centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1201

Procedimiento de empleo seguro AuthUsb SafeDoor

Octubre de 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
2019.10.11 12:49:08 +02'00'

NIPO: 083-19-004-5

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

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

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, modificado 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 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. El dispositivo safeDoor es una herramienta de análisis, protección y detección de ataques por medio de dispositivos de almacenamiento USB, actuando como barrera entre éstas y los equipos de una organización, identificando amenazas a tres niveles:

   - **Eléctrico**: Monitoriza continuamente el comportamiento de la memoria USB a nivel eléctrico, identificando y deteniendo ataques destructivos de sobretensión tipo usbKiller
   - **Hardware**: Monitoriza continuamente el comportamiento de la memoria USB a nivel hardware, detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc.
   - **Software:** Dispone de antivirus integrado (compatible con varios fabricantes) con el que realiza un análisis previo a la descarga de cualquier contenido.

2. Safedoor ofrece dos conectores hembra USB tipo A para la introducción de memorias USB a analizar y un puerto ethernet para su conexión a la red o punto a punto directamente a un ordenador. A través de esta conexión de red ofrece una interfaz web para la interacción con el usuario.

2 OBJETO Y ALCANCE

3. Este documento constituye el procedimiento de empleo seguro para la instalación y operación del producto **authUsb safedoor**, dispositivo hardware para la protección contra amenazas derivadas del uso de memorias USB.

Modelo	safeDoor
Versión software	2.0.0.8
Certificación	LINCE
Contacto soporte	soporte@authusb.com

3 ORGANIZACIÓN DEL DOCUMENTO

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

   a) Apartado 4. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.

   b) Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

c) Apartado 6. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente:

   a) Albarán de envío. En el proceso de recepción del dispositivo SafeDoor en destino, junto con el paquete que se envía se incluirá un albarán referenciando el número de serie y la MAC de cada uno de los dispositivos SafeDoor que se van a entregar. Los dispositivos se incluirán en un doble embalaje.

   b) Embalaje externo. Es un embalaje de cartón de color blanco irá precintado por el auto cierre que dispone el propio embalaje y llevará en la posición de su apertura una pegatina con el sello de authUSB. Es necesario comprobar que no ha existido manipulación ni en el auto cierre ni en el sello.

   c) Embalaje interno. Una vez procedido a la apertura del embalaje externo, procedemos a la apertura del *packaging* del dispositivo. Es de cartón con la serigrafía propia de authUSB. Estará precintada en su cierre por una pegatina. Comprobar que esta no ha sido manipulada existencia de maltrato o manipulación evidente. En el interior del *packaging* encontramos en primer lugar el dispositivo SafeDoor dentro de una bolsa de plástico precintada con una pegatina. (Realizar la comprobación que esta no ha sido manipulada). En el compartimento inferior encontraremos un cable ethernet, adaptador AC/DC y la garantía del producto.

   d) Una vez procedido al desempaquetado comprobar el número de serie y MAC (en la etiqueta de seguridad situada en la parte inferior del dispositivo si coincide con las referenciadas en el albarán. Se realizará una doble comprobación a través del certificado de licencia que se puede descargar de la página web www.authusb.net, una vez registrado el usuario.

6. En caso de identificarse algún problema durante la inspección, el usuario deberá ponerse en contacto inmediatamente con el proveedor, al que se le indicará una descripción del problema.

4.2 ENTORNO DE INSTALACIÓN SEGURO

7. Para la utilización en condiciones óptimas de seguridad del producto, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:

   - **Administración confiable**: El Administrador será un miembro de plena confianza y estará capacitado y formado en el uso del sistema respetando

las buenas prácticas y protocolos relativos a la configuración de red, seguridad criptológica, gestión de usuarios y contraseñas.

