seguro, deberá identificarse previamente frente al equipo mediante el uso del correspondiente nombre de usuario y contraseña asociada, asumiendo de este modo el perfil de “Administrador de Configuración” u “Operador”, según corresponda.
FIA_UID.2	El TOE implementa un control de accesos para asegurar que un usuario, accediendo a través del interfaz de consola (lo cual requiere acceso físico al TOE), no podrá realizar ninguna operación antes de acceder al sistema identificándose frente a él, asumiendo de este modo el perfil de “Administrador de Configuración” u “Operador”, según corresponda.
CLASE FMT: SECURITY MANAGEMENT	
FMT_MSA.1(IFC)	Tanto las políticas de seguridad como las credenciales de identificación del TOE, necesarias para cumplir la SFP “UserData_Flow_Control_SFP”, pueden ser gestionadas (creadas, consultadas, modificadas o eliminadas) por los siguientes usuarios: ○ Usuario con perfil “Administrador de Configuración”. ○ Usuario con perfil “Operador”, si tiene los permisos correspondientes habilitados.

FMT_MSA.1(INY)	El código PIN del inyector asignado a un usuario con perfil “Administrador de Seguridad” únicamente se puede modificar (desde el TOE) por el propio usuario con perfil “Administrador de Seguridad” una vez autenticado y siempre que disponga del correspondiente permiso habilitado en el inyector (permiso para cambiar PIN). Nótese que la asignación del PIN inicial del inyector únicamente puede realizarse durante su programación en el Centro de Gestión (fuera del TOE).
FMT_MSA.1(USR1)	La contraseña asignada al usuario con perfil “Administrador de Configuración” únicamente asignar inicialmente y/o modificar (según operación) por: o El propio usuario con perfil “Administrador de Configuración” una vez autenticado. o Un usuario autenticado con perfil “Administrador de Seguridad”, siempre que disponga del correspondiente permiso habilitado en el inyector (permiso para cambiar contraseña “admin”). La asignación inicial de la contraseña del usuario con perfil “Administrador de Configuración” únicamente puede realizarse mediante este último método. Una vez realizado el primer acceso, el usuario con perfil “Administrador de Configuración” debe establecer su nueva contraseña de acceso conforme a las recomendaciones y políticas de acceso aplicables en la Organización, siendo responsable de establecer contraseñas de fortaleza suficientemente alta, renovarlas con la frecuencia oportuna y custodiarlas adecuadamente, de forma que, en colaboración con los mecanismos de control de acceso implementados en el TOE, se contrarresten posibles ataques por fuerza bruta al mismo.

FMT_MSA.1(USR2)	La contraseña para un usuario con perfil “Operador” únicamente se puede asignar inicialmente y/o modificar (según operación) por: ○ El propio usuario con perfil “Operador” una vez autenticado. ○ El usuario autenticado con perfil “Administrador de Configuración”. ○ Otro usuario autenticado con perfil “Operador”, siempre que disponga del correspondiente permiso habilitado (permiso para gestionar usuarios). La asignación inicial de la contraseña de un usuario con perfil “Operador” únicamente puede realizarse mediante una de las dos últimas opciones indicadas (según quien cree el nuevo usuario con rol de “Operador”). El esquema de permisos asignado a un usuario con perfil “Operador” únicamente se puede asignar inicialmente, consultar y/o modificar por: ○ El usuario autenticado con perfil “Administrador de Configuración”. ○ Otro usuario autenticado con perfil “Operador”, siempre que disponga del correspondiente permiso habilitado (permiso para gestionar usuarios). Nótese, que un usuario autenticado con perfil “Operador” NO está autorizado, independientemente de su esquema de permisos asignado, a modificar su propio conjunto de permisos habilitados. Una vez realizado el primer acceso, el usuario con perfil “Operador” debe establecer su nueva contraseña conforme a las recomendaciones aplicables en la Organización, siendo responsable de establecer contraseñas de fortaleza suficientemente alta, renovarlas con la frecuencia oportuna y custodiarlas adecuadamente, de forma que, en colaboración con los mecanismos de control de acceso implementados en el TOE, se contrarresten posibles ataques por fuerza bruta al mismo.
FMT_MSA.3(IFC)	Por defecto, en el sistema no existe ninguna política de seguridad ni ninguna credencial de identificación del TOE, necesarias para cumplir la SFP “Red_Data_Flow_Control_SFP”. La gestión (creación, consulta, modificación y/o eliminación) de dichos atributos puede realizarse por los siguientes usuarios autorizados: ○ Usuario con perfil “Administrador de Configuración”. ○ Usuarios con perfil “Operador”, si tienen los permisos correspondientes habilitados.
FMT_MSA.3(INY)	Por defecto, el inyector asignado a un usuario con perfil “Administrador de Seguridad”, tendrá un código PIN asignado inicialmente durante su programación (fuera del TOE). La longitud mínima de dicho código PIN es de 8 dígitos decimales. El código PIN asignado inicialmente a este inyector, únicamente se puede modificar (desde el TOE) por el propio usuario con perfil “Administrador de Seguridad”, una vez autenticado y siempre que disponga del correspondiente permiso habilitado en el inyector (permiso para cambiar PIN).

