centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1405

Procedimiento de Empleo Seguro IS101

Noviembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.11.25 09:43:36 +01'00'

NIPO: 083-19-008-7

Fecha de Edición: noviembre de 2019
Istria ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. OBJETO Y ALCANCE

1. En la presente guía se recoge el procedimiento de empleo seguro para el equipo IP IS101, del fabricante Istria, un cifrador de altas prestaciones diseñado para su instalación en emplazamientos donde se maneja información crítica o sensible que necesita ser transmitida de forma segura entre sitios remotos a través de una red IP de transporte no confiable (pública o privada) de forma segura, protegiendo su confidencialidad, integridad y proporcionando autenticación entre los cifradores extremos empleados;
2. Dispone de un conjunto de funcionalidades de seguridad y mecanismos de auto-protección que permiten que la operación y aplicación del control de flujo y el manejo, configuración y gestión del propio equipo se puedan llevar a cabo de forma segura.
3. Las medidas recogidas en este documento son de dos tipos: obligatorias y recomendadas. Para cumplir con el procedimiento de empleo seguro sería necesario implementar, al menos, las medidas obligatorias.
4. Para llevar a cabo la implantación de dichas medidas, se deberán realizar las tareas y seguir los procedimientos relacionados con la instalación y configuración del cifrador IS101, descritos en mayor detalle en el Manual de Usuario [1]. Así mismo, para la utilización del Centro de Gestión IS101M como elemento para la gestión centralizada de una red de cifradores, el lector deberá consultar el Manual de Usuario del CdG [2].
5. Todos los algoritmos criptológicos utilizados por equipo cumplen con los requisitos estipulados en la CCN-STIC-807 Criptología de empleo en el ENS para la Categoría Alta [3].

2. ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en cuatro partes fundamentales, que son:
    - **a)** Apartado 3. En él se describe el producto desde un punto de vista funcional, junto con sus interfaces externos y aquellos elementos adicionales que componen el criptosistema completo como son el inyector de claves y la herramienta de gestión centralizada.
    - **b)** Apartado 4. En él se recogen requisitos relativos al entorno del equipo, tanto en lo referente a la operación, como a la operación y el mantenimiento.
    - **c)** Apartado 5. En él se recogen requisitos o recomendaciones asociadas a la fase de instalación y puesta en marcha segura del equipo.
    - **d)** Apartado 6. En este apartado se recogen requisitos o recomendaciones relativas a las tareas de mantenimiento durante la fase de operación y mantenimiento del producto.

3. INTRODUCCIÓN

3.1 DESCRIPCIÓN GENERAL

7. El equipo IS101 es un cifrador de altas prestaciones certificado *Common Criteria* (nivel EAL4+) que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPsec en modo túnel (con encapsulado ESP y protocolo IKEv2), lo que permite establecer redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada).
8. Para el cifrado del tráfico de datos de usuario, el IS101 implementa en hardware y permite ejecutar de forma simultánea dos algoritmos criptográficos independientes: uno estándar (AES256-GCM) y un segundo algoritmo personalizable.
9. El IS101 tiene una velocidad de transferencia de 2Gbps agregados.

Figura 1. Cifrador IS101

10. El cifrador opera sobre el nivel 3 del modelo OSI y emplea el protocolo IPsec en modo túnel (con encapsulado ESP y protocolo IKEv2 para la identificación / autenticación mutua entre extremos y la negociación de claves y algoritmos a utilizar) para llevar a cabo el procesamiento, filtrado y manejo de forma controlada del tráfico de datos de usuario que lo atraviesa. De este modo, el IS101 permite proteger la confidencialidad e integridad de la información sensible intercambiada (incluidas cabeceras IP) entre distintas redes locales geográficamente distantes (redes rojas) durante su tránsito a través de la red IP no confiable (red negra). El IS101 permite establecer y gestionar hasta 4096 asociaciones de seguridad simultáneas.
11. 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.

12. Asimismo, dispone de mecanismos anti-tamper pasivos y activos, físicos y lógicos y auto-tests específicos para arranque seguro y protección de los componentes y datos internos sensibles que almacena.
13. 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 permite un manejo y configuración del mismo que minimice las acciones requeridas por parte del usuario.
14. 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.
15. 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, configuración y gestión del propio equipo se llevan a cabo de forma segura. Entre estos servicios destacan:
    - **a)** 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.
    - **b)** Identificación y Autenticación de usuarios y establecimiento de canales seguros para usuarios conectados de forma remota.
    - **c)** Control de acceso a las operaciones de administración, gestión y configuración mediante perfiles de usuario y esquemas de permisos.
    - **d)** Protecciones físicas y lógicas (activas y pasivas).
    - **e)** Almacenamiento seguro de datos sensibles, permitiendo verificar su integridad en cada arranque, y chequeos periódicos (auto-tests).
    - **f)** Trazabilidad de eventos relevantes desde el punto de vista de seguridad.

3.2 INTERFACES EXTERNOS

16. 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 ilustra en las siguientes figuras:
    - **a)** Interfaces de configuración, presentación de estado y pulsadores (ubicados en panel frontal):

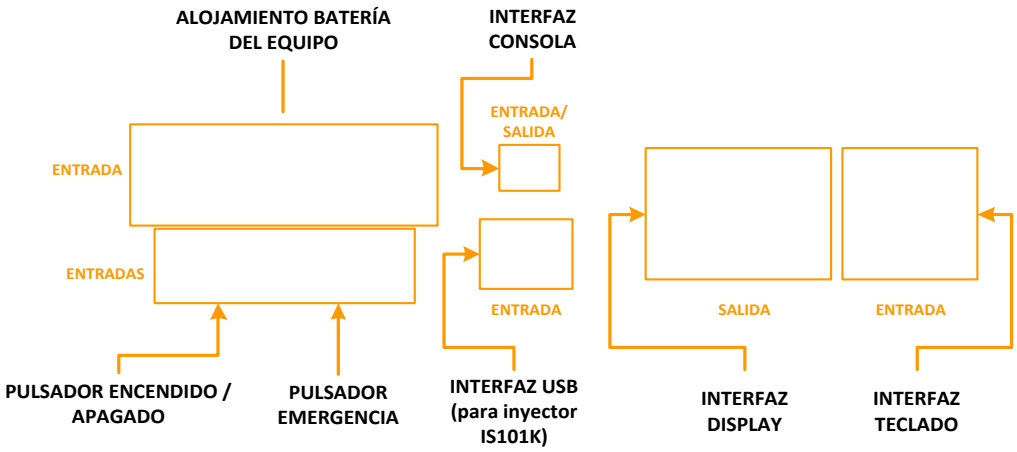

Figura 2. Interfaces Externos Cifrador IS101 (Panel Frontal)

b) Interfaces de datos (LAN y WAN) y entrada de alimentación (ubicados en panel trasero):

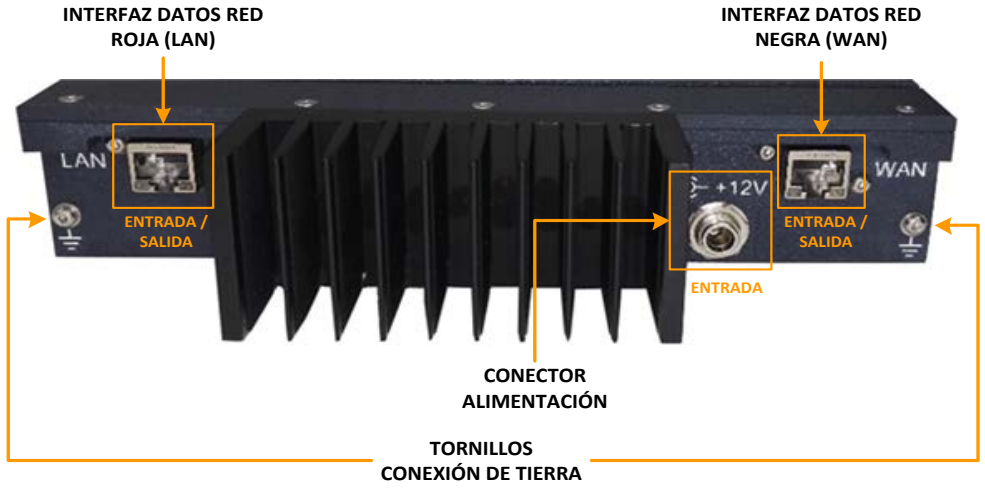

Figura 3. Interfaces Externos Cifrador IS101 (Panel Trasero)

17. Para más información sobre las características y propósito de los interfaces externos del equipo presentados anteriormente, consultar el apartado “Interfaces Externos” del documento IS101. Manual de Usuario [1].

3.3 OTROS COMPONENTES DEL CRIPTOSISTEMA

18. Además del cifrador IS101, el criptosistema incluye los siguientes componentes:

a) Inyector IS101K

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

Este dispositivo de transporte compatible, denominado inyector, funciona como token de seguridad (tarjeta criptográfica tipo *smartcard*) y se encarga de aportar los permisos necesarios para llevar a cabo las operaciones de administración (disponibles a través del menú "*display*") y/o de almacenar la información que se ha de cargar en el equipo.

Figura 4. Inyector IS101K

El contenido del inyector se programa desde el Centro de Gestión correspondiente y está protegido de forma que, al insertar el inyector en el IS101, su contenido sólo es accesible desde el equipo una vez que se supera con éxito el correspondiente proceso de validación (con intervención del usuario autorizado correspondiente), autenticación mutua y apertura de canal seguro entre el inyector y el cifrador.

b) Centro de Gestión IS101M

El Centro de Gestión es un equipo independiente basado en el uso de los siguientes componentes:

i) hardware del cifrador IS101 programado con una versión de software específica para Centro de Gestión y

ii) dispositivo de almacenamiento externo para alojar la BBDD vinculada al Centro de Gestión.

El Centro de Gestión (CdG) permite realizar, de forma segura, operaciones remotas sobre cada uno de los cifradores de la red, a través de un interfaz de administración. Para ello, se establecen canales de gestión seguros entre el cifrador del CdG y cada cifrador IS101 que vaya a gestionar. Estos canales estarán embebidos, a su vez, en las correspondientes asociaciones de seguridad IPsec establecidas a través de la red IP de transporte empleada.

