

Guía de Seguridad de las TIC Anexo C CCN-STIC-106

Plantilla de Procedimiento de Empleo Seguro (PES)



Octubre 2026

Edita:



Centro Criptológico Nacional, 2026



CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.10.08 12:53:42 +02'00'

Fecha de Edición: Octubre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	7
1.1 DESCRIPCIÓN DEL PRODUCTO	7
1.2 OBJETO Y ALCANCE	7
1.3 ORGANIZACIÓN DEL DOCUMENTO.....	7
2 FASE PREVIA A LA INSTALACIÓN	8
2.1 ENTREGA SEGURA DEL PRODUCTO	8
2.2 ENTORNO DE INSTALACIÓN SEGURO	8
2.3 REGISTRO Y LICENCIAS	8
2.4 CONSIDERACIONES PREVIAS.....	8
2.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	8
3 FASE DE INSTALACIÓN.....	8
4 FASE DE CONFIGURACIÓN	9
4.1 MODO DE OPERACIÓN SEGURO	9
4.2 IDENTIDAD Y ACCESO.....	9
4.2.1 AUTENTICACIÓN	9
4.2.2 ADMINISTRACIÓN LOCAL Y REMOTA	9
4.2.3 CONFIGURACIÓN DE ADMINISTRADORES	10
4.2.4 SERVIDORES DE AUTENTICACIÓN	11
4.3 COMUNICACIONES Y CRIPTOGRAFÍA.....	11
4.3.1 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	11
4.3.2 GESTIÓN DE CERTIFICADOS	11
4.3.3 SINCRONIZACIÓN	11
4.4 REGISTRO Y AUDITORÍA	12
4.4.1 REGISTRO DE EVENTOS.....	12
4.4.2 ALMACENAMIENTO LOCAL.....	12
4.4.3 ALMACENAMIENTO REMOTO	12
4.5 DISPONIBILIDAD Y RESPALDO	12
4.5.1 ALTA DISPONIBILIDAD.....	12
4.5.2 COPIAS DE SEGURIDAD	12
4.6 ACTUALIZACIONES Y AUTO-CHEQUEOS.....	12
4.6.1 ACTUALIZACIONES	12
4.6.2 AUTO-CHEQUEOS	13
4.7 RESUMEN DE LA CONFIGURACIÓN SEGURA.....	13
5 FASE DE OPERACIÓN Y MANTENIMIENTO	14
5.1 SOPORTE DE SEGURIDAD	14
5.2 NOTIFICACIÓN DE VULNERABILIDADES	14
5.3 APLICACIÓN DE ACTUALIZACIONES DE SEGURIDAD	14
5.4 FIN DE VIDA DEL PRODUCTO	14
6 PARTICULARIDADES PARA PRODUCTOS APROBADOS	14
6.1 REGISTRO Y LICENCIAS	14
6.2 DESPLIEGUE EXCLUSIVO ON-PREMISE.....	15
6.3 ACTUALIZACIONES OFFLINE	15
6.4 NO ENVÍO DE TRAZAS A LA NUBE	15
6.5 AUTO-CHEQUEOS.....	15
7 REFERENCIAS	15
8 ABREVIATURAS.....	16

ÍNDICE DE TABLAS

TABLA 1: EJEMPLO TABLA5

ÍNDICE DE FIGURAS

FIGURA 1: EJEMPLO FIGURA5

INSTRUCCIONES DE CUMPLIMENTACIÓN, ENVÍO Y PUBLICACIÓN

Esta plantilla constituye el Anexo C de la CCN-STIC-106. El documento resultante de su cumplimentación será el procedimiento de empleo seguro (PES) del producto y el CCN lo publicará como guía de la serie CCN-STIC-1000, asignándole el número de guía y completando la portada, las cabeceras y la página de créditos.

El Anexo C de la CCN-STIC-106 se publica en formato PDF. La versión editable de la plantilla, en formato Word, puede solicitarse a través del buzón soporte.cpstic@ccn.cni.es.

Los textos de esta plantilla son instrucciones de cumplimentación y deberán eliminarse del documento final, al igual que la tabla, la figura y la nota incluidas a título de ejemplo. Los apartados que no resulten de aplicación se mantendrán, haciendo constar expresamente su no aplicabilidad.

