centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1204

Procedimiento de Empleo Seguro
ESET Endpoint Security 11

Mayo 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-185-6

Fecha de Edición: Mayo 2025

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2025.09.25 15:42:04 +02'00'

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

ÍNDICE

1 INTRODUCCIÓN

1. **ESET Endpoint Security 11** representa un nuevo enfoque para la seguridad del equipo plenamente integrada. La versión más reciente del motor de análisis ESET LiveGrid®, en combinación con nuestros módulos personalizados de *firewall* y *antispam* del cliente de correo electrónico, utilizan velocidad y precisión para mantener el equipo seguro. El resultado es un sistema inteligente constantemente alerta frente a los ataques y el software malicioso que pongan en peligro su equipo.
2. ESET Endpoint Security es una solución de seguridad completa producida mediante un esfuerzo de largo plazo con el fin de combinar la protección máxima con un tamaño mínimo en el sistema. Las tecnologías avanzadas, basadas en la inteligencia artificial, son capaces de eliminar proactivamente las infiltraciones de *virus*, *spyware*, *troyanos*, *gusanos*, *adware*, *rootkits* y otros ataques provenientes de Internet sin entorpecer el rendimiento del sistema ni perturbar el equipo.
3. ESET Endpoint Security está diseñado principalmente para usar en estaciones de trabajo de un entorno empresarial.

2 OBJETO Y ALCANCE

4. El presente documento tiene como objeto establecer un procedimiento detallado y seguro para el empleo del producto **ESET Endpoint Security 11** en su versión 11.0.2044.0 para todos los sistemas informáticos Windows de tipo escritorio. Este procedimiento está diseñado para garantizar el cumplimiento de los requisitos establecidos por el **Esquema Nacional de Seguridad** (**ENS**), facilitando la protección adecuada de los activos digitales y la mitigación de riesgos asociados a la ciberseguridad.

5. El alcance del documento abarca todas las fases necesarias para la instalación, configuración, operación y mantenimiento de **ESET Endpoint Security 11**, asegurando que las prácticas aquí descritas se alineen con las medidas de seguridad definidas en el **ENS**.

6. Asimismo, el documento está destinado a ser una herramienta de referencia para los responsables de seguridad, administradores de sistemas y otros agentes involucrados en la gestión de la seguridad de la información, proporcionando directrices claras y adaptadas a las normativas vigentes.

7. El producto **ESET Endpoint Security 11** ha sido cualificado en el catálogo CPSTIC para categoría ENS MEDIA en las familias “Anti-virus / EPP (Endpoint Protection Platform)”.

3 ORGANIZACIÓN DEL DOCUMENTO

8. El documento se organiza en los siguientes apartados:

   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 y activación del producto.

   c) Apartado.**6** En este apartado se recogen las tareas recomendadas para la fase de configuración segura del producto.

   d) Apartado.**7** En este apartado se recogen las tareas de operación o mantenimiento de la solución.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Antes de realizar la instalación de **ESET Endpoint Security 11**, es necesario descargar el instalador de **32** o **64 bits**, dependiendo del tipo de 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.

    - Para la opción de **32 bits**:
        - https://download.eset.com/com/eset/apps/business/ees/windows/latest/ees_nt32.msi
        - Hash (SHA256) del archivo ESET Endpoint Security: AEE9E743AE00250DB62E6E4AFB463DC9418C616F2CFC9437E4C73709AB62201F
    - Para la opción de **64 bits**:
        - https://download.eset.com/com/eset/apps/business/ees/windows/latest/ees_nt64.msi
        - Hash (SHA256) del archivo ESET Endpoint Security: F69D1AD34A9ECDB13CB8B08115EDDF6C9D5755A462D6296158B206089638D674
    - Para la opción de **64 bits ARM**:
        - https://download.eset.com/com/eset/apps/business/ees/windows/latest/ees_arm64.msi
        - Hash (SHA256) del archivo ESET Endpoint Security: 9AD530515492B2821A66B1C40344FE393CEE72CC341D056D9C3A809D7F9DD7B9

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. La solución **ESET Endpoint Security 11** no tiene que instalarse en un Centro de Proceso de Datos (CPD), por lo tanto, su acceso no está limitado a un conjunto de personas que posean una autorización expresa. Sin embargo, es fundamental garantizar la separación de roles entre administradores y usuarios regulares del equipo para minimizar riesgos de seguridad. Esto asegura que solo personal autorizado pueda realizar configuraciones críticas o gestionar políticas de seguridad, mientras que los usuarios regulares operen con privilegios limitados, reduciendo la superficie de ataque y el impacto de errores involuntarios.

4.3 REGISTRO Y LICENCIAS

11. En este apartado se indica como registrar una licencia ya adquirida en **ESET Business Account** (**EBA**), paso previo a la instalación del software: https://help.eset.com/eba/es-ES/add_license.html?add_license.html.

12. Para activar una licencia en una instalación del producto determinada, seguid las instrucciones que se encuentran en la sección 5.1 ACTIVACIÓN DEL PRODUCTO.

4.4 CONSIDERACIONES PREVIAS

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

    - El ordenador donde se vaya a instalar el antivirus NO debe tener otra solución de seguridad instalada.
    - Sistemas Operativos compatibles: Microsoft Windows 11/10.
    - 0,3 GB de memoria libre en el sistema.
    - 1 GB de espacio libre en el disco duro.
    - Conexión a Internet.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. Para la correcta instalación y puesta en funcionamiento de **ESET Endpoint Security 11**, no se requiere ningún componente adicional más allá de los elementos básicos necesarios para su ejecución.

15. En concreto, los únicos requisitos indispensables son un ordenador que cumpla con las especificaciones técnicas mínimas del software, acceso a Internet para la descarga de actualizaciones y validación de licencias, el archivo del instalador correspondiente al producto y la clave de activación proporcionada por el fabricante.

16. La ausencia de dependencia de componentes externos adicionales simplifica el proceso de implementación y garantiza la autonomía del procedimiento en entornos estándar.

5 FASE DE INSTALACIÓN

17. A continuación, se facilita la guía pública de instalación de **ESET Endpoint Security 11**: https://help.eset.com/ees/11/es-ES/installation_msi.html

18. El componente **ESET Endpoint Security 11** se instalará sobre un ordenador Windows que cumpla con los requisitos mínimos anteriormente descritos en este procedimiento.

19. A continuación, se detallan los pasos a seguir para una instalación segura de la solución de seguridad **ESET Endpoint Security 11**.

20. Descargar el instalador desde el enlace anteriormente proporcionado y ejecutarlo. Tras esto, pulsar en "*Siguiente*":

Ilustración 1. Bienvenida del asistente de instalación

21. Aparecerá el contrato de licencia de usuario final. Revise la licencia y en caso de estar de acuerdo, seleccionar la opción de "*Acepto las condiciones del acuerdo de licencia*" y pulsar en "*Siguiente*":