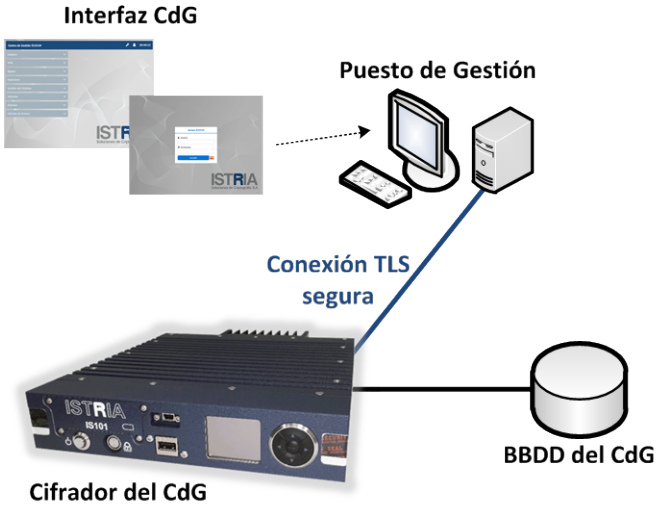

Figura 5. Centro de Gestión IS101M

Las operaciones realizadas por el CdG incluyen:

i. Configuración remota de parámetros de red e IPsec de los equipos.

ii. Actualización de SW.

iii. Monitorización del registro de auditoría.

iv. Distribución y actualización de claves, certificados y listas de revocación.

v. Configuración y programación de los dispositivos de transporte (inyectores IS101K).

4. ASPECTOS GENERALES Y ENTORNO

4.1 CONEXIÓN TÍPICA

19. El Cifrador IP IS101 de ISTRIA está diseñado para su instalación en emplazamientos donde se maneja información crítica o sensible que necesita ser transmitida entre sitios remotos a través de una red IP de transporte no confiable (pública o privada) de forma segura, protegiendo su confidencialidad, integridad y proporcionando autenticación entre los cifradores extremos empleados.

20. El cifrador IS101 opera como un equipo de nivel 3 y, por tanto, puede emplearse directamente como elemento de cifrado y enrutamiento para determinados tipos de redes. Sin embargo, para redes a partir de cierto tamaño, su instalación típicamente se lleva cabo entre el dispositivo que agrega las conexiones (switch/es) de la LAN a proteger y el router que proporciona acceso a la correspondiente red IP de transporte no confiable.

21. Adicionalmente, para facilitar la gestión y mantenimiento de los cifradores IS101 desplegados en la Organización usuaria, el criptosistema IS101 cuenta con un Centro de Gestión que permite y facilita las tareas de gestión de forma segura y centralizada de la configuración de los diferentes cifradores IS101 distribuidos en la red y su monitorización desde el punto de vista de seguridad.

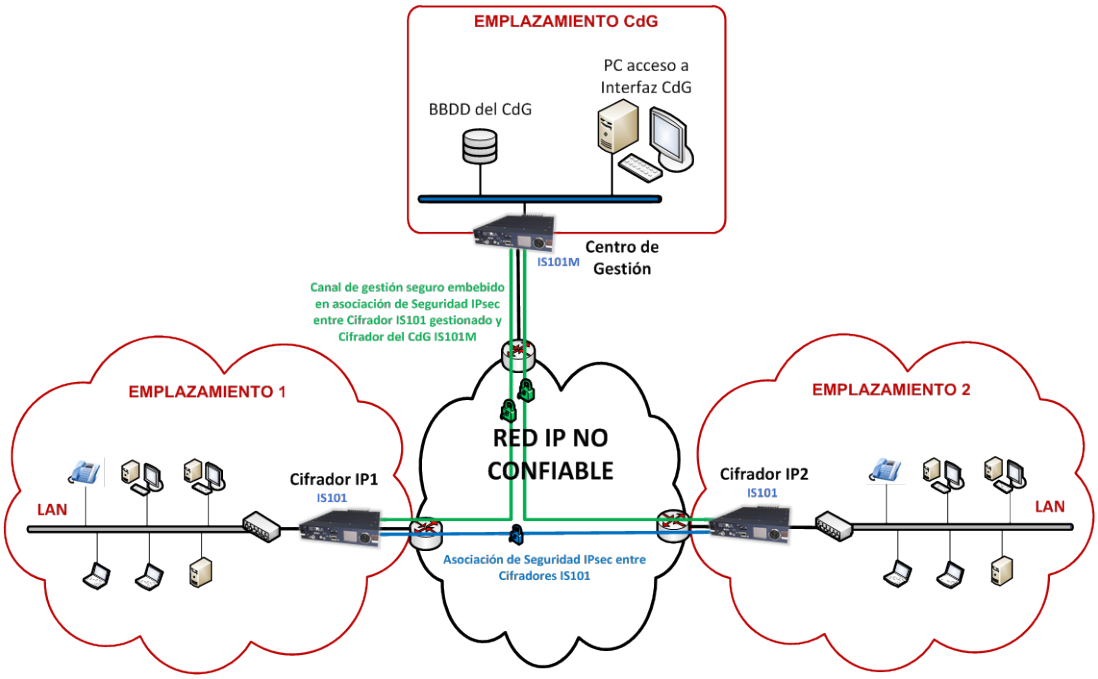

Figura 6. Conexión Típica Criptosistema IP ISTRIA

22. No obstante, excede del ámbito de esta guía el prescribir una determinada ubicación concreta para el cifrador dentro de la infraestructura, ya que este factor vendrá fuertemente determinado por la topología de la red y las necesidades de protección de comunicaciones IP aplicables a cada Organización usuaria o caso de uso.

4.2 ENTORNO DE OPERACIÓN

23. Desde el punto de vista operativo y de seguridad, es importante que en el entorno se puedan establecer y hacer cumplir las directrices y recomendaciones generales recogidas a continuación, relacionadas con la ubicación, conectividad y acceso a los equipos; de forma que los cifradores IS101 dispuestos en la red y, en su caso, el Centro de Gestión IS101M, puedan garantizar la protección deseada a los flujos de datos de usuarios que manejan:

CONDICIONES DE ENTORNO Y OPERACIÓN
Redes LAN/WAN aisladas
Se debe garantizar que la LAN roja no dispone de conexiones físicas o lógicas por otros medios (distintos al cifrador) a la red de transporte negra a utilizar, de forma que pudiera hacerse bypass de las protecciones proporcionadas por el cifrador a través de estos caminos alternativos.
Planificación previa de la instalación
Como en cualquier otro tipo de implantación, se recomienda que con anterioridad al despliegue de los cifradores en la red se realice un análisis mínimo del entorno en el que se desean instalar, de modo que se pueda: • Dimensionar adecuadamente el número de cifradores necesarios, considerando el caudal de flujos que se van a manejar, así como las posibles necesidades en cuanto a redundancia. • Garantizar que es posible asignar direccionamiento independiente a los interfaces LAN y WAN de cada cifrador, ya que éstos NO permitirán la asignación de direccionamiento solapado en su lado rojo (LAN) y lado negro (WAN). • Disponer de una planificación o visión inicial de las políticas de seguridad aplicables (tipo de autenticación, origen de las credenciales, flujos de datos que se deben proteger y, en su caso, excepciones o conexiones con requisitos específicos, etc.), de forma que la configuración de las políticas de seguridad IPsec que se va a desplegar inicialmente en los equipos sea consistente con dichas necesidades, con independencia de su posterior evolución o necesidades de modificación durante la operación de la red.
Rangos de temperatura
Tanto a la hora de instalar el equipo para su operación como de almacenarlo o transportarlo, es altamente recomendable garantizar que el entorno correspondiente cumple las recomendaciones del fabricante en cuanto a rangos de temperatura de operación y de almacenamiento (o transporte). Dichos rangos se recogen en el apartado “Características Generales, Físicas y Eléctricas” del Manual de Usuario [1].
Acceso al entorno
• El entorno operacional debe implementar las medidas físicas y organizativas adecuadas para que el acceso físico al equipo en su entorno de explotación quede restringido a los usuarios autorizados para su conexión, configuración y manejo en local. Esto contribuye a evitar que se manipule indebidamente del equipo o a que sea sustraído con fines de análisis de ingeniería inversa. • Adicionalmente, el cifrador implementa un conjunto de mecanismos anti-tamper que permiten al equipo auto-protegerse frente a ciertas condiciones de operación anómalas (intencionadas o fortuitas) y frente a

determinados intentos de manipulación física y/o ataque a su comportamiento lógico del equipo (aunque se disponga de acceso físico autorizado al equipo o, incluso, en previsión de un hipotético fallo de las medidas de seguridad y/u organizativas de control de acceso físico previstas por el entorno de operación).

Tabla 1 Condiciones de entorno de operación

4.3 ENTORNO DE ADMINISTRACIÓN Y MONITORIZACIÓN

24. El entorno de administración y monitorización de los cifradores IS101 estará compuesto por uno o varios de los siguientes componentes:

    a) Centro de Gestión IS101M asociado a la red de cifradores IS101 e Inyectores IS101K necesarios.

    El Centro de Gestión IS101M es el medio recomendado preferente para la gestión y monitorización de la red de cifradores IS101, por proporcionar múltiples funcionalidades avanzadas que simplifican sustancialmente dichas tareas con respecto a la gestión de la red mediante la configuración individualizada de cada cifrador.

    Estas capacidades lo hacen especialmente útil a la hora de gestionar de forma centralizada la configuración IPsec y de parámetros IP de toda la red de cifradores, ya que puede actuar como elemento para generación y distribución segura en línea de credenciales y parámetros IPsec (certificados de comunicaciones, PSS y/o políticas de seguridad); y a la hora de monitorizar el estado global y alarmas de todos los cifradores desplegados de forma conjunta.