El solicitante remitirá la propuesta de PES, en formato editable, a la dirección soporte.cpstic@ccn.cni.es, indicando en el asunto el nombre del producto y el código de expediente del CPSTIC.

El PES se remitirá en formato Word, respetando la estructura, los estilos y los apartados de esta plantilla, de modo que el CCN pueda revisarlo y publicarlo como guía CCN-STIC de la serie 1000.

El plazo de entrega es de seis (6) meses desde la notificación del RITI favorable, conforme al apartado 4.5.5 de la CCN-STIC-106. La falta de entrega en plazo conlleva la exclusión del producto del catálogo.

El CCN revisará la propuesta y podrá devolverla con comentarios. El solicitante remitirá las versiones corregidas por el mismo canal hasta obtener la conformidad del CCN.

Obtenida la conformidad, el CCN publicará la guía, momento en el que la inclusión del producto adquiere carácter definitivo conforme al apartado 4.5.6 de la CCN-STIC-106.

Toda ampliación del alcance o nueva versión cualificada que afecte al contenido del PES exigirá remitir una versión actualizada por el mismo canal, que dará lugar a una nueva edición de la guía.

Instrucciones de contenido

Deberá describirse íntegramente en este documento todo aquello que el administrador tenga que ejecutar para dejar el producto en su configuración segura: los pasos, los parámetros y los valores concretos.

Podrá referenciarse a la documentación del fabricante aquello que no condicione la configuración segura, siempre que el documento referenciado sea público y accesible, esté identificado por título, versión y fecha, se relacione en el apartado de referencias y se cite en el texto como [REFn].

No se incluirán credenciales, claves, datos de clientes ni contenido de carácter comercial.

Cuando un apartado no resulte de aplicación, se mantendrá el epígrafe y se hará constar expresamente su no aplicabilidad, justificándola.

Si el documento cubre varios modelos o plataformas y la configuración difiere entre ellos, se indicará expresamente a qué modelos aplica cada paso.

Instrucciones de formato

Se emplearán los estilos de la plantilla: Título 1 a 3 para los epígrafes, Párrafo para el texto, Código para los comandos y Descripción para los pies de tabla y de figura.

Las tablas y las figuras se numerarán con su pie correspondiente y se citarán en el texto. No se emplearán cuadros de texto ni imágenes de texto, y las capturas de pantalla deberán resultar legibles.

No se modificarán la portada, las cabeceras ni los pies de página: el CCN los sustituye al publicar la guía, junto con la página de créditos y el número de la serie CCN-STIC-1000.

Las tablas, las figuras, los pies y los fragmentos de código se insertarán con el formato que se muestra a continuación.

El texto redactado por el fabricante se escribirá con el estilo Párrafo, en color negro y sin cursiva, como en el ejemplo siguiente:

Este es un ejemplo de texto de párrafo. El contenido que redacte el fabricante deberá presentar este formato, de modo que se distinga de las instrucciones de la plantilla, que figuran en gris y cursiva y deben eliminarse del documento final.

TITULOS	TITULOS
SUBTITULOS	SUBTITULOS

Tabla : Ejemplo tabla

Esto es texto de código



Figura : Ejemplo figura

NOTA: Ejemplo de nota, válido para todo el documento

Comprobaciones antes del envío

- *Se han eliminado todos los textos en gris y cursiva de la plantilla, incluidos los ejemplos de tabla, figura, nota y código.*
- *Se han actualizado el índice general, el índice de tablas y el índice de figuras.*
- *Los apartados que no resultan de aplicación se mantienen con su justificación.*
- *Todas las referencias citadas en el texto figuran en el apartado de referencias, con título, versión y fecha.*
- *Las capturas de pantalla son legibles y no contienen información sensible.*
- *El documento se remite en formato editable a soporte.cpstic@ccn.cni.es.*

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL PRODUCTO

Descripción General del producto.

1.2 OBJETO Y ALCANCE

Indicar para qué producto – versión – modelos hardware – plataformas hardware – etc. se desarrolla esta guía.

