centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1204

Procedimiento de empleo seguro
ESET Endpoint Security 7

Octubre 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.10.06 20:10:36 +02'00'

NIPO: 083-20-125-2

Fecha de Edición: octubre de 2020
ESET ha participado en la realización y modificación del presente documento

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

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Octubre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN

1. ***ESET Endpoint Security 7*** representa un nuevo enfoque de la seguridad informática realmente integrada. El motor de análisis *ThreatSense®*, combinado con el cortafuegos personalizado y el módulo *antispam* garantiza la protección del ordenador gracias a su velocidad y precisión. Estas características lo convierten en un sistema inteligente que está constantemente en alerta frente a ataques y software malicioso que puedan poner en peligro su ordenador.

2. Es una solución de seguridad integral que busca combinar el nivel máximo de protección con un impacto mínimo en el sistema. Las tecnologías avanzadas basadas en la inteligencia artificial son capaces de eliminar de forma proactiva la infiltración de virus, *spyware*, troyanos, gusanos, *adware*, *rootkits* y otros ataques que albergan en Internet sin dificultar el rendimiento del sistema ni interrumpir la actividad del ordenador.

2 OBJETO Y ALCANCE

3. El objeto de este documento es proporcionar un procedimiento de empleo seguro del producto *ESET Endpoint Security 7* que pueda ser utilizado en los sistemas de información del sector público bajo el alcance del Esquema Nacional de Seguridad.

3 ORGANIZACIÓN DEL DOCUMENTO

4. El documento se divide en:

   a) Apartado 4. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de 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.

   d) Apartado 7. En este apartado aparece un *checklist* con las tareas a realizar y el estado de cada una de ellas.

   e) Apartado 8. Referencias usadas en este documento.

   f) Apartado 9. Abreviaturas usadas en este documento.

4 FASE DE INSTALACIÓN

4.1 DESCARGA SEGURA DEL PRODUCTO

5. Para la instalación de *ESET Endpoint Security 7*, es necesario descargar el instalador de 32 o 64 bits, dependiendo del procesador del sistema. El *hash* de cada uno de los instaladores se puede comprobar ejecutando el comando de ***powershell Get-FileHash*** sobre los archivos descargados.

    a) 32 bits:

    https://download.eset.com/com/eset/apps/business/ees/windows/latest/ees_nt32.msi

    Hash (SHA256) del archivo (versión de EES[2] 7.3.2039):

    630ED0399D6ADF587892B181A330E8E5C0850B41CFEFC7AD8BCAE8A592198DD6

    b) 64 bits:

    https://download.eset.com/com/eset/apps/business/ees/windows/latest/ees_nt64.msi

    Hash (SHA256) del archivo (versión de EES[2] 7.3.2039):

    CD58476493DDAA42CD2B436356E5D9AFF8865F6248632AFC0148C6D94EDB19D7

4.2 CONSIDERACIONES PREVIAS

6. A continuación, se recoge una serie de aspectos a tener en cuenta antes de proceder con la instalación de la solución:

    a) El ordenador donde se vaya a instalar el antivirus NO debe tener otra solución de seguridad instalada.

    b) Sistemas Operativos compatibles: Microsoft Windows 10/8.1/8/7 SP1 con las más recientes actualizaciones de Windows (como mínimo, KB4474419 y KB4490628).

    c) 0,3 GB de memoria libre en el sistema.

    d) 1 GB de espacio libre en el disco duro.

    e) Conexión a Internet.

4.3 INSTALACIÓN

7. Ejecutar el instalador y pulsar en "*Siguiente*".

Figura 1. Bienvenida del asistente de instalación

8. A continuación, aparecerá el contrato de licencia de usuario final. Seleccionar la opción de *"Acepto las condiciones del acuerdo de licencia"* y pulsar en "*Siguiente*".

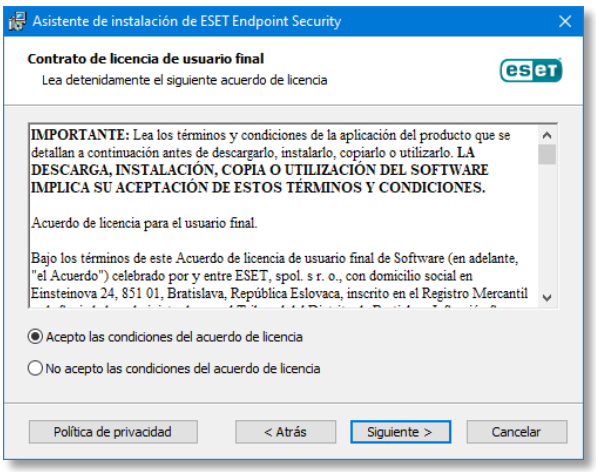

Figura 2. Aceptación de condiciones

9. Activar el sistema de respuesta *ESET Live Grid* (recomendado).

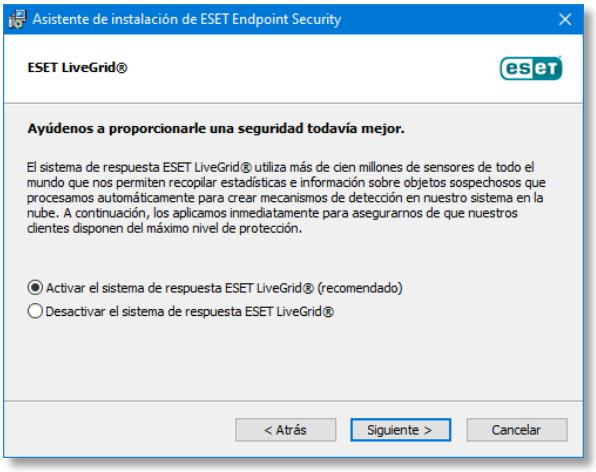

Figura 3. Activación ESET Live Grid

10. Realizar lo mismo con las “Aplicaciones potencialmente indeseables” y pulsa en “Instalar”.

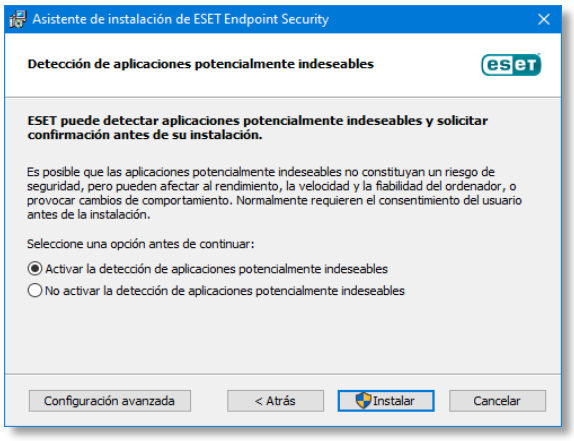

Figura 4. Activación de la detección de aplicaciones potencialmente indeseables

11. Esperar hasta que finalice la instalación.

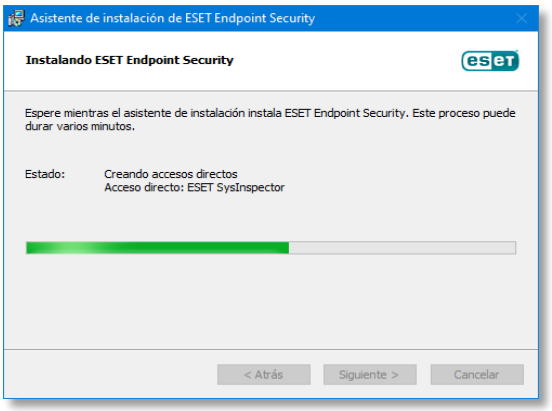

Figura 5. Instalación en proceso

12. Una vez finalizada la instalación pulsar en “*Finalizar*” y pasar al siguiente procedimiento, activar el antivirus con la licencia adquirida.

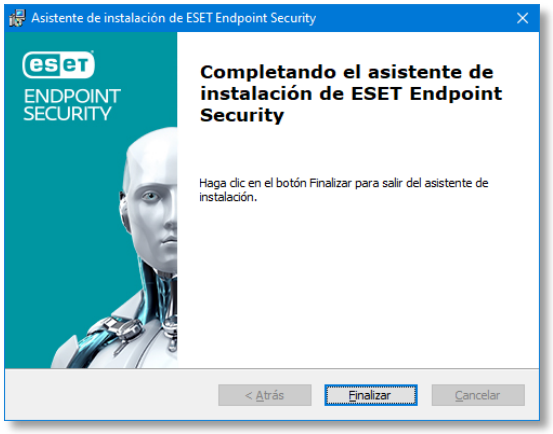

Figura 6. Finalización de la instalación

4.4 ACTIVACIÓN CON CLAVE DE LICENCIA

13. A continuación, se describe el procedimiento para la activación de la solución con una clave de activación válida.

14. Cuando se haya instalado, aparecerá una ventana como la que aparece debajo. Seleccionar la opción "*Utilizar la clave de licencia adquirida*".