FMT_MSA.3(USR1)	Por defecto, la contraseña del usuario con rol de "Administrador de Configuración" no está definida, lo que significa que NO es posible acceder al equipo empleando este rol mientras no se defina el valor inicial para dicha contraseña. La definición inicial de la contraseña del "Administrador de Configuración" únicamente puede llevarla a cabo el usuario con perfil "Administrador de Seguridad", una vez autenticado y siempre que disponga del correspondiente permiso habilitado en el inyector (permiso para cambiar contraseña "admin"). Una vez definido el valor inicial, esta contraseña podrá modificarse únicamente conforme a lo descrito en el requisito FMT_MSA.1(USR1).
FMT_MSA.3(USR2)	Por defecto, al crearlo, a un usuario con perfil "Operador" se le debe asignar una contraseña de al menos 8 caracteres alfanuméricos y no dispone de ningún permiso habilitado (valores por defecto seguros restrictivos). Tanto la contraseña de usuarios como el esquema de permisos aplicable a un usuario con perfil "Operador" puede ser definido/modificado, directamente al crearlo o posteriormente durante la operación, únicamente por un usuario autenticado cuyo perfil sea "Administrador de Configuración" o bien por otro usuario autenticado cuyo perfil sea "Operador", siempre que éste disponga del permiso correspondiente habilitado (permiso para gestionar usuarios). Nótese, que adicionalmente un usuario autenticado con perfil "Operador", independientemente de su esquema de permisos asignado, está autorizado a cambiar su propia contraseña de acceso pero NO está autorizado a modificar su propio conjunto de permisos habilitados.
FMT_MTD.1	La configuración TSF del TOE puede ser gestionada por los diferentes roles de usuario definidos a través del requisito FMT_SMR.1 ("Administrador de Seguridad", "Administrador de Configuración", u "Operador"). Sin embargo, se debe tener en cuenta que las operaciones disponibles para cada uno de ellos dependerán de su perfil de usuario y, cuando aplique, del conjunto de permisos habilitados para él, conforme a lo definido a través del requisito FMT_SMF.1.
FMT_SMF.1	El TOE permite llevar a cabo las siguientes operaciones de gestión y administración: o Usuario con perfil "Administrador de Configuración u "Operador" (según esquema de permisos asignado): ▪ Visualización y configuración del registro de auditoría (incluyendo los filtros asociados para visualización y/o registro) y/o de la funcionalidad de envío de alarmas tipo "traps SNMPv3" a un supervisor externo (incluyendo el filtro asociado para envío y la configuración de los parámetros del supervisor SNMP). Nótese que la desactivación de la funcionalidad de envío de traps SNMP puede realizarse mediante el establecimiento de parámetros vacíos para el supervisor

SNMP.

- Creación, consulta, modificación y/o borrado de parámetros de configuración TSF (configuración de red, configuración IPsec…) y sus atributos de seguridad.
- Configuración ajustes horarios del TOE (fecha / hora y/o zona horaria).
- Operaciones permitidas previa a la identificación y autenticación del usuario, cuando el acceso se realiza a través del interfaz web seguro (ver requisito(s) FIA_UID.1(USR) y FIA_UAU.1(USR)).
- Descarga, restauración y borrado de la configuración del TOE e invocación de la operación de reinicio del mismo.
- Invocación de utilidades para chequear la alcanzabilidad / rutabilidad de otros equipos desde los interfaces rojo / negro.
- Gestión de usuarios con perfil “Operador” (creación, borrado y modificación) y sus atributos de seguridad.
- Modificación de la contraseña y el nombre completo del propio usuario.
- Sólo para usuarios autorizados a través del interfaz de consola, consulta de la ayuda sobre comandos disponibles y gestión local del espacio de almacenamiento temporal de ficheros (necesario para carga / descarga de ficheros durante otras operaciones a través del interfaz de consola).