    Además, el Centro de Gestión IS101M es el encargado de programar los inyectores IS101K que se van a emplear en la red de cifradores.

    b) PCs (con navegador y/o interfaz serie y periféricos asociados), cables, switches y/u otros elementos de red empleados para la conexión a los interfaces de configuración individuales del equipo (CLI y/o WEB), manejo y gestión de su configuración.

    c) Administradores y operadores de la red de cifradores, entendidos como tales el conjunto de usuarios autorizados para gestionar y monitorizar los cifradores de la red.

    d) PKI externa para la generación y distribución de certificados de comunicaciones o bien dispositivo para generación y distribución de claves PSS para las políticas de seguridad IPsec de los equipos (elemento opcional, como alternativa en caso de no utilizar para ello un Centro de Gestión IS101M).

    e) Supervisor SNMP externo para la monitorización de alarmas del equipo enviadas como traps SNMPv3 (elemento opcional).

25. Desde el punto de vista de operativo y de seguridad es importante que en el entorno se puedan establecer y hacer cumplir las directrices y recomendaciones generales recogidas a continuación, relacionadas con la infraestructura y medios dispuestos para la gestión y monitorización segura de los cifradores IS101:

CONDICIONES ENTORNO DE ADMINISTRACIÓN Y MONITORIZACIÓN
Centro de Gestión IS101M e Inyectores IS101K
Siempre que se emplee el Centro de Gestión IS101M como medio para la gestión y monitorización remota centralizada de la red de cifradores: • Se debe garantizar la disponibilidad de un medio de almacenamiento en red alcanzable desde el interfaz rojo del cifrador del CdG con capacidad suficiente para alojar la BBDD del CdG (el espacio necesario dependerá del tamaño de la red) y vincular (montar) dicha BBDD al cifrador del CdG (operación de montaje de la BBDD) para permitir que éste opere como Centro de Gestión de la red de cifradores. • Se debe garantizar la disponibilidad de al menos un puesto de gestión alcanzable desde el interfaz rojo del cifrador del CdG que éste libre de virus, configurado de forma segura y no conectado a otras redes ajenas no controladas. En este puesto se deberán importar los certificados correspondientes para permitir el acceso al interfaz CdG (servido por el cifrador del CdG) mediante la conexión vía https a una de sus direcciones IP rojas. • Se debe garantizar la disponibilidad de personal confiable, competente, debidamente formado y en disposición de los medios necesarios para llevar a cabo sus tareas asignadas de forma correcta, responsable y siguiendo las directrices y recomendaciones estipuladas. • La ubicación, conexión y configuración del cifrador del CdG (y elementos de red auxiliares empleados para ello) deberán permitir que los distintos cifradores de la red que se vayan a gestionar de forma centralizada sean alcanzables por el cifrador del CdG a través de la red IP de transporte empleada (ver Figura 6). • El cifrador del CdG, además de permitir el acceso al interfaz CdG y la gestión remota del resto de equipos de la red, puede desempeñar su papel como un cifrador más de la red, capaz de cursar tráfico de usuario (adicionalmente al propio tráfico de gestión de la red). No obstante, desde el punto de vista operativo y/o procedimental, NO es recomendable por diferentes motivos (posible carga de tráfico de gestión vs carga de tráfico de usuario, necesidad de segregación de funciones de los usuarios que lo gestionan, etc.). Es por ello que, con el fin de optimizar y garantizar su correcto uso, especialmente en redes a partir de cierto tamaño, se recomienda que el cifrador del CdG se dedique de forma exclusiva a las tareas de gestión remota centralizada. • Los inyectores IS101K cuando se reciben de fábrica NO están programados y, por tanto, no es posible utilizarlos en los cifradores IS101. Para dotarlos de su funcionalidad, deben ser previamente programados en el Centro de Gestión

IS101M correspondiente con los permisos de administración y/o datos de configuración oportunos.

- Si se utiliza el Centro de Gestión como medio principal para la gestión de la red de cifradores de forma centralizada, para favorecer la operación de la forma más eficiente posible, se recomienda que todos los cifradores de la red (salvo fallos de conectividad puntuales o imposibilidad mayor por condiciones de entorno) sean gestionables y permanezcan alcanzables para el cifrador del CdG durante su operación y que se minimice el número de operaciones de gestión y configuración realizadas sobre los mismos a través de sus interfaces de configuración individuales (CLI y/o WEB).

Medios para gestión individual

- Medios directos para gestión individual de cifradores: el entorno operacional debe garantizar que 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 cifrador y su configuración (a través de CLI y/o WEB) y que éstos están libres de virus y configurados de forma segura y no conectado a otras redes ajenas no controladas[1].
- Medios para custodia tokens y credenciales: el entorno operacional debe garantizar que se dispone de los medios materiales adecuados, políticas de uso y procedimientos necesarios para que los usuarios autorizados puedan cumplir su deber de custodia sobre los tokens y/o credenciales de acceso que se les asignen.

Usuarios autorizados

- Competencia y formación: todos los usuarios autorizados (en posesión de tokens y/o credenciales válidas para acceder a los equipos[2]) deberán ser confiables y competentes, haber recibido la formación adecuada y disponer 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 cifrador.
- Deber de custodia: cada usuario autorizado debe asumir la responsabilidad de custodiar los tokens y/o credenciales de acceso que se le asignen de forma responsable y correcta, mantener sus credenciales de acceso en secreto y gestionarlas de forma adecuada de acuerdo con las directrices y recomendaciones estipuladas.

[1] En el caso de los PCs empleados para acceso a través del interfaz de consola se recomienda que estén aislados (no conectados a ninguna otra red) y en el caso de los empleados para acceso a través del interfaz de configuración web segura se deberá estudiar la posibilidad de tener dichos elementos conectados simultáneamente a otras redes diferentes a la empleada para alcanzar el equipo a gestionar y/o las restricciones aplicables.

[2] Esto puede incluir uno o varios de los siguientes elementos / datos en función del tipo de acceso considerado: inyectores IS101K y códigos PIN, nombres de usuario y contraseñas, certificados de cliente web.

La descripción de los perfiles de usuarios autorizados, esquemas de permisos, mecanismos de acceso y operaciones posibles para cada uno se describe en el apartado “Perfiles de Usuario y Permisos” del Manual de Usuario [1].

PKI externa o dispositivo generador de PSS (cuando aplique)

En caso de utilizarse una PKI externa, ésta:

- Debe ser capaz de proporcionar y gestionar las claves y certificados de comunicaciones X.509v3 a distribuir a los cifradores IS101 de la red.
- Los certificados generados y gestionados por la PKI deben ser compatibles con los aceptados por los cifradores, para lo cual deberá emplear claves de curva elíptica (curva P-384 del NIST) y permitir la inclusión de campos SAN que puedan ser empleados como selectores por nombre para las políticas de seguridad a configurar.
- Debe poder exportar su certificado CA raíz (público) para que pueda ser cargado en los correspondientes cifradores de la red, bien sea directamente o a través del Centro de Gestión IS101M. De este certificado CA raíz dependerán jerárquicamente, de forma directa, los certificados de comunicaciones generados.
- Debe disponer de los medios necesarios para gestionar la generación y distribución de CRLs para la red (o, al menos, para facilitar la ejecución manual de esta tarea).

En caso de utilizarse un dispositivo de generación de claves PSS, éste:

- Debe ser capaz de proporcionar claves secretas pre-compartidas PSS de la complejidad y fortaleza requeridas (al menos hasta el máximo tamaño admitido por el cifrador y nunca inferior a 128 bits).

En ambos casos:

- El dispositivo correspondiente debe estar gestionado por personal confiable y disponer de las medidas técnicas y/u organizativas de control de acceso necesarias para garantizar que sólo se generan y distribuyen a los IS101 parámetros criptográficos para un uso final conocido y aceptado y que dichos parámetros criptográficos NO se distribuyen a dispositivos no autorizados.

Supervisor SNMP externo (cuando aplique)

En caso de utilizarse un supervisor SNMP externo, éste:

- Debe emplear SNMPv3 con autenticación y cifrado para garantizar su compatibilidad con los cifradores IS101.
  - Se debe configurar en el mismo las correspondientes claves de autenticación y cifrado, siguiendo los mismos criterios que se emplean para ello en los cifradores (ver pautas recogidas en el apartado “Directrices para Gestión de Contraseñas / Claves” del documento IS101. Manual de Usuario [1]).

El dispositivo correspondiente debería estar gestionado por personal confiable y

disponer de las medidas técnicas y/u organizativas de control de acceso necesarias para garantizar su uso conforme a las políticas de seguridad implantadas en la Organización.

Tabla 2. Condiciones de entorno de administración y monitorización

5. CONEXIÓN Y PUESTA EN MARCHA

26. El cifrador se suministra desde fábrica como un único equipo ya programado (HW + SW/FW embebido), empaquetado y etiquetado conforme a los procedimientos de entrega establecidos y junto con su correspondiente dotación y documentación asociada.
27. En función de las necesidades de la Organización usuaria, el conexionado y puesta en marcha inicial del equipo puede realizarse en su emplazamiento final o en otro emplazamiento de la organización donde, a modo de procedimiento de "pre-configuración", se establezca una configuración inicial para éste.
28. Siempre que sea viable, se recomienda que la instalación y puesta en marcha se realice en su emplazamiento final, ya que de esta forma se simplifica el proceso y es posible detectar fallos en la red o en la configuración inicial del equipo.
29. En cualquier caso, si se opta por realizar una pre-configuración del equipo en un emplazamiento intermedio y posteriormente realizar la conexión y puesta en marcha en el emplazamiento definitivo se deberán tener en cuenta, además de las recogidas en este apartado, las directrices y recomendaciones aplicables para su traslado de ubicación (ver apartado 6.6.- Traslado de Ubicación del Cifrador de esta guía).