- **Entorno controlado**. El producto se usará en un entono controlado y observable.
- **Acceso a actualizaciones**: El dispositivo será actualizado por el administrador cuando esté disponible una nueva actualización de seguridad del firmware. De la misma manera el dispositivo deberá tener acceso al servicio de actualización de firmas del antivirus ya sea de forma automática (online) o manual (offline)
- **Equipo cliente:** El equipo cliente está libre de malware y actualizado con las últimas actualizaciones de seguridad de su sistema operativo, disponiendo de uno de los siguientes navegadores web con javascript habilitado:
    - Google Chrome v70.0.x o superior
    - Firefox 64.0 o superior
    - Opera 57.0 o superior
    - Internet Explorer 11 o superior
    - Safari 10.0 o superior

4.3 REGISTRO Y LICENCIAS

8. Una vez cumplido con la recepción segura del dispositivo e integrado en un entorno operacional que cumpla con los requisitos del apartado anterior. Para el caso de que la licencia de Anti Virus (AV) no venga precargada, authUSB le proporcionará el nombre de usuario, contraseña y archivo de licencia del motor de antivirus que introducirá en la ventana de configuración del apartado AV, en caso necesario.

4.4 INSTALACIÓN

9. Con el dispositivo safeDoor se incluye un adaptador de alimentación de 5V/2A y un cable ethernet. El dispositivo dispone de una carcasa de aluminio cerrado sin refrigeración activa, un conector para alimentación, un pulsador de encendido / apagado, un puerto ethernet para su conexión a la red o punto a punto, dos puertos USB tipo A y tres LEDs de estado.
10. Conecte el adaptador a la red eléctrica (220V) y al dispositivo. El led central de color azul se iluminará indicando que el equipo está encendido, y tras unos 40 segundos los leds de ambos puertos USB mostrarán una secuencia Rojo/Naranja/verde tras la cual el dispositivo estará activo para su uso.
11. La interacción del usuario con el dispositivo se llevará a cabo a través de un navegador, accediendo a la aplicación web embebida en el safeDoor. Para ello se debe proporcionar una conexión IP a través del cable ethernet, soportándose dos escenarios:

    - **Uso compartido en red**. Conecte un extremo del cable ethernet al dispositivo y el otro a un switch de la red a la que deba dar servicio.

- **Punto a punto**. Indicado para usuarios en movilidad o servicio a equipos aislados. Conecte el cable ethernet[1] directamente del dispositivo a la tarjeta de red del equipo destino.

5 FASE DE CONFIGURACIÓN

5.1 CONFIGURACIÓN DE RED

12. Por defecto safeDoor está configurado como cliente DHCP. En la etiqueta situada en la parte inferior del dispositivo está disponible la dirección MAC de la tarjeta de red, lo que permitirá al administrador de la red identificar la dirección IP asignada al dispositivo, reservar una IP estática o asignarle un nombre dentro de la red para facilitar el acceso a los usuarios.
13. Adicionalmente el dispositivo siempre estará accesible en la dirección 20.0.0.1/24 lo que permite recuperar el acceso al mismo en caso de introducir una configuración de red errónea, y simplifica la configuración en el caso de conexión punto a punto.
14. La configuración de red se lleva a cabo a través de la interfaz web del dispositivo, por lo que el primer paso es obtener acceso a ésta identificando la dirección IP del safeDoor.

5.2 ACCESO A LA INTERFAZ WEB

15. La URL de acceso es dependiente del tipo de conexión seleccionado en el punto anterior:

- **Uso compartido en red.**

  Consulte con el administrador de la red la dirección IP asignada a la MAC especificada en la etiqueta de identificación del dispositivo. Una vez obtenida abra en un navegador web la dirección https://<DirecciónIP>

  Si esta información no está disponible, es posible acceder a través de la IP privada de recuperación siguiendo los pasos descritos en el siguiente punto aun cuando la conexión física se realice a través de un switch de red y no con cable directo.

- **Conexión directa punto a punto.**

  En un equipo conectado directamente a safeDoor o con ambos conectados al mismo switch de red, configure el adaptador de red para acceso a la subred 20.0.0.0/24.