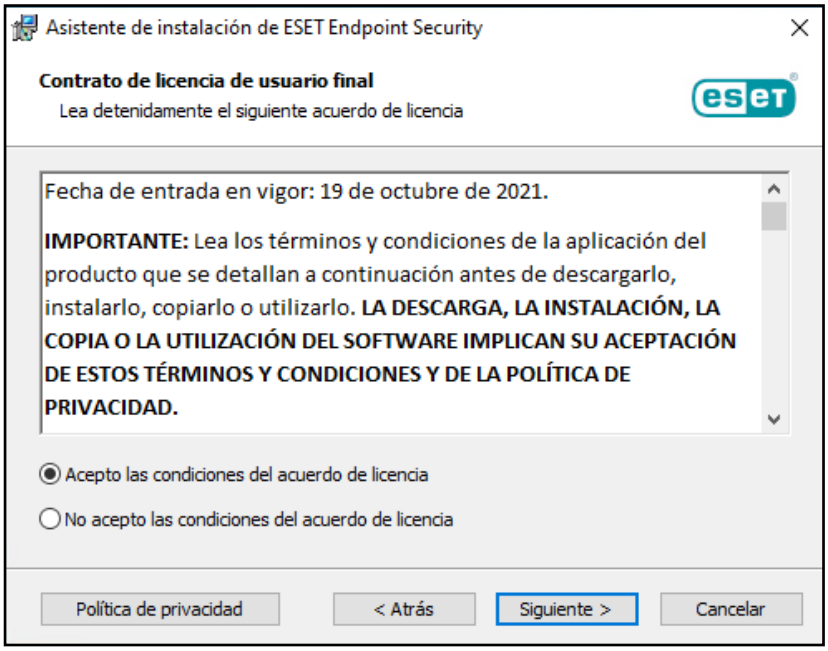

Ilustración 2. Aceptación de condiciones

22. Activar el sistema de respuesta **ESET LiveGrid** (recomendado).

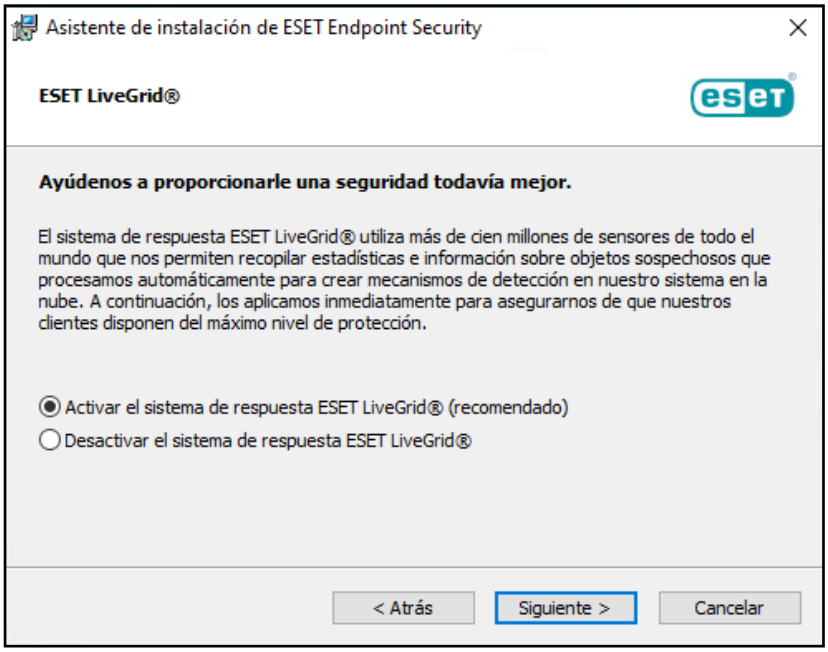

Ilustración 3. Activación ESET LiveGrid

23. Activar también las "*Aplicaciones potencialmente indeseables*" y pulsar en "*Instalar*".

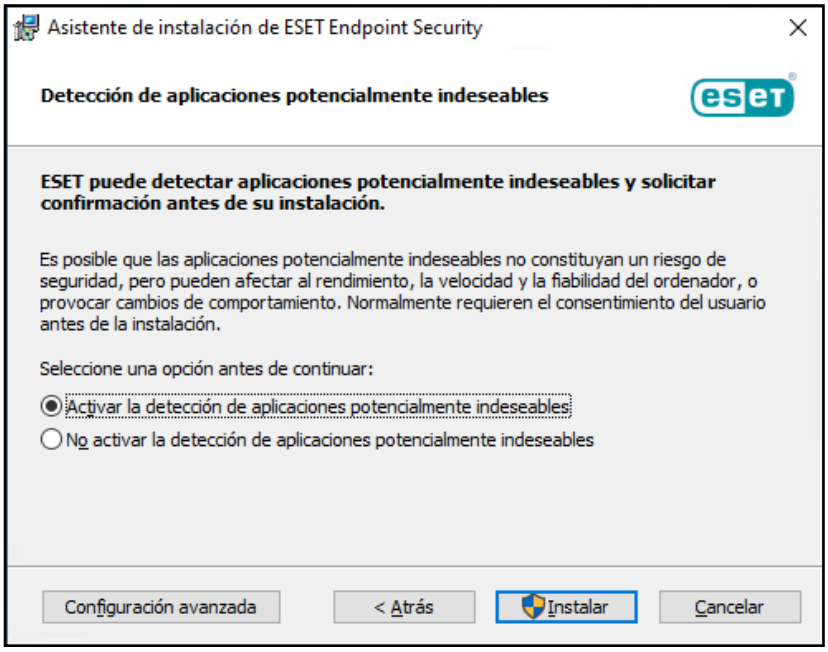

Ilustración 4. Activación de la detección de aplicaciones potencialmente indeseables

24. Esperar hasta que finalice la instalación.

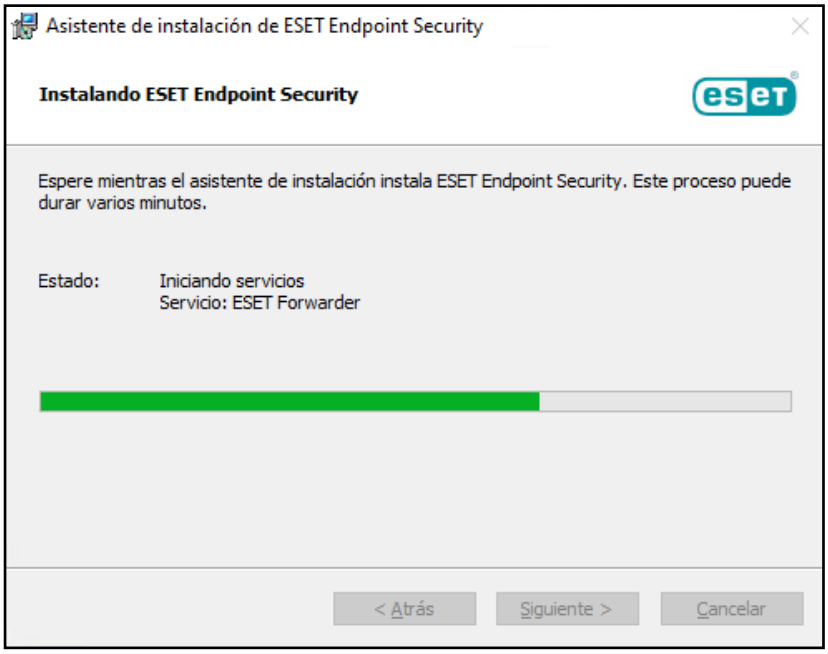

Ilustración 5. Instalación en proceso

25. Una vez finalizada la instalación pulsar en "*Finalizar*" y pasar al siguiente procedimiento que es activar el antivirus con la licencia adquirida.

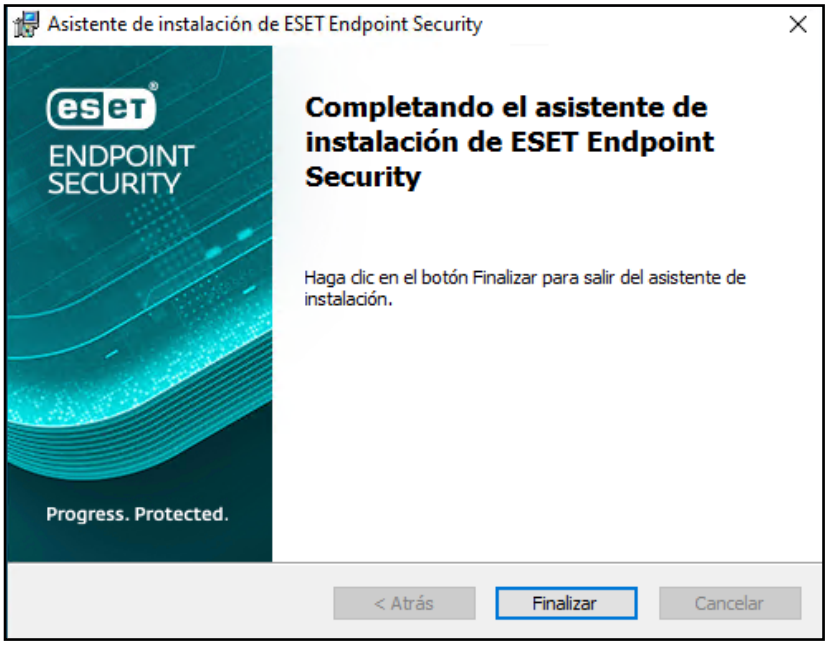

Ilustración 6. Finalización de la instalación

5.1 ACTIVACIÓN DEL PRODUCTO

26. Una vez finalizada la fase de instalación es necesario activar el producto de seguridad con una clave de activación válida.