5.1 CHEQUEOS A LA RECEPCIÓN DEL EQUIPO

30. Tras recibir el equipo desde fábrica, antes de realizar ninguna operación, se deberán llevar a cabo las verificaciones recogidas a continuación:

VERIFICACIONES SOBRE EL MATERIAL RECIBIDO
Verificación de embalaje
Verificar visualmente que el embalaje no ha sido abierto o manipulado y que no presenta daños externos o desperfectos reseñables.
Verificación de contenido
Una vez abierto el embalaje, verificar que se incluye todos los ítems asociados al cifrador, conforme a lo especificado en el apartado "Chequeos Previos" del Manual de Usuario [1].
Verificación de integridad física
Verificación de integridad física:

• Verificar que los precintos de seguridad del cifrador, situados a ambos lados del frontal, se encuentran intactos y revisar los tornillos de la tapa, la mecánica completa del equipo y sus interfaces externos para verificar que están en perfectas condiciones y que no presentan evidencias de manipulación. • Se recomienda registrar por algún medio dispuesto por la Organización usuaria (medios técnicos u organizativos ajenos al producto IS101) el número de serie de los precintos de seguridad del equipo, de forma que éstos puedan ser verificados posteriormente durante las inspecciones periódicas del equipo que se estipulen.

Tabla 3 Verificaciones sobre el material recibido

5.2 INSTALACIÓN Y CONEXIONES FÍSICAS

31. Para proceder a la instalación física y conexión del equipo en su ubicación designada, se deberán seguir las directrices y recomendaciones recogidas a continuación:

INSTALACIÓN Y CONEXIONES FÍSICAS
Instalación física
Colocación del equipo: se recomienda situar el equipo siempre en posición horizontal y evitar cubrir el cifrador o colocar objetos que dificulten el proceso de disipación de calor a través del chasis y radiador trasero del mismo.
Conexión de alimentación
Alimentación compatible: para garantizar la compatibilidad y evitar posibles daños se deberá emplear siempre con cada cifrador IS101 la fuente de alimentación proporcionada por el fabricante junto con el equipo, y asegurarse de que el conector de alimentación queda correctamente fijado al equipo, empleando para ello la rosca incluida a tal efecto.
Conexión de tierra
Conexión de tierra única: con carácter general, se deberá emplear únicamente uno de los dos tornillos disponibles en el panel trasero para la conexión a tierra del equipo.
Conexión de interfaces de datos LAN y WAN
Cableado de datos compatible: • Cifrador con interfaces eléctricos (10/100/1000BaseT, RJ45): se podrán emplear cables Ethernet estándar (RJ45) para su conexión a la red roja (interfaz LAN) y la red negra (interfaz WAN). Se recomienda el uso de cableado de categoría 6 o superior. • Cifrador con interfaces ópticos (1000BaseSX con conectores de rosca

específicos, tipo LC): se deberán emplear los cables suministrados por el fabricante para su conexión a la red roja (interfaz LAN) y la red negra (interfaz WAN) y tomar las precauciones habituales en el manejo de interfaces de fibra óptica para evitar posibles daños oculares por mirar directamente al interfaz o al extremo de la fibra óptica. Conexiones LAN / WAN aisladas: en ambos casos, se debe verificar durante la instalación (es responsabilidad del entorno garantizar que así sea) que la red roja que se desea proteger no dispone de conexiones físicas o lógicas por otros medios (distintos al cifrador) a la red negra de transporte, de forma que pudiera hacerse bypass de las protecciones proporcionadas por el cifrador a través de estos caminos alternativos.
Conexión de interfaz de consola
• Acceso físico: el interfaz de consola requiere acceso físico. En NINGÚN caso se podrán emplear medios que permitan hacer uso de éste de forma remota (como accesos remotos de consola, extensores o similar). • Conexión bajo demanda: se recomienda que el cable de consola (proporcionado por el fabricante) y el emulador de terminal correspondiente permanezcan conectados al equipo únicamente mientras se esté haciendo uso del interfaz de configuración por parte de un usuario autorizado para ello.
Conexión de interfaz USB
• Acceso físico: el uso del interfaz USB (para inyectores IS101K) requiere acceso físico. En NINGÚN caso se podrán emplear medios que permitan hacer uso de éste remotamente (como extensores o similar). • Conexión bajo demanda: el inyector IS101K deberá permanecer conectado al equipo únicamente mientras se estén realizando operaciones para las cuales sea necesario (instalación inicial, operaciones a través del menú *"display"* o carga *off-line* de parámetros de configuración) por parte de un usuario autorizado para ello.

Tabla 4. Instalación y conexiones físicas

5.3 INSTALACIÓN LÓGICA DEL EQUIPO

32. El cifrador debe llegar al responsable de su conexión y puesta en marcha en estado NO INSTALADO (estado en el que se entrega desde fábrica y en el que se debería transportar el cifrador cuando fuese necesario).

33. Para llevar a cabo la instalación lógica del equipo, el cifrador deberá estar arrancado (en caso contrario, con la alimentación externa conectada, se deberá presionar el pulsador de encendido-apagado situado en el panel frontal) y sin ninguna causa de tamper activa al iniciar el proceso de arranque, dado que, si

así fuese, la instalación lógica del cifrador no podría realizarse mientras no se hubiese resuelto.

34. A continuación, el Administrador de Seguridad al que haya sido asignada esta tarea deberá introducir el inyector IS101K correspondiente en el interfaz USB del equipo y, cuando se solicite, validarlo insertando su código PIN. Si el inyector está programado adecuadamente, con el permiso de instalación activo, el proceso de instalación se lleva a cabo automáticamente y el equipo será capaz de alcanzar el estado OPERATIVO.

35. El procedimiento a seguir y posibles situaciones de partida tras arrancar el equipo se describen en el apartado "Proceso de Arranque y Paso al Estado OPERATIVO" del Manual de Usuario [1].

5.4 CONSULTA DE LA VERSIÓN DEL EQUIPO

36. Durante la puesta en marcha inicial, antes de continuar con la instalación y configuración del cifrador en su entorno operativo, se recomienda comprobar que la versión del equipo se corresponde a la última versión liberada.

37. Para consultar la versión del equipo en este punto de la instalación, es necesario acceder al menú "*display*" (requiere acceso físico) y navegar hasta la pantalla " ⓘ - Información". La versión cargada en el equipo se corresponde con la mostrada en dicha pantalla mediante el epígrafe "Versión: X.XX".

38. Posteriormente, durante la fase de operación (una vez establecida la configuración oportuna para el cifrador), la consulta de la versión del equipo podrá realizarse cuando se requiera a través de sus interfaces de configuración (CLI y/o WEB) o desde el Centro de Gestión.

5.5 CONFIGURACIÓN INICIAL

39. Tras recibir el equipo desde fábrica y llevar a cabo su instalación física y lógica, antes de proceder a su configuración inicial básica es necesario ejecutar los pasos recogidos a continuación:

PASOS PREVIOS A LA CONFIGURACIÓN INICIAL
Habilitar primer login del Administrador de Configuración
En primer lugar, el Administrador de Seguridad al que haya sido asignada esta tarea deberá introducir y validar en el equipo el inyector IS101K correspondiente (programado con los permisos adecuados) y ejecutar las siguientes operaciones: • Definir contraseña inicial del Administrador de Configuración a través del menú "*display*". • Habilitar al menos una opción de acceso a la configuración del cifrador (CLI y/o WEB) a través del menú "*display*". • Comunicar por los medios seguros oportunos (medios técnicos u organizativos ajenos al producto IS101) al correspondiente Administrador de

Configuración su contraseña inicial y el / los interfaces configuración que debe / puede emplear (CLI y/o WEB) para su primer login y cambio de la contraseña inicial.

Asistir al Administrador de Configuración durante su primer *login* en caso de que se deba realizar a través del interfaz de configuración web seguro, para garantizar que éste dispone de una dirección IP roja en el cifrador (asignada automáticamente por DHCP, si se dispone de uno en el lado rojo, o bien manualmente a través del interfaz de consola) alcanzable por el PC empleado para acceder vía web y que puede realizar la descarga e instalación del correspondiente certificado de cliente web emitido por el cifrador (operación gestionada a través del menú "*display*").

Primer *login* del Administrador de Configuración

A continuación, el Administrador de Configuración deberá:

- Autenticarse frente al equipo (primer *login*) por el interfaz correspondiente (CLI o WEB) empleando su nombre de usuario "admin" y la contraseña inicial configurada para él. Si el primer *login* del Administrador de Configuración se debe realizar a través del interfaz de configuración web seguro, se requerirá para ello asistencia por parte del Administrador de Seguridad, como se ha indicado anteriormente.
- Cambiar la contraseña inicial asignada para él por el Administrador de Seguridad por una de mayor fortaleza y, a continuación, cerrar la sesión. Se recomienda realizar esta operación lo antes posible tras el establecimiento de la contraseña inicial por parte del Administrador de Seguridad.
- Comunicar por medios técnicos u organizativos ajenos al producto IS101 al Administrador de Seguridad que el cambio de su contraseña inicial ha sido completado.

Configuración de opciones de acceso deseadas

- Finalmente, el Administrador de Seguridad deberá dejar establecida en el equipo la configuración de opciones de acceso (CLI y/o WEB) que sea necesaria para la operación habitual del cifrador. Las necesidades en este sentido son dependientes de la infraestructura y medios de administración que se vayan a emplear durante la operación del cifrador. En general, se deberán mantener habilitadas las opciones de acceso CLI y/o WEB únicamente cuando sea necesario hacer uso de ellas durante la operación habitual del equipo.
- Para favorecer el manejo seguro del equipo, en aquellos entornos de instalación que se consideren más "hostiles" se recomienda que la opción de acceso CLI permanezca deshabilitada siempre que no se vaya a hacer uso del interfaz de consola, especialmente cuando el cifrador vaya a quedar desatendido o fuera de la supervisión del usuario autorizado.
- Por otro lado, para prolongar al máximo posible la vida útil del *display* integrado en el cifrador, se recomienda habilitar la opción "Salvapantallas".

