

Guía de Seguridad de las TIC CCN-STIC 1483

Procedimiento de Empleo Seguro Invishield



Julio 2026

Edita:



Centro Criptológico Nacional, 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	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	4
4 FASE PREVIA A LA INSTALACIÓN	5
4.1 ENTREGA SEGURA DEL PRODUCTO	5
4.2 ENTORNO DE INSTALACIÓN SEGURO	5
4.3 REGISTRO Y LICENCIAS	5
4.4 CONSIDERACIONES PREVIAS	5
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	6
5 FASE DE INSTALACIÓN	7
6 FASE DE CONFIGURACIÓN	8
6.1 MODO DE OPERACIÓN SEGURO	8
6.2 AUTENTICACIÓN	8
6.3 ADMINISTRACIÓN DEL PRODUCTO	8
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	8
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	9
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	9
6.5 GESTIÓN DE CERTIFICADOS	9
6.6 SERVIDORES DE AUTENTICACIÓN	10
6.7 SINCRONIZACIÓN	10
6.8 ACTUALIZACIONES	10
6.9 AUTO-CHEQUEOS	10
6.10 ALTA DISPONIBILIDAD	10
6.11 AUDITORÍA	10
6.11.1 REGISTRO DE EVENTOS	10
6.11.2 ALMACENAMIENTO LOCAL	10
6.12 BACKUP	10
6.13 RESTAURACIÓN DE FÁBRICA	11
7 REFERENCIAS	12
8 ABREVIATURAS	13

1 INTRODUCCIÓN

1. **InvisiShield** es un sistema HARDWARE/SOFTWARE que automatiza la interconexión de todos los sistemas y dispositivos conectados a él. Permite programar, basado en el tiempo, la conexión y desconexión de cada puerto de salida con sus puertos de entrada de manera independiente según las necesidades de cada usuario.
2. La programación de las interfaces se realiza mediante la creación de reglas a través de una aplicación Android (APK), diseñada para que la programación de cada puerto sea sencilla e intuitiva. Esta aplicación permite crear programas en modo offline y visualizar la planificación en tablas semanales antes de enviarlos.
3. El dispositivo **Hardware** es un *switch* de tres puertos USB y tres Gigabit Ethernet (RJ45) configurables a través de la aplicación Android. La conexión que ofrece el dispositivo hardware de InvisiShield es vía Bluetooth (BLE v4.2).
4. Una entrada USB y otra entrada Gigabit Ethernet cuentan, respectivamente, con dos salidas del mismo tipo que se pueden activar de manera independiente según lo que el usuario decida. Solamente una de las salidas de USB puede estar activa, no las dos a la vez.
5. Las principales funcionalidades que ofrece el producto son las siguientes:
 - a) Gestión de *programas*: Los *programas* son una serie de reglas que aplica el **Hardware** para activar o desactivar los puertos según un horario establecido. Estas políticas se almacenan en su memoria interna y se transmiten desde el **Software** vía Bluetooth. A su vez, el **Hardware** permite la extracción de sus reglas almacenadas para volcarse en el **Software**.
 - b) Gestión de *políticas*: A través del **Software** se puede realizar la configuración de las políticas, que se aplican sobre una única salida. En caso de que alguna regla se solape con la normativa de activación previamente mencionada para las salidas USB, no se permitirá la configuración.
 - c) Configuración **Hardware**: El dispositivo físico permite recibir la configuración mediante comandos enviados en una única comunicación Bluetooth. Las acciones configurables son:
 - i. Sincronización fecha y hora.
 - ii. Gestión de *programas*.
 - iii. Gestión de las salidas.
 - iv. Actualizaciones firmware.
6. A través de estas funcionalidades, logra aislarse e invisibilizar en la red los medios de almacenamiento que no están siendo utilizados.

2 OBJETO Y ALCANCE

7. Este documento de Procedimiento de Empleo Seguro (PES) del producto **INVISHIELD** está orientado para los siguientes componentes:
 - **INVISHIELD Hardware:** v01.00.007 (HW 3.0)
 - **INVISHIELD Software:** v1.0.17
8. El producto **INVISHIELD** ha sido incluido en el CPSTIC. Para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [REF2].
9. El alcance de este documento cubre las recomendaciones de seguridad necesarias para el despliegue y configuración segura del producto en entornos empresariales y organismos públicos.