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

Ilustración 7. Opciones de activación

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

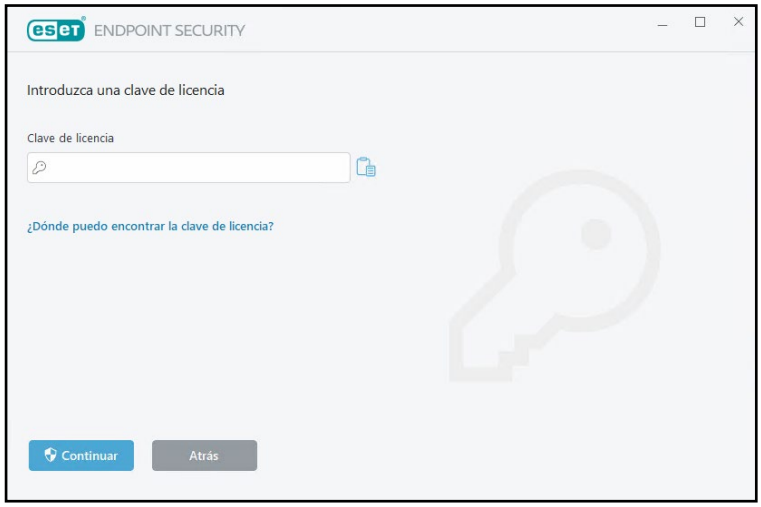

Ilustración 8. Introducción de clave de licencia

29. Una vez activado, aparecerá el siguiente mensaje:

Ilustración 9. Activación realizada correctamente

30. Posteriormente, el producto ya está activado:

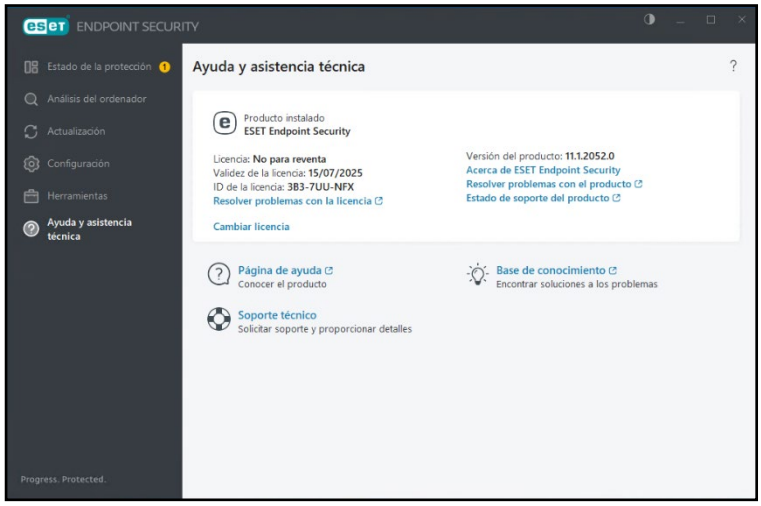

Ilustración 10. Producto activado

31. 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.

6 FASE DE CONFIGURACIÓN

32. En este apartado se indica la configuración de seguridad a aplicar sobre la solución **ESET Endpoint Security 11**.

33. La ventana principal del programa **ESET Endpoint Security** 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.

34. 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 Security**.
    - **Análisis del ordenador**: esta opción 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**: apartado para ajustar la configuración de seguridad de cada uno de los motores del antivirus.
    - **Herramientas**: proporciona acceso a "*Archivos de registro*", "*Estadísticas de protección*", "*Observar actividad*", "*Procesos en ejecución*", "*Planificador de tareas*", "*Cuarentena*" y "*ESET SysInspector*". También da la opción de 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.

35. 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.

36. En la ventana de estado también se proporcionan enlaces rápidos a las características más habituales de **ESET Endpoint Security** e información sobre la última actualización.

6.1 HABILITAR CORTAFUEGOS

37. Lo primero que se debe realizar al instalar **ESET Endpoint Security 11** es habilitar el cortafuegos. Para ello, hay que pulsar en "*Activar cortafuegos*" dentro del menú "Estado de la protección".

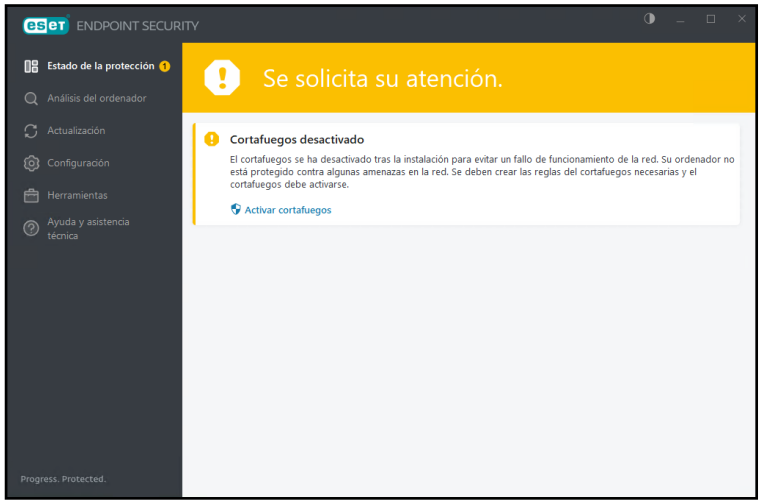

Ilustración 11. Habilitar cortafuegos

38. Una vez habilitado, el estado de protección cambia a color "*verde*".

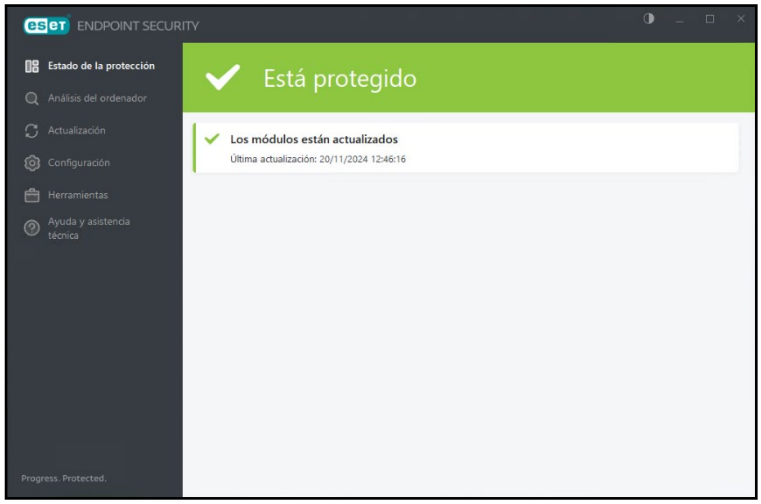

Ilustración 12. Módulos activados

6.2 CONFIGURACIÓN DE LA PROTECCIÓN

39. 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.
    - Aplicaciones Potencialmente peligrosas.
    - Aplicaciones sospechosas.

40. 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).