Tabla 5 Pasos previos a la configuración inicial

40. Una vez completados los pasos anteriores, la configuración del resto de parámetros requeridos para la operación del cifrador podrá hacerse manualmente a través de los interfaces de configuración de éste (CLI y/o WEB, según opciones de acceso habilitadas) o bien de forma automática mediante el uso de un inyector IS101K programado para ello o desde el Centro de Gestión IS101M asociado al equipo (según infraestructura y medios de administración dispuestos para la operación del equipo). Dicha configuración, así como su posterior gestión y monitorización, se consideran parte de la fase de operación y mantenimiento y, por tanto, serán de aplicación las directrices y recomendaciones de uso recogidas a tal efecto en el apartado 6.- OPERACIÓN Y MANTENIMIENTO de esta guía.
41. Los procedimientos que se deben seguir para llevar cabo las operaciones anteriormente indicadas combinan acciones realizadas a través del menú "*display*" (especialmente en los pasos previos indicados) con otras realizadas a través de los interfaces de configuración CLI o WEB del equipo o bien desde el Centro de Gestión.
42. Para más detalles sobre el procedimiento completo y la configuración inicial básica requerida para que el cifrador pueda comenzar a cursar tráfico en la red, consultar el apartado "Configuración Inicial" del Manual de usuario [1] y los apartados correspondientes referidos desde éste para cada acción.

6. OPERACIÓN Y MANTENIMIENTO

6.1 GESTIÓN DE CONFIGURACIÓN Y MONITORIZACIÓN DEL CIFRADOR

43. En general, la configuración requerida de ajustes horarios, usuarios, parámetros de red e IPsec y configuración de alarmas en cada cifrador instalado son fuertemente dependientes de las necesidades de la Organización usuaria en cada instalación concreta y, en particular, de los medios dispuestos para su administración y de la topología de la red y conexiones que se desean proteger y gestionar a través del cifrador. Por tanto, excede del ámbito de esta guía proporcionar una lista de parámetros concretos a configurar.
44. No obstante, desde el punto de vista operativo y de seguridad, es importante tener en cuenta las directrices y recomendaciones recogidas a continuación:

GESTIÓN DE CONFIGURACIÓN Y MONITORIZACIÓN
Ajustes horarios
• Ajuste horario preciso: debe ajustarse la fecha, la hora y la zona horaria del cifrador de forma correcta y precisa durante la puesta en marcha del equipo, ya que la fecha / hora configurada se emplea como referencia temporal para

el registro de auditoría y para verificar la validez de los diferentes certificados usados por el equipo.

- Supervisión ajuste horario: se recomienda comprobar regularmente (por ejemplo, durante las tareas habituales de monitorización y/o inspecciones periódicas que se determine), que el valor de la fecha y la hora configurada es correcto.
- Reinicio tras cambio de fecha/hora: dadas las posibles implicaciones para la operación del cifrador, se recomienda reiniciarlo siempre que se realice un cambio en la fecha / hora. Esta operación de reinicio no será necesaria en el caso de realizar únicamente cambios de la zona horaria (el cambio de la zona horaria tiene efectos a nivel de presentación pero no afecta al valor de fecha / hora absoluto almacenado en el equipo y usado como referencia temporal por el equipo).

Gestión de usuarios

- Mínimo nº de usuarios "Operador": se deberán dar de alta y mantener únicamente aquellos usuarios con perfil "Operador" que sean estrictamente necesarios para la operación del equipo (gestión de configuración y monitorización), teniendo en cuenta los medios dispuestos para dichas tareas.
- Privilegios mínimos: para cada usuario con perfil "Operador" se deberán habilitar y mantener en la configuración del equipo los mínimos permisos necesarios que le permitan desempeñar sus funciones asignadas.
- Política de contraseñas: todos los usuarios autorizados (perfil "Operador" y "Administrador de Configuración"), con independencia del interfaz de configuración que empleen para acceder al equipo, deberán seguir al menos las pautas recogidas en el apartado "Directrices para Gestión de Contraseñas / Claves" del documento IS101. Manual de Usuario [1] para la definición, modificación y gestión de sus correspondientes contraseñas de acceso.
- Higiene de la configuración vigente: si un determinado usuario autorizado de tipo "Operador" deja de ser necesario para la operación del equipo, deberá ser eliminado de la configuración. Este requisito cobra especial relevancia en los casos en los que el operador causa baja en la Organización o se le asignan otras tareas. No es posible eliminar el usuario "Administrador de Configuración", por lo que cualquier cambio de la persona física que desempeña dichas tareas (baja en la Organización o reasignación de tareas) deberá llevar a aparejado el correspondiente cambio de contraseña y, en su caso, retirada del certificado de cliente web utilizado para acceder al interfaz de configuración web seguro.
- Supervisión de usuarios configurados: se recomienda revisar regularmente la configuración de usuarios de los equipos, prestando especial atención a que los permisos asignados a cada uno sean, en todo momento, consistentes con las tareas de gestión y/o monitorización que debe realizar dicho usuario.
- Usuario para tareas de monitorización: por seguridad, deberá crearse un usuario (o varios en caso de requerir segregación de funciones) que disponga

de permisos de visualización pero no de gestión sobre los parámetros de red, IPsec y alarmas, para que pueda llevar a cabo el control del estado del sistema y su supervisión sin que exista el riesgo de que modifique su configuración.
Gestión de los parámetros de red
• Mínimo número de parámetros de red: se deberán dar de alta y mantener en la configuración del equipo únicamente aquellos parámetros de red (protocolos automáticos, direcciones, rutas, vecinos, VLANs, etc.) que sean estrictamente necesarios para la operación del equipo, teniendo en cuenta las particularidades de conexión y comunicaciones requeridas en cada instalación. • Higiene de la configuración vigente: si por necesidades operativas un determinado parámetro de red deja de ser necesario para la operación del equipo, éste deberá ser eliminado de la configuración. • Supervisión parámetros de red: se recomienda revisar regularmente la configuración de parámetros de red de los equipos, prestando especial atención al estado de éstos y a los avisos respecto a potenciales errores, incoherencias o inconsistencias presentados a través de los interfaces de configuración de cada equipo o del conjunto de ellos en el Centro de Gestión (cuando se disponga de uno).
Gestión de los parámetros IPSec
• Mínimo número de parámetros IPsec: se deberán dar de alta y mantener en la configuración del equipo únicamente aquellos parámetros IPsec (certificados de comunicaciones y/o claves PSS, CAs confiables, políticas de seguridad y selectores asociados) que sean estrictamente necesarios para la operación del equipo, teniendo en cuenta las particularidades de conexión y comunicaciones requeridas en cada instalación. Este requisito cobra especial importancia, en el caso de la definición de políticas de seguridad IPsec cuya acción asociada sea “bypass”. • Priorización de mecanismos de autenticación: se emplearán certificados X.509v3 (compatibles con el equipo) o claves secretas pre-compartidas (PSS) para la autenticación entre extremos para las políticas de seguridad IPsec cuya acción asociada sea “proteger”. El orden de preferencia será certificados X.509v3 sobre PSS. • Precisión políticas de seguridad y selectores: para cada política de seguridad se deberán definir los selectores de tráfico locales y remotos de la forma más precisa y restrictiva posible, teniendo en cuenta las necesidades en cuanto a conexiones permitidas (rangos de direcciones, protocolos y, en su caso, rangos de puertos) y, cuando aplique, exclusiones requeridas dentro de las mismas en cada caso (mediante políticas de seguridad IPsec específicas cuya acción asociada sea “descartar”). Cuando sea de aplicación (según tipo de política de seguridad y método de autenticación empleado), se recomienda el uso de selectores por nombre. Se recomienda evitar siempre la definición

de selectores de tráfico solapados entre diferentes políticas de seguridad definidas para un mismo equipo. Es decir, se recomienda que los selectores de tráfico de cada política no presenten colisiones con los de otras políticas de seguridad dadas de alta en el mismo cifrador. Esta recomendación cobra especial importancia en el caso de la definición de políticas de seguridad IPsec cuyas acciones asociadas sean diferentes y, en particular, cuando para alguna de ellas la acción asociada sea "bypass".

- Parámetros opcionales en políticas de seguridad: algunos de los parámetros que definen una política de seguridad IPsec (como la dirección remota y local) son opcionales. Su inclusión o no dentro de la definición de la política de seguridad correspondiente puede depender de diferentes factores (tipo de política, otros parámetros de configuración de red...) por lo que se recomienda tener en consideración las pautas generales indicadas en el apartado "Configuración IPsec" del Manual de Usuario [1].
- Higiene de la configuración vigente: si por necesidades operativas un determinado parámetro IPsec deja de ser necesario para la operación del equipo, se deberá eliminar de la configuración.
- Supervisión parámetros IPsec: se recomienda revisar regularmente la configuración de parámetros IPsec de los equipos, prestando especial atención al estado de los mismos y a los avisos respecto a potenciales errores, incoherencias o inconsistencias presentados a través de los interfaces de configuración de cada equipo o del conjunto de ellos en el Centro de Gestión (cuando se disponga de uno).

Gestión del registro de auditoría

- Supervisión regular de alarmas registradas: se deberá establecer una periodicidad adecuada para la revisión de las alarmas registradas por el equipo, consistente con las necesidades de la Organización usuaria y la criticidad de las comunicaciones a gestionar a través del cifrador. Se deberán disponer los medios y procedimientos oportunos en la Organización para garantizar que las alarmas registradas en el equipo son adecuadamente supervisadas por el usuario autorizado correspondiente (antes de que se alcance la capacidad máxima del registro de auditoría).
- Filtro de alarmas a registrar suficiente: siempre que los medios dispuestos para la monitorización y revisión de las alarmas del equipo lo permitan, se recomienda que el filtro de alarmas a registrar se configure de la forma más amplia posible.
- Filtro de alarmas a registrar correctamente dimensionado: se debe configurar el filtro de alarmas a registrar (nivel mínimo, orígenes y tipos) de forma consistente con la periodicidad establecida para la monitorización y revisión de las alarmas del equipo, para evitar que una potencial saturación de los medios dispuestos para su supervisión pudiera derivar en la no supervisión de alarmas de mayor relevancia antes de que se alcance la capacidad máxima del registro de auditoría.

Gestión del envío de traps SNMPv3

La activación del servicio de envío de alarmas como traps SNMPv3 (con autenticación y cifrado) a un supervisor externo no es obligatoria.