- Usuario con perfil “Administrador de Seguridad”: funciones de administración disponibles a través del menú display, incluyendo:
  - Operaciones permitidas previa a la identificación y autenticación del usuario (ver requisito(s) FIA_UID.1(INY) y FIA_UAU.1(INY)).
  - Consulta de las direcciones configuradas para los interfaces de red y sus estadísticas;
  - Consulta del esquema de permisos del inyector;
  - Carga de parámetros de configuración (parámetros de red y/o parámetros IPsec) transportados en el inyector.
  - Otras operaciones de administración bajo el control de la política de acceso aplicable como: instalación del TOE, configuración de opciones de seguridad, configuración de la contraseña del usuario “Administrador de Configuración”, modificación del código PIN del inyector, actualización del software principal del MÓDULO PRINCIPAL (MP) del TOE y gestión de certificados para acceso web.

Como se puede apreciar, la disponibilidad (o no disponibilidad) de estas operaciones para un usuario, dependerá de su perfil de usuario (“Administrador de Seguridad”, “Administrador de Configuración” u “Operador”) y, cuando aplique, de su esquema de permisos, conforme al

	sistema de control de acceso implementado en el TOE.
FMT_SMR.1	En el TOE se define un sistema de control de acceso de acuerdo a una serie de perfiles de usuario: o Usuario con perfil “Administrador de Seguridad”. o Usuario con perfil “Administrador de Configuración”. o Usuario con perfil “Operador”. Cada uno de estos perfiles tiene asociado un mecanismo de autenticación y un conjunto diferente de operaciones posibles en función del rol de usuario que asume al autenticarse y, si aplica, del esquema de permisos asignado, tal como se describe en otros requisitos de la declaración (requisitos FIA y FDP para políticas de control de acceso).
CLASE FPT: PROTECTION OF THE TSF	
FPT_FLS.1	El TOE considera una serie de situaciones como potencialmente peligrosas, ya que pueden poner en compromiso la TSF y/o los activos a proteger. Estas situaciones (consideradas como eventos de tamper) pueden darse al detectar el equipo un intento de manipulación física (ataque), la activación del pulsador de emergencia o un comportamiento anómalo en el supervisor de seguridad (reset o fallo en self-tests ejecutados por éste). En cualquier caso, el TOE entra en un estado seguro (NO operativo), desde el cual, para recuperar el estado operativo de nuevo, será necesaria, al menos, la intervención de un “Administrador de Seguridad” autorizado.
FPT_ITK.1	El TOE implementa un mecanismo para permitir, a los usuarios con perfil “Administrador de Seguridad”, llevar a cabo la actualización del software principal del MÓDULO PRINCIPAL (MP) de forma segura. Una vez autenticado un usuario con perfil “Administrador de Seguridad” y siempre que el inyector empleado para ello disponga de los datos necesarios para permitir la invocación del proceso de actualización; se proporciona a dicho usuario autorizado la posibilidad de cargar (desde un navegador a través de una página específica servida por el equipo) un fichero firmado y cifrado (para garantizar su confidencialidad, integridad y autenticidad) que contenga la nueva versión a cargar. El proceso de actualización sólo podrá completarse con éxito si la clave de transporte contenida en el inyector empleado por el usuario para su autenticación (perfil “Administrador de Seguridad”) coincide con la que se empleada en origen para cifrar el fichero de actualización (firmado) antes de su distribución al usuario que está invocando el proceso. Una vez aceptada la actualización de software, el TOE debe reiniciarse para que ésta se haga efectiva, comprobando así la integridad y coherencia del sistema de doble copia empleado.