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

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

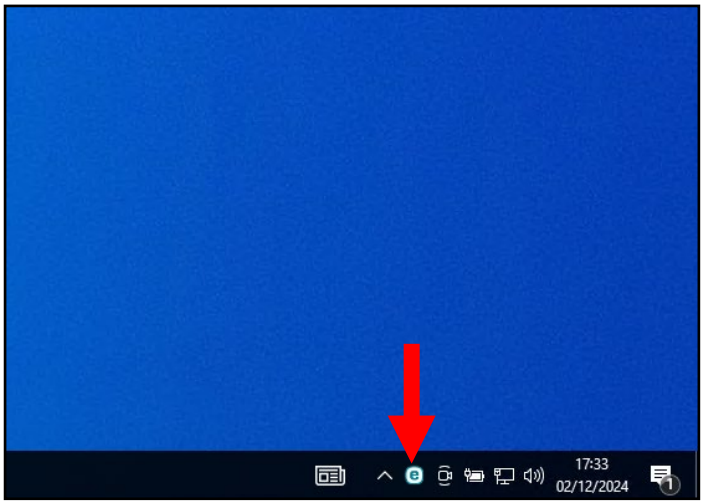

Ilustración 13. Acceder a ESET Endpoint Security

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

44. Acceder al apartado de "*Protecciones*" y configurar el apartado de "*Respuestas de detección*", categoría "*Aplicaciones potencialmente indeseables*" como "*Equilibrado*". De esta forma, se obtiene la mejor configuración entre rendimiento y protección.

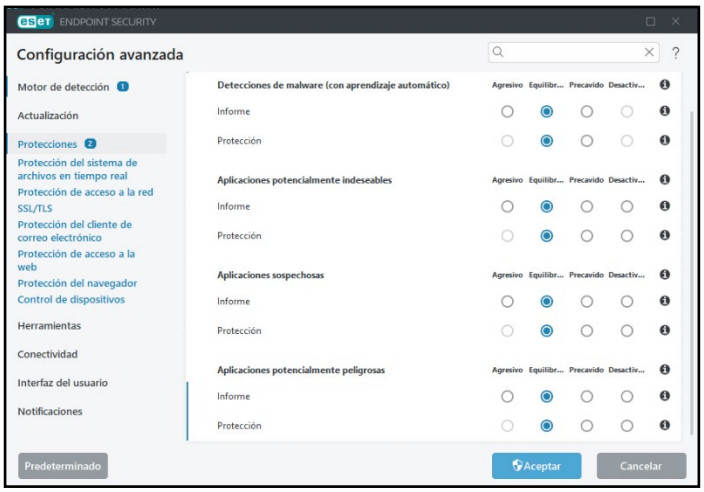

Ilustración 14. Opciones de configuración del motor de protección

45. 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.

46. 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 se aconseja que el umbral seleccionado sea el "*Equilibrado*". Los ajustes de informes no influyen en la acción de bloquear, desinfectar o eliminar objetos.

47. 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

48. 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.

49. 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 los niveles de protección

6.3 CONFIGURACIÓN PROTECCIÓN EN TIEMPO REAL

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

Umbral	Explicación
Reparar la detección siempre	Intentar corregir la detección durante la desinfección de objetos sin la intervención del usuario final. En algunos casos raros (por ejemplo, archivos del sistema), si no se puede corregir la detección, el objeto del que se informa se deja en su ubicación original. Corregir siempre las detecciones es el ajuste predeterminado recomendado en entornos administrados
Reparar la detección si es seguro, mantener de otro modo	Intentar corregir la detección 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 detección no se puede corregir, el objeto del que se informa se deja en su ubicación original
Reparar la detección si es seguro, preguntar de otro modo	Intentar corregir la detección 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 de corrección (por ejemplo, eliminar o ignorar). Este ajuste se recomienda en la mayoría de los casos
Preguntar siempre al usuario final	El usuario final recibe una ventana interactiva durante la desinfección de objetos y debe seleccionar una acción correctiva (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 reparación

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

52. Para configurar el nivel de desinfección, acceder al apartado de "*Protecciones*", "*Protección del sistema de archivos en tiempo real*". Abrir el subapartado de "*Parámetros de "ThreatSense*" y modificar el parámetro de "*Nivel de Desinfección*" a "*Reparar la detección siempre*".

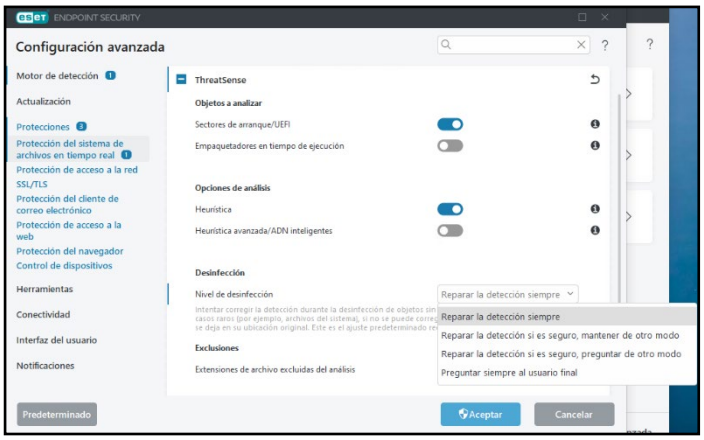

Ilustración 15. Opciones de configuración del motor de desinfección

6.4 CONFIGURACIÓN DEL ANÁLISIS DE MALWARE

6.4.1 ANÁLISIS EN ESTADO INACTIVO

53. 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.

54. Para configurarlo hay que abrir **ESET Endpoint Security** y pulsar el botón F5 para acceder a la configuración avanzada.

55. 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.

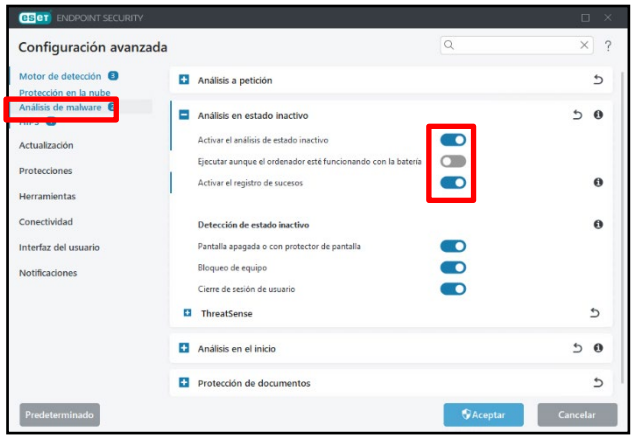

Ilustración 16. Configuración análisis en estado inactivo

6.4.2 ANÁLISIS A PETICIÓN DEL USUARIO

56. 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 el 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.

57. **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.

58. Lo primero, abrir **ESET Endpoint Security** pulsando en el icono que aparece bajo a la derecha, al lado del reloj de Windows.

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

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

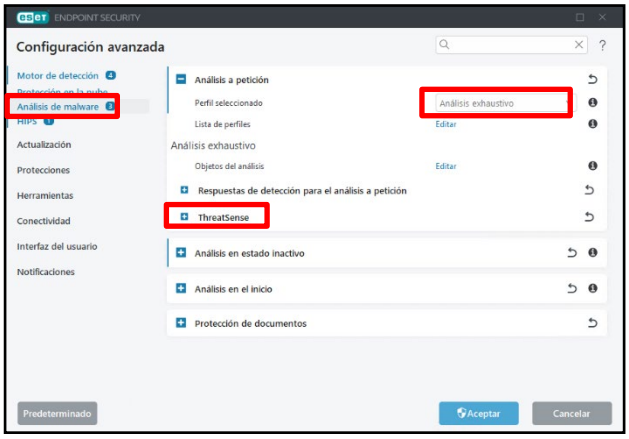

Ilustración 17. Configuración perfil de análisis bajo demanda

61. Cambiar el valor de "*Nivel de desinfección*" a "*Reparar la detección siempre*" para que el antivirus elimine automáticamente cualquier tipo de malware que detecte.