Siempre que se disponga de un Centro de Gestión IS101M en la red es preferible (y ofrece mayores ventajas) realizar la monitorización remota del conjunto de alarmas generadas por los equipos IS101 de la red desde dicho CdG en vez de realizarla desde un supervisor SNMP externo.

Siempre que no se vaya a hacer uso en la instalación de un supervisor SNMP externo, el servicio de envío de traps SNMPv3 desde el equipo deberá estar desactivado.

No obstante, si se desea activar este servicio para integrar las alarmas generadas por los cifradores en un sistema de monitorización global de la Organización, se deberán tener en cuenta las siguientes directrices y recomendaciones:

- Configuración supervisor SNMPv3: se deberá configurar en el equipo la dirección IP del supervisor SNMPv3 (y puerto deseado) y garantizar que ésta es alcanzable desde el interfaz rojo del cifrador. Dicho supervisor SNMPv3 deberá estar en la red roja local o en una red roja remota alcanzable a través de una política de seguridad cuya acción asociada sea “proteger”. Para la definición de las claves de autenticación y cifrado empleadas por el protocolo SNMPv3, se deberán seguir al menos las pautas recogidas en el apartado “Directrices para Gestión de Contraseñas / Claves” del Manual de Usuario [1].
- Supervisión regular de alarmas enviadas como traps SNMPv3: se deberá establecer una periodicidad adecuada para la revisión de las alarmas enviadas como traps SNMPv3 por el equipo, consistente con las necesidades de la Organización usuaria y la criticidad de las comunicaciones a gestionar a través del cifrador. Se deberán disponer los medios y procedimientos oportunos en la Organización para garantizar que las alarmas enviadas como traps SNMPv3 por el equipo son adecuadamente supervisadas por el usuario al que se asigne dicha tarea.

Filtro de traps SNMPv3 mínimo: dado que los usuarios que operan el supervisor SNMPv3 externo al que se envían los traps generados por el equipo no tienen por qué coincidir con usuarios autorizados del cifrador o tener la misma necesidad de conocer, se recomienda que el filtro de alarmas a enviar como traps SNMPv3 (nivel mínimo, orígenes y tipos) se configure de la forma más restrictiva posible, teniendo en cuenta las necesidades concretas de la cada instalación.

Gestión de Sistema (Backup ficheros configuración y restauración)

Dentro de las opciones de configuración y gestión del cifrador, existe una opción que permite al usuario descargar un fichero (cifrado) con la configuración vigente del cifrador en un determinado momento. Siempre que se emplee esta opción para mantener un *backup* de la configuración de uno varios equipos o se realice una operación de restauración de la configuración desde un fichero previamente descargado para el equipo, se deberán tener en cuenta las recomendaciones recogidas al respecto en el apartado "Gestión de la Configuración del Sistema" Manual de Usuario [1]

Tabla 6. Gestión de configuración y monitorización

45. La gestión de configuración y monitorización de la red de cifradores IS101 puede llevarse a cabo individualmente para cada equipo (a través de sus interfaces de configuración CLI y/o WEB) o bien de forma conjunta para todos ellos desde el Centro de Gestión. Así mismo, durante la operación del equipo, puede requerirse el uso de inyectores IS101K para distintos propósitos. En función del medio empleado para estas tareas, se deberán tener en consideración adicionalmente las directrices y recomendaciones correspondientes a cada uno (ver apartado 6.2.- Uso Seguro de los Interfaces de Gestión del Cifrador y los Inyectores IS101K de esta guía).

6.2 USO SEGURO DE LOS INTERFACES DE GESTIÓN DEL CIFRADOR Y LOS INYECTORES IS101K

46. Durante la operación habitual del cifrador en la red y acorde a las necesidades operativas de cada instalación se emplearán uno o varios de los siguientes interfaces de configuración y/o componentes adicionales del criptosistema:

    a) Centro de Gestión asociado IS101M.

    b) Interfaz de consola del cifrador.

    c) Interfaz de configuración web seguro del cifrador.

    d) Inyectores IS101K.

47. Para garantizar que se lleva a cabo un uso seguro de estos medios, se deberán tener en consideración y seguir las directrices y recomendaciones recogidas a continuación para cada uno:

USO SEGURO DE INTERFACES DE GESTIÓN E INYECTORES
Centro de Gestión IS101M e Inyector de Gestión
El Centro de Gestión IS101M está formado por un cifrador del CdG junto con su correspondiente BBDD asociada y un puesto de gestión (PC con navegador y certificados compatibles) para acceder al interfaz proporcionado por el cifrador del CdG que permite gestionar la red completa de cifradores de forma centralizada y segura.

Considerando lo anterior, se deberán tener en cuenta las siguientes directrices y recomendaciones:

- Cifrador del CdG: carácter general, se seguirán las mismas directrices y recomendaciones que en el caso de un cifrador IS101 genérico (proporcionadas a lo largo de esta guía) para su conexión, instalación, puesta en marcha, configuración y operación, así como las recomendaciones específicas ya recogidas en la Tabla 2 (sección "Centro de Gestión IS101M e Inyectores IS101K").
- Acceso y uso del interfaz CdG: el acceso al interfaz CdG se produce mediante la conexión por https a una de las direcciones IP rojas del cifrador del CdG, siempre que la BBDD esté correctamente montada y que el usuario autorizado del cifrador del CdG que se autentique tenga habilitado el correspondiente permiso de gestión. Por tanto, al tratarse de un acceso vía web seguro, serán de aplicación las mismas directrices y recomendaciones expresadas a lo largo de esta guía para el uso seguro del interfaz de configuración web seguro de los cifradores IS101.
- Mínimo número de usuarios con permiso de gestión: en el cifrador del CdG, se deberán dar de alta y mantener en la configuración del equipo únicamente aquellos usuarios con permiso de gestión (también denominado permiso de "manager" o de "Usuario Centro de Gestión") que sean estrictamente necesarios (para la gestión y monitorización de la red de cifradores desde el interfaz CdG), teniendo en cuenta los medios dispuestos para dichas tareas. En general, puede ser recomendable que esta capacidad quede restringida exclusivamente al "Administrador del Configuración" del cifrador del CdG.
- Higiene de la configuración vigente: si por necesidades operativas un equipo (cifrador) de la red, VPN o red de bypass dada de alta deja de ser necesaria para la operación de la red de cifradores, se deberá eliminar dicho elemento de la BBDD del CdG y de la configuración de los cifradores implicados[3].
- Supervisión de parámetros de configuración de la red de cifradores: se recomienda revisar regularmente la configuración de la red de cifradores (equipos, VPNs, redes de bypass, alarmas y errores detectados), prestando especial atención al estado de conexión de los equipos, la posible presencia de parámetros definidos manualmente (y, en su caso, incorporación de éstos a la BBDD del CdG), conjunto de alarmas de los equipos recogidas por el CdG, la lista de errores detectados por éste y avisos respecto a potenciales errores, incoherencias o inconsistencias presentados a través del interfaz CdG.
- Mínimo nº de inyectores, privilegios mínimos y distribución controlada: se recomienda que el número de inyectores IS101K generados para la red de cifradores se mantenga en el mínimo imprescindible para la operación en la red, que en cada uno se programen desde el CdG IS101M asociado

[3] Esta operación se realizará automáticamente al eliminar el elemento de la BBDD del CdG en el caso los equipos implicados que sean gestionables y alcanzables por el CdG.

únicamente los permisos y datos necesarios, y que éstos se entreguen únicamente a el/los correspondiente/s usuario/s con perfil "Administrador de Seguridad".

- Operación de actualización SW: ver directrices y recomendaciones al respecto incluidas en el apartado 6.3.- Actualizaciones de Software de esta guía. Nótese que desde el CdG se puede llevar a cabo también la actualización del SW del propio cifrador del CdG. Para evitar conflictos, es altamente recomendable que las operaciones de actualización SW del cifrador del CdG y de actualización SW del resto de cifradores IS101 de la red desde el CdG NO se lleven a cabo al mismo tiempo (para más detalles sobre el procedimiento recomendado, consultar el apartado "Actualización Software de un Cifrador desde el Centro de Gestión" del Manual de Usuario del CdG [2].
- Backups de la BBDD: para garantizar que es posible recuperar la BBDD del CdG ante una potencial corrupción de la misma, se recomienda configurar desde la puesta en marcha inicial del CdG el mecanismo de *backups* periódicos de la BBDD integrado en el interfaz CdG, teniendo en cuenta tanto el tamaño de la red de cifradores, criticidad de los servicios proporcionados y estabilidad en el tiempo de su configuración como el espacio de almacenamiento disponible en el dispositivo externo de almacenamiento en red donde resida la BBDD del CdG. Se recomienda que la hora configurada para el backup diario programado se establezca en horas valle de la actividad del CdG. Además, opcionalmente la Organización usuaria podrá establecer los procedimientos adicionales que considere oportunos para llevar a cabo *backups off-line* del propio dispositivo externo de almacenamiento en red donde resida la BBDD del CdG, siguiendo en dicho caso las recomendaciones recogidas para ello en el apartado "Copias de Seguridad de la BBDD" del Manual de Usuario del CdG [2].
- Cierre de sesión: cualquier "Administrador de Configuración" u "Operador" del cifrador del CdG con permiso de gestión en posesión de credenciales válidas que acceda al cifrador del CdG a través del interfaz CdG para gestionar de forma conjunta la red de cifradores deberá cerrar su sesión activa cuando finalice su operación y siempre que el PC empleado para ello vaya a quedar desatendido o fuera de su supervisión directa.
- Inyector de Gestión: el inyector de gestión es un inyector IS101K especial programado por el fabricante para la puesta en marcha del cifrador del CdG. En general, su uso debe restringirse a la puesta en marcha del Centro de Gestión IS101M de la Organización (inicial o para recuperación tras eventos excepcionales, como un tamper alto del cifrador del CdG). Se recomienda que únicamente el responsable máximo del CdG ("Administrador de Seguridad" al que esté asignado dicho inyector) haga uso de éste (asumiendo la responsabilidad de custodiar adecuadamente su código PIN asociado) y que, siempre que no esté en uso, lo almacene en un lugar seguro.