3 ORGANIZACIÓN DEL DOCUMENTO

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. En primer lugar, la organización que desee adquirir el producto deberá ponerse en contacto con el equipo comercial de **INVISHIELD** a través de la web referenciada en REF1.
11. El componente **Hardware** se recibe por transporte domiciliario en la localización seleccionada por la organización que lo adquiera. Se debe comprobar que la caja recibida no ha sido abierta o manipulada. El contenido de esta ha de ser el siguiente:
 - Fuente de alimentación de 5V-DC 10W.
 - Dispositivo físico de INVISHIELD (**Hardware**).
12. El componente **Software** del producto se puede instalar de dos formas:
 - A través de la tienda de aplicaciones *Play Store* de Google.
 - A través de una instalación manual con el APK.
13. Para la configuración cualificada, se hará uso de la **instalación manual a través del APK**. Este archivo es proporcionado por el fabricante, **AMLO Sistemas de Seguridad S.L.**, a la organización que adquiere el producto. La verificación de la integridad de este APK viene definida en la sección 4.4 CONSIDERACIONES PREVIAS.

4.2 ENTORNO DE INSTALACIÓN SEGURO

14. El componente **Hardware** ha de instalarse en un entorno donde esté físicamente protegido y no esté sujeto a ataques físicos que puedan interferir en su seguridad u operación.
15. Respecto a las comunicaciones Bluetooth con este componente, solamente usuarios autorizados podrán interactuar vía **BLE v4.2**, por lo que se recomienda que el dispositivo móvil que tiene la aplicación de Invisshield instalada sea un dispositivo confiable.
16. El componente **Software** del producto ha de instalarse en un dispositivo móvil que cuenta con Android 8.0 o superior. La configuración cualificada consideró el uso de dispositivos Android con versiones **Android 9 y Android 14**.

4.3 REGISTRO Y LICENCIAS

17. El producto **INVISHIELD** no requiere de registro ni licencia más allá de la contratación del servicio y recepción del componente **Hardware** (dispositivo Invisshield) y **Software** (aplicación móvil de Invisshield).

4.4 CONSIDERACIONES PREVIAS

18. Para poder realizar la configuración segura de la solución Invisshield, es preciso tener los dos componentes: hardware y software.
19. Los manuales del fabricante, disponibles a través de la propia aplicación Android, contienen las consideraciones previas a la puesta en marcha de Invisshield:
 - a) En primer lugar, **la instalación de la aplicación se realiza a través del APK** recibida del fabricante. Es preciso verificar el hash SHA-256 para verificar la integridad de este

software, según viene indicado en la sección “*Instalación de aplicación vía APK*” de [GUIA-USUARIO].

- b) Para la configuración relativa a la seguridad, previa a la instalación y configuración del **Hardware**, se requiere tener los servicios de ubicación activados en el dispositivo móvil donde se instala el **Software** para poder buscar dispositivos Bluetooth, para la puesta en marcha del dispositivo **Hardware**.
 - c) A su misma vez, se ha de encender el Bluetooth (modo BLE) del componente **Hardware**, tal y como indica la sección “*Encender Bluetooth dispositivo*” de [GUIA-USUARIO].
20. Cabe destacar que para la operación normal del hardware de InvisiShield, no es necesario que tenga el Bluetooth activo, por lo que **se recomienda solo activarlo cuando se precise hacer alguna gestión en el componente Hardware** a través de la aplicación móvil. En caso contrario, la interfaz BLE del hardware deberá estar apagada.
21. El **componente Hardware** estará guardado en la lista de dispositivos conocidos en la aplicación móvil, de forma que la funcionalidad de búsqueda de dispositivos no será necesaria para futuras conexiones.
22. No se precisa de algún otro aspecto adicional, aparte de las consideraciones necesarias para el entorno operacional o la propia configuración del producto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. El entorno de operación ha de estar compuesto por:
- Un dispositivo móvil, con las características mencionadas en la sección 4.2 ENTORNO DE INSTALACIÓN SEGURO, donde se instalará y ejecutará el **Software**.
 - De uno (1) a cuatro (4) dispositivos de almacenamiento o *backup* que deben conectarse al **Hardware** por sus salidas USB y/o Gigabit Ethernet.
 - De uno (1) a dos (2) dispositivos y/o servidores de entrada que deben conectarse al **Hardware** por sus entradas USB y/o Gigabit Ethernet.