[1] *La mayoría de los adaptadores de red modernos soportan conexiones directas con un cable de red estándar. Si el equipo es antiguo, se necesitará un cable de red cruzado.*

- **Opción 1**: Modifique la configuración IP4 estableciendo IP estática 20.0.0.5, máscara 255.255.255.0, puerta de enlace y DNS vacíos.

- **Opción 2**: En opciones avanzadas, añada una IP adicional, 20.0.0.5 con máscara 255.255.255.0. Esta opción es dependiente del sistema operativo del equipo cliente, y permite el acceso a la red privada del safeDoor sin perder la conectividad de red existente en el equipo.

Abra el navegador web con la URL https:/20.0.0.1/

16. Cada dispositivo safeDoor genera en su primer arranque un certificado digital temporal antes de su configuración definitiva para el cifrado del tráfico HTTPS derivado de su interfaz web.
17. Por este motivo el primer acceso del navegador a la interfaz web mostrará una alerta de seguridad ya que el certificado web no está firmado por una autoridad reconocida por el equipo cliente. Acepte la excepción de seguridad y accederá a la pantalla de inicio de sesión. Inicie sesión con las credenciales por defecto (admin/admin)
18. Es **obligatorio el cambio de la contraseña por defecto** del usuario admin con la que se entrega el dispositivo safeDoor. En el menú superior acceda a configuración / usuarios y modifíquela.
19. La contraseña debe ser de acuerdo a la Política segura de contraseñas que disponga la organización. Se recomienda que cumpla con los siguientes requisitos mínimos:
    - Longitud de la contraseña: mínimo 8 caracteres.
    - Complejidad:
    - Uno o más caracteres en minúscula.
    - Uno o más caracteres en mayúscula.
    - Uno o más números.
    - Uno o más caracteres especiales.
    - Cuando se cambia la contraseña, esta tendrá que diferir de la anterior en, al menos, 4 caracteres.

5.3 SELECCIÓN DE MODO DE RED

20. Acceda a la pantalla configuración / red. Aquí podrá definir el modo y configuración de red deseada.
    - **Servidor DHCP**. Esta opción está indicada únicamente para el modo de conexión punto a punto. El dispositivo actuará como un servidor DHCP que asignará direcciones en el rango 20.0.0.0/24 al equipo cliente conectado directamente al puerto ethernet, simplificando de esta manera el uso por parte de un usuario no técnico.

- **IP Estática**. Permite asignar IP / máscara y en caso de salida directa a internet, puerta de enlace y servidores DNS. En caso de redes administradas consulte con el administrador de la red antes de establecer esta opción.
- **Cliente DHCP.** Es la opción por defecto, activa siempre que las opciones Servidor DHCP e IP Estática estén desactivadas. El dispositivo adquirirá su configuración IP automáticamente desde el servidor DHCP de la red destino. El administrador de la red podrá, utilizando la dirección MAC disponible en la etiqueta de identificación del safeDoor, aplicarle configuraciones específicas como reserva de IP o asignación de nombre en la red local.
- **Proxy HTTP.** Si la red dispone de proxy HTTP/s para proporcionar acceso a internet o a la consola central de supervisión, en esta sección el usuario proporcionará dirección, puerto y en su caso usuario y contraseña. También deberá especificar en qué cados debe ser utilizado el proxy como pasarela (acceso a firmas de antivirus y/o acceso a consola central). Se proporciona un botón de test para verificar el acceso a estos servicios en función de la configuración proporcionada.

5.4 CONFIGURACIÓN DEL CERTIFICADO HTTPS

En pantalla configuración / estado es obligatorio cambiar el certificado digital de la aplicación web de forma que se adecue a las necesidades de la organización y a la configuración de red, existiendo dos posibilidades:

- **Importación**. Si la organización dispone de PKI o certificados generados específicamente para el dispositivo, en la opción certificado / importar el usuario podrá cargarlo en el dispositivo. El certificado deberá utilizar una longitud de clave de al menos 4096 bits (en caso contrario safeDoor la rechazará) y su duración no deberá superar los 2 años.