Interfaz de consola

- Medios empleados y Usuarios autorizados: ver directrices y recomendaciones al respecto ya incluidas en Tabla 2Tabla 2 (secciones “Medios para gestión individual” y “Usuarios autorizados”).
- Acceso físico y conexión bajo demanda: ver directrices y recomendaciones al respecto ya incluidas en Tabla 4 (sección “Conexión interfaz de consola”).
- Política de contraseñas: ver directrices y recomendaciones al respecto ya incluidas en Tabla 6 (sección “Gestión de Usuarios”).
- Cierre de sesión: cualquier “Administrador de Configuración” u “Operador” en posesión de credenciales válidas que acceda al cifrador a través del interfaz de consola deberá cerrar su sesión activa cuando finalice su operación con el mismo y siempre que el PC empleado para ello vaya a quedar desatendido o fuera de su supervisión directa.

Interfaz de configuración Web seguro

Interfaz de configuración Web seguro

- Medios empleados y Usuarios autorizados: ver directrices y recomendaciones al respecto ya incluidas en Tabla 2 (secciones “Medios para gestión individual” y “Usuarios autorizados”).
- Ubicación medios empleados: se recomienda que los PCs empleados para acceso a través de este interfaz estén ubicados en la red roja local del cifrador a gestionar o, en su defecto, en una red roja remota alcanzable a través de una política de seguridad cuya acción asociada sea “proteger”.
- Gestión de certificados importados: durante la importación del certificado raíz de la red de cifradores (entregado junto con el manual de usuario), se debe comprobar que su huella digital es la correspondiente al certificado raíz emitido por el fabricante. Durante la importación del certificado de cliente web de cada cifrador, se deberá comprobar que en el campo “Sujeto” se muestran al menos los datos CN=webclient y OU= EQUIP#n, donde n es el número de serie del equipo al que pertenece dicho certificado de cliente web. Así mismo, se recomienda revisar periódicamente los certificados de cliente web importados en el navegador del PC empleado para este tipo de acceso a los cifradores, manteniendo en su configuración únicamente aquellos certificados correspondientes a los cifradores que el usuario autorizado deba gestionar a través de este medio y únicamente mientras sigan en vigor.
- Protocolo seguro con autenticación bidireccional: una vez importados los correspondientes certificados, se accederá por https a una de las direcciones IP del lado rojo del cifrador y se seleccionará el certificado de cliente web correspondiente al equipo para iniciar el establecimiento del canal seguro https (con TLS v1.2). El usuario autorizado NO deberá continuar, en ningún caso, con la conexión o introducir sus credenciales de acceso si no se ha verificado previamente que la conexión https se ha completado correctamente con éxito en ambos sentidos, es decir, si la ventana de acceso mostrada en el navegador no va acompañada de las correspondientes marcas que denotan que el canal https establecido es seguro.

- Uso del Navegador: Se utilizará un navegador actualizado a la última versión. Para mantener la debida custodia de claves y contraseñas de acceso, los usuarios NO deberán emplear en ningún caso la opción "recordar contraseña" del navegador. Además, se recomienda al usuario que borre la caché y, si es posible, el historial de acceso antes de comenzar a utilizar el navegador para acceder al interfaz de configuración web seguro del equipo. Esta operación se repetirá tras cada actualización SW del cifrador.
- Múltiples sesiones: a través del interfaz de configuración web del equipo se pueden establecer varia sesiones simultáneas (hasta un máximo de 8) por parte del mismo u otros usuarios autorizados. Si durante la operación a través de este interfaz se advierte que hay otras sesiones activas (icono indicativo en la barra superior del interfaz gráfico correspondiente) y se desea realizar operaciones de introducción/modificación de parámetros de configuración, se recomienda al usuario ejecutar previamente la operación de refresco de la tabla/ventana sobre la que se desea realizar modificaciones.
- Política de contraseñas: ver directrices y recomendaciones al respecto ya incluidas en Tabla 6 (sección "Gestión de Usuarios").
  Cierre de sesión: cualquier "Administrador de Configuración" u "Operador" en posesión de credenciales válidas que acceda al cifrador a través del interfaz de configuración web seguro deberá cerrar su sesión activa (y asegurarse de que no hay otras sesiones web pendientes de cierre) cuando finalice su operación y siempre que el PC empleado para ello vaya a quedar desatendido o fuera de su supervisión directa.

Inyectores IS101K y menú del teclado / *display*

- Medios empleados y Usuarios autorizados: ver directrices y recomendaciones al respecto ya incluidas en Tabla 2 (secciones "Medios para gestión individual" y "Usuarios autorizados").
- Acceso físico y conexión bajo demanda: ver directrices y recomendaciones al respecto ya incluidas en Tabla 4 (sección "Conexión interfaz USB").
- Inyectores compatibles: el cifrador IS101 es compatible con inyectores IS101K, que habrán sido suministrados originariamente por el fabricante y debidamente programados en el CdG IS101M asociado. El equipo rechazará cualquier inyector o dispositivo USB que no sea compatible con él.
- Configuración de opciones de acceso: ver directrices y recomendaciones al respecto ya incluidas en Tabla 5 (sección "Configuración de opciones de acceso deseada").
- Control certificados de cliente web generados / distribuidos: el número de certificados de cliente web generados y distribuidos desde el equipo (bajo el control del "Administrador de Seguridad" en posesión de un inyector IS101K con los permisos oportunos) deberá mantenerse en el mínimo imprescindible para que únicamente los usuarios autorizados (desde el mínimo número de PCs necesarios) tengan posibilidad de acceder remotamente al interfaz de configuración web seguro del equipo. Ante

cambios en las personas físicas o medios técnicos empleados para dicho acceso se deberán retirar estas credenciales de los PCs correspondientes. Ante una sospecha justificada de que alguna de dichas credenciales (certificados) ha sido violada, accedida o redistribuida de forma no autorizada se recomienda revocar la raíz de certificados de clientes web y generar una nueva en el equipo (operación gestionada a través del menú "*display*"); y se distribuirán nuevos certificados de cliente web a aquellos usuarios autorizados que lo requieran.

- Operación de actualización SW: ver directrices y recomendaciones al respecto incluidas en el apartado 6.3.- Actualizaciones de Software de esta guía.
- Carga de datos de configuración: cuando un inyector IS101K esté programado para cargar ("off-line") parámetros de configuración en un determinado cifrador (identificado por su número de serie), se recomienda que, antes de emplearlo para ello, el usuario se asegure de que se parte de la configuración por defecto o, al menos, de que los parámetros a cargar (procedentes del inyector) NO entran en conflicto con otros posibles datos previamente configurados en el cifrador.
- Cierre de sesión (desconexión inyector): cualquier "Administrador de Seguridad" en posesión de un inyector IS101K deberá desconectarlo del cifrador IS101 en el que lo haya validado previamente (cierre de la sesión activa) cuando finalice su operación con él y siempre que el equipo vaya a quedar desatendido o fuera de su supervisión directa.
- Apagado del *display*: con objeto de prolongar al máximo la vida útil del *display*, se recomienda apagarlo presionando el botón izquierdo del teclado de navegación siempre que el equipo vaya a quedar desatendido o no sea necesario visualizar la información de estado. Esta operación apaga el *display* y mantiene el equipo encendido y funcionando normalmente. Desde este estado, es posible volver a encender el *display* del equipo en cualquier momento que sea necesario presionando cualquiera de los botones del teclado de navegación.
- Devolución al entorno del CdG: cualquier "Administrador de Seguridad" en posesión de un inyector IS101K cuyo uso ya no sea necesario o cuyas necesidades de programación hayan cambiado deberá devolverlo al entorno del Centro de Gestión IS101M asociado en el que se programó; de forma que dicho inyector pueda ser debidamente borrado y, en su caso, reprogramado.

Tabla 7. Uso seguro de interfaces de gestión e inyectores

6.3 ACTUALIZACIONES DE SOFTWARE

48. Dentro de su entorno operativo, únicamente se llevarán a cabo en los cifradores actualizaciones de SW cuando la correspondiente versión a cargar haya sido debidamente autorizada para su distribución en planta y haciendo uso para ello

de los medios y procedimientos descritos en el apartado "Actualización de Software" del Manual de Usuario [1].

49. Se debe tener en cuenta que, para que una actualización de SW realizada sobre el equipo se haga efectiva, una vez cargada, el equipo debe reiniciarse. Por tanto, se recomienda planificar adecuadamente esta intervención de forma que se realice en horas valle de la actividad de la red de cifradores y, siempre que sea posible, de forma conjunta para todos los equipos afectados.

6.4 SUSTITUCIÓN DE LA BATERÍA

50. Tan pronto como se detecte que la batería del equipo está baja se deberá proceder a su sustitución. El nivel de batería podrá comprobarse a través del *display* integrado o mediante la monitorización del estado del equipo a través de sus interfaces de configuración o desde el Centro de Gestión asociado.

51. El procedimiento que se debe seguir, así como las precauciones y recomendaciones que se deben tener en cuenta para ello se describen en el apartado "Sustitución de la Batería" del Manual de Usuario [1].

6.5 INSPECCIONES PERIÓDICAS

52. El cifrador dispone de un conjunto de mecanismos *tamper resistant* que permitirán al equipo (y, por tanto, a los correspondientes usuarios autorizados encargados de su monitorización) detectar, sin necesidad de supervisión física constante, diferentes intentos de manipulación o comportamientos anómalos, así como auto-protegerse frente a posibles ataques físicos o situaciones que puedan suponer un riesgo para su funcionamiento.

53. No obstante, también se recomienda realizar inspecciones físicas periódicas del equipo, de cara a poder detectar intentos de violación de los mecanismos *tamper evident* dispuestos. La periodicidad de estas revisiones debe establecerse de forma consistente con las necesidades de la Organización usuaria, según las condiciones concretas de entorno, infraestructura de protección física de las instalaciones en las que opera el cifrador y criticidad de las comunicaciones a gestionar a través del cifrador.