El producto NOMBRE PRODUCTO ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF1].

1.3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado 2. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.*
- b) Apartado 3. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.*
- c) Apartado 4. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.*
- d) Apartado 5. En este apartado se recogen los aspectos relativos al mantenimiento seguro del producto durante su vida útil.*
- e) Apartado 6. En este apartado se recogen las particularidades aplicables cuando el producto, además de cualificado, vaya a ser aprobado para el manejo de información nacional clasificada.*
- f) Productos desplegados en nube. En estos casos, los apartados 2 y 3 se cumplimentarán con las particularidades del servicio: alta y acceso seguro al mismo, configuración del tenant o suscripción y reparto de responsabilidades entre el proveedor del servicio y el usuario.*

2 FASE PREVIA A LA INSTALACIÓN

2.1 ENTREGA SEGURA DEL PRODUCTO

Describir el procedimiento de recepción segura del producto.

- *En caso de que sea un dispositivo hardware (appliance), describir **paso a paso en este documento** cómo verificar el embalaje externo e interno, sellos de garantía, etc.*
- *En caso de que sea un producto software, describir **paso a paso en este documento** cómo verificar la integridad de la descarga. Por ejemplo, si se recibe vía email puede llevar una firma electrónica, si se descarga vía URL podría descargarse un fichero de hash, etc.*

*En caso de utilizar claves hash para la verificación de archivos, se deben utilizar **funciones SHA-256** o superiores.*

En el caso de productos desplegados en nube, describir el proceso de alta en el servicio y la entrega segura de las credenciales iniciales de acceso, así como la forma de verificar la autenticidad del punto de acceso al servicio (dominio y certificado).

2.2 ENTORNO DE INSTALACIÓN SEGURO

Indicar si alguno de los componentes del producto debe instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.

2.3 REGISTRO Y LICENCIAS

*Referenciar a la **documentación** pública donde se describa el proceso para el registro del hardware, software y/o licencias. Cuando el producto vaya a ser aprobado además de cualificado, se tendrá en cuenta lo indicado en el apartado 6.*

2.4 CONSIDERACIONES PREVIAS

*Si fuese necesaria una configuración adicional **relativa a la seguridad, previa a iniciar la instalación y configuración** del producto, deben indicarse **paso a paso en este documento** aquellos aspectos que se deban tener en cuenta, puesto que influirán en la forma de configurarlo de forma segura.*

Por ejemplo: preparación de otros componentes necesarios (token de entropía, almacén de claves criptográficas, plataformas hardware, etc.), decisión sobre aspectos de arquitectura física (por ejemplo, alta disponibilidad), o lógica (por ejemplo, métodos de autenticación).

2.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

Indicar qué componentes deben estar presentes en el entorno de operación del producto: servidor externo de autenticación, servidor externo syslog, workstation de gestión, etc.

3 FASE DE INSTALACIÓN

En este apartado se hará referencia a la documentación pública donde se describa cómo llevar a cabo la instalación de cada componente del producto:

- *Appliance: cómo debe instalarse el firmware correspondiente.*
- *Software: cómo se debe instalar el componente software, e indicar la plataforma sobre la que se ejecutará (servidor, workstation, etc.), incluyendo el sistema operativo y cualquier software de base que sea necesario.*

Se incluirá en este documento una indicación y descripción de los **parámetros relevantes y aspectos necesarios** para una instalación segura.

En caso de que el producto requiera de instalación de otros componentes adicionales, se indicará en este documento de **cuáles son y para qué se configuran**, haciendo referencia a su proceso de instalación en la documentación pública correspondiente.

En el caso de productos desplegados en nube, este apartado recogerá el proceso de aprovisionamiento y la configuración inicial del tenant o suscripción, indicando qué elementos son responsabilidad del proveedor del servicio y cuáles del usuario.

4 FASE DE CONFIGURACIÓN

4.1 MODO DE OPERACIÓN SEGURO

Se debe **describir paso a paso en este documento** cómo activar la configuración específica del producto para que este opere en el modo de operación seguro.