5 FASE DE INSTALACIÓN

24. Los pasos para instalar el componente **Software** están descritos en la sección “*Instalación de aplicación vía APK*” de [GUIA-USUARIO].
25. El *firmware* del componente **Hardware** no precisa de ninguna configuración pues el fabricante de **INVISHIELD** se encarga de la misma antes de entregarlo a la organización que adquiera el producto.
26. Comprobar que el firmware está en su versión más reciente y en caso contrario actualizarlo. Para realizar esta operación consultar la sección 6.8 ACTUALIZACIONES.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

27. Para garantizar que el producto **INVISHIELD** opere de forma segura y conforme a los estándares evaluados de seguridad, es necesario activar configuraciones específicas que aseguren su funcionamiento acorde a dicha evaluación. En este documento se recogen los pasos necesarios para configurar el producto de acuerdo con las guías del CCN.
28. Para la puesta en marcha del producto, el usuario administrador debe de seguir las indicaciones recogidas en la sección “*Puesta en marcha de Invishield*” de [GUIA-USUARIO].

6.2 AUTENTICACIÓN

29. La autenticación se realiza de forma local en el componente **Software**. Los mecanismos de autenticación existentes son:
 - Autenticación del componente **Hardware** y componente **Software**. Esta autenticación se hace, de acuerdo con la sección “*Puesta en marcha de Invishield*” de [GUIA-USUARIO], a través de la vinculación por Bluetooth introduciendo la “*Pairing Password*”. Esta contraseña se ubica en la etiqueta de la parte inferior del componente **Hardware**.
 - Autenticación del usuario administrador y el **Hardware**. Esta autenticación requiere únicamente de introducir el PIN para poder gestionar dicho componente, introducido a través del componente **Software**.
30. Se recomienda modificar el PIN de acceso que viene por defecto, de acuerdo con la sección “*Cambiar código PIN*” de [GUIA-USUARIO]. Este PIN deberá estar compuesto por 6 dígitos numéricos.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. La administración local, a través de los botones físicos del Hardware de Invishield, permite:
 - Habilitar o deshabilitar la interfaz Bluetooth mediante el botón RST.
 - Reiniciar las configuraciones del Hardware presionando el botón RST.
32. Para más información sobre el reinicio del dispositivo Hardware, ver la sección 6.13 RESTAURACIÓN DE FÁBRICA.
33. La administración remota, a través del **Software** de Invishield, permite:
 - Gestión de programas.
 - El usuario administrador debe seguir las pautas mostradas en la sección “*Programas*” de [GUIA-USUARIO].
 - Configuración del componente **Hardware**.
 - El usuario administrador, para configurar el dispositivo, debe seguir las indicaciones mostradas en la sección “*Configuración de Invishield*” de [GUIA-USUARIO].

- La configuración que puede realizarse siguiendo las pautas indicadas es la siguiente:
 - Sincronización de fecha y hora.
 - *Programa* actual.
 - Enviar *programa*.
 - Recuperar *programa*.
 - Si existe un programa creado en el **Software** con el mismo nombre que el extraído del **Hardware**, el producto da la opción a *Usar el de Invisshield (Hardware)*, sobrescribiendo el programa en el **Software**, *Usar el del teléfono (Software)*, sobrescribiendo el programa en el **Hardware**, o *Guardar como ...*, que almacena el programa en el **Software** con un nombre diferente para poder ser visualizado o editado.
 - Cambiar nombre al **Hardware**. Este nombre es el que se muestra cuando se busca el dispositivo a través de BLE.
 - Leer versión de *firmware* y actualizar *firmware*.
 - Modificar PIN de acceso al **Hardware**.
 - Leer registros de actividad o *log*.
 - Modo apagado BLE. El producto permite dos configuraciones para el apagado BLE:
 - *Modo temporizado*. Mantiene el BLE encendido tras la desconexión por 5 minutos, lo que permite la conectividad entre **Software** y **Hardware** sin necesidad de acceder físicamente al dispositivo en cada conexión durante el periodo indicado.
 - *Modo instantáneo*. Esto hace que se requiera pulsar el botón de RST cada vez que se desee acceder de nuevo al componente **Hardware** a través del **Software**. Este es el modo que debe de estar activo para la configuración cualificada.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. No se precisa de configuración de usuarios administradores para el empleo seguro del producto **INVISHIELD**. Esta solución no cuenta con usuarios propios, solamente la persona que sea autorizada a utilizar el móvil que tiene la aplicación de Invisshield instalada, y conozca el PIN de acceso, podrá gestionar la funcionalidad el **Hardware**.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

35. Para poder configurar las interfaces de salidas del componente **Hardware**, el usuario administrador debe seguir los pasos definidos en la sección “*Forzar estado de salida*” de [GUIA-USUARIO].
36. Para la configuración cualificada, y para la aplicación de *programas* correctamente, el estado de todas las salidas debe ser “Auto”.