Figura 7. Opciones de activación

15. Introducir la clave de licencia que ha sido enviada por correo y pulsar en "Continuar".

Figura 8. Introducción de clave de licencia

16. Una vez activado, aparecerá el siguiente mensaje:

Figura 9. Activación realizada correctamente

17. Posteriormente, el producto ya está activado:

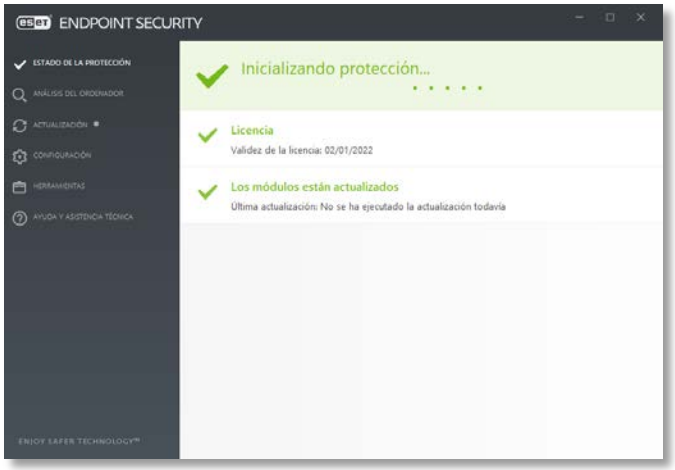

Figura 10. Inicialización del producto

18. Posteriormente a la activación, **se realiza automáticamente la actualización de los diferentes módulos de protección**. En el caso de que no se disponga de conexión

a Internet de forma puntual, la actualización se realizará automáticamente cuando se detecte conectividad a Internet. Revise el punto **6.4.2 ACTUALIZACIÓN SIN CONEXIÓN** para configurar la actualización sin conexión a Internet.

5 FASE DE CONFIGURACIÓN

En este apartado se indica la configuración de seguridad a aplicar sobre la solución *ESET Endpoint Security 7.*

5.1 INTERFAZ DE USUARIO

19. La ventana principal del programa ESET Endpoint Antivirus se divide en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.
20. A continuación, se muestra una descripción de las opciones del menú principal:
    - **Estado de la protección**: proporciona información sobre el estado de protección de ESET Endpoint Antivirus.
    - **Análisis del ordenador**: esta opción le permite configurar e iniciar el análisis estándar, el análisis personalizado o el análisis de medios extraíbles. También se puede repetir el último análisis ejecutado.
    - **Actualización**: muestra información sobre el motor de detección.
    - **Configuración**: seleccione esta opción para ajustar su ordenador o configuración de seguridad de la Web y el correo electrónico.
    - **Herramientas**: proporciona acceso a Archivos de registro, Estadísticas de protección, Observar actividad, Procesos en ejecución, Planificador de tareas, Cuarentena, ESET SysInspector y ESET SysRescue para crear un CD de recuperación. También puede enviar una muestra para su análisis.
    - **Ayuda y asistencia técnica**: proporciona acceso a los archivos de ayuda, la base de conocimiento de ESET y el sitio web de ESET. Aquí también se proporcionan enlaces para abrir una solicitud de soporte de atención al cliente, herramientas de soporte e información sobre la actividad del producto.
21. En la pantalla **Estado de la protección** se proporciona información sobre el nivel de seguridad y de protección actual del ordenador. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.
22. En la ventana de estado también se proporcionan enlaces rápidos a las características más habituales de ESET Endpoint Antivirus e información sobre la última actualización.

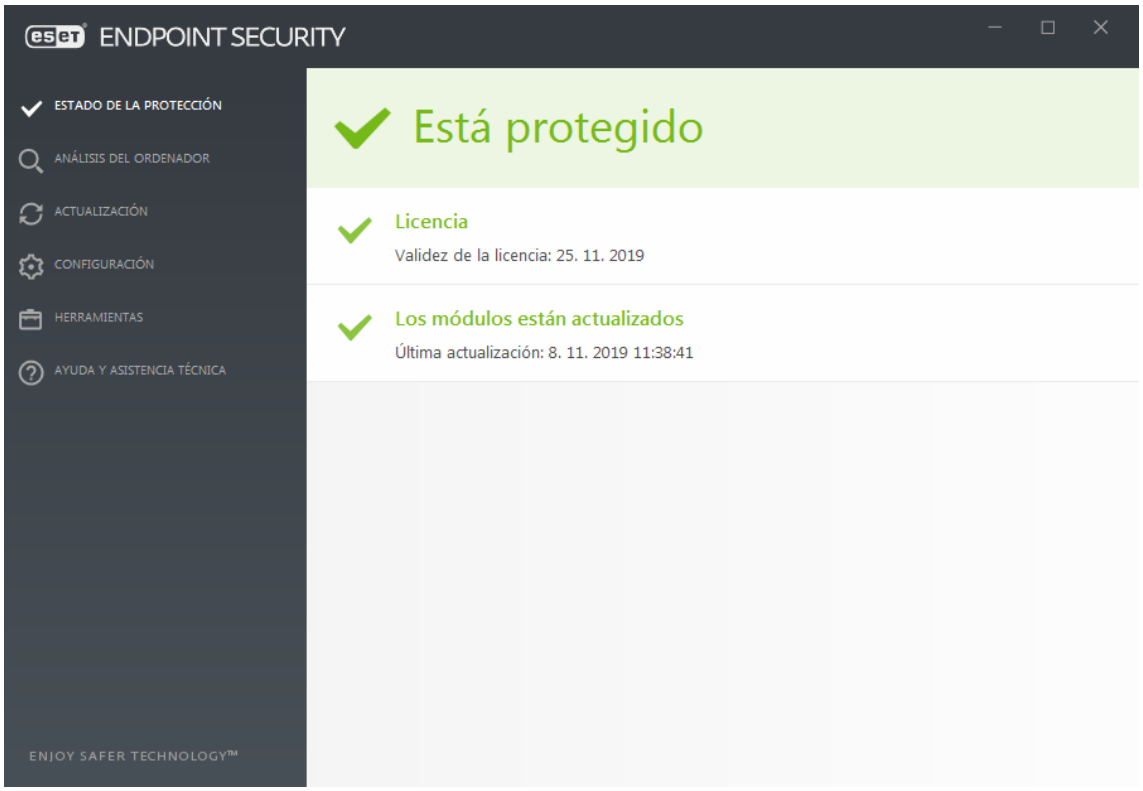

Figura 11. Información del estado de la protección de ESET Endpoint Security

5.2 PROTECCIÓN EN TIEMPO REAL

23. Existen dos (2) tipos de parámetros de configuración para el funcionamiento del producto en tiempo real: los informes y la protección. Dichos parámetros pueden ser aplicados según la categoría de los eventos:

    - Malware
    - Aplicaciones potencialmente indeseables
    - Potencialmente peligrosas
    - Aplicaciones sospechosas

24. Una aplicación potencialmente peligrosa es un *software* comercial legítimo que puede utilizarse con fines maliciosos. Entre los ejemplos de este tipo de aplicaciones se encuentran herramientas de acceso remoto, aplicaciones para detectar contraseñas y *keylogers* (programas que registran cada tecla pulsada por un usuario).

25. Las aplicaciones sospechosas son programas comprimidos con empaquetadores o protectores que son explotados por ciberdelincuentes para evitar la detección.

26. Para aplicar la configuración, se debe abrir *ESET Endpoint Security* pulsando en el icono que aparece en la parte inferior derecha del escritorio, al lado del reloj de *Windows*.

Figura 12. Acceder a ESET Endpoint Security

27. Pulsar el botón F5 para acceder a la configuración avanzada.

28. Acceder al apartado de Motor de Detección y configurar el apartado de "*Malware*", categoría "*Aplicaciones potencialmente indeseables*" como "*Equilibrado*". De esta forma, se obtiene la mejor configuración entre rendimiento y protección.

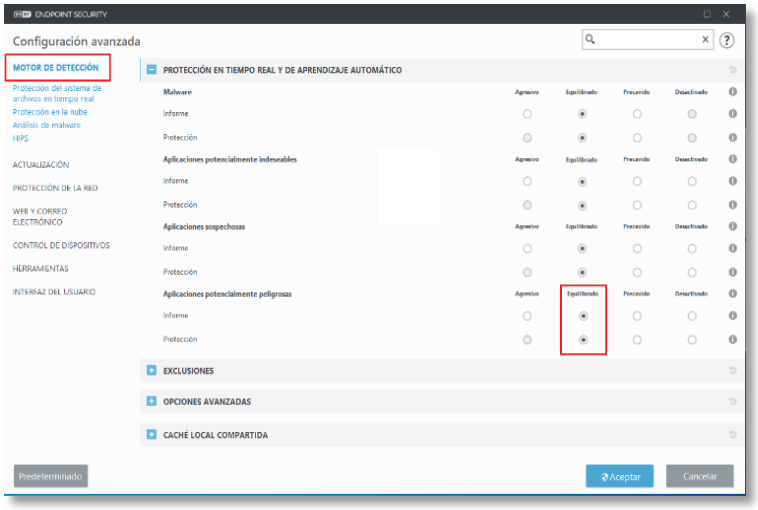

Figura 13. Opciones de configuración del motor de detección

29. En el caso de los *informes*, cuando se produce una detección (por ejemplo, identificación de una amenaza clasificada como *malware*), se registra información en el Registro de Detecciones, y se producen notificaciones en el escritorio si así está configurado.

30. Los informes son realizados con el motor de detección junto con el componente de aprendizaje automático. Es posible establecer un umbral de informes más elevado que el umbral de protección, aunque aconsejamos que el umbral seleccionado sea el "**Equilibrado**". Los ajustes de informes no influyen en la acción de bloquear, desinfectar o eliminar objetos.

31. Las características de los umbrales de informes se encuentran en la siguiente tabla:

Umbral	Explicación
Agresivo	Los informes recogen un elevado número de posibles detecciones. Esto puede generar la inclusión de falsos positivos.
Equilibrado	Este ajuste está optimizado para equilibrar el rendimiento y la precisión de las detecciones y el número de falsos positivos notificados.
Precavido	Reducen al mínimo los falsos positivos a la vez que se mantiene un nivel de protección suficiente. Solo se informa de los objetos cuando la gravedad de la detección es evidente.
Desactivado	Los informes no están activos, y no se detectan, notifican ni desinfectan detecciones. Este valor no está disponible para los informes de *malware* y es el valor predeterminado para las aplicaciones potencialmente peligrosas.