4.2 IDENTIDAD Y ACCESO

4.2.1 AUTENTICACIÓN

Describir en el documento los mecanismos de autenticación que utiliza el producto para:

- *Autenticación de usuarios (credenciales locales, servidor externo de autenticación, certificado, etc.).*
- *Autenticación entre componentes del producto y con servidores o dispositivos externos (certificado, claves pre-compartidas, etc.).*
- *Autenticación de sesiones (p.e SSH con clave pública, etc.).*

No se debe recomendar el uso de claves precompartidas si el producto soporta otro método (por ejemplo: certificados).

4.2.2 ADMINISTRACIÓN LOCAL Y REMOTA

Indicar qué mecanismos se utilizarán para la administración del producto: tanto local (consola), como remota (GUI y/o CLI).

NO deben permitirse protocolos **inseguros** para la administración, tales como:

- *Telnet (debe utilizarse SSH)*
- *Versión TLS inferior a 1.2 (debe utilizarse TLSv1.2 o superior)*
- *IKEv1 (debe utilizarse IKEv2)*
- *SSHv1 (debe utilizarse SSHv2)*

- FTP (debe utilizarse SFTP o SCP)
- HTTP (debe utilizarse HTTPS)

Debe describirse paso a paso en este documento cómo desactivar los protocolos inseguros, en caso de que sea posible. En caso de que no sea posible, debe indicarse que no se recomienda su uso.

Incluir una referencia a la documentación pública donde se describa cómo se configuran los protocolos seguros de administración (por ejemplo, HTTPS/TLS, SSH).

Describir paso a paso en este documento cómo se configuran los algoritmos y funciones criptográficas del producto deben cumplir con las especificaciones de la guía CCN-STIC-807. Esto significa que la configuración de estos protocolos deberá especificarse para utilizar, únicamente, los siguientes algoritmos y funciones:

- DSA o RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- Funciones Hash SHA-256 o superior.
- Cifrado AES-128 o superior.
- Grupos Diffie-Hellman 15, 16, 19, 20, 21, 28, 29 o 30.
- Elliptic Curve Diffie-Hellman P-256 o superior.

Como criterio general, siempre que se mencione algún algoritmo de cifrado, hash o función criptográfica en el procedimiento de empleo seguro, debe indicarse qué parámetros se utilizan. En caso de que el usuario administrador deba realizar alguna configuración para que estos sean seguros, debe incluirse una referencia a la documentación pública donde se describa como configurarlos (por ejemplo: cómo hacer uso de los algoritmos y funciones indicadas anteriormente, configurar las contraseñas protegidas por un valor hash o almacenamiento de backup cifrado).

4.2.3 CONFIGURACIÓN DE ADMINISTRADORES

Incluir una referencia a la documentación del fabricante donde se describan los roles de usuario de administración que permite el producto y cómo configurarlos.

Tener en cuenta los siguientes aspectos:

- **Configuración de la Política segura de contraseñas.** Deberá cumplir con los siguientes requisitos mínimos:
 - Longitud mínima de la contraseña: doce (12) caracteres.
 - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos.
 - Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5).
 - Tiempo de validez en días de las contraseñas tras el cual expiran: aproximadamente dos meses (60 días).
 - Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.
- **Configuración de los parámetros de sesión.** Deberá cumplir con los siguientes requisitos mínimos:

- Tiempo de inactividad de las sesiones: cinco (5) minutos.
- Número de intentos fallidos de inicio de sesión: tres (3) intentos.
- Tiempo de bloqueo tras los intentos fallidos: cinco (5) minutos.
- Configuración del mensaje de aviso y consentimiento en el inicio de sesión (**login banner**).

4.2.4 SERVIDORES DE AUTENTICACIÓN

Si el producto utiliza servidores externos de autenticación (RADIUS, LDAP, SAML, Kerberos, etc.), **hacer referencia a la documentación** que describa cómo configurarlos e indicar los parámetros relevantes para una configuración segura (por ejemplo, uso de RADSEC, LDAPv3, o TLSv1.2).

4.3 COMUNICACIONES Y CRIPTOGRAFÍA

4.3.1 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

En caso de que proceda, **describir paso a paso en este documento** las recomendaciones para la configuración segura de interfaces, puertos y servicios necesaria.