FPT_PHP.3	El TOE dispone de elementos anti-tamper activos, que incluyen detectores de apertura, sensores de temperatura y detectores de sobre-tensión, que permiten detectar diferentes intentos de manipulación o ataques físicos, tanto en presencia como en ausencia de la alimentación externa, gracias a la batería de respaldo. Al activarse alguno de estos mecanismos se produce un evento de tamper que hace que el TOE entre en un estado seguro (NO operativo) para auto-protegerse.
FPT_RCV.1	El TOE diferencia entre dos niveles de tamper, nivel ALTO y nivel BAJO, dependiendo de la gravedad del suceso (evento de tamper) ocurrido: o Nivel BAJO: el TOE se sitúa en estado “NO INSTALADO”. Para recuperarlo de este estado, es necesario llevar a cabo un nuevo proceso de Instalación, que puede ser llevado a cabo en campo. o Nivel ALTO: el TOE se sitúa en estado “DESPROGRAMADO”. Para recuperarlo de este estado es necesario llevar a cabo de nuevo el proceso de Programación del mismo en un entorno protegido y, a continuación, el proceso de Instalación. En cualquier caso, para llevar a cabo el proceso de Instalación, se requiere la presencia del “Administrador de Seguridad”, en posesión de un inyector especialmente programado para ello y de su código PIN asociado.
FPT_STM.1	El TOE dispone de un reloj de tiempo real (RTC) que le permite mantener la fecha/hora del equipo, base del sistema de alarmas, aun en ausencia de la alimentación externa, gracias a la batería de respaldo.
FPT_TST.1	Por un lado, el TOE invoca durante toda su operación, tanto en ausencia como en presencia de alimentación externa, chequeos periódicos sobre el estado de sus sensores y mecanismos anti-tamper activos, con el objetivo de detectar diferentes intentos de manipulación o ataques físicos. Los usuarios autorizados con acceso físico al equipo pueden verificar el estado de integridad de los mecanismos anti-tamper activos, a través de la pantalla principal de estado del display y los indicadores incluidos para ello en el panel frontal del equipo. Por otro lado, los usuarios autorizados con perfil de “Administrador de Configuración” u “Operador” (dependiendo de su esquema de permisos asignados), mediante la invocación de la operación de reinicio del equipo, pueden provocar la verificación de la integridad de ciertos datos sensibles, necesarios para completar con éxito el proceso de arranque (ya que, sin ellos, no es posible llevar a cabo la carga del SW y FW del procesador principal o de la configuración almacenada en el equipo). Dichos datos sensibles se almacenan cifrados con AES256-GCM (para proteger su confidencialidad e integridad) en la memoria interna no volátil del supervisor de seguridad. Durante cada arranque del equipo, el supervisor de seguridad debe, antes de que dichos datos puedan utilizarse en otros componentes, descifrarlos empleando dicho algoritmo, lo que supone la verificación implícita de su integridad dadas las características del algoritmo empleado.

CLASE FTA: TOE ACCESS	
FTA_SSL.3	El TOE, dentro de su sistema de control de acceso, implementa un mecanismo por el cual todas las sesiones de los usuarios con perfil "Administrador de Configuración" u "Operador" se cierran automáticamente trascurrido un tiempo de inactividad, descartando toda la información temporal (no almacenada ya en la configuración del TOE) asociada a dicha sesión. El tiempo máximo de inactividad de la sesión depende del medio empleado para acceder, siendo de 10 minutos para el acceso a través del interfaz web seguro y de 5 minutos para el acceso a través del interfaz de consola. Si el usuario desea continuar gestionando el TOE, deberá volver a establecer una nueva sesión, autenticándose de nuevo frente al equipo mediante la introducción del nombre de usuario y contraseña correctos.
FTA_SSL.4	El TOE, dentro de su sistema de control de acceso, implementa mecanismos para permitir el cierre de la sesión de un usuario autenticado mediante uno de los siguientes métodos, en función del perfil de usuario considerado: ○ Usuario con perfil "Administrador de Configuración" u "Operador": invocación de un comando de cierre de sesión (acceso a través del interfaz de consola) o de la opción de desconexión (acceso a través del interfaz web seguro). ○ Usuario con perfil "Administrador de Seguridad": extracción/desconexión física del inyector.
CLASE FTP: TRUSTED PATH/CHANNELS	
FTP_ITC.1	Entre el TOE y otros dispositivos IT con los que intercambia datos TSF se establecen canales de comunicación confiables, en los que se lleva a cabo el proceso de autenticación de una o de ambas partes: ○ Canales de comunicación para inicialización y gestión remota del IS101 desde el correspondiente interfaz web seguro. Se lleva a cabo la autenticación mutua entre las dos entidades implicadas en la comunicación, mediante el uso de certificados X.509. La comunicación a través del canal seguro la inicia el dispositivo IT remoto (PC desde el que se accede al interfaz web seguro). Una vez establecido, el flujo de información es bidireccional. Una vez establecidos estos canales confiables, el intercambio (o envío) de datos TSF a través de los mismos se realiza de forma que la confidencialidad e integridad de dichos datos TSF queda protegida frente a interceptación y/o manipulación tal como establece el requisito.

Tabla 13. Conclusión de SFRs