Tabla 1. Umbrales de configuración de informes

32. El parámetro de configuración de la **protección** determina las acciones a realizar en caso de detección en un objeto, el umbral que se aconseja utilizar es el **Equilibrado**. El programa puede bloquear el objeto y, a continuación, puede desinfectarlo, eliminarlo o moverlo a un estado de cuarentena.

33. El detalle de los umbrales para la configuración de la protección es el siguiente:

Umbral	Explicación
Agresivo	Los objetos asociados a las detecciones de nivel agresivo (o inferior) se bloquean, y se inicia la corrección automática (es decir, la desinfección). Se recomienda aplicar esta configuración cuando se han analizado todos los puntos de conexión con ajustes agresivos y se han agregado los falsos positivos a las exclusiones de detección.
Equilibrado	Las detecciones de nivel equilibrado (o inferior) se bloquean, y se inicia la corrección automática (es decir, la desinfección).
Precavido	Las detecciones de nivel precavido se bloquean, y se inicia la corrección automática (es decir, la desinfección).
Desactivado	Esta opción no está disponible para la protección contra *malware* y es el valor predeterminado para las aplicaciones potencialmente peligrosas. Es útil para identificar y excluir falsos positivos.

Tabla 2. Umbrales de configuración de los niveles de protección

5.3 PROTECCIÓN DE SISTEMA DE ARCHIVOS EN TIEMPO REAL

34. La protección en tiempo real del producto tiene los siguientes niveles de corrección o desinfección:

Nivel de desinfección	Descripción
Desinfectar siempre	Elimina la amenaza durante la desinfección de objetos sin la intervención del usuario final. En algunos casos no comunes (por ejemplo, archivos del sistema), si no se puede eliminar la amenaza, el objeto del que se informa se deja en su ubicación original. **Este nivel de desinfección es el ajuste recomendado.**
Desinfectar si es seguro; si no, mantener	Elimina la amenaza durante la desinfección de objetos sin la intervención del usuario final. En algunos casos (por ejemplo, archivos del sistema o archivos comprimidos con archivos limpios e infectados), si la amenaza no se puede eliminar, el objeto del que se informa se deja en su ubicación original.
Desinfectar si es seguro; si no, preguntar	Eliminar la amenaza durante la desinfección de objetos. En algunos casos, si no se puede realizar ninguna acción, el usuario final recibe una alerta interactiva y debe seleccionar una acción a realizar (por ejemplo, eliminar o ignorar).
Preguntar siempre al usuario final	El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción a realizar (por ejemplo, eliminar u omitir). Este nivel se ha diseñado para usuarios más avanzados que conocen los pasos necesarios en caso de detección.

Tabla 3. Niveles de desinfección

35. Para aplicar la configuración deseada, es necesario abrir el producto y pulsar el botón F5 para acceder a la configuración avanzada.

36. Para configurar el nivel de desinfección, acceder al apartado de "*Protección del sistema de archivos en tiempo real*". Se abre el subapartado de "*Parámetros de "ThreatSense"* y modificamos el parámetro de "*Nivel de Desinfección*" a *"Desinfectar siempre"*.

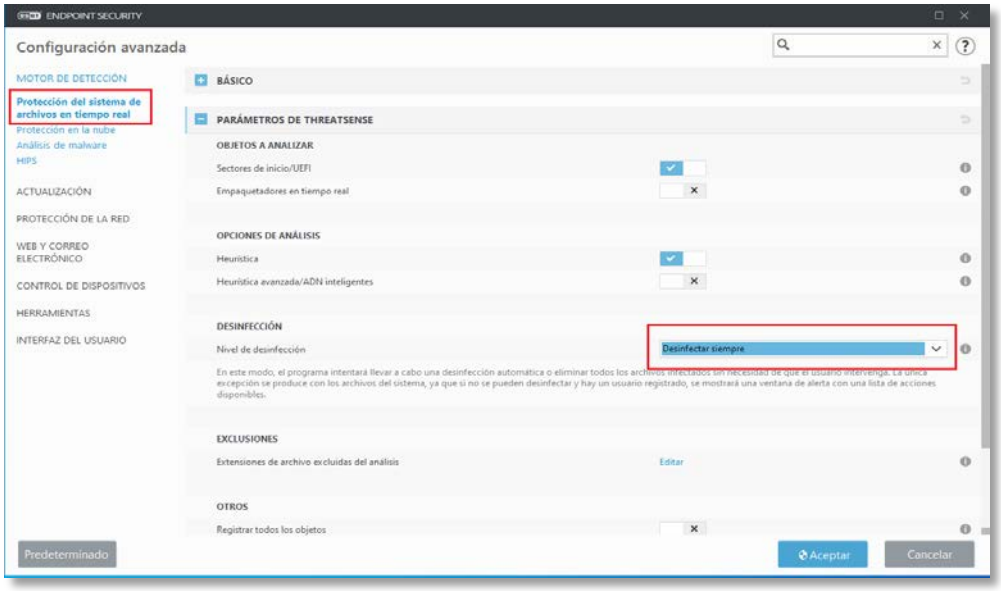

Figura 14. Configuración de los niveles de desinfección

5.4 ANÁLISIS DE MALWARE

5.4.1 ANÁLISIS EN ESTADO INACTIVO

37. En este apartado se detalla la configuración para la activación del *'Análisis en Estado Inactivo'.* Este análisis consiste en que cuando el ordenador está encendido, pero no está siendo utilizado por el usuario, el antivirus realice un análisis profundo del sistema. Cuando el usuario toma control de nuevo del equipo, este análisis se para.

38. Abrir *ESET Endpoint Security* y pulsar el botón F5 para acceder a la configuración avanzada.

39. Tras esto, pulsar en "*Análisis de malware*", en la parte izquierda. Desplegar la opción "*Análisis en estado inactivo*" y habilitar el "*Análisis en estado inactivo*" y "*Activar el registro de sucesos*". Esto guardará un informe detallado del análisis que se está realizando en el apartado de Archivos de Registro. De esta forma el usuario o administrador de la red tendrá acceso directo a qué ha sido analizado durante el análisis en estado inactivo.

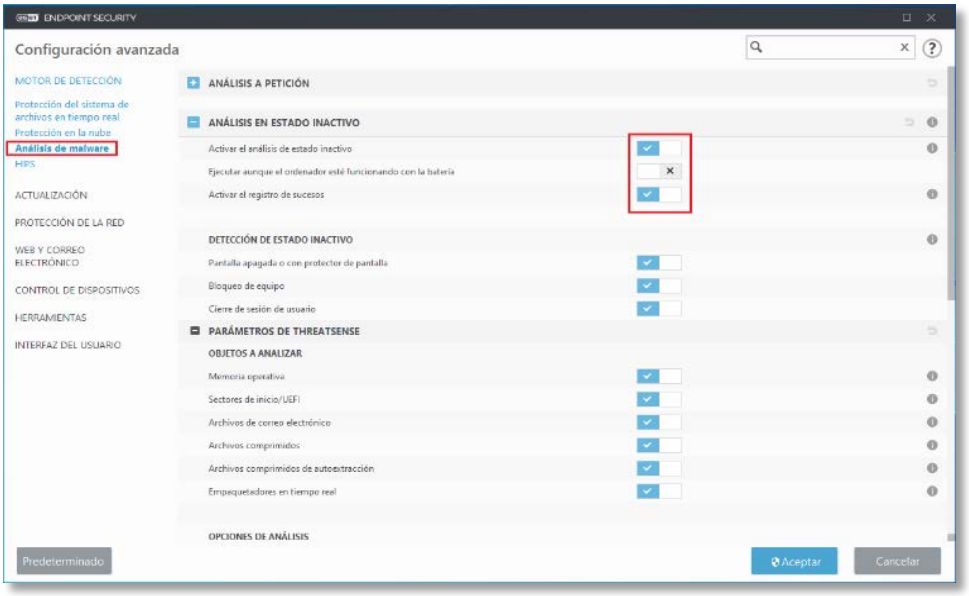

Figura 15. Configuración de los análisis de *malware*

5.4.2 ANÁLISIS A PETICIÓN DEL USUARIO

40. El análisis a petición o bajo demanda es una parte importante de ESET *Endpoint Security*. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Desde el punto de vista de la seguridad, es esencial que los análisis no se ejecuten únicamente cuando se sospecha que existe una infección, sino que se realicen periódicamente como parte de las medidas de seguridad.

41. **Se recomienda realizar un análisis en profundidad del sistema periódicamente**, por ejemplo, una vez al mes. A continuación, se indica como configurar el análisis a petición del usuario para que el antivirus elimine automáticamente las amenazas que detecte.

42. Abrir *ESET Endpoint Security* pulsando en el icono que aparece bajo a la derecha, al lado del reloj de Windows.

43. Pulsar el botón F5 para acceder a la configuración avanzada.

44. Acceder al apartado de Módulo de Protección, Análisis de *Malware* y Análisis a petición. Seleccionar el perfil "*Análisis exhaustivo*" y pulsar en Parámetros de *ThreatSense*.