  Nota: No se debe utilizar no utilizar un mismo certificado en distintos safeDoor. En el caso de que un dispositivo sea comprometido físicamente podría comprometer la seguridad de aquellos que compartan certificado.

- **Generación automática**. Una vez conocido en nombre o IP final que tendrá el dispositivo en la red, desde la opción certificado / generar el usuario podrá utilizar esta información para generar y activar una CA y certificado digital único, con una duración de 1 año y una longitud de clave de 4096 bits. Este certificado es generado en memoria a partir de una autoridad de certificación (CA) temporal creada con este único fin y cuya clave privada es destruida tras la firma, garantizando de esta manera que ningún otro certificado pueda ser generado y firmado por esta CA.

21. En ambos casos es importante que el *common name* o *alternate name* del certificado coincida con el nombre o IP asignado al dispositivo en la red, de forma que la URL final que utilicen los usuarios para acceder al dispositivo coincida con la configuración del certificado.
22. Una vez definido el certificado final que usará el dispositivo, desde la opción configuración / estado el usuario podrá descargar la CA pública para su instalación en los equipos o navegadores cliente, eliminando de esta manera las excepciones de seguridad y estableciendo un canal confiable hacia la interfaz web.

5.5 GESTIÓN DE USUARIOS

23. El usuario admin dispone de control total sobre todos los parámetros de configuración del dispositivo y solo debe ser utilizado para labores administrativas (puesta en marcha, gestión de usuarios, cambios de configuración de red).
24. Para la operativa diaria es necesario utilizar una cuenta de usuario estándar sin privilegios. Desde la pantalla configuración / usuarios el administrador podrá crear y gestionar las cuentas de usuario necesarias.
25. Todos los nuevos usuarios creados tienen un único perfil de acceso, limitado a la operativa habitual del dispositivo. La cuenta admin es la única con privilegios de administrador.
26. Para cada nuevo usuario el administrador definirá el nombre de usuario, contraseña, y le otorgará o no permisos de escritura (por defecto sólo se concede permisos de lectura). Las contraseñas de los usuarios deberán tener una longitud mínima de 6 caracteres. No se fuerza la inclusión de caracteres especiales, pero se deben utilizar contraseñas fuertes y ser renovadas periódicamente. En caso de olvido, sólo el administrador podrá restablecer la cuenta del usuario.
27. Existe la opción de desactivar el control de acceso al dispositivo (no se solicitará usuario y contraseña para acceder a la interfaz web). Esta opción solamente puede ser utilizada en conexiones punto a punto para usuarios en movilidad donde no exista conectividad por red con más equipos y se garantice la seguridad en el acceso al equipo cliente.
28. Una vez creados los usuarios necesarios, es preciso concederles acceso a los puertos USB del dispositivo desde la pantalla configuración / gestión de puertos. En una configuración de uso compartido, permite distribuir los dos puertos USB del safeDoor entre los distintos usuarios permitiendo una mayor granularidad en control de acceso a las memorias USB conectadas al dispositivo.

5.6 ANTIVIRUS

29. El dispositivo SafeDoor dispone como mínimo de un motor de antivirus para realizar análisis a nivel software. Todo fichero antes de proceder a su descarga será analizado por lo menos por uno de los motores de antivirus embebidos en la solución.

30. El proceso de análisis del dispositivo de almacenamiento USB puede realizarse con dos metodologías.
31. Una de manera automatizada. Desde el primer momento que se inserta una memoria USB en el dispositivo SafeDoor se procederá a analizar los tres niveles de ataques, nivel eléctrico, nivel hardware y nivel software.
32. Otra opción es la que permite el análisis software en una fase posterior. Una vez SafeDoor haya analizado con éxito que no existe ninguna amenaza, ni hardware ni eléctrica, (estos dos análisis se siguen monitorizando hasta su extracción), procederemos a navegar en el contenido del dispositivo pudiendo seleccionar la totalidad de los ficheros o los que le interese al usuario descargar con el fin de realizar por parte de los motores de antivirus activados en el SafeDoor un análisis a nivel Software de las posibles amenazas contenidas en él.
33. Una vez se haya procedido al análisis de los tres nivel de ataque y si todo es correcto podremos proceder a la descarga de los ficheros contenidos en el dispositivo de almacenamiento USB.