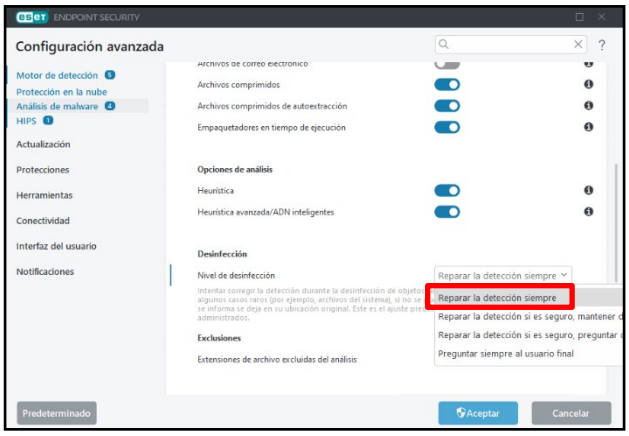

Ilustración 18. Configuración nivel de reparación

6.5 CONFIGURACIÓN DE LA AUTENTICACIÓN

62. **ESET Endpoint Security 11** se autentica durante el proceso de activación del producto, el cual se realiza mediante una clave de activación proporcionada al usuario al adquirir la licencia. Este método asegura que solo los usuarios con licencias válidas puedan activar y utilizar el software, garantizando la legitimidad y el acceso autorizado al producto. Una vez introducida la clave de activación, el sistema verifica la validez de la licencia y habilita las funcionalidades correspondientes del producto. Cabe destacar que únicamente los usuarios con privilegios de administrador en la máquina tienen la capacidad de acceder y modificar las configuraciones del producto, reforzando la seguridad del sistema y asegurando que los ajustes críticos solo puedan ser gestionados por personal autorizado. Esta autenticación inicial es esencial para proteger la integridad del sistema y asegurar el cumplimiento de las políticas de licenciamiento.

6.6 CONFIGURACIÓN DE LA ADMINISTRACIÓN DEL PRODUCTO

63. **ESET Endpoint Security 11** ofrece diversas opciones para su administración, tanto de forma local como remota.

6.6.1 ADMINISTRACIÓN LOCAL

64. **Interfaz gráfica de usuario (GUI):** Se puede gestionar **ESET Endpoint Security** directamente en cada equipo mediante su interfaz gráfica, accediendo a la configuración y realizando tareas de mantenimiento. No requiere protocolos de comunicación externos.

65. **ESET RMM (ERMM) - Interfaz de línea de comandos (CLI)**: **ESET Endpoint Security** proporciona la utilidad ermm.exe, ubicada en el directorio de instalación (por defecto, *C:\Program Files\ESET\ESET Security\ermm.exe*). Esta herramienta permite la administración del producto a través de comandos, facilitando la automatización de tareas y la integración con scripts. Esta interacción es interna y no depende de protocolos de red.

6.6.2 ADMINISTRACIÓN REMOTA

66. **ESET PROTECT (EP)**: Es la solución centralizada de ESET para la gestión remota de sus productos. A través de **ESET PROTECT**, se administran tareas, políticas de seguridad, se supervisa el estado del sistema y se responde rápidamente a problemas o amenazas en equipos remotos desde una ubicación central. Los certificados y las autoridades de certificación de los agentes usan *SHA-256*. El servidor de **ESET PROTECT** usa ***TLS 1.3 o 1.2*** para la comunicación con agentes.

67. **Supervisión y administración remotas (RMM)**: **ESET Endpoint Security**, a través del complemento ERMM es compatible con herramientas de RMM, permitiendo la supervisión y control de sistemas mediante un agente instalado localmente. Para activar esta función, se debe acceder a la configuración avanzada del producto, "*Herramientas avanzadas*", "*ESET RMM*" y activar la opción correspondiente. **La comunicación entre estos componentes utiliza protocolos estándar como HTTPS**.

6.6.3 CONFIGURACIÓN DE ACCESO ADMINISTRADORES

68. Para ofrecer la máxima seguridad al 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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

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

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

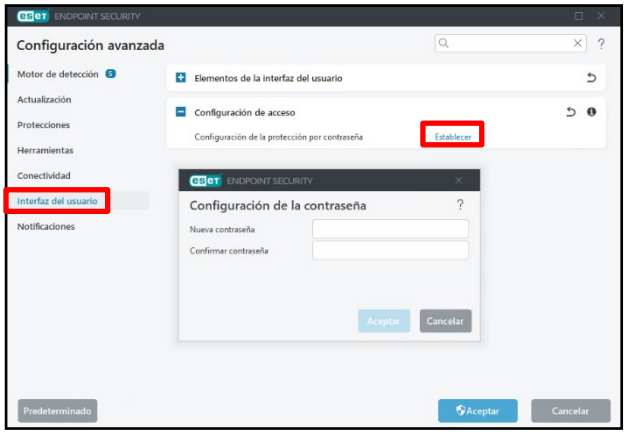

Ilustración 19. Configuración de la contraseña de administrador

6.7 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

71. Las opciones de configuración de la interfaz de usuario (*GUI*) de **ESET Endpoint Security** permiten ajustar el entorno de trabajo según las necesidades del usuario. 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 Security**.

72. En la sección "*Elementos de la interfaz del usuario*" se puede ajustar el entorno de trabajo. Se debe usar 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 se necesita conservar los recursos del sistema. El modo silencioso solo lo puede iniciar el administrador.

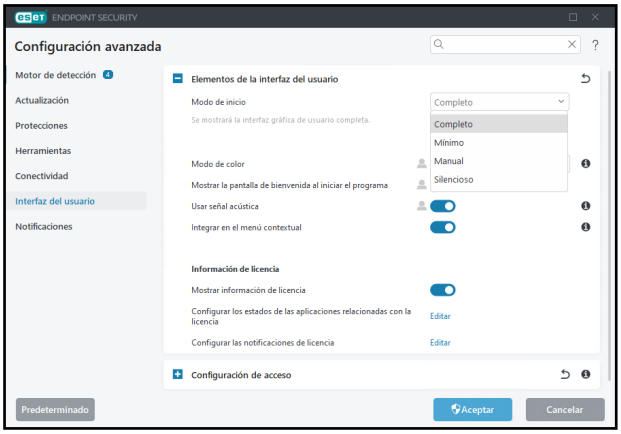

Ilustración 20. Configuración de la interfaz del usuario

73. Si se desea desactivar la pantalla inicial de **ESET Endpoint Security**, se debe anular la selección de "*Mostrar pantalla inicial con la carga del sistema*".

74. Si se desea que **ESET Endpoint Security** reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo, al detectar una amenaza o al finalizar el análisis, se debe seleccionar "*Usar señal acústica*".

75. **Integrar en el menú contextual**: integra los elementos de control de **ESET Endpoint Security** en el menú contextual.

6.8 GESTIÓN DE CERTIFICADOS

76. **ESET Endpoint Security 11** no requiere certificados. Este punto no aplica.

6.9 SERVIDORES DE AUTENTICACIÓN

77. **ESET Endpoint Security 11** no requiere de servidores externos de autenticación. Este punto no aplica.

6.10 SINCRONIZACIÓN

78. **ESET Endpoint Security 11** no realiza sincronización segura del producto y sus componentes. Este punto no aplica.

6.11 CONFIGURACIÓN DE LAS ACTUALIZACIONES

79. 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 y en la mayoría de los casos no es necesario realizar ninguna configuración adicional para que el producto se actualice automáticamente.**

80. Asimismo, puede haber casos donde el ordenador no tenga acceso directo a Internet, o tenga una conexión limitada, y por ello se requiere que el antivirus vaya a descargar las actualizaciones a través de un proxy HTTP o un servidor.

81. Para acceder a las opciones de configuración la actualización, se tiene que acceder a la "*Configuración avanzada*", "*Actualización*", "*Perfiles*", "*Actualizaciones*", "*Opciones de conexión*."

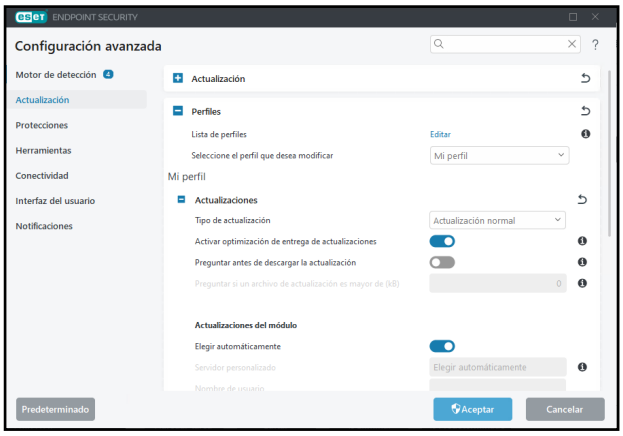

Ilustración 21. Configuración de la conexión

6.11.1 CONFIGURACIÓN PROXY

82. Para modificar la parte del proxy, hay que pulsar en el menú desplegable "M*odo proxy*" y seleccionar una de las tres opciones siguientes:

    - No usar servidor Proxy
    - Conexión a través de un servidor Proxy específico
    - Utilizar la configuración predeterminada

83. Seleccionar "*Usar la configuración global del servidor proxy*" para utilizar la configuración del servidor proxy ya especificada en la sección "*Configuración avanzada*", "*Conectividad*", "*Servidor proxy*".