54. Durante dichas inspecciones periódicas deberán realizarse, al menos, las verificaciones recogidas a continuación:

VERIFICACIONES DURANTE INSPECCIONES PERIÓDICAS
Precintos de seguridad
• Verificar que los precintos de seguridad del equipo permanecen intactos y que no se han roto y/o deteriorado. • Se recomienda verificar que el número de serie único de los precintos de seguridad presentes en el equipo coincide con el registrado cuando se instaló el equipo en su ubicación correspondiente.

Verificación de la integridad física
• Revisar los tornillos de la tapa, la propia mecánica completa del equipo y los interfaces externos de éste para verificar que están en perfectas condiciones y que no presentan evidencias de manipulación.
Disipación
• Se recomienda verificar que no hay ningún objeto en las inmediaciones del equipo que pueda dificultar o bloquear la disipación del calor del cifrador, especialmente en la zona trasera, donde se encuentra el radiador.
Conexiones físicas
• Se recomienda verificar que el conector de alimentación está debidamente fijado a la entrada de alimentación del equipo a través de la rosca incluida para ello. • Se recomienda verificar, en lo posible, durante la inspección (es responsabilidad del entorno garantizar que así sea) que la red roja (a proteger) no dispone de conexiones físicas o lógicas por otros medios (distintos al cifrador) a la red negra de transporte a utilizar, de forma que pudiera hacerse bypass de las protecciones proporcionadas por el cifrador a través de estos caminos alternativos. • Se recomienda verificar que los interfaces de configuración disponibles en el panel frontal (interfaces de consola y USB) no tienen cableado o elementos conectados, salvo que en ese momento se estuviera haciendo uso de ellos.
Estado del equipo y de la batería
• Se recomienda verificar (por ejemplo, visualizando los iconos correspondientes en la pantalla principal de estado del *display* integrado) que el cifrador se encuentra en estado OPERATIVO (), que sus interfaces LAN y WAN permanecen activos (enlace levantado) y que el estado de carga de la batería del equipo es correcto (). En caso contrario, se deberán iniciar las tareas correspondientes para identificar y solventar el problema detectado en cada caso (revisión de las conexiones y cableado conectado al equipo, sustitución de la batería...).
Versión del equipo
• Se recomienda verificar que la versión del equipo es la correcta, conforme a la última versión liberada. Para ello, se debe acceder al menú *display* del equipo y navegar hasta la pantalla “ - Información”. La versión cargada en el equipo se corresponde con la mostrada en dicha pantalla mediante el epígrafe “Versión: X.XX”.

Tabla 8 Verificaciones durante inspecciones periódicas

6.6 TRASLADO DE UBICACIÓN DEL CIFRADOR

55. De acuerdo con las recomendaciones generales de distribución y transporte del equipo, si durante su ciclo de vida éste debe trasladarse de ubicación, bien por necesidades operativas de la Organización usuaria o bien por haber requerido su paso por el entorno de programación (por ejemplo, tras haber detectado un *tamper* de nivel alto), el transporte deberá hacerse siempre en estado NO INSTALADO y, siempre que sea posible, en su embalaje original, junto con todos los ítems incluidos originalmente cuando se recibió desde fábrica. Así mismo, antes de proceder a su traslado, es recomendable que se realice un borrado de su configuración, salvo que la Organización usuaria disponga lo contrario por necesidades operativas.

56. Partiendo del equipo en estado OPERATIVO, para situarlo en el estado NO INSTALADO se deberá presionar el botón de emergencia situado en el panel frontal del cifrador y esperar a que finalice el reinicio del equipo, verificando que tras dicho reinicio el icono de estado mostrado en el *display* del equipo es  . Una vez realizada esta acción, se puede proceder a apagar el equipo ordenadamente, mediante una pulsación larga sobre el botón de encendido / apagado, desconectarlo y embalarlo adecuadamente para su traslado de ubicación.

57. Una vez recibido el equipo en su nueva ubicación, los responsables de su instalación y puesta en marcha deberán seguir, con carácter general, las mismas indicaciones ya proporcionadas en el apartado 5 CONEXIÓN Y PUESTA EN MARCHA de esta guía, teniendo en cuenta las siguientes recomendaciones adicionales:

    a) En el caso de traslados de ubicación de un equipo que ya estuviera previamente operativo dentro de la Organización usuaria, el embalaje en el que se entregue no será nuevo, e incluso podría darse el caso de que no fuera el embalaje original proporcionado por el fabricante. En este supuesto, se recomienda acompañar el equipo de la documentación interna oportuna que acredite este hecho (generada por los responsables del traslado dentro de la Organización usuaria).

    b) Así mismo, se recomienda verificar que el número de serie único de los precintos de seguridad presentes en el equipo coincide con el registrado cuando se recibió el equipo originalmente.

    c) En función de las necesidades operativas de la Organización usuaria, el equipo podría estar ya configurado total o parcialmente (por ejemplo, si tras su recepción desde fábrica se requiere realizar la configuración inicial o una determinada pre-configuración en alguna ubicación de la Organización usuaria diferente al emplazamiento final en el que el cifrador quedará instalado). En este supuesto, durante su conexión y puesta en marcha se deberá verificar que dicha configuración se ajusta

perfectamente a las necesidades de operación del equipo o, en su defecto, modificarla convenientemente.

6.7 ACTUACIÓN EN CASO DE EMERGENCIA

58. El cifrador IS101 dispone de un mecanismo anti-tamper activo (pulsador de emergencia) que puede ser activado por cualquier usuario con acceso físico al equipo con el fin de llevarlo a un estado seguro (NO INSTALADO) ante una situación de emergencia.

59. Para activar dicho mecanismo, se debe presionar el botón de emergencia situado en el panel frontal del cifrador y esperar a que finalice el reinicio del equipo, verificando que tras dicho reinicio el icono de estado mostrado en el *display* es  .

60. Una vez que se ha resuelto el incidente que provocó la pulsación del botón de emergencia, si se desea recuperar el equipo del estado NO INSTALADO es necesario llevar a cabo nuevamente el proceso de instalación lógica (consultar apartado 5.3.- Instalación Lógica del Equipo de esta guía).

6.8 ACTUACIÓN EN CASO DE DETECCIÓN DE TAMPER

61. El cifrador dispone de diversos mecanismos anti-tamper que le permiten auto-protegerse frente a ciertas condiciones de operación anómalas (intencionadas o fortuitas) y frente a determinados intentos de manipulación física y/o ataque a su comportamiento lógico (eventos de tamper). Así mismo, dispone de medios para notificar la detección de estas situaciones potencialmente peligrosas mediante las correspondientes alarmas e iconos representativos a través del *display* integrado.

62. Si mediante las tareas de monitorización de las alarmas del equipo o durante las inspecciones periódicas realizadas sobre él se detecta la ocurrencia de un evento de tamper se deberá:

    a) Determinar el nivel del evento de tamper detectado (nivel bajo o nivel alto).

    b) Investigar las causas que produjeron la situación de tamper para determinar si se trata de un evento causado por un intento de manipulación intencionado o provocado por condiciones de operación fuera de rango (fortuitas o intencionadas).

    c) En caso de que, a través de esta investigación, se concluya que el evento que lo provocó ya no está presente y que fue un evento aislado fortuito (ya no supone un riesgo para la operación del equipo en condiciones seguras), se podrá proceder a recuperar el equipo.

63. Tras una situación de tamper será necesaria la intervención de un "Administrador de Seguridad", para realizar una inspección y análisis del

cifrador, acorde con el nivel de la amenaza detectada, antes de poner de nuevo el equipo en estado operativo:

a) Si el evento detectado provocó un tamper de nivel bajo, tras la correspondiente inspección física completa del equipo, las conexiones y las condiciones ambientales del entorno de operación, el "Administrador de Seguridad" en posesión del inyector con el permiso adecuado podrá llevar a cabo de nuevo el proceso de instalación lógica del cifrador para recuperar el estado operativo (recuperación posible en campo) y, a continuación, realizar una revisión completa de la configuración del equipo antes de volver a utilizar el cifrador normalmente.

b) Si el evento detectado provocó un tamper de nivel alto, la recuperación del equipo no podrá realizarse en campo sino en el entorno de programación, donde se deberá realizar una inspección completa para determinar si es factible y/o adecuado llevar a cabo su re-programación y devolución al entorno operativo. En este supuesto, la recepción de vuelta en el entorno operativo del cifrador (una vez re-programado) requerirá llevar a cabo las mismas verificaciones y acciones para su conexión y puesta en marcha que en el caso de un equipo nuevo, acorde a lo descrito a lo largo de esta guía.

7. REFERENCIAS

[1] IS101. Manual de Usuario. Ref. IS240101ZZ01.
[2] IS101M. Manual de Usuario del Centro de Gestión. Ref. IS240101MZ01.
[3] CCN-STIC-807 Criptografía de empleo en el ENS.

8. ABREVIATURAS

AES	*Advanced Encription Standard*
BBDD	Base de Datos
CA	*Certificate Authority*
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CdG	Centro de Gestión
CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
DHCP	*Dynamic Host Configuration Protocol*
EAL	*Evaluation Assurance Level*
ESP	*Encapsulating Security Payload*
FW	Firmware
Gbps	Gigabit por segundo
GCM	*Galois Counter Mode*
https	*HyperText Transfer Protocol Secure*
HW	*Hardware*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
IPv4	*Internet Protocol (versión 4)*
IPv6	*Internet Protocol (versión 6)*
IT	*Information Technology*
LAN	*Local Area Network*
NIST	National Institute of Standard and Technology
OSPF	*Open Shortest Path First*
PC	*Personal Computer*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PSS	*Pre-Shared Secret*
RIP	*Routing Information Protocol*
SAN	*Subject Alternate Name*
SNMP	*Simple Network Management Protocol*
SW	*Software*
TLS	*Transport Layer Security*
USB	*Universal Serial Bus*
VLAN	*Virtual Local Area Network*

VPN	*Virtual Private Network*
VRRP	*Virtual Router Redundancy Protocol*
WAN	*Wide Area Network*