5.7 SINCRONIZACIÓN HORARIA

34. El dispositivo automáticamente actualizará su fecha contra un servidor NTP. En el caso en que el servidor NTP no esté disponible o no exista conectividad el usuario podrá establecer la fecha del dispositivo desde la página de configuración. En cuyo caso el dispositivo tomará la fecha del equipo cliente.

5.8 ACTUALIZACIONES

35. Para realizar las actualizaciones de firmware y software de manera segura debemos realizarlas siempre desde fuentes confiables, en este caso siempre desde el fabricante. Podrá realizarse la descarga por dos vías, o bien desde la plataforma que existe a disposición de los clientes una vez hayan solicitado su registro se les facilitarán unas claves o bien a través del correo electrónico que el cliente indique.
36. El proceso de actualización de firma de firmware como de software se realizará por los mismos procedimientos que se utilizan para la actualización de firmas de AV.(relación detallada de los procesos en el punto 5.8.1) o en la versión 1.4 del manual de usuario del authUSB SafeDoor.

5.8.1 ACTUALIZACIÓN DE FIRMAS AV

37. Para un uso seguro del dispositivo es necesario la actualización periódica de las firmas de los motores de antivirus.
38. En función de la topología de la red y su nivel de restricción este proceso podrá ser llevado a cabo de forma automática o manual. En la pantalla configuración / estado el administrador podrá seleccionar el método de actualización más adecuado (botón “Origen de firmas”. Las opciones disponibles son:

- **Directa**: Si la red a la que está conectada el dispositivo dispone de salida a internet, ya sea a través de puerta de enlace o proxy HTTP/s, safeDoor comprobará automáticamente cada hora la versión disponible de firmas y las actualizará en su caso directamente desde los servidores del fabricante Antivirus.
- **Consola**: Cada safeDoor puede ser vinculado a una consola central a la que reportará informes de auditoría sobre cada operación realizada. Este servidor tiene además la capacidad de actuar como mirror de los servidores de firmas, por lo que será utilizado por el dispositivo como origen de actualización de forma automática cada hora.

  Nota: Si la consola central dispone de salida a internet sincronizará automáticamente el repositorio de firmas del mirror. En el caso de redes restringidas o cerradas, este proceso podrá ser realizado de forma offline utilizando una utilidad proporcionada por authUSB.

- **Offline**: Indicado para equipos aislados o en redes cerradas. Se trata de un proceso manual apoyado en una memoria USB y una utilidad portable para Windows, que implica los siguientes pasos:

  a) Ejecución de la utilidad en un equipo con salida a internet, con la memoria USB conectada. La utilidad creará o actualizará (se soportan actualizaciones incrementales) un repositorio local en la memoria USB con la última versión de las firmas de antivirus.

  b) Una vez finalizado el proceso, se conecta la memoria USB directamente a cada uno de los safeDoor a actualizar. En la página configuración / estado pulse el botón “Actualizar AVs”. Tras unos segundos se mostrará la nueva versión de firmas instalada

  El repositorio generado en la memoria USB puede ser utilizado también para actualizar las firmas disponibles en el mirror de la consola central, automatizando de esta manera la actualización de los safeDoor vinculados aun cuando éstos pertenezcan a una red cerrada. Para ello conecte la memoria -previo análisis en un safeDoor- a un equipo de la misma red donde esté alojada la consola central y ejecute de nuevo la utilidad proporcionando su URL de acceso.