84. Seleccionar "*No usar servidor Proxy*" para especificar que no se utilice ningún servidor Proxy para actualizar **ESET Endpoint Security.**

85. La opción "Conexión a través de un servidor proxy" debe seleccionarse si:

    - Se utiliza un servidor proxy distinto del definido en "*Herramientas*", "*Servidor proxy*" para actualizar **ESET Endpoint Security**. En esta configuración, la información del nuevo proxy se debe especificar en "*Servidor proxy*": *dirección*, *Puerto de comunicación* (*3128* de forma predeterminada), *Nombre de usuario* y *Contraseña del servidor proxy*, en caso de ser necesarios.
    - La configuración del servidor proxy no se ha definido globalmente, pero **ESET Endpoint Security** se conecta a un servidor proxy para las actualizaciones.
    - El ordenador se conecta a Internet mediante un servidor proxy. La configuración se obtiene de navegador durante la instalación del programa; no obstante, si se modifica (por ejemplo, al cambiar de proveedor de Internet), hay que asegurarse de que la configuración del servidor proxy que aparece en esta ventana es la correcta. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

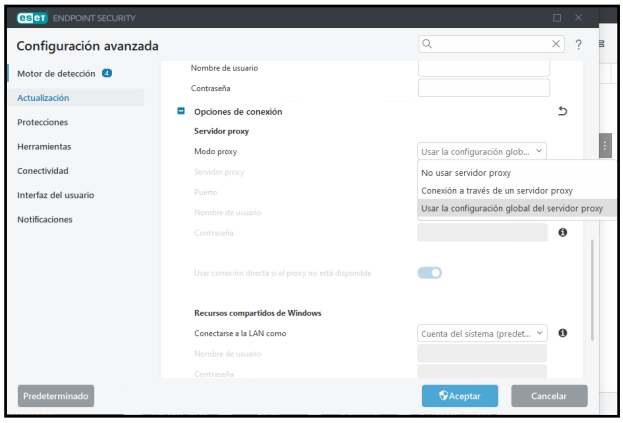

Ilustración 22. Configuración del proxy

86. La configuración predeterminada del servidor Proxy es "*Usar la configuración global del servidor proxy*".

6.11.2 CONFIGURACIÓN SERVIDOR LOCAL

87. Para realizar una actualización desde un servidor local con una versión del sistema operativo Windows NT, es necesario autenticar todas las conexiones de red de forma predeterminada.

88. Para configurar una cuenta de este tipo, seleccione en el menú desplegable Conectarse a la LAN como:

    - Cuenta del sistema (predeterminado)
    - Usuario actual
    - Usuario especificado

89. Seleccionar "*Cuenta de sistema (predeterminado)*" para utilizar la cuenta del sistema para la autenticación. Normalmente, no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.

90. Para garantizar que el programa se autentique con la cuenta de un usuario registrado actualmente, seleccionar "*Usuario actual*". El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.

91. Seleccionar "*Especificar usuario*" si se desea que el programa utilice una cuenta de usuario específica para la autenticación. Se debe usar este método cuando falle la conexión predeterminada con la cuenta del sistema. La cuenta del usuario especificado debe tener acceso al directorio de archivos actualizados del servidor local. De lo contrario, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

92. Los campos "*Nombre de usuario*" y "*Contraseña*" son opcionales.

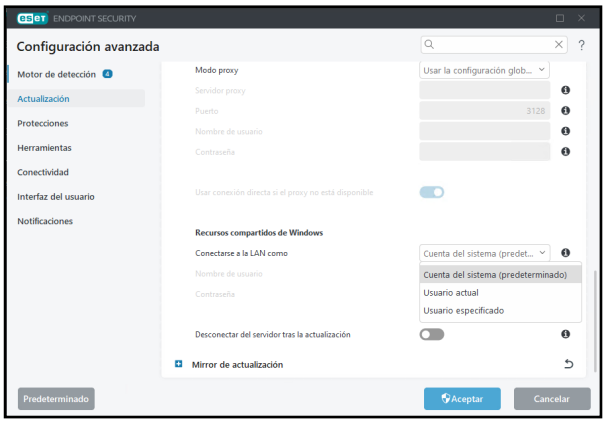

Ilustración 23. Configuración del proxy

6.12 AUTO-CHEQUEOS

93. **ESET Endpoint Security 11** realiza auto-chequeos de integridad tanto al inicio del sistema como bajo demanda del administrador. Estos auto-chequeos verifican la integridad de los módulos del programa y la correcta operación de los algoritmos y funciones de los motores. Al iniciarse el sistema, el software ejecuta una serie de comprobaciones para asegurar que todos los componentes esenciales están intactos y operativos. Además, el

administrador puede iniciar manualmente estos chequeos a través de la interfaz del programa o mediante herramientas de administración remota como **ESET PROTECT**.

94. En caso de que se detecte una falla durante un auto-chequeo, **ESET Endpoint Security 11** notifica al usuario o al administrador sobre el problema identificado. Esta notificación aparece y queda registrada en la propia interfaz gráfica del antivirus como un registro en el apartado de "Herramientas", "Archivos de registro", "Visor de Eventos" o como alerta interactiva del escritorio (ventana emergente en el escritorio). Dependiendo de la gravedad de la falla, el software puede intentar una reparación automática o solicitar la intervención del usuario para resolver el problema. Es fundamental atender estas notificaciones de inmediato para mantener la eficacia de la protección del sistema.

6.13 ALTA DISPONIBILIDAD

95. **ESET Endpoint Security 11** no dispone de opciones de alta disponibilidad del producto. Este punto no aplica.

6.14 AUDITORÍA

6.14.1 REGISTRO DE EVENTOS

96. El registro de auditoría de **ESET Endpoint Security** 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.

97. Al pulsar con el botón derecho del ratón sobre cualquier tipo de registro de la auditoría y seleccionar "*Mostrar*" aparecerá la información detallada sobre el cambio realizado. Además, se puede restaurar el cambio del ajuste al hacer clic en "*Restaurar*" desde el menú contextual. Al pulsar "*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*.

98. 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.

99. Si la opción "*Eliminar automáticamente los registros con una antigüedad de más de (días)*" está activada, las entradas del registro que tengan una antigüedad superior al número de días especificado se eliminarán automáticamente.

100. Los registros se pueden exportar en formato **.xml o .txt**

6.14.2 ALMACENAMIENTO LOCAL

101. **ESET Endpoint Security 11** almacena localmente todos los registros generados por la herramienta, desde la anteriormente mencionada *auditoría* (para proporcionar un historial detallado de los cambios en la configuración y el estado de protección del sistema), *como registros de eventos, amenazas detectadas, detecciones de HIPS, análisis del ordenador, archivos enviados a la nube de ESET, protección del navegador, protección de la red, sitios web filtrados, antispam del cliente de correo, control de acceso web,*

control de dispositivos y la administración y revisión de parches de seguridad y vulnerabilidades.

102. Para acceder a los registros hay que abrir la ventana principal de **ESET Endpoint Security**, acceder al apartado "*Herramientas*", "*Archivos de Registro*".

103. **ESET Endpoint Security** también permite configurar cómo se gestionan estos registros:

- **Nivel mínimo de detalle al registrar**: Permite especificar el nivel de detalle de los eventos que se registrarán, desde errores críticos hasta información de diagnóstico detallada.
- **Eliminar automáticamente los registros con una antigüedad de más de (días)**: Define el período tras el cual los registros antiguos se eliminarán automáticamente para ahorrar espacio en el disco duro.
- **Optimizar archivos de registro automáticamente**: Si está activada, **ESET Endpoint Security** desfragmentará automáticamente los archivos de registro cuando el porcentaje de fragmentación supere un valor especificado, mejorando así el rendimiento y la velocidad de procesamiento de los registros.