Por ejemplo: deshabilitar los servicios no utilizados en el dispositivo, introducir una etiqueta que identifique el uso para el que está destinado cada interfaz, asociar a cada interfaz la dirección IP y MAC de la máquina conectada, etc.

4.3.2 GESTIÓN DE CERTIFICADOS

Deben **indicarse** los algoritmos y funciones criptográficas del producto que cumplan con las especificaciones de la guía CCN-STIC-807 y **hacer referencia a la documentación pública** donde se describa cómo configurarlos. Estos parámetros son:

- RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- DSA con claves de, al menos, 3072 bits de longitud.
- Funciones Hash SHA-256 o superior.

Se deberá **hacer referencia a la documentación** donde se describa cómo hacer la solicitud de certificado (CSR), importar el certificado de servidor, importar los certificados de CAs y otros parámetros necesarios.

4.3.3 SINCRONIZACIÓN

Incluir referencia a la documentación pública donde se describa cómo debe configurarse la sincronización segura del producto y sus componentes. Se debe recomendar **la integración con servicio NTP** en caso de que sea posible y cómo activar la autenticación en caso de que sea posible.

4.4 REGISTRO Y AUDITORÍA

4.4.1 REGISTRO DE EVENTOS

Hacer referencia a la documentación pública donde se indique qué eventos se registran y cómo se efectúa el registro. Por ejemplo: fichero de logs de configuración, fichero de logs de sistema, etc.

Indicar el formato de los registros de log, incluyendo un ejemplo de estos.

4.4.2 ALMACENAMIENTO LOCAL

Hacer referencia a la documentación pública donde se describa cómo funciona el almacenamiento local de registros de auditoría en el producto.

En caso de que fuera necesaria alguna configuración para el almacenamiento seguro de registros, describir en este documento.

4.4.3 ALMACENAMIENTO REMOTO

Hacer referencia a la documentación pública donde se indique cómo se configura el envío de registros a un servidor remoto syslog y cómo se configura este. Deberá utilizarse siempre un protocolo seguro para el envío de los registros (Por ejemplo, TLSv1.2 o IPsec).

4.5 DISPONIBILIDAD Y RESPALDO

4.5.1 ALTA DISPONIBILIDAD

Hacer referencia a la documentación pública donde se describa la configuración de alta disponibilidad del producto. Indicar en este documento los parámetros de configuración necesarios para una configuración segura.

4.5.2 COPIAS DE SEGURIDAD

Deben indicarse los componentes, datos y configuraciones sobre las que han de realizarse los backups.

Hacer referencia a la documentación pública donde describa el proceso de configuración y realización de las copias de seguridad de forma segura.

Se debe recomendar la realización de backups periódicos.

4.6 ACTUALIZACIONES Y AUTO-CHEQUEOS

4.6.1 ACTUALIZACIONES

Hacer referencia a la documentación donde se describa el proceso a seguir para realizar actualizaciones de firmware, software, servicios, etc. de forma segura.

*En caso de que sea necesario, se debe **indicar en este documento el uso de protocolos seguros** como SCP o SFTP y hacer referencia a la documentación donde se describa como configurarlos en caso de que sea necesario. La política de actualizaciones de seguridad se*

describe en el apartado 5.3. Cuando el producto vaya a ser aprobado además de cualificado, se tendrá en cuenta lo indicado en el apartado 6.

4.6.2 AUTO-CHEQUEOS

Describir los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas, indicar cuándo los realiza (en el startup o bajo demanda del administrador) y qué ocurre en caso de fallo. Cuando el producto vaya a ser aprobado además de cualificado, se tendrá en cuenta lo indicado en el apartado 6.

4.7 RESUMEN DE LA CONFIGURACIÓN SEGURA

Incluir un cuadro resumen con los parámetros de seguridad configurados y el valor establecido en cada uno, indicando el apartado de este documento en el que se describe su configuración.

Parámetro	Valor configurado	Apartado
[Parámetro de seguridad]	[Valor establecido]	[4.x]

5 FASE DE OPERACIÓN Y MANTENIMIENTO

En este apartado se recogen los aspectos relativos al mantenimiento seguro del producto durante su vida útil.