- **Custom:** Indicado en el caso de no existir consola central o se desee trasladar únicamente la funcionalidad de mirror a un servidor independiente. Se deberá propocionar la URL de acceso a este servidor.

6 FASE DE OPERACIÓN

39. Existen dos casos de uso diferenciados en función de las necesidades operativas y de los recursos disponibles. Desde el momento en que se introduce una memoria USB al dispositivo hasta que ésta es extraída físicamente se realiza automáticamente y de forma continua la monitorización y análisis a nivel eléctrico y hardware. La diferencia entre ambos radica en el análisis a nivel software del contenido (antivirus):

6.1 USO INTERACTIVO

40. Opción por defecto, es necesaria la intervención de un operador accediendo a la interfaz web del safeDoor desde el navegador web de un equipo cliente conectado punto a punto o a la misma red que el dispositivo.
41. Cuando el usuario conecte una memoria USB a uno de los puertos se llevará a cabo automáticamente el análisis eléctrico y hardware, proceso durante el cual el LED del puerto permanecerá encendido en color naranja.
    - En el caso de detección de amenaza el LED pasará a Rojo y se mostrará una alerta en la interfaz web con la descripción del problema detectado, denegándose el acceso al contenido.
    - En el caso contrario el LED pasará a Verde y se mostrará en la interfaz web información acerca del dispositivo de almacenamiento. Pulsando sobre ella se mostrarán las particiones de las que dispone y sus características (en el caso de particiones ocultas éstas se mostrarán en Rojo). El usuario podrá navegar por el contenido de forma similar a un explorador de archivos y seleccionar aquellos ficheros y/o carpetas que desee descargar.
42. Una vez seleccionados se habilitará el botón “Analizar”, paso obligatorio e ineludible previo a la descarga de contenido. Es este paso los motores de antivirus analizarán el contenido seleccionado (LED en naranja, mostrándose en la interfaz web el estado del proceso).
    - En caso de detección de malware el LED pasará a rojo, mostrándose en la interfaz web la descripción de la amenaza reportada por cada motor AV, y se denegará la descarga del contenido.
    - En caso contrario el LED pasará a verde y se iniciará la descarga web. Si se trata de un único fichero éste se descargará respetando su nombre y formato original, en caso contrario se descargará un fichero ZIP conteniendo la estructura de ficheros y carpetas seleccionados.

6.2 USO DESATENDIDO O AUTOMÁTICO

43. En esta opción safeDoor actúa como un equipo autónomo, sin necesidad de conexión de red ni equipo cliente, basando la interacción con el usuario en el estado de las luces LED de cada puerto USB.

Cuando el usuario conecte una memoria USB a uno de los puertos, además del análisis eléctrico y hardware se analizará automáticamente todo el contenido de la memoria con los motores de antivirus embebidos en el dispositivo. Durante este proceso el LED del puerto permanecerá encendido en color naranja, cambiando a su finalización a Rojo (amenaza detectada) o Verde (limpio).

44. Se deberán desarrollar procedimientos operativos para llevarse a cabo durante fase de operación y mantenimiento del producto que contemplen, al menos, las siguiente actividades:

    - Comprobar de manera visual el funcionamiento correcto de los Leds incorporados en el SafeDoor.
    - Comprobar los mensajes recibidos en la aplicación web se corresponden con el tipo de amenaza detectada.
    - Comprobar que su firmware como su Software y AV disponen de una versión validada por el fabricante y libre de vulnerabilidades públicas.
    - Comprobar periódicamente los permisos dados a los usuarios, si se corresponden con lo autorizado por el Administrador.
    - Mantenimiento de los registros de auditoria. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
    - La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.
    - Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

7 REFERENCIAS

REF1	Manual de Usuario de authUSB SafeDoor V.1.4.
REF2	Guía de Instalación Rápida.

8 ABREVIATURAS

AV	Antivirus
ENS	Esquema Nacional de Seguridad.
HW	Hardware
SW	Software
V	Versión