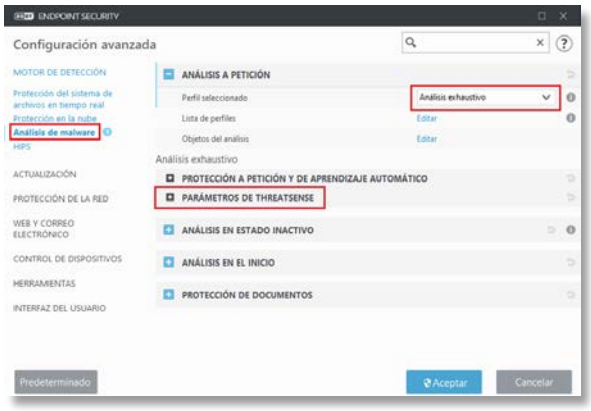

Figura 16. Configuración de análisis bajo demanda

45. Cambiar el valor de *"Nivel de desinfección"* a "*Desinfectar siempre*" para que el antivirus elimine automáticamente cualquier tipo de malware que detecte.

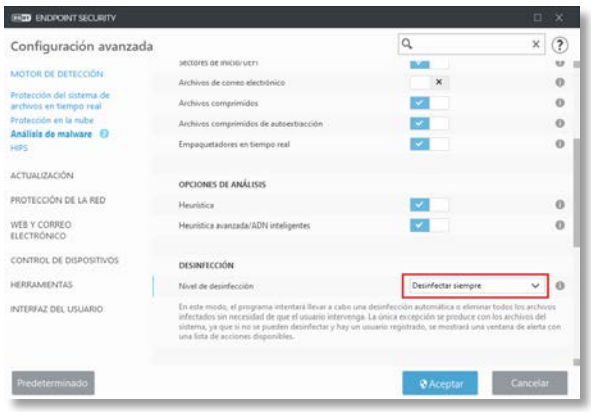

Figura 17. Configuración del nivel de desinfección

5.5 PROTECCIÓN DE LA CONFIGURACIÓN E INSTALACIÓN DEL ANTIVIRUS CON UNA CONTRASEÑA

Para ofrecer la máxima seguridad a su sistema, es esencial que ESET Endpoint Security se haya configurado correctamente ya que una configuración incorrecta puede provocar la pérdida de datos importantes. **Para evitar modificaciones o desinstalaciones no autorizadas, los parámetros de configuración de *ESET Endpoint Security* se deben proteger mediante contraseña,** que deberá ser de una longitud mínima o igual a 12 caracteres y componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales ["!", "@", "#", "$","%", "^", "&", "*", "(", "]

46. Para configurar la protección del antivirus por contraseña, abrir el producto y pulsar el botón F5 para acceder a la configuración avanzada.

47. Acceder al apartado "Interfaz del usuario", *"Configuración de acceso"*. En este punto activar la opción "*Configuración de protección por contraseña*", introducir la contraseña en la ventana que aparece y pulsar en "*Aceptar*".

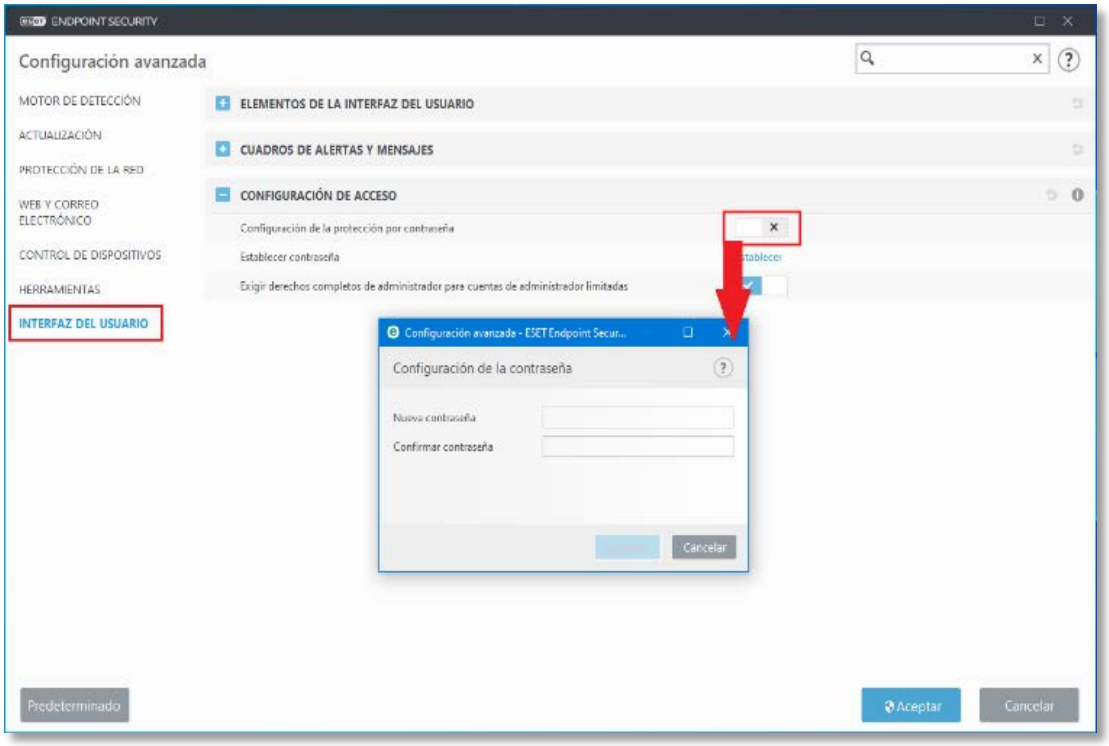

Figura 18. Configuración de la contraseña

5.6 SISTEMA AVANZADO DE PREVENCIÓN DE INTRUSIONES (HIPS)

48. El Sistema de prevención de intrusiones del host (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos; solo supervisa los procesos que se ejecutan dentro del sistema operativo.

49. Los ajustes de HIPS están en **Configuración avanzada** (F5) > **Motor de detección** > **HIPS** > **Básico**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal del programa de ESET Endpoint Security, en **Configuración** > **Ordenador**.

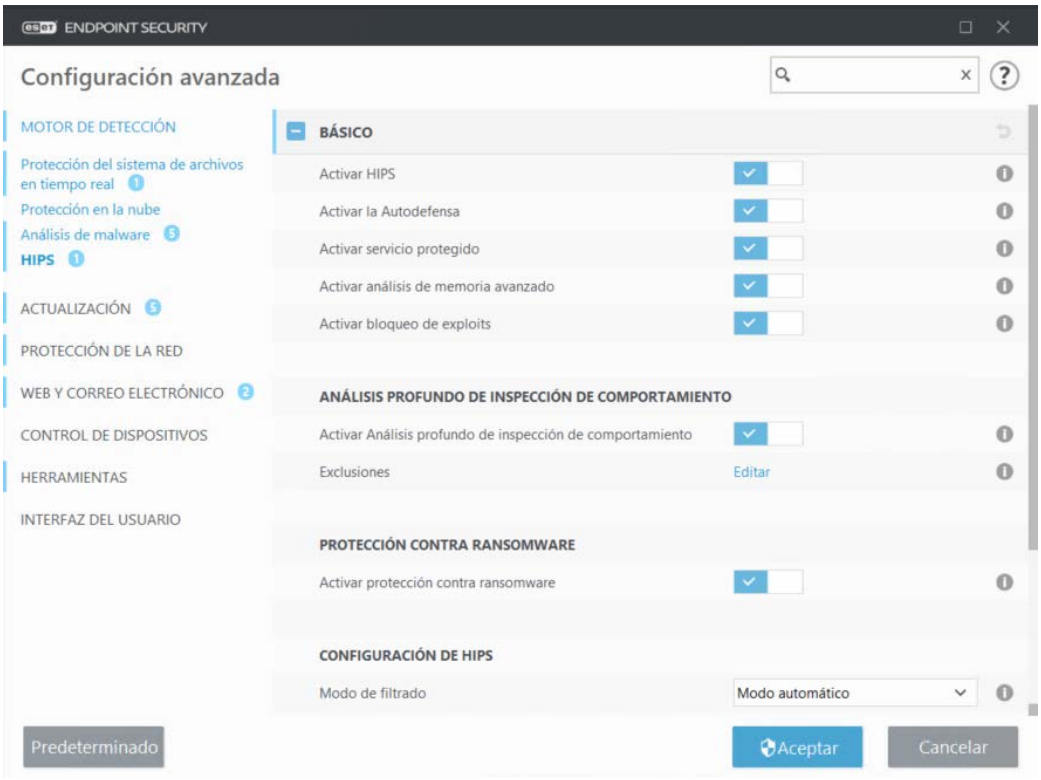

Figura 19. Configuración del módulo HIPS

En el apartado BÁSICO:

50. **Activar HIPS**: HIPS está activado de forma predeterminada en ESET Endpoint Security. Si desactiva HIPS, se desactivarán las demás características de HIPS, como Bloqueador de exploits.
51. **Activar la Autodefensa**: ESET Endpoint Security utiliza la tecnología de Autodefensa integrada como parte del HIPS para impedir que software malicioso dañe o desactive su protección antivirus y antiespía. La autodefensa evita la manipulación de procesos, claves de registro y archivos cruciales del sistema y de ESET. ESET Management Agent también se protege cuando se instala. Se recomienda tener habilitada esta opción.
52. **Activar servicio protegido**: activa la protección para ESET Service (ekrn.exe). Cuando está activado, el servicio se inicia como un proceso de Windows protegido para defenderle de ataques de malware. Esta opción está disponible en Windows 8.1 y Windows 10.
53. **Activar análisis de memoria avanzado**: funciona en combinación con Bloqueador de exploits para reforzar la protección contra malware diseñado para evitar su detección mediante productos antimalware gracias al uso de ofuscación o cifrado. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.
54. **Activar bloqueo de exploits**: se ha diseñado para fortalecer los tipos de aplicaciones que sufren más ataques, como navegadores, lectores de PDF, clientes

de correo electrónico y componentes de MS Office. El bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

55. **Habilitar Análisis profundo de inspección de comportamiento**: es otra capa de protección que funciona como parte de la función HIPS. Esta extensión del HIPS analiza el comportamiento de todos los programas que se ejecutan en el ordenador y le advierte si el comportamiento del proceso es malicioso.