6.5 GESTIÓN DE CERTIFICADOS

37. No se precisa de configuración o gestión de certificados para el Procedimiento de Empleo Seguro (PES) de **INVISHIELD**.

6.6 SERVIDORES DE AUTENTICACIÓN

38. No se precisa de configuración o gestión de servidores de autenticación para el Procedimiento de Empleo Seguro (PES) de **INVISHIELD**.

6.7 SINCRONIZACIÓN

39. Para la sincronización de fecha y hora del componente **Hardware**, a través del componente **Software**, el usuario administrador debe seguir los pasos especificados en la subsección “*Sincronización de Fecha y Hora*” de la sección “*Configuración de Invisield*” de [GUIA-USUARIO].

6.8 ACTUALIZACIONES

40. Para la actualización del firmware del componente **Hardware**, a través del componente **Software**, el usuario administrador debe seguir los pasos especificados en la subsección “*Actualización de firmware*” de la sección “*Configuración de Invisield*” de [GUIA-USUARIO].
41. Para la actualización del componente **Software**, el usuario administrador debe de instalar la nueva APK tal y como se define en la sección 5 FASE DE INSTALACIÓN.
42. Conforme se liberan nuevas actualizaciones, el fabricante notifica por correo electrónico las nuevas versiones del **Software**.

6.9 AUTO-CHEQUEOS

43. El producto **INVISHIELD** no requiere de la realización de auto chequeos al arrancar.

6.10 ALTA DISPONIBILIDAD

44. No se precisa de configuración o gestión de alta disponibilidad para el Procedimiento de Empleo Seguro (PES) de **INVISHIELD**.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

45. Para la lectura de registros de actividad a través del componente **Software**, el usuario administrador debe seguir los pasos especificados en la subsección “*Lectura de registros de actividad*” de la sección “*Configuración de Invisield*” de [GUIA-USUARIO]

6.11.2 ALMACENAMIENTO LOCAL

46. El almacenamiento de registros de auditoría se realiza de forma local en el componente **Hardware**.

6.12 BACKUP

47. No se precisa de configuración de *backups* en el producto **INVISHIELD**.

6.13 RESTAURACIÓN DE FÁBRICA.

48. Para restaurar de fábrica el componente **Hardware** el usuario administrador debe seguir los pasos descritos en la sección “*Restauración de fábrica*” de [GUIA]. Las consecuencias que lleva consigo esta restauración se encuentran descritas en dicha sección.
49. Esta restauración también puede hacerse desde el componente **Software**, siguiendo estos pasos:
 - a) Pulsar y mantener el botón RST hasta que las luces LED del dispositivo **Hardware** parpadeen en verde (aproximadamente, diez (10) segundos).
 - b) Esperar a que acabe el parpadeo. El LED indicador de Bluetooth también debe apagarse.
 - c) Pulsar sobre el botón RST para encender el Bluetooth.
 - d) Buscar el dispositivo y emparejarlo desde el componente **Software**, siguiendo la misma metodología para el emparejamiento indicada en la sección 6.2 *AUTENTICACIÓN*.
 - e) Si se ha realizado todo correctamente, aparece el mensaje en rojo “*PIN Incorrecto*”.
 - f) Pulsar tres (3) veces, una por segundo, la esquina inferior izquierda del cuadro blanco de diálogo de introducción de PIN.
 - g) Pulsar el botón “*Reparar Dispositivo*”, usando el mismo PIN.
 - h) Verificar que el dispositivo se ha añadido correctamente. Pulsar sobre el dispositivo (el símbolo de Bluetooth debería aparecer a la derecha).
 - i) Introducir el PIN para finalizar el emparejamiento.
 - j) En caso de error, repetir los pasos f, g y h.
 - k) En caso de finalizar el emparejamiento, se debe sincronizar fecha y hora del dispositivo, tal y como se indica en la sección 6.7 *SINCRONIZACIÓN*.

7 REFERENCIAS

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

[GUIA-
USUARIO] Invisiield, Manual de usuario. Revisión 1.0.10, 05 de febrero de 2025.

REF1 [Consigue Invisiield - Invisiield](#)

REF2 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación del CCN.
<https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic>

8 ABREVIATURAS

APK	Android Package Kit
BLE	Bluetooth Low Energy
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios TIC
DC	Direct Current
ENS	Esquema Nacional de Seguridad
HW	Hardware
LED	Light-Emitting Diode
PES	Procedimiento de Empleo Seguro
PIN	Personal Identification Number
RST	Reset
SHA	Secure Hash Algorithm
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TIC	Tecnologías de la Información y la Comunicación
USB	Universal Serial Bus