5.1 SOPORTE DE SEGURIDAD

Indicar el periodo de soporte de seguridad de la versión cualificada y la fecha prevista de fin de soporte. El fabricante está obligado a notificar al CPSTIC la finalización del soporte de seguridad, conforme a lo establecido en la CCN-STIC-106.

5.2 NOTIFICACIÓN DE VULNERABILIDADES

Indicar el canal de notificación de vulnerabilidades del fabricante, los plazos de respuesta comprometidos y el medio por el que se comunican los avisos de seguridad a los usuarios del producto.

5.3 APLICACIÓN DE ACTUALIZACIONES DE SEGURIDAD

Describir la política de actualizaciones de seguridad: periodicidad, verificación de la autenticidad e integridad de los paquetes antes de su instalación y efecto de la actualización sobre la configuración segura descrita en este documento. La configuración del mecanismo de actualización se describe en el apartado 4.6.1.

5.4 FIN DE VIDA DEL PRODUCTO

Describir el procedimiento de borrado seguro de la información, las credenciales y el material criptográfico almacenados en el producto antes de su retirada, devolución o reasignación.

6 PARTICULARIDADES PARA PRODUCTOS APROBADOS

Cuando, además de su inclusión en el CPSTIC como producto cualificado o en el listado de Conformidad y Gobernanza, el producto vaya a ser aprobado para el manejo de información nacional clasificada conforme a la CCN-STIC-102 [REF4], el procedimiento de empleo seguro deberá cubrir además el caso de uso descrito en este apartado, caracterizado por la ausencia de conexión a Internet.

El fabricante podrá hacer constar que la configuración descrita en los apartados anteriores resulta igualmente válida para este caso de uso, o bien aportar un anexo al PES que recoja las modificaciones necesarias. En este último caso, el anexo se remitirá por el mismo canal indicado al comienzo de este documento.

6.1 REGISTRO Y LICENCIAS

Describir el proceso para el registro del hardware, el software y las licencias teniendo en cuenta que el producto no puede conectarse a Internet.

6.2 DESPLIEGUE EXCLUSIVO ON-PREMISE

El producto debe poder desplegarse completamente de forma local, incluido el servidor que implementa la lógica del producto. Describir la arquitectura de despliegue local y los componentes que la integran.

6.3 ACTUALIZACIONES OFFLINE

El producto se debe poder actualizar de forma local, sin necesidad de conexión externa a Internet. Describir paso a paso en este documento cómo el administrador obtiene el paquete de actualización correspondiente y lo despliega de forma local.

Estas actualizaciones engloban tanto las correspondientes al software del producto como aquellas relacionadas con la lógica del mismo; por ejemplo, las actualizaciones de las firmas del antivirus.

6.4 NO ENVÍO DE TRAZAS A LA NUBE

El producto no enviará ningún tipo de traza a la nube ni fuera del entorno del cliente o, al menos, deberá ser configurable para ello. Describir paso a paso en este documento cómo desactivar cualquier envío de este tipo.

6.5 AUTO-CHEQUEOS

Indicar expresamente que el producto no enviará información de diagnóstico en ningún caso.

7 REFERENCIAS

Indicar documentación que se haya referenciado a lo largo de la guía.

REF1	CPSTIC https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic
REF2	CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.
REF3	Guía CCN-STIC-106 y sus anexos.
REF4	CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información nacional clasificada.

8 ABREVIATURAS

ENS	Esquema Nacional de Seguridad.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CA	Autoridad de certificación (Certification Authority).
CLI	Interfaz de línea de comandos (Command Line Interface).
CPD	Centro de Proceso de Datos.
CSR	Solicitud de firma de certificado (Certificate Signing Request).
GUI	Interfaz gráfica de usuario (Graphical User Interface).
LDAP	Protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol).
NTP	Protocolo de tiempo de red (Network Time Protocol).
PES	Procedimiento de Empleo Seguro.
RADIUS	Remote Authentication Dial-In User Service.
SAML	Security Assertion Markup Language.
SSH	Secure Shell.
TLS	Seguridad de la capa de transporte (Transport Layer Security).