6.14.3 ALMACENAMIENTO REMOTO

104. **ESET Endpoint Security 11** almacena todos los datos y registros en local, no en remoto. Este punto no aplica.

6.15 BACKUP

105. **ESET Endpoint Security 11** no requiere o tiene la capacidad de realizar backup de sus datos o componentes. Este punto no aplica.

7 MODO DE OPERACIÓN SEGURO

106. En este apartado se indican algunas de las operaciones o mantenimiento más importantes a realizar para mantener una protección segura con **ESET Endpoint Security 11**.

7.1 REALIZAR UN ANÁLISIS A PETICIÓN DEL USUARIO

107. 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.

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

109. Ahora, pulsar en "*Análisis personalizado*".

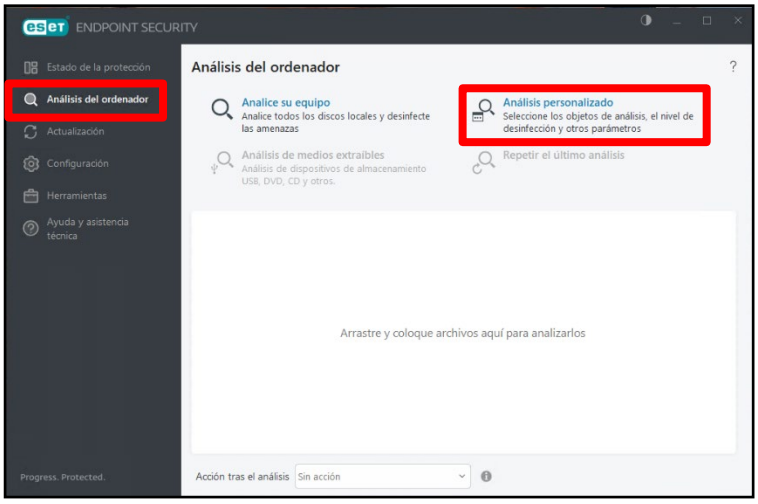

Ilustración 24. Realizar un análisis del sistema

110. Marcar "Este equipo" y cambiar la opción de "Perfil" por "Análisis exhaustivo" y pulsar "Analizar como administrador".

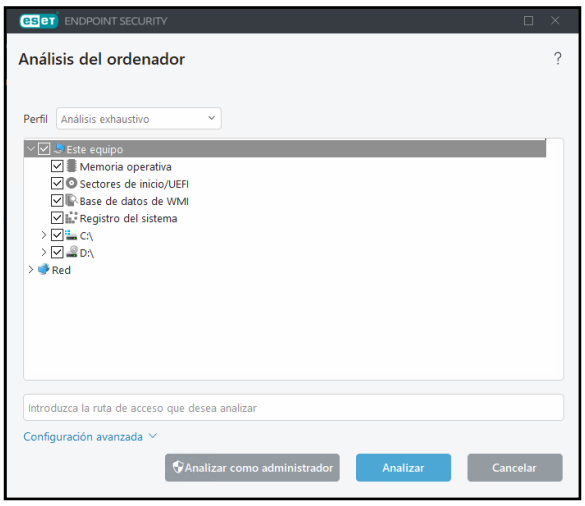

Ilustración 25. Realizar un análisis del sistema

7.2 COMPROBAR EL ESTADO DE LOS MÓDULOS Y FORZAR ACTUALIZACIÓN

111. Tras la instalación, **ESET Endpoint Security** tiene activadas de forma predeterminada las actualizaciones, tanto de los motores como de los módulos. De todas formas, es recomendable comprobar el estado de actualización de los módulos y el producto para obtener la máxima protección en el sistema. En este enlace, se indica los pasos a seguir para actualizar **ESET Endpoint Security 11**: https://help.eset.com/ees/11/es-ES/idh_page_update.html

112. Para ello, se debe acceder al apartado "Actualización" en la parte izquierda de la ventana.

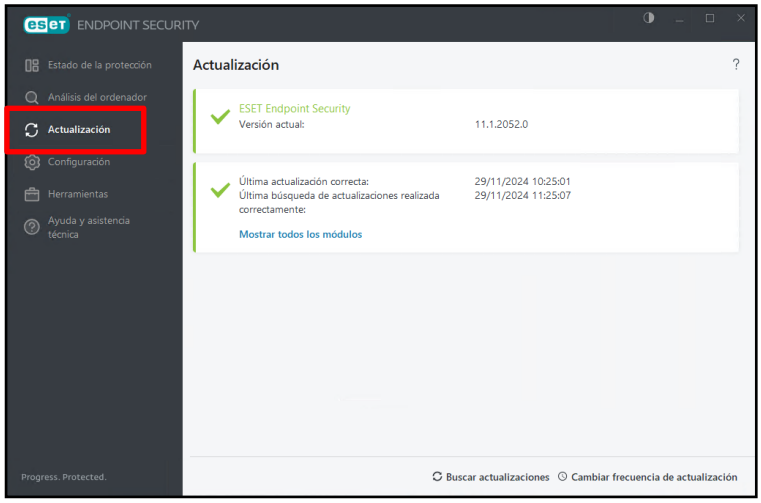

Ilustración 26. Consulta del estado de actualización del producto

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

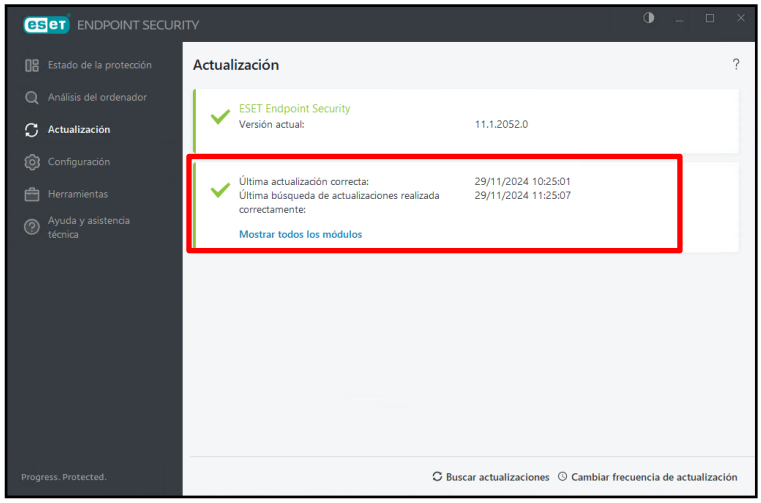

Ilustración 27. Última actualización del producto

114. 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.

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

116. 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.