5.6.1 PROTECCIÓN CONTRA EL RANSOMWARE

56. **Activar protección contra ransomware**: es otra capa de protección que funciona como parte de la característica HIPS. Para que la protección contra ransomware funcione, debe tener activado el sistema de reputación ESET LiveGrid®.

57. Activar modo de auditoría: todo lo que detecta la protección contra ransomware no se bloquea automáticamente, sino que **se registra con una advertencia de severidad** y se envía a la consola de administración con el indicador "MODO DE AUDITORÍA". El administrador puede decidir excluir dicha detección para evitar una posterior detección, o mantenerla activa, lo que significa que una vez que finalice el modo de auditoría, esta se bloqueará o eliminará. La activación o desactivación del modo de auditoría también se registrará en ESET Endpoint Security. Esta opción está disponible solo en ESMC o en el editor de configuración de políticas de ECA.

5.6.2 CONFIGURACIÓN DEL MÓDULO HIPS

58. El Modo de filtrado se puede realizar en uno de los siguientes modos:

Modo de filtrado	Descripción
Modo automático	Las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema.
Modo inteligente	Solo se informará al usuario de los sucesos muy sospechosos.
Modo interactivo	El usuario debe confirmar las operaciones.
Modo basado en reglas	Bloquea todas las operaciones no definidas por una regla específica que las permita.
Modo de aprendizaje	Las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el editor de Reglas de HIPS, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el Modo de aprendizaje en el menú desplegable Modo de filtrado, el ajuste El modo de aprendizaje finalizará a las estará disponible. Seleccione el periodo de tiempo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada se le pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

Tabla 4. Umbrales de configuración de informes

59. **Modo establecido tras conocer la caducidad del modo**: seleccione el modo de filtrado que se utilizará cuando caduque el modo de aprendizaje. Tras el vencimiento, la opción Preguntar al usuario requiere privilegios administrativos para realizar un cambio en el modo de filtrado de HIPS.

60. El sistema HIPS supervisa los sucesos del sistema operativo y reacciona en consecuencia basándose en reglas similares a las que utiliza el cortafuegos. Haga clic en Editar junto a Reglas para abrir el editor de reglas de HIPS. En la ventana de reglas de HIPS puede seleccionar, agregar, editar o quitar reglas. Puede obtener más información sobre la creación de reglas y las operaciones de HIPS en Editar una regla de HIPS.

5.7 ALGORITMOS DE CIFRADO

61. ESET Endpoint Security hace uso de HTTPS y TLS1.2 para establecer canales de comunicación seguros para todas aquellas comunicaciones que puedan transmitir. La protección de estas comunicaciones es automática y se realiza de forma interna desde EES.

5.8 ANÁLISIS AVANZADO DE MEMORIA

62. El Análisis avanzado de memoria trabaja conjuntamente con **el Bloqueador de exploits** para mejorar la protección frente a código malicioso, que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. En aquellos casos en los que la emulación o la heurística normales no detectan una amenaza, el Análisis de memoria avanzado consigue identificar comportamientos sospechosos y analiza las amenazas que se presentan en la memoria del sistema. Esta solución es eficaz incluso para código malicioso que utiliza técnicas avanzadas de ofuscación. A diferencia del Bloqueador de exploits, se trata de un método posterior a la ejecución, lo cual significa que existe la posibilidad de que haya habido actividad maliciosa antes de la detección de una amenaza. No obstante, ofrece una capa de seguridad adicional cuando las otras técnicas de detección fallan.

5.9 BLOQUEADOR DE EXPLOITS

63. El **Bloqueador de exploits** se ha diseñado para fortificar aquellas aplicaciones como los navegadores de Internet, los lectores de archivos PDF, los clientes de correo electrónico y los componentes de MS Office. Este producto supervisa el comportamiento de los procesos en busca de actividad sospechosa que pueda indicar la presencia de un exploit. Además, añade otra capa de protección, un paso más cerca de los atacantes, con una tecnología totalmente diferente en comparación con las técnicas centradas en la detección de archivos maliciosos.

64. Cuando detecta un proceso sospechoso, el Bloqueador de exploits lo detiene inmediatamente y registra los datos de la amenaza; después los envía al sistema de nube de ESET LiveGrid®. El laboratorio de amenazas de ESET procesa estos datos y los utiliza para mejorar la protección que ofrece a los usuarios frente a amenazas desconocidas y ataques 0-day (código malicioso reciente para que el que no hay ninguna solución preconfigurada).

5.10 PROTECCIÓN CONTRA BOTNETS

65. La protección contra botnets detecta código malicioso mediante el análisis de sus protocolos de comunicación de red. A diferencia de los protocolos de red, que no han cambiado en los últimos años, el código malicioso botnet cambia con frecuencia. Esta nueva tecnología ayuda a ESET a acabar con el código malicioso que intenta conectar su ordenador a redes de botnets.

5.11 AUDITORÍA

66. El registro de auditoría de ESET Endpoint controla los cambios de configuración o el estado de la protección, y registra instantáneas que pueden consultarse en un futuro. Estos registros de auditoría se ubican dentro de **Herramientas > Archivos de Registro** > **Auditoría**, y es donde se registran todos los y eventos relacionados con la funcionalidad del antivirus.

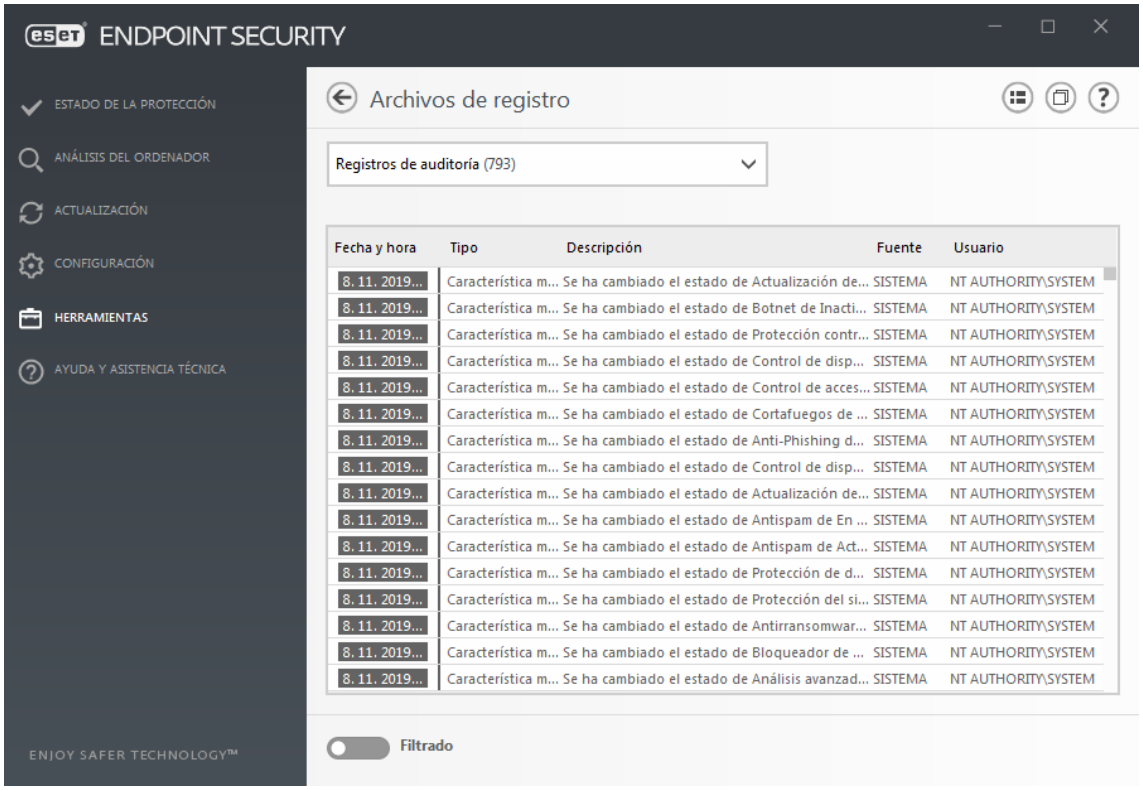

Figura 20. Panel de archivos de registro

67. Pulse con el botón derecho del ratón sobre cualquier tipo de registro de auditoría > **Configuración modificada** en la ventana de archivos de registro, y seleccione **Mostrar cambios** en el menú contextual para mostrar información detallada sobre el cambio realizado. Además, puede restaurar el cambio del ajuste si hace clic en **Restaurar** desde el menú contextual. Si selecciona **Eliminar todo** en el menú contextual, se creará un registro con información sobre esta acción. El registro de auditoría incluye: Fecha y hora de la ocurrencia; Tipo de evento; Descripción; Fuente; Usuario;

68. Si la opción **Optimizar archivos de registro automáticamente** está activada en **Configuración avanzada** > **Herramientas** > **Archivos de registro**, los registros de auditoría se desfragmentarán automáticamente como otros registros.

69. Si la opción Eliminar automáticamente los registros con una antigüedad de más de (días) está activada en Configuración avanzada > Herramientas > Archivos de registro, las entradas del registro que tengan una antigüedad superior al número de días especificado se eliminarán automáticamente.

6 FASE DE OPERACIÓN

70. En este apartado se indican algunas de las operaciones más importantes a realizar para mantener una protección segura con *ESET Endpoint Security 7.*

6.1 REALIZAR UN ANÁLISIS A PETICIÓN DEL USUARIO

71. Se recomienda que se realice un análisis en profundidad del sistema al menos una vez al mes para garantizar en el equipo está completamente libre de amenazas.

72. Para ello abrir *ESET Endpoint Security* y pulsar en "*Análisis del Ordenador*" de la parte izquierda de la ventana.

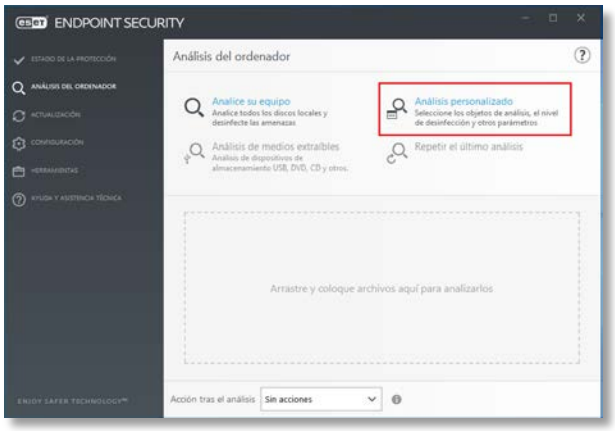

Figura 21. Configuración de los análisis del ordenador

73. Y, para realizar un análisis exhaustivo, pulsar en "*Análisis personalizado*".

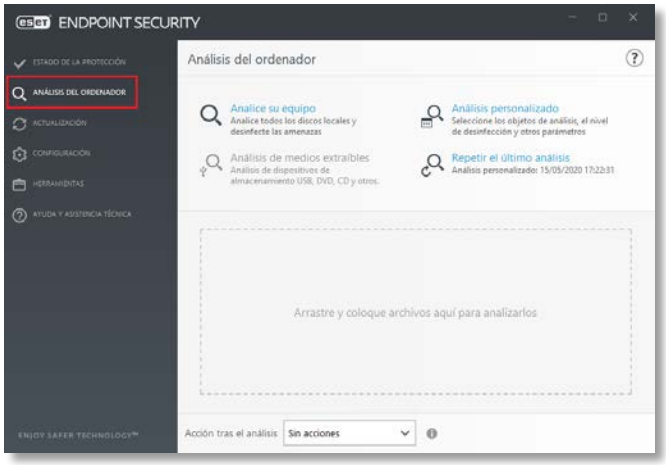

Figura 22. Selección de configuración de un análisis personalizado

74. Marcar "*Este equipo*" y pulsar en el icono de la rueda de engranaje.

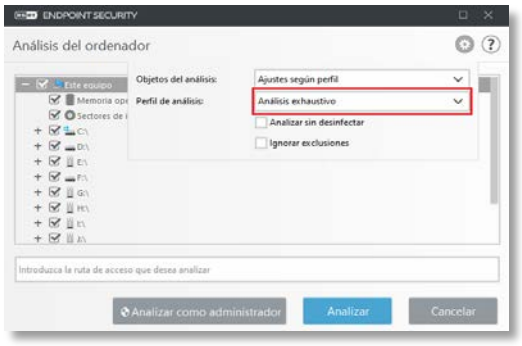

Figura 23. Selección del objeto a analizar

75. Cambiar la opción de Perfil de análisis por "*Análisis exhaustivo*" y pulsar *"Analizar como administrador".*

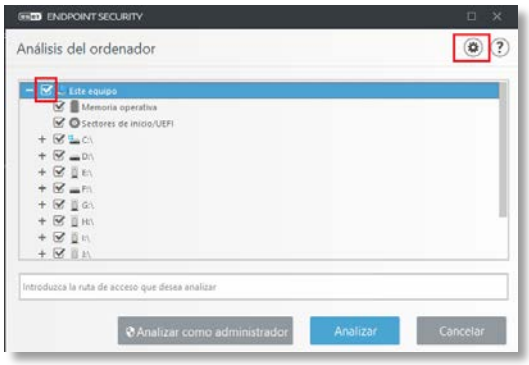

Figura 24. Selección del grado de análisis

6.2 COMPROBAR EL ESTADO DE LOS MÓDULOS DE ACTUALIZACIÓN

76. Es necesario actualizar ESET Endpoint Security de forma periódica.

77. El módulo "Actualización" garantiza que el programa está siempre actualizado de dos (2) maneras: a través de la actualización del motor de detección y de los componentes del sistema. Cuando se activa el programa, las actualizaciones están activadas de forma predeterminada.

78. **Se recomienda comprobar que la solución está actualizada.** Para ello, se debe acceder al apartado "Actualización" en la parte izquierda de la ventana.

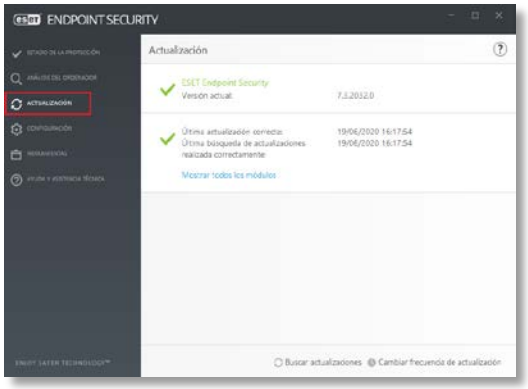

Figura 25. Opción de consulta del estado de actualización del producto

79. En este punto se indica cuando fue la última actualización correcta de las firmas:

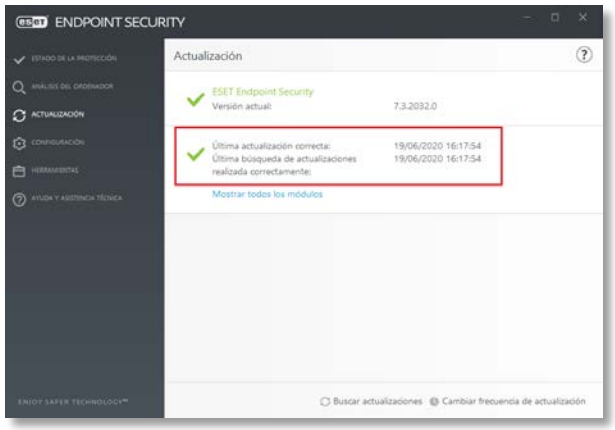

Figura 26. Estado de actualización del producto

80. La **última actualización correcta** corresponde con la fecha y hora de la última actualización que ha sido realizada correctamente. Es necesario validar que es una fecha reciente, lo que significa que el motor de detección está actualizado.

81. La **última búsqueda correcta de actualizaciones** corresponde con la fecha y hora del último intento correcto de actualización de los módulos.

82. Para ver el estado y actualización de los módulos pulsar en “Mostrar todos los módulos” para acceder a la información del estado de los módulos.

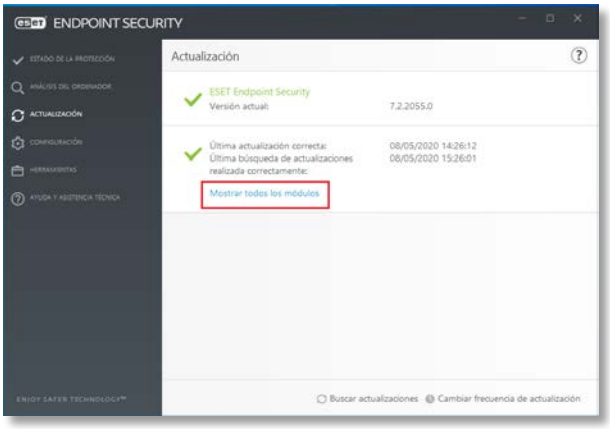

Figura 27. Opción para visualizar

83. Se abrirá una ventana donde aparece la siguiente información:

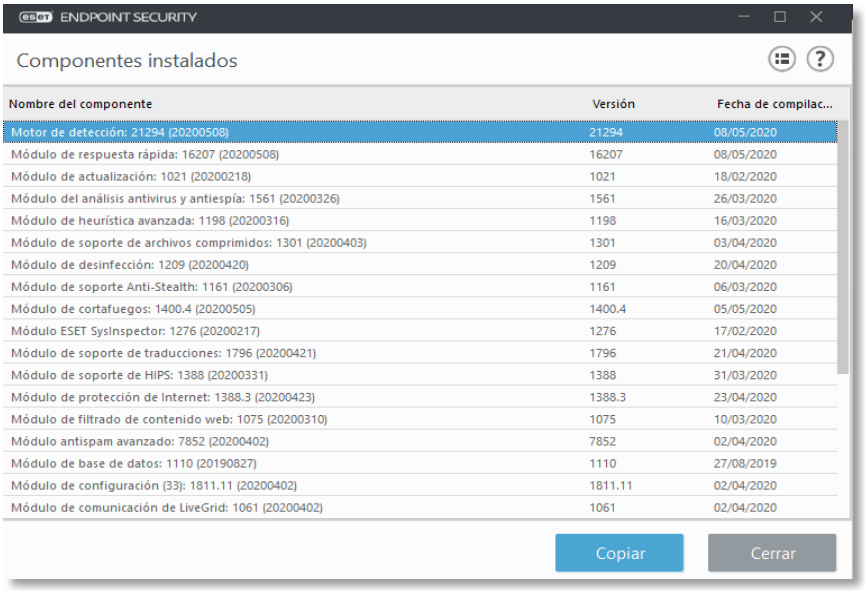

Figura 28. Consulta de fechas de actualización de los distintos componentes

84. Para comprobar si los módulos del antivirus están actualizados se debe analizar la línea que incluye *"Motor de detección".* En la Figura 28, aparecen los valores 21294 (20200508).

85. El valor entre paréntesis corresponde con la fecha de actualización de los módulos en formato: *yyyymmdd*, es decir: año-mes-día.

6.3 PLANIFICADOR DE TAREAS

86. El planificador de tareas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas.

    Se puede acceder al Planificador de tareas desde la ventana principal del programa de ESET Endpoint Security haciendo clic en **Herramientas** > **Planificador de tareas**.

87. El Planificador de tareas contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

88. El Planificador de tareas sirve para programar las siguientes tareas: actualización del motor de detección, tarea de análisis, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana Planificador de tareas (haga clic en **Agregar tarea** o Eliminar en la parte inferior). Haga clic con el botón derecho en cualquier parte de la ventana Planificador de tareas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

89. De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

    - Mantenimiento de registros
    - Actualización automática de rutina
    - Actualización automática al detectar la conexión por módem
    - Actualización automática después del registro del usuario
    - Verificación automática de archivos en el inicio (tras inicio de sesión del usuario)
    - Comprobación de la ejecución de archivos en el inicio (tras una actualización correcta del módulo)

    Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho del ratón en la tarea y, a continuación, haga clic en Modificar, o seleccione la tarea que desea modificar y haga clic en el botón Modificar.

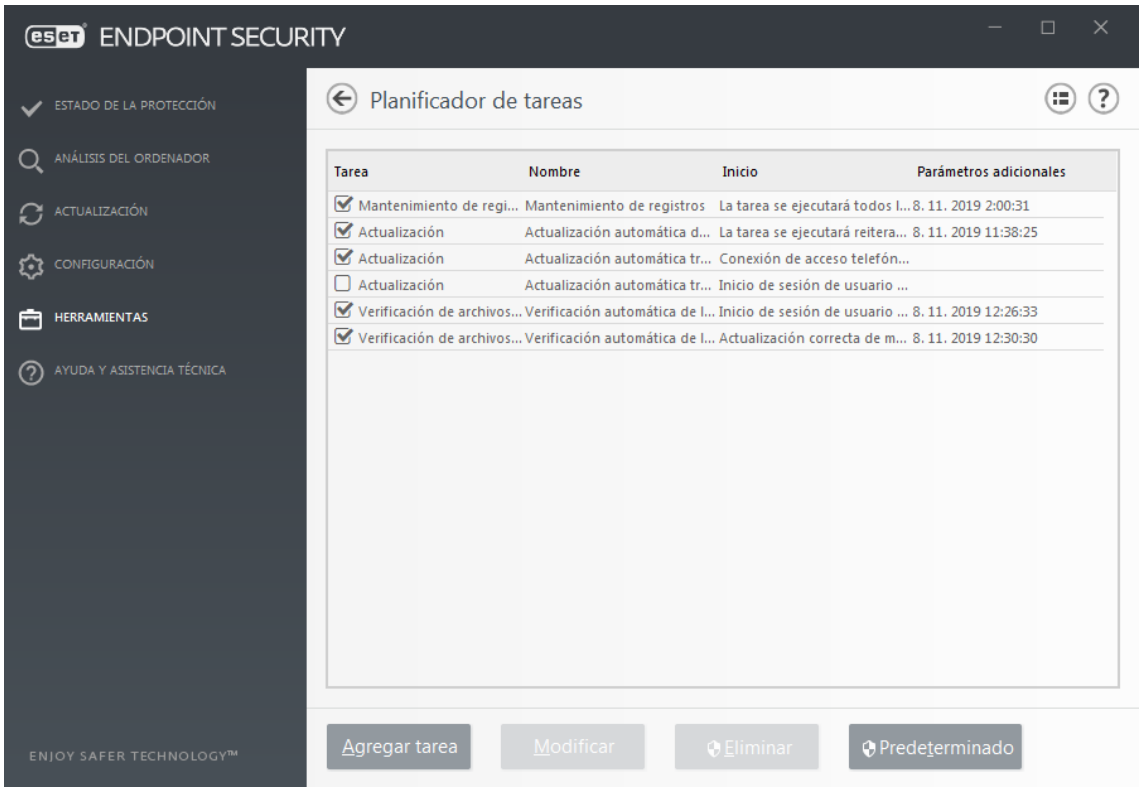

Figura 29. Panel del Planificador de tareas

90. Agregar una nueva tarea

    1. Pulsar en **Agregar tarea**, en la parte inferior de la ventana.
    2. Introducir un nombre para la tarea.
    3. Seleccionar la tarea deseada en el menú desplegable:

        - **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
        - **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
        - **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
        - **Crear una instantánea de estado del equipo**: crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo, controladores y aplicaciones) y evalúa el nivel de riesgo de cada componente.
        - **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
        - **Actualización**: programa una tarea de actualización mediante la actualización del motor de detección y los módulos del programa.

91. Activar la opción **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programas), hacer clic en **Siguiente** y seleccionar una de las opciones de programación:

    - **Una vez**: la tarea se ejecutará en la fecha y a la hora predefinidas.
    - **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado.
    - **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
    - **Semanalmente**: la tarea se ejecutará el día y a la hora seleccionados.
    - **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

4. Seleccionar **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo Ejecución de la tarea. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

    - En la siguiente hora programada
    - Lo antes posible
    - Inmediatamente, si la hora desde la última ejecución excede un valor especificado (el intervalo se puede definir con el cuadro Tiempo desde la última ejecución)

Si se desea revisar la tarea programada, haga clic con el botón derecho del ratón y, después, haga clic en **Mostrar detalles de la tarea**.

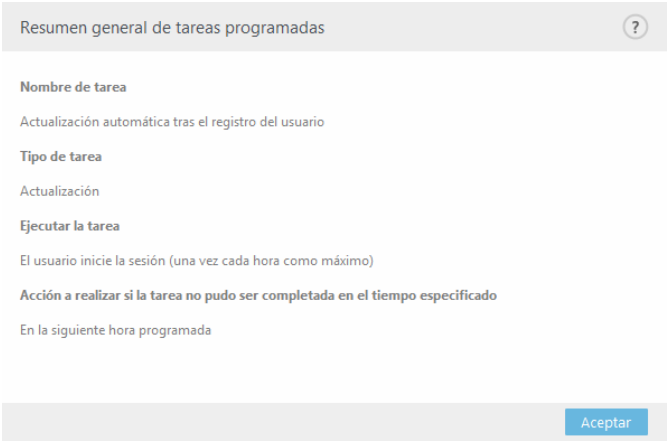

Figura 30. Ventana con detalles de la tarea programada

6.4 ACTUALIZACIÓN PRODUCTO

6.4.1 ACTUALIZACIÓN CON CONEXIÓN A INTERNET

92. La actualización del motor de detección de virus y la actualización de los componentes del programa son partes importantes a la hora de mantener una protección completa frente a código malicioso.

93. El proceso de actualización manual comienza tras hacer clic en **Buscar actualizaciones**. Se muestran una barra de progreso de la descarga y el tiempo que falta para que finalice la descarga. Para interrumpir la actualización, haga clic en Cancelar actualización.

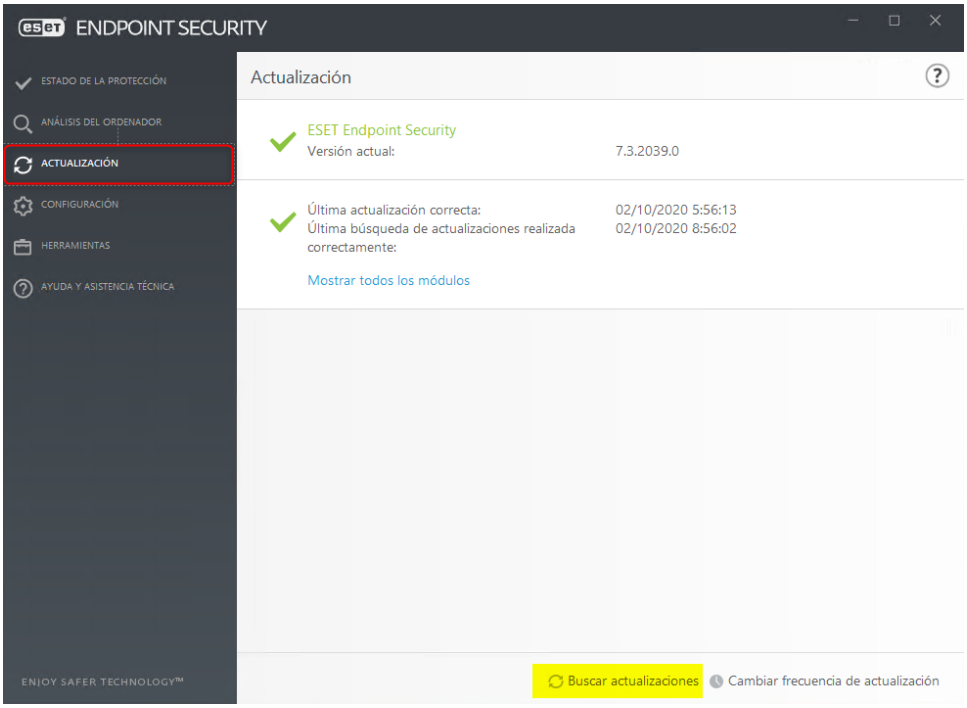

Figura 31. Actualización manual de ESET

6.4.2 ACTUALIZACIÓN SIN CONEXIÓN

94. La función mirror de ESET por HTTP **se desaconseja absolutamente y es una función obsoleta**. Desde hace más de 10 años se utiliza únicamente la actualización a través de USB para actualizar equipos aislados totalmente de la red.

95. Actualización por USB

    a) Introducir un USB con los archivos de actualización.

b) En el equipo cliente añadir la ruta del contenido de los archivos del USB y Aceptar los cambios:

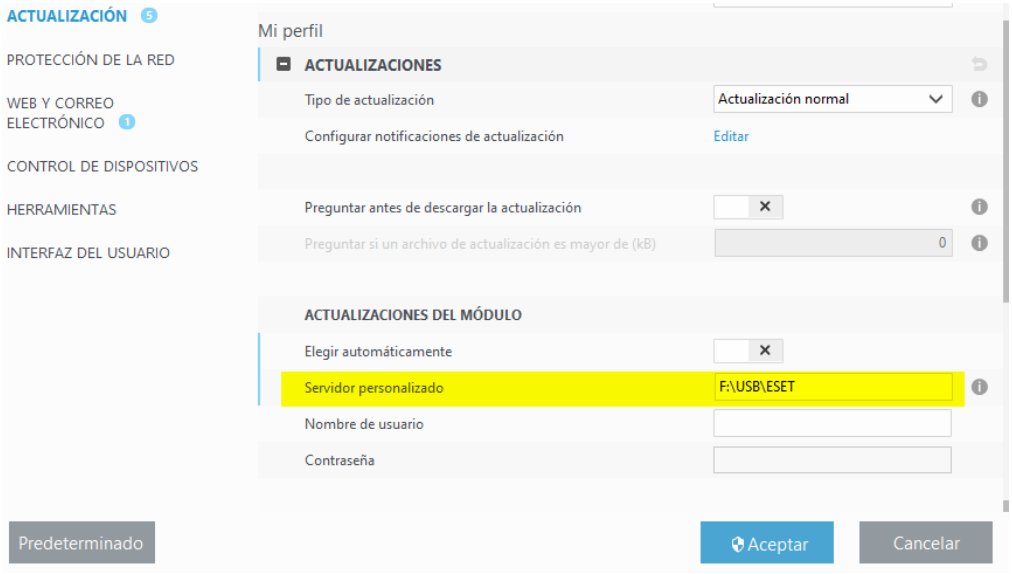

Figura 32. Actualización offline a través de USB

6.5 CONFIGURACIÓN DE LA INTERFAZ DE USUARIO

96. Las opciones de configuración de la interfaz de usuario de ESET Endpoint Antivirus le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración están disponibles en la sección **Interfaz de usuario** > **Elementos de la interfaz del usuario** del árbol de configuración avanzada de ESET Endpoint Antivirus.

97. En la sección **Elementos de la interfaz del usuario** puede ajustar el entorno de trabajo. Utilice el menú desplegable **Modo de inicio GUI** para seleccionar uno de los siguientes modos de inicio de la interfaz gráfica de usuario (GUI):

- **Completo**: se muestra la GUI completa.
- **Mínimo**: la interfaz gráfica está disponible, pero el usuario solo ve las notificaciones.
- **Manual**: no se muestra ninguna notificación ni alerta.
- **Silencioso**: no se muestra la interfaz gráfica de usuario, las notificaciones ni las alertas. Este modo puede resultar útil en aquellas situaciones en las que necesita conservar los recursos del sistema. El modo silencioso solo lo puede iniciar el administrador.

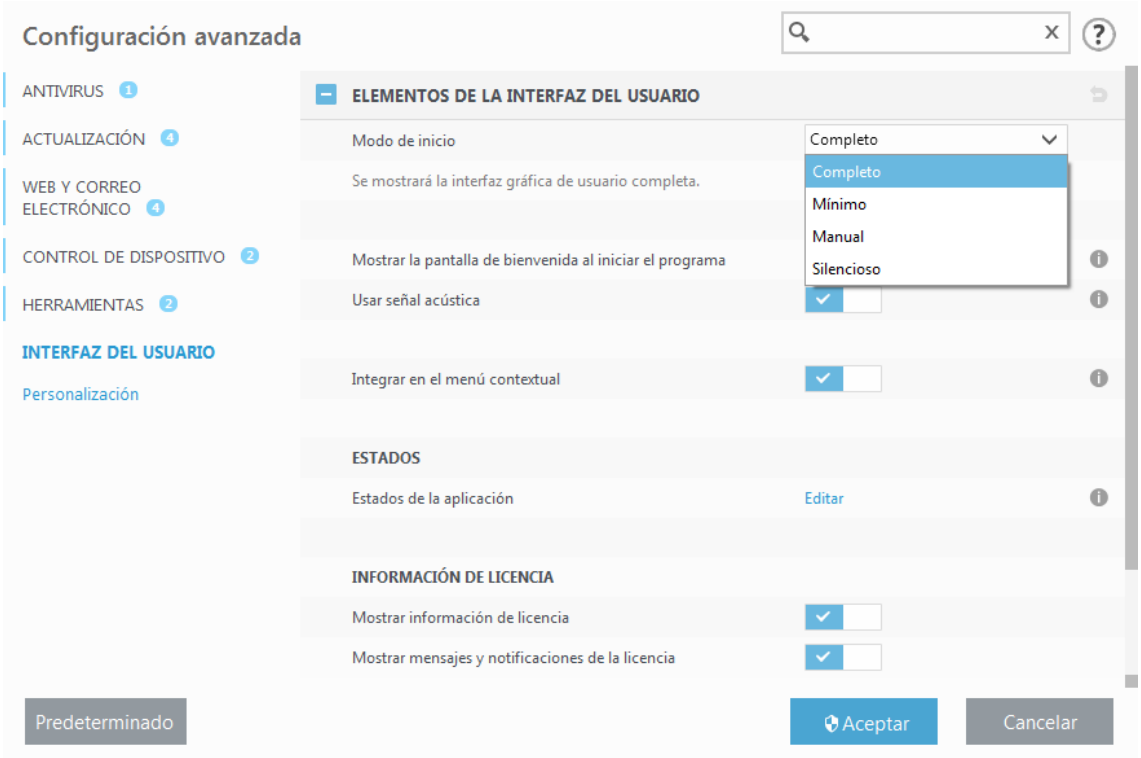

Figura 33. Configuración de la interfaz de usuario

98. Si desea desactivar la pantalla inicial de ESET Endpoint Antivirus, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

99. Si desea que ESET Endpoint Antivirus reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar señal acústica**.

100. **Integrar en el menú contextual**: integra los elementos de control de ESET Endpoint Antivirus en el menú contextual.

6.6 ESTADOS

101. **Estados de la aplicación**: haga clic en el botón **Editar** para administrar (desactivar) los estados que se muestran en el menú **Estado de protección** del menú principal.

6.7 INFORMACIÓN DE LA LICENCIA

102. **Mostrar información de licencia**: cuando esta opción esté desactivada, no se mostrará la información de la licencia en las pantallas Estado de protección y Ayuda y asistencia técnica.

    Mostrar mensajes y notificaciones de la licencia: cuando esta opción está desactivada, las notificaciones y los mensajes solo se mostrarán cuando la licencia caduque.

7 CHECKLIST

ACCIONES	SÍ	NO	RECOMENDADO	OBSERVACIONES
INSTALACIÓN				
Ordenador sin antivirus	☐	☐	☐	
Se cumplen los requisitos mínimos para la instalación	☐	☐	☐	
Activar ESET *Live Grid* ®	☐	☐	☐	
Activadas la detección de Aplicaciones potencialmente Indeseables	☐	☐	☐	
Producto activado	☐	☐	☐	
Módulos actualizados	☐	☐	☐	
CONFIGURACIÓN				
Activar *"Aplicaciones potencialmente Peligrosas"*	☐	☐	☐	
Configurar sistema de prevención de intrusiones del host (HIPS)	☐	☐	☐	
Activar "Protección contra el ransomware"	☐	☐	☐	
Cambiar nivel de desinfección a *"Desinfectar siempre"*	☐	☐	☐	
Activar el análisis en estado inactivo	☐	☐	☐	
Configurar perfil de análisis exhaustivo	☐	☐	☐	
Proteger la configuración e instalación del antivirus con contraseña	☐	☐	☐	
Revisar la configuración de la auditoría	☐	☐	☐	

Tabla 4. Checklist

8 REFERENCIAS

[1] «Guía del usuario de ESET Endpoint Security para Windows,» [En línea]. Available: https://download.eset.com/com/eset/apps/business/ees/windows/latest/eset_ees_7_userguide_esn.pdf?_ga=2.63787880.653547648.1599145457-1951229890.1590757977&_gac=1.116201972.1595510424.Cj0KCQjw6uT4BRD5ARIsADwJQ18JEOpg5OEBKEoiiQCXdX2FITJ_HP1bugCPKS2uiLM1qMph.

[2] «Ayuda en línea de ESET,» [En línea]. Available: https://help.eset.com/ees/7/es-ES/.

9 ABREVIATURAS

EES *ESET Endpoint Security*