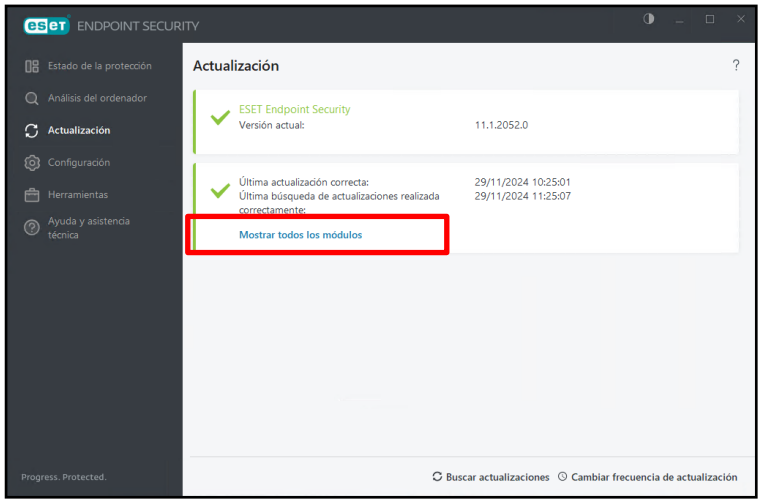

Ilustración 28. Opción para visualizar en detalle los módulos

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

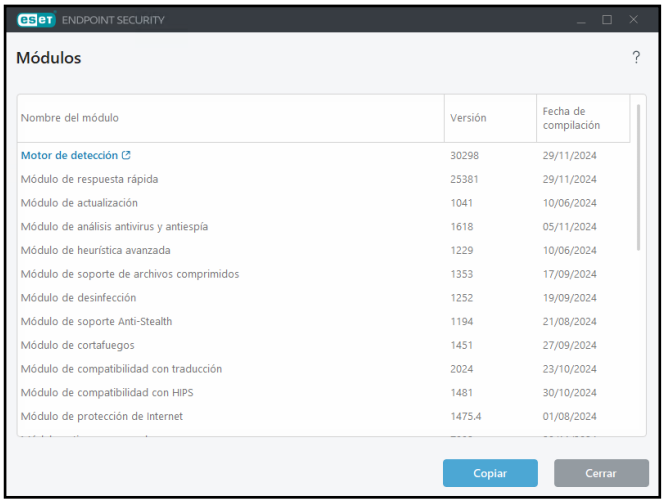

Ilustración 29. Consulta de fechas de actualización de los distintos módulos

118. Para comprobar si los módulos del antivirus están actualizados se debe analizar la línea que incluye "*Motor de detección*". En la Ilustración 29, aparecen los valores *30298* y la fecha de compilación *(29/11/2024).*

119. El valor entre paréntesis corresponde con la fecha de actualización de los módulos en formato: *dd/mm/aaaa.*

120. Si por algún caso puntual es necesario forzar la actualización de módulos manualmente, tan solo se tiene que pulsar en "*Buscar actualizaciones*" en la ventana principal de la "*Actualización*":

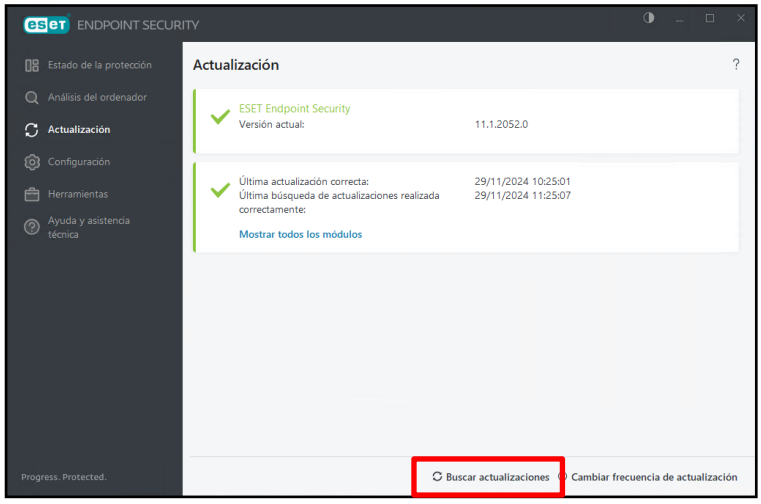

Ilustración 30. Buscar actualizaciones

7.3 PLANIFICADOR DE TAREAS

121. 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*".

122. 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.

123. 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*. Se pueden agregar o eliminar tareas directamente desde la ventana "*Planificador de tareas*" (pulsar en "*Agregar tarea*" o "*Eliminar*" en la parte inferior). Al pulsar con el botón derecho en cualquier parte de la ventana planificador de tareas se realizan las siguientes acciones: *mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente*.

124. 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)

125. Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), se debe pulsar con el botón derecho del ratón en la tarea y, a continuación, en "*Modificar*"", o seleccionar la tarea que se desea modificar y hacer clic en el botón "*Modificar*".

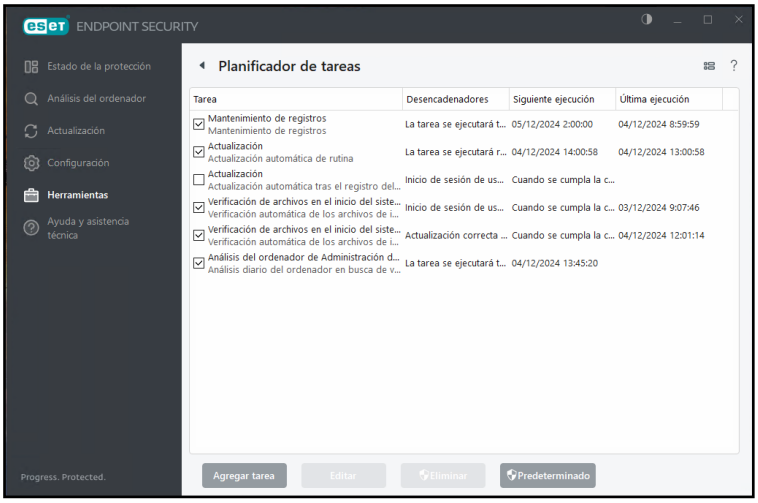

Ilustración 31. Ventana principal de la actualización

7.3.1 AGREGAR UNA NUVEA TAREA

126. Para agregar una tarea nueva, hay que pulsar en "*Agregar tarea*", en la parte inferior de la ventana.

127. Introducir un nombre para la tarea.

128. 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

129. Activar la opción "*Activado*" si se desea activar la tarea (se puede hacer 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.

130. 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, se 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).

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

Ilustración 32. Detalles de la tarea

7.4 INFORMACIÓN DE LA LICENCIA

132. En este apartado se indica cómo consultar el período vigente de la licencia.

133. Primero, abrir la ventana de ESET y acceder al apartado de "*Ayuda y asistencia técnica*".

134. En este apartado aparecen los datos del identificador de la licencia, la fecha de validez de la licencia y también otros datos interesantes como la versión del producto instalado y la fecha del soporte vigente para esa versión en concreto del producto.

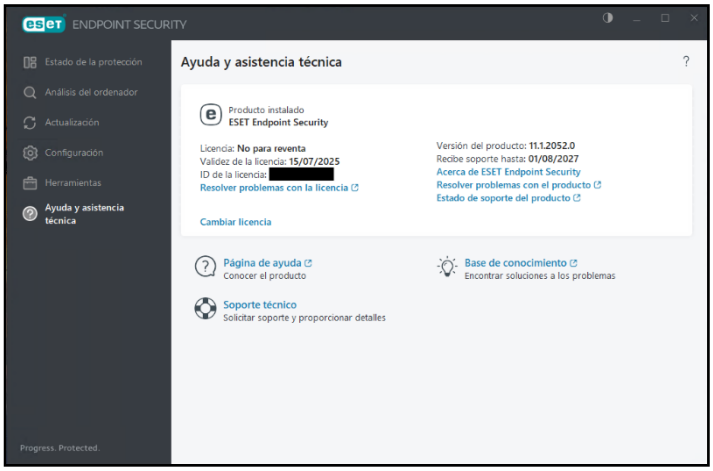

Ilustración 33. Información licencia

8 REFERENCIAS

[REF1] Guía general de la solución ESET Endpoint Security.
https://help.eset.com/ees/11/es-ES/

[REF2] Ficha del producto ESET Endpoint Security.
https://www.eset.com/fileadmin/ESET/ES/Productos/Empresas/Endpoint/ESET_Endpoint_Security_overview_esp.pdf

[REF3] Base de conocimiento de productos de empresa
https://support.eset.com/es/business

9 ABREVIATURAS

CLI	Command Line Interface / Interfaz de línea de comandos
CPD	Centro de Proceso de Datos
CPSTIC	Catálogo de Productos de Seguridad TIC
EBA	ESET Business Account
EES	ESET Endpoint Security
ENS	Esquema Nacional de Seguridad
EP	ESET PROTECT
EPP	Endpoint Protection Platform
ERMM	ESET Remote Monitoring and Management
ESET	Essential Security against Evolving Threats
GUI	Graphical User Interface / Interfaz gráfica de usuario
HIPS	Host-based Intrusion Prevention System
NT	New Technology (used in Windows NT, an operating system family)
RMM	Remote Monitoring and Management / Supervisión y Administración Remotas
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL