

ESET Mobile Security

Manual de usuario

[Haga clic aquí para ver la versión de la Ayuda de este documento](#)

Copyright ©2024 de ESET, spol. s r.o.

ESET Mobile Security está desarrollado por ESET, spol. s r.o.

Para obtener más información, visite <https://www.eset.com>.

Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación ni transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la autorización por escrito del autor.

ESET, spol. s r.o. se reserva el derecho de modificar cualquier parte del software de aplicación descrito sin previo aviso.

Soporte técnico: <https://support.eset.com>

REV. 12/04/2024

1	Introducción	1
1.1	Novedades	1
1.2	Requisitos mínimos del sistema	1
2	Instalación	2
3	Asistente de inicio	3
4	Funciones de las licencias gratuita y versión Premium	5
5	Activación	6
6	Desinstalación	8
7	Conexión a ESET HOME	9
8	Antivirus	11
8.1	Registros de análisis	14
8.2	Configuración avanzada	14
8.3	Adware Detector	16
9	Informe de seguridad	16
10	Registro de actividad	18
11	Antirrobo	19
11.1	Configuración de Antirrobo	20
11.2	Optimización	21
11.3	Portal web	22
11.4	ESET HOME contraseña	22
12	Antiphishing	23
12.1	Protección de SMS y Protección de notificaciones	25
13	Bloqueo de aplicación	26
13.1	He olvidado mi código PIN de bloqueo de aplicación	27
14	Protección de pagos	28
15	Filtro de llamadas	29
15.1	Agregar una nueva regla	30
16	Inspector de red	31
17	Auditoría de seguridad	32
17.1	Supervisión de dispositivo	32
17.2	Auditoría de aplicación	33
18	Códigos de referencia	33
18.1	Recomendar a un amigo	33
18.2	Canjear código	34
19	Configuración	34
20	Atención al cliente	35
21	Acuerdo de licencia para el usuario final	36
22	Política de privacidad	44

Introducción

ESET Mobile Security es una solución de seguridad completa que protege su dispositivo contra amenazas emergentes y páginas objeto de phishing, y le permite controlar su dispositivo de manera remota en caso de pérdida o robo.

Entre sus principales funciones se incluyen:

- [Antivirus](#)
- [Antirrobo](#)
- [Anti-Phishing](#)
- [Integración con el portal ESET HOME](#)
- [Filtro de llamadas](#)
- [Auditoría de seguridad](#)
- [Informe de seguridad](#)
- [Inspector de red](#)
- [Bloqueo de aplicación](#)
- [Protección de pagos](#)

Novedades

Nuevas funciones de la versión 8 de ESET Mobile Security:

Añadidos


- Compatibilidad con Android 14
- [Antismishing \(Protección de SMS y Protección de notificaciones\)](#)
- [Uso de comodines en el filtro de llamadas](#)

Mejorado

- Nuevo diseño de la pantalla de inicio
- Nuevo diseño del menú principal

Requisitos mínimos del sistema

Para poder instalar ESET Mobile Security, su dispositivo Android debe cumplir con los siguientes requisitos mínimos del sistema:

- Sistema operativo:  Android 6 (Marshmallow) o posterior
- Resolución de la pantalla táctil: 240 × 320 píxeles mínimo
- CPU: más de 500 MHz ARM7+
- RAM: Más de 512 MB
- Conexión a Internet

Exclusiones de soporte

- No es compatible con dispositivos con doble SIM o acceso raíz. Las funciones Antirrobo y Filtro de llamadas no están disponibles en tabletas que no permiten realizar llamadas ni enviar mensajes.
- Android Go no admitido
- ESET Mobile Security requiere que los servicios de Google Play funcionen correctamente. ESET Mobile Security no es compatible con dispositivos sin servicios de Google Play, como algunos dispositivos Huawei.
- La función de Antirrobo Tarjetas SIM de confianza no está disponible en los dispositivos CDMA.
- La funcionalidad de algunas funciones depende de la versión del sistema operativo.

Instalación

Hay tres formas de instalar ESET Mobile Security:

1. **Google Play Store:** abra la aplicación Google Play Store en su dispositivo Android y busque ESET Mobile Security (o simplemente ESET).



2. **Código QR:** escanee el código QR que aparece a continuación con su dispositivo móvil y una aplicación de escaneo de códigos QR.



3. **Desde la cuenta ESET HOME:** en su ESET HOME, descargue el instalador de ESET Mobile Security en su dispositivo o envíe el instalador a otro dispositivo.

Nota

-  Si desea instrucciones visuales, visite nuestra [guía de instalación paso a paso](#) (este artículo no está disponible en todos los idiomas).

Tras la instalación de ESET Mobile Security, pulse **Abrir** para iniciar el [asistente de inicio](#).

Para proteger su información personal y los recursos de su dispositivo Android, ESET Mobile Security necesitará acceso a las funciones de su dispositivo y, en algunos casos, tendrá que controlarlas. Para obtener una explicación detallada de cada tipo de permiso y de cómo se utiliza, consulte la tabla de este [artículo de la base de conocimiento](#) (el artículo no está disponible en todos los idiomas).

Asistente de inicio

Tras la instalación, siga los mensajes que aparecen en la pantalla del asistente de inicio:

Activar permisos para ESET Mobile Security




Esta guía se basa en la configuración básica de Android. El proceso de activación de permisos puede variar en función del fabricante del dispositivo.

1. Pulse **País** y seleccione el país correspondiente.
 2. Pulse **Idioma** y seleccione el idioma correspondiente.
 3. Pulse **Siguiente** y acepte el [Acuerdo de licencia para el usuario final](#) y la [Política de privacidad](#).
 4. Si corresponde, permita las siguientes opciones y pulse **Siguiente**.
 - **Permitir ESET LiveGrid®**: para obtener más información sobre el sistema de respuesta ESET LiveGrid®, [visite la sección Configuración avanzada](#).
 - **Permitir que los análisis nos ayuden a mejorar nuestros productos**: ESET Mobile Security enviará información anónima sobre la aplicación (rendimiento, estadísticas operativas) que nos ayudará a mejorar nuestra aplicación y nuestros servicios. Para obtener más información sobre la información que recopilamos, visite el [capítulo Política de privacidad](#).
 - **Permitir el uso de datos con fines de marketing**
 - **Permitir que ESET envíe descuentos promocionales y noticias sobre productos**: se mostrarán en el producto noticias y las ofertas más recientes de ESET.
 5. Revise sus datos de activación cuando haya instalado ESET Mobile Security desde el vínculo de descarga enviado a su dirección de correo electrónico [desde la cuenta ESET HOME](#). Pulse **Continuar** y [siga las instrucciones de activación de ESET Mobile Security con la cuenta ESET HOME](#). Si no acepta, pulse **No acepto** y siga los pasos que se indican a continuación.
 6. Inicie sesión en su cuenta ESET HOME para conectar su dispositivo móvil a su cuenta y activar ESET Mobile Security.
- ✓ [Continuar con Google.](#)
- a. Seleccione su cuenta de Google.
 - b. Si se conecta por primera vez a una cuenta de ESET HOME existente con su cuenta de Google, se le pedirá que escriba la contraseña de ESET HOME. Pulse **Confirmar contraseña**.
- ✓ [Continuar con Apple.](#)

- a. Escriba el Apple ID y la contraseña.
- b. Pulse **Iniciar sesión**.
- c. Escriba el código enviado a su dispositivo Apple.
- d. Pulse **Continuar**.
- e. Si confía en su navegador web, haga clic en **Confiar**.
- f. Pulse **Continuar** para acceder a ESET HOME con su Apple ID.
- g. Pulse el icono **X** de la esquina superior izquierda para volver a ESET Mobile Security.

✓ [Escanear código QR](#)

Esta opción requiere otro dispositivo con la aplicación ESET HOME.

- a. Abra la aplicación ESET HOME en otro dispositivo.
- b. Pulse el botón de menú  > **Escanear código QR**.
- c. Pulse **Escanear código QR**. Es posible que se le pida que permita ESET HOME que saque fotos y grabe vídeos. Pulse **Mientras se usa la aplicación** o **Solo esta vez**.
- d. Utilice la cámara para escanear el código QR.
- e. Pulse **Conectar dispositivo**.
- f. Pulse **Finalizar** en ESET Mobile Security.

✓ [Crear cuenta o iniciar sesión](#)

Cree una cuenta de ESET HOME

- a. Escriba su dirección de correo electrónico y su contraseña.



Requisitos de contraseña

La contraseña debe tener al menos diez caracteres y contener al menos una minúscula, una mayúscula y un número.

- b. Pulse **Crear cuenta** para recibir un vínculo de confirmación por correo electrónico.
- c. Cree un sobrenombre para su dispositivo y pulse **Siguiente**.
- d. Para que ESET Mobile Security funcione correctamente, pulse **Continuar** para permitir permiso de acceso Todos los archivos.
- e. Pulse **Iniciar primer análisis**.
- f. Para finalizar el registro, pulse el vínculo del mensaje de correo electrónico de confirmación.

Iniciar sesión en ESET HOME

- a. Pulse **Iniciar sesión** en el botón **Crear cuenta**.
- b. Escriba su correo electrónico y su contraseña.
- c. Pulse **Iniciar sesión**.

Tras iniciar sesión en su cuenta ESET HOME, tendrá que crear un sobrenombre para su dispositivo. Ayudará a identificar este dispositivo en su cuenta ESET HOME. Escriba el sobrenombre y pulse **Siguiente**.

✓ [Omitir](#)

Si no tiene cuenta de ESET HOME o no quiere conectar su dispositivo móvil a su cuenta de ESET HOME, pulse **Omitir**. Puede iniciar sesión en su cuenta de ESET HOME más tarde en la aplicación ESET Mobile Security. Si omite este paso, se le pedirá que seleccione la cuenta de correo electrónico que recibirá el registro de licencia de ESET y los mensajes de correo electrónico del Soporte técnico. Pulse **Seleccione su dirección de correo electrónico** para mostrar la lista de cuentas de correo electrónico disponibles. Seleccione el correo electrónico de la lista de cuentas o pulse **Agregar cuenta** para agregar una nueva cuenta de correo electrónico al dispositivo. Pulse **Aceptar** para continuar. Para utilizar una cuenta de correo electrónico distinta sin agregar la cuenta a su dispositivo, pulse **Seleccione su dirección de correo electrónico** > **Cancelar**. Repita esta acción dos veces. Escriba su correo electrónico y pulse **Seleccionar** para continuar.

7. Los últimos pasos del asistente de inicio varían en función de la versión de Android de su dispositivo.

✓ [Android 6–10](#)

- a. Para activar la búsqueda de dispositivos, ESET Mobile Security necesita varios permisos. Revise los permisos de ESET Mobile Security en la pantalla **Permitir acceso** y pulse **Continuar**.
- b. Pulse **Permitir** para permitir el acceso a ESET Mobile Security. Si pulsa **Omitir**, ESET Mobile Security no analizará su dispositivo en busca de amenazas hasta que se concedan estos permisos, y recibirá una notificación de riesgo para la seguridad.

✓ [Android 11 y versiones posteriores](#)

- a. Pulse **Continuar**.
- b. Seleccionar ESET Mobile Security.
- c. Active el interruptor situado junto a ESET Mobile Security.
- d. El Asistente de inicio ha finalizado. Pulse **Iniciar primer análisis**.

Protector de baterías



Muchos fabricantes de dispositivos introdujeron opciones de ahorro y protección de batería en Android 6 y en dispositivos posteriores. Cuando se activa, esta función desactiva la funcionalidad Antiphishing en ESET Mobile Security. En los dispositivos que cuenten con esta función, tendrá que crear una excepción para permitir que la funcionalidad Anti-Phishing de ESET Mobile Security funcione con la función de ahorro de batería activa. Para crear una excepción, consulte la documentación del fabricante de su dispositivo.

Funciones de las licencias gratuita y versión Premium

ESET Mobile Security tiene dos versiones disponibles:

- Gratuita: las funciones básicas pueden utilizarse de forma gratuita durante un tiempo ilimitado
- De pago: las funciones de pago se activan hasta que caduca su licencia.

En esta tabla se indica qué funciones están disponibles en las versiones gratuita y Premium:

	Gratis	Premium
Antivirus	✓	✓
Antivirus: análisis automáticos		✓
Actualizaciones automáticas de módulos de detección		✓
Bloqueo de aplicación		✓
Anti-Theft: portal web		✓
Anti-Theft: Protección de SIM		✓
Inspector de red		✓
Anti-Phishing		✓
Filtro de llamadas		✓
Protección de pagos		✓
Auditoría de seguridad		✓
Informe de seguridad	✓	✓

Seleccione el periodo de suscripción. Se le puede cobrar mensual o anualmente. Seleccione también la versión de su licencia de suscripción.

Tipo de licencia	Uso de la licencia
Móvil	Puede utilizar la licencia de ESET Mobile Security en un máximo de cinco dispositivos Android con ESET Mobile Security y ESET Smart TV Security en la misma cuenta de Google.
PC/Mac/Móvil	Recibirá una licencia de ESET Internet Security que puede utilizar para proteger tres dispositivos. Se asignará automáticamente un puesto de licencia a ESET Mobile Security en el dispositivo con el que haya adquirido la licencia. Igual que con una licencia para dispositivos móviles, puede utilizar este puesto para activar un máximo de cinco dispositivos Android con ESET Mobile Security y ESET Smart TV Security en la misma cuenta de Google.

Ejemplo de uso de licencia para dispositivos móviles

Sam utiliza un smartphone Android, una tableta Android y un televisor inteligente Android TV. En todos estos dispositivos, Sam ha iniciado sesión con la misma cuenta de Google.


- i** Sam compró una suscripción para dispositivos móviles a ESET Mobile Security desde un smartphone. Tras la compra, Sam recibe una clave de licencia en el correo electrónico asociado a la cuenta de Google de Sam. Sam puede usar esa licencia para activar ESET Mobile Security en la tableta Android y ESET Smart TV Security en el televisor inteligente con ESET HOME o la clave de licencia.

Activación

Para desbloquear las funciones de la versión Premium, debe activar ESET Mobile Security.

Hay varias formas de activar ESET Mobile Security. La disponibilidad de un método de activación determinado podría variar en función de su país y del medio de distribución (página web de ESET, Google Play).

Si aún no tiene una clave de licencia

1. Pulse el botón de menú  para abrir el menú principal.
2. Pulse **Licencia** en el menú principal.
3. En la sección **Su licencia**, pulse **Actualizar a versión Premium**.
4. Seleccione un plan de suscripción **Mensual** o **Anual**. Pulse el botón **Actualizar a versión Premium** para confirmar el plan seleccionado. La licencia de la versión Premium se renovará automáticamente en función del intervalo de suscripción elegido.
5. Será redirigido para completar la compra en Google Play.
6. Recibirá un recibo de orden de Google Play con su Número de orden en la dirección de correo electrónico asociada con su cuenta de Google Play. También recibirá un mensaje de correo electrónico de ESET (noreply) con la información de su licencia en esta misma cuenta de correo electrónico. Guarde estos mensajes de correo electrónico para consultarlos en un futuro.
7. Su producto se activará automáticamente tras la compra correcta en Google Play.

Si compró una licencia en ESET.com:

Una clave de licencia es una cadena única con el siguiente XXXX-XXXX-XXXX-XXXX-XXXX, y se utiliza para

identificar al propietario de la licencia. Está en el mensaje de correo electrónico que le ha enviado ESET o en la tarjeta de licencia incluida en la caja que ha adquirido.

Disponibilidad de las funciones



Algunas funciones, como los Códigos de referencia, solo están disponibles para los propietarios de licencias de Google Play. Estas funciones quedarán inactivas si el producto se activa con una licencia comprada en eset.com.

Si ya tiene una licencia

Active ESET Mobile Security con una licencia que ya esté asociada a ESET HOME

Siga los pasos de activación indicados a continuación si ya tiene una licencia de ESET Mobile Security en su cuenta ESET HOME y también cuando ha instalado ESET Mobile Security desde el correo electrónico de verificación enviado desde [su cuenta ESET HOME o la de otra persona](#):

1. Revise los detalles de activación en la aplicación ESET Mobile Security y pulse **Continuar** para aceptar que la dirección de correo electrónico mostrada administrará su dispositivo.

Detalles de activación



Cuando alguien le envíe la protección de ESET por correo electrónico, ESET Mobile Security lo administrará la cuenta ESET HOME del remitente. Si acepta, desconecte el dispositivo de su cuenta ESET HOME. Si no acepta, pulse **No acepto** y continúe en el [asistente de inicio con el paso 4](#). Consulte este [artículo de la base de conocimiento](#) para obtener instrucciones ilustradas sobre cómo desconectar el dispositivo de la cuenta de ESET HOME (puede estar disponible en inglés y en otros idiomas).

2. Cree un sobrenombre para su dispositivo y pulse **Siguiente**.
3. Una vez realizada correctamente la activación, pulse **Finalizar**.
4. Pulse **Iniciar primer análisis**.
5. Para que ESET Mobile Security funcione correctamente, pulse **Continuar** para permitir permiso de acceso Todos los archivos.

Si surge algún problema y no puede asociar ESET Mobile Security a su cuenta ESET HOME, visite el tema [Conexión a ESET HOME](#).

Después de activar ESET Mobile Security con la cuenta de ESET HOME, puede [administrar la licencia en ESET HOME](#) pulsando el icono de menú > **ESET HOME** > **Administrar en ESET HOME** bajo su licencia.

Activación sin ESET HOME

1. Vaya al menú principal pulsando el botón de menú .
2. Pulse **Licencia** en la pantalla de inicio de ESET Mobile Security y seleccione **Introducir una clave de licencia**.
3. Escriba su clave de licencia en el campo y pulse **Activar**.
4. Cuando se haya verificado correctamente su licencia, se mostrará **Activación realizada correctamente**.


5. Pulse **Finalizar** para cerrar la ventana.

Desinstalación

ESET Mobile Security puede desinstalarse con el asistente **Desinstalar** disponible en el menú principal de ESET Mobile Security.

Nota

Al desinstalar el producto ESET Mobile Security, quedará libre un puesto de la licencia.


1. Pulse Menú .
2. Pulse **Configuración**.
3. Pulse **Desinstalar**.
4. Si la protección Antirrobo está activada, se le pedirá que introduzca su PIN/patrón de seguridad de ESET Mobile Security o su huella dactilar.
5. Pulse **Desinstalar**.

También puede seguir los pasos que se indican a continuación para desinstalar el producto manualmente:


Android 7 y versiones posteriores:

1. Vuelva a Configuración y pulse **Administrar aplicaciones > ESET Mobile Security > Desinstalar**. Si la protección Antirrobo está activada, puede que se le pida que desactive la función de Administrador del dispositivo para ESET Mobile Security antes de desinstalarla.

O

1. En ESET Mobile Security, pulse el botón del menú principal  para abrir el menú principal.
2. Seleccione **Configuración**.
3. Pulse **Desinstalar**.
4. Pulse **Desinstalar** de nuevo para confirmar su decisión.

Android 6:

1. Pulse el icono de inicio  en la pantalla de inicio de Android (o vaya a **Inicio > Menú**) y pulse **Configuración > Seguridad > Administradores del dispositivo**. Seleccione **ESET Mobile Security** y pulse **Desactivar**. Pulse **Desbloquear** e introduzca su PIN/patrón de seguridad. Puede omitir este paso si la aplicación ya no está definida como Administrador del dispositivo.

2.Vuelva a **Configuración** y pulse **Administrar aplicaciones > ESET Mobile Security > Desinstalar**.

Conexión a ESET HOME

Para utilizar esta función, actualice a ESET Mobile Security versión 6.3 o posterior.

Activación de ESET Mobile Security con ESET HOME



Si desea activar un dispositivo con ESET HOME por segunda vez (por ejemplo, después de reinstalar ESET Mobile Security), debe eliminar manualmente de la licencia el dispositivo en ESET HOME para continuar. De lo contrario, no podrá activar este dispositivo con ESET HOME.

Conecte el dispositivo a una cuenta de ESET HOME existente.

1. Pulse el botón del menú
2. Pulse **Cuenta de ESET HOME**.

✓ [Continuar con Google.](#)

- a. Seleccione su cuenta de Google.
- b. Si se conecta por primera vez a una cuenta de ESET HOME existente con su cuenta de Google, se le pedirá que escriba la contraseña de ESET HOME. Pulse **Confirmar contraseña**.

✓ [Continuar con Apple.](#)

- a. Escriba el Apple ID y la contraseña.
- b. Pulse **Iniciar sesión**.
- c. Escriba el código enviado a su dispositivo Apple.
- d. Pulse **Continuar**.
- e. Si confía en su navegador web, haga clic en **Confiar**.
- f. Pulse **Continuar** para acceder a ESET HOME con su Apple ID.
- g. Pulse el icono **X** de la esquina superior izquierda para volver a ESET Mobile Security.

✓ [Escanear código QR](#)

Esta opción requiere otro dispositivo con la aplicación ESET HOME.

- a. Abra la aplicación ESET HOME en otro dispositivo.
- b. Pulse el botón de menú > **Escanear código QR**.
- c. Pulse **Escanear código QR**. Es posible que se le pida que permita ESET HOME que saque fotos y grabe vídeos. Pulse **Mientras se usa la aplicación o Solo esta vez**.
- d. Utilice la cámara para escanear el código QR.
- e. Pulse **Conectar dispositivo**.
- f. Pulse **Finalizar** en ESET Mobile Security.

✓ [Continuar con correo electrónico](#)

- a. Escriba su dirección de correo electrónico y su contraseña.
- b. Pulse **Iniciar sesión**.

3. Si inicia sesión en su cuenta de ESET HOME por primera vez con este dispositivo, cree un sobrenombre para el dispositivo para que le ayude a identificar el dispositivo en ESET HOME. Pulse **Siguiente**.


4. Si utiliza una licencia gratuita o de prueba y tiene una licencia disponible en ESET HOME, se le ofrecerá la opción de activar ESET Mobile Security.

a. Seleccione las licencias pertinentes.

b. Pulse **Activar**.

5. Pulse **Finalizar**.

Crear una cuenta de ESET HOME y conectar su dispositivo a ella

1. Pulse el botón del menú .
2. Pulse **Cuenta de ESET HOME**.
3. Pulse **Crear cuenta**.
4. Escriba su dirección de correo electrónico y su contraseña.




Requisitos de contraseña

La contraseña debe tener al menos 10 caracteres y contener al menos un carácter en mayúscula y minúscula y un número.

5. Pulse **Crear cuenta** para recibir un vínculo de confirmación por correo electrónico.
 6. Cree un sobrenombre para su dispositivo y pulse **Siguiente**.
 7. Para que ESET Mobile Security funcione correctamente, pulse **Continuar** para permitir permiso de acceso Todos los archivos.
 8. Pulse **Iniciar primer análisis**.
 9. Para finalizar el registro, pulse el vínculo del mensaje de correo electrónico de confirmación.
-

Desconectar el dispositivo de ESET HOME

1. Pulse el botón del menú .
2. Pulse **Cuenta de ESET HOME**.
3. Pulse **Desconectar dispositivo**. Si el dispositivo no está conectado a ESET HOME, esta opción no está disponible.
4. Utilice su huella dactilar o escriba su PIN.
5. Pulse **Desconectar**.

Antivirus

El módulo Antivirus protege su dispositivo de código malicioso mediante el bloqueo de las amenazas y, posteriormente, desinfectándolas.



Descubra y elimine amenazas con una profundidad de análisis variable.

🔍 Analizar dispositivo

Análisis automáticos



Análisis al cargar
Activado



Análisis programado
Desactivado




Actualización




Actualizar módulos de detección
Versión: 27121 (actualizada)

Protección en tiempo real

Protección del sistema de archivos en tiempo real controla todos los archivos de las carpetas de descarga para asegurarse de que no haya código malicioso al abrirlos, crearlos o ejecutarlos.

De forma predeterminada, Protección del sistema de archivos en tiempo real se inicia al arrancar el sistema y proporciona un análisis ininterrumpido. No recomendamos desactivar Activar Protección del sistema de archivos en tiempo real en la sección **Antivirus**. Si tiene que ir a los ajustes de Protección en tiempo real, pulse los tres puntos  en la sección **Antivirus > Configuración avanzada > Protección en tiempo real**.

Analizar dispositivo

Puede realizar un análisis a petición en cualquier momento pulsando el botón **Analizar dispositivo** en la sección **Antivirus**. De forma predeterminada, el nivel de análisis está establecido en Análisis inteligente. Puede cambiar el nivel de análisis en **Configuración avanzada** en el antivirus. Pulse el botón de los tres puntos  > **Configuración avanzada > Nivel de análisis**.

Es posible elegir entre dos niveles de análisis:

- **Estándar:** el Análisis estándar analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos con una profundidad de análisis máxima de tres archivos anidados y el contenido de la tarjeta SD.
- **En profundidad:** el Análisis en profundidad analizará todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Un breve resumen del análisis se guarda en un archivo de registro disponible en la sección [Registros del análisis](#).

Si desea anular un análisis que ya está en curso, pulse **Cancelar**. El resultado del análisis y las estadísticas se mostrarán en el panel de ajustes del **antivirus** durante el análisis.

Análisis de tarjetas de memoria



ESET Mobile Security no permite el análisis de tarjetas de memoria en dispositivos con Android 6 y versiones anteriores.

Amenazas no resueltas

Cuando ESET Mobile Security detecte una amenaza, esta opción estará disponible hasta que seleccione una acción de respuesta a la amenaza. Las acciones de respuesta disponibles son eliminar la amenaza o ignorarla.

Ignorar amenazas

Tras optar por ignorar una amenaza, aparecerá la opción **Ignorar amenazas**. Esta opción sigue permitiéndole eliminar más tarde una amenaza ignorada.

Análisis al cargar

Cuando se seleccione esta opción, el análisis comenzará automáticamente cuando el dispositivo esté en estado de

inactividad, totalmente cargado y conectado a un cargador.

Análisis programado

El Análisis programado le permite programar un análisis automático del dispositivo a una hora predefinida. Para programar un análisis, pulse el conmutador junto a **Análisis programado** y especifique las fechas y horas a las que deba iniciarse el análisis.

Actualizar módulos de detección

De forma predeterminada, ESET Mobile Security incluye una tarea para garantizar que el programa se actualice regularmente. Para ejecutar la actualización manualmente, pulse **Actualizar módulos de detección**.

Cobros por transferencia de datos



Para evitar un uso innecesario del ancho de banda, las actualizaciones se envían según sea necesario. Las actualizaciones son gratuitas, aunque su proveedor de servicios móviles podría cobrarle las transferencias de datos.

Para obtener más información sobre análisis, consulte los siguientes vínculos:

- [Registros de análisis](#)
- [Configuración avanzada](#)

Registros de análisis

La sección Registros de análisis contiene datos completos de cada análisis programado o análisis del dispositivo iniciado manualmente.

En cada registro se incluye la siguiente información:

- Fecha y hora del análisis
- Nivel de análisis (Estándar o Exhaustivo)
- Duración del análisis
- Número de archivos analizados
- Resultado del análisis o errores detectados durante el mismo
- Número de amenazas detectadas y lista de amenazas detectadas

Configuración avanzada

Abra la aplicación ESET Mobile Security y pulse el icono de menú > **Antivirus** > tres puntos en la esquina superior derecha > **Configuración avanzada**.

Nivel de análisis

Es posible elegir entre dos niveles de análisis:

- **Estándar:** el Análisis estándar analizará las aplicaciones instaladas, los archivos DEX (archivos ejecutables del SO Android), los archivos del SO (bibliotecas), los archivos con una profundidad de análisis máxima de tres archivos anidados y el contenido de la tarjeta SD.
- **En profundidad:** el Análisis en profundidad analizará todos los tipos de archivo, sea cual sea su extensión, tanto de la memoria interna como de la tarjeta SD.

Protección en tiempo real

El análisis en tiempo real se inicia automáticamente cuando se inicia el sistema y analiza los archivos con los que usted interactúa. Analiza automáticamente la carpeta Descargas y las aplicaciones instaladas o actualizadas.

Sistema de reputación ESET LiveGrid©

ESET LiveGrid© es un sistema preventivo diseñado para proporcionar un nivel adicional de seguridad a su dispositivo. Controla de manera constante los programas y procesos en ejecución del sistema comparándolos con los datos más recientes recopilados de millones de usuarios de ESET de todo el mundo. Esto nos permite ofrecer una protección proactiva más precisa y mayores velocidades de análisis a todos los usuarios de ESET. Se recomienda activar esta función.

Sistema de respuesta ESET LiveGrid©

Este sistema de respuesta nos permite recopilar estadísticas anónimas, informes de bloqueo y datos de diagnóstico sobre objetos sospechosos, que procesamos automáticamente para crear el mecanismo de detección en nuestro sistema en la nube.

Medios extraíbles

ESET Mobile Security analiza todos los medios extraíbles conectados a su dispositivo (unidades USB, discos duros externos, etc.).

Detectar aplicaciones potencialmente indeseables

Una aplicación potencialmente no deseada es un programa que contiene software publicitario, instala barras de herramientas, realiza un seguimiento de los resultados de sus búsquedas o tiene otros objetivos poco claros. Pueden darse casos en los que crea que las ventajas de la aplicación potencialmente no deseada compensan los riesgos asociados. Por ello, ESET asigna a esta categoría de aplicaciones un riesgo menor que el del software malintencionado.


Detectar aplicaciones potencialmente peligrosas

Existen muchas aplicaciones legítimas cuya función es simplificar la administración de los dispositivos que están en red. En esta clasificación se incluyen programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones. Aplicaciones potencialmente no seguras es una clasificación utilizada para software comercial legítimo. Sin embargo, en las manos equivocadas, se pueden utilizar con fines

maliciosos. Active la opción **Detectar aplicaciones potencialmente no seguras** para supervisar esta categoría de aplicaciones y bloquearlas, si así lo prefiere.

Servidor de actualización


Con esta opción puede activar las actualizaciones de su dispositivo desde el **Servidor de prueba**. Las actualizaciones previas a su lanzamiento se han sometido a pruebas internas estrictas y pronto estarán disponibles al público en general. Puede aprovechar el acceso anticipado a los métodos y soluciones de detección más recientes. Sin embargo, las actualizaciones de prueba podrían no ser totalmente estables en todo momento.

Para comprobar las versiones de los módulos del programa actuales, pulse los tres puntos  en la pantalla principal de ESET Mobile Security y pulse **Acerca de > ESET Mobile Security**. Recomendamos que los usuarios básicos dejen seleccionada la opción **Servidor de lanzamiento** de forma predeterminada.

Adware Detector

Adware Detector es la respuesta de ESET a las aplicaciones de adware. Las aplicaciones de adware pueden ser aplicaciones legítimas o aplicaciones que intentan presentarse como legítimas (como la Calculadora o la linterna). A continuación, estas aplicaciones mostrarán anuncios a pantalla completa, incluso cuando la aplicación está cerrada. Por lo tanto, el usuario no puede detectar qué aplicación está mostrando estos anuncios emergentes.

Adware Detector le ayuda a identificar estas aplicaciones de adware. Para utilizarlo, haga lo siguiente cuando se muestre un anuncio emergente:

1. Abrir ESET Mobile Security.
2. En la pantalla principal de ESET Mobile Security, pulse **Antivirus**.
3. Pulse  en la esquina superior derecha para mostrar el menú.
4. Pulse **Adware Detector** en el menú.
5. Cuando Adware Detector muestre una guía para detectar aplicaciones de adware, pulse **Continuar**.

Adware Detector muestra las aplicaciones que se han abierto en los últimos cinco minutos. Identifique las aplicaciones sospechosas y pulse **Quitar** para quitarlas del dispositivo. Normalmente, una aplicación sospechosa es una que se supone usted no ha abierto o que no estaba usando en ese momento.

Informe de seguridad

Informe de seguridad contiene una completa visión global de cada módulo del programa y sus respectivos estado y estadísticas. También, desde la pantalla **Informe de seguridad**, puede activar los módulos que no se encuentran activados. En cada sección del módulo del programa se incluye la siguiente información.

Si falta parte de la información, significa que no ha habido ningún caso.

Antivirus

- Escaneos de aplicaciones

- Amenazas detectadas
- Actualizaciones de la base de datos
- Detección realizada
- Archivos analizados
- Aplicaciones actualizadas

Bloqueo de aplicación

- Número de aplicaciones protegidas
- Número de desbloques de la aplicación correctos
- Número de intentos de desbloqueo sin éxito

Antiphishing

- Vínculos analizados
- Notificaciones analizadas
- Amenazas detectadas

Filtro de llamadas

- Llamadas salientes
- Llamadas recibidas
- Llamadas bloqueadas

Protección de pagos

- Número de aplicaciones protegidas
- Número de análisis de aplicaciones protegidas
- Número de problemas encontrados
- Número de veces que ha iniciado una aplicación de banca o pagos desde Ejecución segura

Auditoría de seguridad

- Las alertas de itinerancia representan el número de veces que ha recibido alertas de conexión a una red de itinerancia
- Avisos de Wi-Fi abiertas

Inspector de red

- Análisis de red
- Dispositivos encontrados
- Vulnerabilidades detectadas


ESET Mobile Security mostrará todos los meses un breve mensaje de informe mensual en la barra de notificaciones de Android. Si no quiere recibir estas notificaciones, active la opción **No mostrar notificación de informe mensual**.

Registro de actividad

El Registro de actividad muestra las actividades diarias de ESET Mobile Security en la pantalla principal de la aplicación ESET Mobile Security. Registro de actividad contiene información sobre los sitios web analizados por ESET Mobile Security, las actualizaciones de ESET Mobile Security, las actualizaciones de la aplicación, las aplicaciones instaladas, los análisis de ESET Mobile Security, etc.

Para ver el historial completo del Registro de actividad, pulse el icono > situado junto al Registro de actividad. En el informe completo del Registro de actividad puede usar los **Filtros** para filtrar las actividades por estado o función de ESET Mobile Security. Por ejemplo: Advertencia, Riesgo, Antirrobo y Licencia. También puede filtrarlas por fecha de aparición, por más recientes o por más antiguas.

Para borrar el historial del registro de actividad:

1. Abrir ESET Mobile Security.
2. Deslice el dedo hacia abajo por la pantalla de inicio.
3. Pulse el icono > situado junto al **Registro de actividad**.
4. Pulse el icono de menú .
5. Pulse **Borrar todo**.

Para eliminar registros individuales del historial del registro de actividad:

1. Abrir ESET Mobile Security.
2. Deslice el dedo hacia arriba por la pantalla de inicio.
3. Pulse el icono > situado junto al **Registro de actividad**.
4. Deslice el registro correspondiente a la izquierda.
5. Pulse **Quitar**.

Antirrobo

La función ESET Anti-Theft protege su dispositivo móvil del acceso no autorizado, le permite supervisar la actividad extraña y rastrea la ubicación del dispositivo. También puede mostrar un mensaje a la persona que encuentra su dispositivo.


ESET Anti-Theft requiere los siguientes permisos:

- Acceso a la cámara para hacer fotos de los intrusos.
- Acceso a la edición de archivos para eliminar datos confidenciales de forma remota.
- Acceso a los datos de ubicación para realizar un seguimiento de su dispositivo si se pierde.
- Acceso a actividad física para reconocer cuándo se mueve el dispositivo.
- Acceso a la ubicación en segundo plano para realizar un seguimiento de su dispositivo si se pierde, aunque ESET Mobile Security esté cerrado o no se esté usando. Cuando conceda este permiso, seleccione **Permitir siempre** para garantizar una protección completa.
- Acceso de uso para permitir recibir llamadas en su dispositivo si se bloquea.
- Acceso a la administración del dispositivo para impedir la desinstalación no autorizada de ESET Mobile Security. Tras activar la administración del dispositivo, se le pedirá que cree un PIN para proteger ajustes importantes de ESET Mobile Security.
- Lectura de la información del teléfono para detectar la extracción de la tarjeta SIM. Su dispositivo se bloqueará cuando se quite la tarjeta SIM.

Visite el [artículo de la base de conocimiento Configurar la protección Antirrobo en ESET Mobile Security for Android](#) para configurar la protección Antirrobo en ESET Mobile Security (los artículos de la base de conocimiento no están disponibles en todos los idiomas).

Bloqueo automático del dispositivo

Además de bloquear su dispositivo desde el portal ESET HOME, puede configurar ESET Mobile Security para bloquear automáticamente su dispositivo cuando se realice una de las siguientes acciones:

- **Si la tarjeta SIM se extrae:** si se extrae la tarjeta SIM de confianza del dispositivo, este se bloqueará. Para extraer e inspeccionar tarjetas SIM de confianza, pulse **Gestionar las tarjetas SIM de confianza**, seleccione la tarjeta SIM que desea extraer y luego pulse el icono de la papelera . Para agregar una tarjeta SIM de confianza, inserte la tarjeta SIM. Si el bloqueo automático está activado, tendrá que desbloquear el dispositivo. ESET Mobile Security le pedirá que confirme la tarjeta SIM recién agregada como de confianza.

Compatibilidad con bloqueo automático al extraer tarjeta SIM

- La función de bloqueo automático al extraer tarjeta SIM no está disponible en los dispositivos CDMA, WCDMA y que solo dispongan de conectividad Wi-Fi.

- **Tras [X] intentos de desbloqueo:** cuando esta opción está activada, el dispositivo se bloquea después de un número determinado de intentos de desbloqueo sin éxito. Puede establecer el número de intentos de desbloqueo sin éxito antes de bloquear el dispositivo en la configuración de Antirrobo. Si el intento incorrecto

se produjo debido a un error, puede corregirlo en 30 segundos y no se contará como un intento incorrecto. Puede cambiar el tiempo de una corrección en la configuración de Antirrobo en la opción **Tiempo de corrección**. También puede desactivar el tiempo de corrección y el dispositivo se bloqueará inmediatamente después del número determinado de intentos sin éxito.

Cuando el dispositivo está bloqueado, puede mostrar información para ponerse en contacto con el propietario del dispositivo. También puede activar el dispositivo para que realice fotos con ambas cámaras para obtener fotos de la persona que intenta desbloquear el dispositivo.


Después de que se haya bloqueado el dispositivo

Puede configurar que suceda lo siguiente después de bloquearse su dispositivo:

- La opción **Mostrar los datos del contacto** muestra los datos de **Contactar con el propietario** cuando se introduce un código de bloqueo de pantalla incorrecto. Pulse **Modificar los datos del contacto** para introducir sus datos de contacto y que se muestren cuando se pierde el dispositivo. Su correo electrónico de ESET HOME se escribe de forma predeterminada.
- La opción **Hacer una foto** guarda las fotos de las cámaras trasera y delantera en la galería del dispositivo y el portal Antirrobo en caso de intento de desbloqueo fallido o retirada de tarjeta SIM.

Cómo desbloquear mi dispositivo móvil


Si bloqueó el dispositivo móvil mediante el portal de ESET Anti-Theft o ESET Mobile Security for Android ha bloqueado el dispositivo móvil, necesitará acceso a su contraseña de ESET HOME.

 **Desbloquear su dispositivo administrado por otra persona**
Si su ESET Mobile Security for Android lo administra la cuenta ESET HOME de otra persona, escriba la contraseña de esa cuenta para desbloquear el dispositivo.

Para obtener instrucciones visuales sobre cómo desbloquear el dispositivo móvil, lea el siguiente artículo de la [base de conocimiento de ESET](#) (disponible en inglés y en otros idiomas).

Configuración de Antirrobo

Bloquear tras intentos fallidos

Seleccione el número de intentos de desbloqueo erróneos permitidos antes de que se bloquee el dispositivo. Para configurar el número de intentos de desbloqueo, pulse  en la pantalla Antirrobo, seleccione **Configuración**, pulse **Bloquear tras intentos fallidos** y seleccione el número de intentos erróneos deseado.

Tiempo de corrección

Si ha activado la opción Bloquear tras intentos fallidos, el dispositivo se bloqueará tras el número de intentos sin éxito establecido. Desactive Tiempo de corrección para bloquear el dispositivo inmediatamente tras alcanzar el número establecido de intentos erróneos o establezca un periodo de tiempo para desbloquear correctamente el dispositivo antes de que se bloquee tras alcanzar el número establecido de intentos erróneos.

Ejemplo

- Bloquear tras intentos fallidos** está activado y el número de intentos erróneos está establecido en 3.
- i** **Tiempo de corrección** está establecido en 15 segundos.
- Tras introducir un patrón de desbloqueo incorrecto en el dispositivo tres veces, tiene 15 segundos para introducir el patrón de desbloqueo correcto y evitar que ESET Mobile Security bloquee el dispositivo.

Modificar los datos del contacto

Si marca su dispositivo como perdido en ESET Anti-Theft, o bien después de un número seleccionado de intentos de desbloqueo erróneos, la información de **Datos de contacto** se mostrará en la pantalla del dispositivo bloqueado para que la persona que lo encuentre pueda ponerse en contacto con usted.

Esta información puede incluir:

- Mensaje mostrado (opcional)
- Su nombre (opcional)
- Número de teléfono (distinto del suyo)
- Dirección de correo electrónico (opcional)

Gestionar las tarjetas SIM de confianza

Esta opción le permite eliminar o cambiar el nombre de la tarjeta SIM insertada. Para agregar una nueva tarjeta SIM de confianza, inserte la tarjeta SIM en el dispositivo. El dispositivo se bloqueará. Desbloquee el dispositivo con su código de seguridad. Se le pedirá que agregue la tarjeta SIM recién introducida a la lista de tarjetas SIM de confianza. Si no agrega esta tarjeta SIM a la lista, el control de SIM permanecerá desactivado.

Cambiar tipo de bloqueo

Seleccione una forma de desbloquear ESET Anti-Theft. Se establece un código PIN como opción predeterminada durante la configuración de Antirrobo. Puede cambiar esta selección a una opción de desbloqueo por patrón.

Usar huella dactilar

Cuando esta opción está activada, puede utilizar la huella dactilar guardada en el dispositivo para desbloquear la opción Antirrobo.

Optimización

la optimización de ESET Anti-Theft consiste en una evaluación técnica medible del estado de seguridad de su dispositivo. La protección Antirrobo analizará el sistema en busca de los siguientes problemas.

Para cada problema de seguridad, puede pulsar **Cambiar los ajustes** para desplazarse hasta la pantalla en la que puede resolver ese problema específico. Si no desea que ESET Mobile Security informe de una cuestión concreta como problema, pulse **Ignorar este problema**.

- **Los servicios de ubicación están desactivados:** para activarlos, vaya a Ajustes > **Servicios de ubicación** y seleccione **Utilizar redes inalámbricas**
- **No se están utilizando los satélites GPS:** acceda a este ajuste en Ajustes > **Ubicación** > **Modo** > **Gran precisión**
- **El bloqueo de pantalla no está protegido:** para proteger su dispositivo con un código de bloqueo de pantalla, una contraseña, un PIN o un patrón, vaya a Ajustes > **Bloquear pantalla** ; **Bloqueo de pantalla** y seleccione una de las opciones disponibles. La mayoría de los dispositivos Android ofrecen deslizamiento, movimiento, desbloqueo facial, facial y voz, patrón, PIN o contraseña. Si alguien intenta desbloquear el dispositivo con un código incorrecto, ESET Anti-Theft le informará de la existencia de una actividad sospechosa en el portal ESET HOME.
- **Los datos móviles no están activados:** acceda a este ajuste en Ajustes > **Conexiones y redes** > **Redes móviles** > **Datos**.
- **No están disponibles los servicios de Google Play:** ESET Anti-Theft utiliza los servicios de Google Play para enviar comandos a su dispositivo en tiempo real y mostrar notificaciones push. Si estos servicios están desactivados o no están disponibles en su dispositivo, las funciones de ESET Anti-Theft administradas desde ESET HOME estarán limitadas.

Portal web

ESET Mobile Security se integra por completo con la protección de ESET Anti-Theft mediante el nuevo portal [ESET HOME](#). Desde el portal ESET Anti-Theft podrá controlar la actividad de su dispositivo, bloquear el dispositivo, enviar mensajes personalizados a la persona que localice el dispositivo, activar una potente sirena o eliminar los datos del dispositivo de forma remota.

Para crear un cuenta ESET HOME, pulse **Crear una nueva cuenta** y cumplimente el formulario de registro. Busque el mensaje de confirmación en su bandeja de entrada y haga clic en el enlace que contiene para activar la cuenta. Tras la activación de la cuenta, puede gestionar de forma remota la función de seguridad ESET Anti-Theft de los dispositivos conectados mediante el portal ESET HOME. Si ya tiene una cuenta ESET HOME, pulse **Iniciar sesión** e introduzca su dirección de correo electrónico y su contraseña. Una vez que complete estos pasos, podrá asociar el dispositivo a su cuenta ESET HOME.

Si desea obtener más información sobre cómo usar las funciones de ESET Anti-Theft, consulte [Guía del usuario de Antirrobo](#) o pulse el icono de **Ayuda** en la esquina superior derecha del portal ESET HOME.

ESET HOME contraseña

Cambie su contraseña olvidada:

1. Visite <https://login.ESET.com/LostPassword>.
2. Introduzca la dirección de correo electrónico que utilizó para registrarse en ESET HOME y haga clic en **Enviar**.
3. Inicie sesión en su cuenta de correo electrónico, abra el mensaje **Restablecimiento de la contraseña de la cuenta de ESET HOME** y haga clic en el vínculo del mensaje de correo.

4.Introduzca y confirme una nueva contraseña, y haga clic en **Confirmar cambio**.

5.Escriba la nueva contraseña en el dispositivo y pulse **Desbloquear** para desbloquear el dispositivo.

Cambie su contraseña de ESET HOME:

1.Vaya al sitio web de [ESET HOME](#).

2.Inicie sesión con su dirección de correo electrónico y su contraseña actual.

3.Haga clic en su correo electrónico junto a la flecha hacia abajo ▾ de la esquina superior derecha.

4.Haga clic en **Cambiar una contraseña**.

5.Escriba su contraseña actual.

6.Escriba la nueva contraseña y confírmela.

7.Haga clic en **Guardar cambios**.

Anti-Phishing

El término phishing describe una actividad delictiva que conlleva la manipulación de usuarios para que proporcionen información confidencial en un sitio web que parece original, pero no lo es. Este tipo de manipulación se conoce como ingeniería social. El phishing suele utilizarse para acceder a datos confidenciales, como números de cuentas bancarias, números de tarjetas de pago, números PIN o nombres de usuario y contraseñas.

Antiphishing de ESET Mobile Security protege contra sitios web que se consideran maliciosos o peligrosos.

Se recomienda mantener la función **Anti-Phishing** activada. Cuando esta función esté activada, se bloquearán todos los posibles ataques de phishing que provengan de sitios web o dominios incluidos en la base de datos de malware de ESET y se le mostrará una notificación de advertencia que informa del intento de ataque.

Anti-Phishing se integra con la mayoría de navegadores web y aplicaciones de redes sociales comunes en el sistema operativo Android. Chrome y los navegadores que se incluyen preinstalados de serie en los dispositivos Android, llamados normalmente *Internet* o *Navegador*). Otros navegadores pueden mostrarse como desprotegidos porque no ofrecen una integración adecuada con Antiphishing. Para aprovechar al máximo la funcionalidad de Antiphishing, se recomienda no utilizar navegadores web no compatibles.



Para garantizar una correcta integración de Antiphishing con los navegadores, ESET recomienda usar Android 6 (Marshmallow) o versiones posteriores.

Mejora de la funcionalidad: ESET Mobile Security le avisa si la protección Anti-Phishing requiere permisos adicionales que el sistema operativo Android debe conceder. Pulse **Permitir** para abrir los ajustes de accesibilidad del sistema y ver las opciones disponibles que ofrecen compatibilidad con más navegadores y activan la protección durante la navegación en modo privado (de incógnito). Si no quiere que esta cuestión se notifique como problema, pulse **Ignorar este problema (no recomendado)**.

Para desactivar Antiphishing, pulse los tres puntos ⋮ de la sección Antiphishing y pulse **Desactivar**.

Conceder el permiso de accesibilidad de ESET Mobile Security al instalarlo desde el archivo .apk en Android 13

Nota

Por motivos de seguridad, Android 13 restringe el uso del permiso de accesibilidad a las aplicaciones instaladas desde archivos .apk para evitar que se acceda a él de forma desinformada.


¿Cómo utiliza ESET Mobile Security este permiso?

- i** Usamos este permiso para acceder a las URL de los sitios web que visita. Analizamos estos sitios web en busca de intención maliciosa, como phishing, malware u otras actividades peligrosas. Cuando se detecta una amenaza, el sitio web se bloquea para proteger al usuario y su información confidencial. Los datos a los que se accede mediante el permiso de accesibilidad no se comparten con terceros.

Para resolver el problema de accesibilidad:

Permiso de permitir accesibilidad

- i** Para obtener instrucciones con ilustraciones, lea el [artículo de nuestra base de conocimiento](#) (puede que solo esté disponible en inglés).

1. Abra **Configuración > Accesibilidad > Aplicaciones descargadas**. La opción ESET Mobile Security no estará disponible.
2. Pulse la aplicación ESET Mobile Security para abrir el cuadro de diálogo **Configuración restringida**.
3. A continuación, pulse **"Aceptar"**.
4. Vaya a **Configuración > Aplicaciones > ESET Mobile Security** para abrir la **información de la aplicación**.
5. Pulse el icono de menú de tres puntos  en la esquina superior derecha > **Permitir configuración restringida**.

Se permitirá la configuración restringida y podrá [empezar a usar la aplicación de forma segura](#).

i Anti-Phishing en Samsung DeX

Anti-Phishing no es compatible con dispositivos conectados a la estación Samsung DeX.

Navegadores protegidos

- Chrome
- Chrome Beta
- Firefox
- Firefox Beta
- Opera
- Opera Beta
- Opera Mini

- Opera Mini Beta
- Navegador para TV Opera
- Samsung Internet
- Mint
- Navegador Yandex
- DuckDuckGo (en la versión 6.1 y posteriores de ESET Mobile Security)
- Navegador Kiwi
- Edge
- Silk en dispositivos de Amazon
- Navegador Mi
- Navegador Xiaomi Mi
- Vewd en Android TV

Aplicaciones protegidas de redes sociales

- Facebook
- Facebook Lite
- Messenger
- Messenger Lite
- Instagram
- Las aplicaciones de redes sociales que utilizan componentes protegidos del navegador para la visualización web también están protegidas.

Protección de SMS y Protección de notificaciones

Protección de SMS y Protección de notificaciones protegen del smishing.

Smishing es la combinación de las palabras phishing y SMS. Por eso a veces se denomina phishing por SMS. Los atacantes utilizan SMS, pues tendemos a confiar en los SMS más que en el correo electrónico.

Protección de SMS protege contra la difusión de smishing desde el mensaje SMS. Sin embargo, la amenaza también puede difundirse desde cualquier plataforma de mensajería. Es aquí donde actúa Protección de notificaciones. Cuando recibe un SMS o una notificación (por ejemplo, tras recibir un mensaje de WhatsApp), ESET Mobile Security analiza el vínculo. Según el análisis, hay tres posibles resultados:

- No se encontraron amenazas.

- Se ha encontrado contenido potencialmente no deseado. Es posible que el contenido del mensaje o la notificación no plantee ningún riesgo directo. La intención no es tan inequívocamente maliciosa como en otros tipos de malware (por ejemplo, virus o troyanos). Sin embargo, puede instalar software no deseado adicional, cambiar el comportamiento del dispositivo digital o realizar actividades no aprobadas ni previstas por el usuario.
- Se ha encontrado contenido peligroso. Este mensaje o esta notificación contienen vínculos peligrosos o de phishing. Le recomendamos que no abra el contenido y que elimine el mensaje o la notificación.

Eliminación de mensajes y notificaciones



Por motivos de seguridad, ESET Mobile Security no puede eliminar mensajes ni notificaciones por usted. Debe eliminar manualmente el contenido peligroso.

Cómo funciona el smishing

1. Un atacante le envía un mensaje que contiene un vínculo a un sitio web.
2. Normalmente, el vínculo lleva a un sitio web de phishing que puede intentar que usted proporcione su información personal. Esto puede utilizarse, por ejemplo, para robarle dinero o para cometer otros fraudes. Este vínculo también puede llevar a un sitio web malicioso que contenga malware o intente engañar al usuario para que lo descargue.

Señales de smishing

- Un número de teléfono sospechoso, como un número extranjero o con una longitud no estándar.
- El mensaje contiene archivos o vínculos desconocidos.
- Por lo general, los mensajes de smishing tienen un tono urgente.
- Por lo general, los mensajes de smishing se hacen pasar por información sobre premios u otro tipo de ganancias.

Bloqueo de aplicación

Bloqueo de aplicaciones le permite acceder de forma segura a las aplicaciones seleccionadas (correo electrónico, mensajes, calendario, etc.) con un código PIN o una huella dactilar. Bloqueo de aplicaciones evita el acceso no autorizado a las aplicaciones seleccionadas, incluso cuando el dispositivo está desbloqueado.

Recomendación




Para que el funcionamiento sea más adecuado, activar el permiso **Superposición (Aplicaciones que pueden aparecer arriba)** para ESET Mobile Security.

Para configurar el Bloqueo de aplicaciones en el dispositivo:

1. Pulse **Bloqueo de aplicaciones** en la pantalla principal de ESET Mobile Security.
2. Pulse **Activar**.
3. Conceda el permiso de acceso de uso y haga clic en **Continuar**.


4. Escriba su PIN, que desbloquea las aplicaciones.
5. Confirme su PIN escribiéndolo de nuevo.
6. Pulse una aplicación para bloquearla o desbloquearla.

Configurar los ajustes de Bloqueo de aplicaciones

Para acceder a la configuración de Bloqueo de aplicaciones, abra el menú  de la esquina superior derecha y haga clic en **Configuración**:

- **Bloquear aplicaciones nuevas:** si está activado el bloqueo de aplicaciones, cuando instale una aplicación nueva en el dispositivo, se le preguntará si desea bloquear la nueva aplicación.
- **Bloquear aplicación de nuevo:** puede configurar el bloqueo de aplicaciones para bloquear una aplicación inmediatamente después de cerrarla, cuando la pantalla se apaga o cuando transcurre un minuto.
- **Tipo de bloqueo:** puede bloquear su aplicación con un PIN o con un patrón.
- **Desbloqueo con huella dactilar:** esta opción solo está disponible si hay una huella dactilar verificada guardada en el dispositivo. Cuando esta opción está activada, puede desbloquear las aplicaciones con la huella dactilar guardada en el dispositivo. Podrá seguir desbloqueando la aplicación con el PIN. Para ello, pulse **Usar PIN** al abrir una aplicación bloqueada.
- **Alerta de intruso:** tras una serie de intentos de desbloqueo sin éxito, ESET Mobile Security hace una fotografía del intruso. La fotografía se muestra la próxima vez que la aplicación se desbloquea correctamente.

Desactivar Bloqueo de aplicaciones

1. Vaya a la función Bloqueo de aplicaciones de ESET Mobile Security.
2. Escriba el PIN de Bloqueo de aplicaciones.
3. Pulse el menú  de la esquina superior derecha.
4. Pulse **Desactivar**.

Activar el modo nocturno

Pulse el icono del modo nocturno situado en la esquina superior derecha para activar Modo nocturno en la pantalla de bloqueo de aplicación y cuidar sus ojos.

He olvidado mi PIN de bloqueo de aplicación


Si olvida el PIN de Bloqueo de aplicaciones y no tiene una huella dactilar guardada en el dispositivo, tiene dos opciones para desbloquear la aplicación bloqueada, que varían en función de la configuración de Antirrobo:

- Si activó la función Antirrobo en ESET Mobile Security:
 1. Abrir ESET Mobile Security.

2. Vaya a la función Bloqueo de aplicaciones.

3. Escriba su PIN. **Pulse ¿Ha olvidado su PIN?** en el medio de la pantalla.

4. Si la función Antirrobo está activa, se le pedirá que escriba su contraseña de ESET HOME. Escriba la contraseña en el campo **Contraseña** y pulse **Entrar**.

5. Escriba el nuevo PIN y pulse  para confirmarlo.

6. Escriba el mismo PIN de nuevo para confirmarlo. Pulse  cuando haya terminado.

- Si no activó la función Antirrobo, [desinstale ESET Mobile Security](#) e instálelo de nuevo.

Protección de pagos



Protección de pagos es una capa adicional diseñada para proteger sus datos financieros en dispositivos Android frente a phishing avanzado y otras amenazas. La protección de pagos impide que otras aplicaciones detecten cuándo se inician sus aplicaciones protegidas, y también les impide sustituir información o leer información en pantalla desde dichas aplicaciones. Protección de pagos analiza todas las aplicaciones que están en su lista de aplicaciones protegidas. Tras activar Protección de pagos, automáticamente agregará algunas aplicaciones de banca y pago a la lista de aplicaciones protegidas.

Agregar una aplicación nueva a una lista de aplicaciones protegidas

1. Abra Protección de pagos en el menú Aplicaciones o en ESET Mobile Security.
2. Pulse **Gestionar**.
3. Seleccione las aplicaciones que desee proteger mediante Protección de pagos.
4. Pulse **Aceptar** para confirmar su selección.

Abrir una aplicación de pago y banca mediante la Protección de pagos

Para garantizar la máxima protección de sus aplicaciones de banca y pagos, abra estas aplicaciones desde Ejecución segura. La función Ejecución segura ofrece un nivel de protección adicional con respecto a la protección estándar de la función Protección de pagos al abrir una aplicación fuera de Ejecución segura. La función Ejecución segura se crea automáticamente cuando se activa la Protección de pagos. Ejecución segura contiene todas las aplicaciones protegidas por Protección de pagos.

¿Qué es Ejecución segura y cómo puedo acceder a ella?

Ejecución segura está disponible en la lista de aplicaciones  y también en ESET Mobile Security > Protección de pagos .

Acceso a la función de ejecución segura

i Para acceder a sus aplicaciones de banca y pagos de una forma más rápida y sencilla, puede agregar Ejecución segura a la pantalla de inicio. Para ello, mantenga pulsado el icono Ejecución segura y arrástrelo a la pantalla de inicio.

Filtro de llamadas

El **Filtro de llamadas** bloquea las llamadas entrantes o salientes en función de las reglas que usted defina.

Cuando se bloquee una llamada de voz entrante, no se mostrarán notificaciones de llamadas. Consulte el **Registro de llamadas** para buscar llamadas que puedan haberse bloqueado por error.

Bloquear la última llamada entrante: pulse para bloquear llamadas entrantes del último número de teléfono. Al hacerlo se creará una nueva regla.

Reglas

Para crear una regla nueva, pulse el icono +. Consulte [el siguiente capítulo](#) para obtener más información.

Para modificar una regla existente, pulse la entrada de la regla en la lista de reglas. Si desea quitar una entrada de la lista **Reglas**, seleccione la entrada y pulse **Quitar**.

Registro de llamadas

En el apartado **Registro de llamadas** se muestra el registro de todas las llamadas bloqueadas por el Filtro de llamadas. Cada registro incluye el nombre de la llamada, el número de teléfono correspondiente, la fecha y la hora del suceso.

i Dispositivos sin tarjeta SIM

El **Filtro de llamadas** no funciona en dispositivos no compatibles con llamadas y mensajería.

Llamadas salientes

⚠ El filtro de llamadas no bloquea la llamada saliente en el producto ESET Mobile Security descargado de Google Play.

⚠ Compatibilidad con Android

El filtro de llamadas solo está disponible en dispositivos con Android 6 o versiones posteriores.



Bloquear números de teléfono con comodines

Puede bloquear un intervalo de números mediante los comodines descritos en la siguiente tabla:

Comodín	Descripción
*	representa varios caracteres
?	representa un solo carácter

Ejemplo

- ✓ Si no desea recibir llamadas de un país concreto, escriba el código del país y el carácter comodín * en el campo **Número de teléfono móvil**, y se bloquearán todas las llamadas entrantes del país que comience por ese patrón de números. Si quiere excluir algún número de teléfono de ese país, [agregue una regla nueva](#) con la acción **Permitir**. En la siguiente imagen se muestra cómo bloquear todas las llamadas de Eslovaquia.

 **NUEVA REGLA** 


Qué

Bloquear ▼


Quién

Persona ▼

Nombre


Nombre (opcional) 

Número de teléfono

+421* 

Cuándo

Siempre ▼



Agregar una nueva regla

Para crear una regla nueva, pulse el icono +.

- 1.En el apartado **Qué**, seleccione **Bloquear** o **Permitir** para especificar el tipo de regla para llamadas y mensajes. Seleccione la dirección de llamadas que desea bloquear (de forma predeterminada está seleccionada la opción Entrantes).
- 2.En la sección **Quién**, seleccione una opción para especificar los números de teléfono a los que afectará la

regla.

- **Persona:** seleccione una persona de su lista de contactos o agregue el nombre y los números manualmente. Puede asignar más números de teléfono a un nombre; para ello, haga clic en el botón + en el apartado **Número de teléfono**.
- **Grupo:** ESET Mobile Security reconocerá los grupos de contactos guardados en sus Contactos (por ejemplo, Familia, Amigos o Trabajo).
- **Todos los números desconocidos** incluirá todos los números de teléfono que no estén guardados en su lista de contactos. Utilice esta opción para bloquear las llamadas de teléfono no deseadas (por ejemplo, las llamadas de empresas que le ofrecen servicios) o para impedir que sus hijos llamen a números desconocidos.
- **Todos los números conocidos** incluirá todos los números de teléfono guardados en su lista de contactos.
- **Todos los números** bloqueará todas las llamadas entrantes.
- **Números ocultos** se aplicará a personas que tengan su número de teléfono oculto intencionadamente a través de la restricción de identificación de llamadas (CLIR).

3. En la sección **Cuándo**, seleccione **Siempre** o **Personalizar** para especificar el intervalo de tiempo y los días de la semana que estará en vigor la regla. De forma predeterminada se seleccionan sábado y domingo.

Visite [este artículo de la base de conocimiento](#) para ver instrucciones con ilustraciones.


Filtro de llamadas en el extranjero

- i** Si está en el extranjero, introduzca todos los números de teléfono en la lista con el código de marcación internacional seguido del número en cuestión (por ejemplo, +1610100100).

Inspector de red

Inspector de red le permite analizar la red en busca de dispositivos conectados a su router y comprobar si hay vulnerabilidades. Inspector de red analiza su red en dos pasos.

En primer lugar, Inspector de red analiza su red en busca de dispositivos conectados. Si se detecta un dispositivo nuevo, verá una notificación y se marcará el dispositivo con el símbolo de la estrella. Para detectar dispositivos nuevos en su red de forma manual, pulse **Analizar red**. También puede detectar dispositivos automáticamente.



Para usar esta opción, pulse el icono de menú  > **Ajustes** y active la opción **Detectar dispositivos automáticamente**.

En el segundo paso del análisis, Inspector de red prueba los dispositivos conectados en busca de vulnerabilidades; para hacerlo, se conecta a ellos y busca vulnerabilidades tales como puertos abiertos, combinaciones de nombre de usuario y contraseña del router débiles, problemas en el firmware del router, etc. Los atacantes pueden aprovechar estas vulnerabilidades para obtener el control de su router y de los dispositivos que están conectados a él. Los routers y dispositivos controlados por atacantes se pueden usar para recopilar información sobre usted, e incluso participar en ataques de denegación de servicio distribuida (DDoS), etc.

Inspector de red le presenta además una completa lista de los dispositivos que están conectados a su red, con el fin de mantenerle al tanto de quién está conectado a su red. Puede usar esta información para gestionar o denegar, desde la interfaz web de su router, el acceso que estos dispositivos tienen a su red. Puede acceder a la interfaz web de su router directamente desde Inspector de red; solo tiene que seleccionar su router y pulsar la

opción **Abrir interfaz web**.

Puede ver los dispositivos conectados en forma de lista o de manera visual:


-  Vista de lista: los dispositivos conectados se muestran en una vista de lista estándar, con el router al principio seguido de los dispositivos que están en línea y el historial de dispositivos que se han conectado anteriormente al final.
-  Vista de sónar: los dispositivos se muestran de forma visual, en un medio círculo con el router en el centro. En la segunda capa desde el centro se muestran los dispositivos que están en línea en ese momento. En la tercera se muestra un historial de los dispositivos que se han conectado anteriormente. Puede moverse entre los dispositivos al pulsar los botones de flecha o desplazarse en la dirección del círculo.

Para una gestión de dispositivos más sencilla, asigne una categoría al dispositivo (como smartphone, televisor, videoconsola, ordenador, etc.), cambie el nombre de los dispositivos del nombre estándar del fabricante o su dirección IP a un nombre que sea más fácil de comprender (por ejemplo: cambiar SM-G955F a Teléfono de Andrés, 192.168.1.52 a Ordenador de Laura, etc.).

Para cambiar el nombre de los dispositivos desde Inspector de red, pulse el icono del dispositivo en Inspector de red > pulse el icono del lápiz de la esquina superior derecha, seleccione la categoría del dispositivo, escriba el nombre del dispositivo y, a continuación, pulse **Aceptar**.

Auditoría de seguridad

La Auditoría de seguridad le ayuda a supervisar y cambiar ajustes importantes del dispositivo. Revise los permisos de las aplicaciones instaladas en el dispositivo para evitar riesgos de seguridad.

Para activar o desactivar la Auditoría de seguridad y sus componentes específicos, pulse el botón Menú  y, a continuación, pulse **Desactivar supervisión del dispositivo** o **Desactivar auditoría de aplicaciones**.


- [Supervisión del dispositivo](#)
- [Auditoría de aplicación](#)

Supervisión del dispositivo

Defina en la sección **Supervisión del dispositivo** qué componentes del dispositivo supervisará ESET Mobile Security.

Pulse cada opción para ver su descripción detallada y su estado actual. En las opciones **Orígenes desconocidos** y **Modo de depuración**, pulse **Abrir configuración** para cambiar los ajustes en **Ajustes del sistema operativo Android**.

Puede desactivar cada componente.

1. Pulse el componente que desee desactivar.
2. Pulse el icono de menú .

3. Pulse **Desactivar**.

Auditoría de aplicación

La Auditoría de aplicaciones realiza una auditoría de las aplicaciones instaladas en el dispositivo que podrían tener acceso a servicios que le suponen un gasto, que controlan su ubicación o que leen su información de identificación, sus contactos o sus mensajes de texto. ESET Mobile Security ofrece una auditoría de dichas aplicaciones clasificadas en categorías. Pulse cada categoría para ver su descripción detallada. Pulse una aplicación para ver sus detalles de permisos.

Códigos de referencia

Importante

- ! Esta función solo está disponible para usuarios que han descargado ESET Mobile Security de Google Play y no tienen activada la licencia versión Premium.


El código de referencia es un número exclusivo asignado a su dispositivo. Comparta y reciba códigos de referencia para obtener una licencia de la versión Premium de ESET Mobile Security gratuita durante un máximo de un año.

Comparta su código de referencia con un amigo y ambos recibirán una licencia de pago gratuita durante 30 días. Si su amigo no dispone de ESET Mobile Security, recibirá un enlace de descarga exclusivo de ESET Mobile Security que incluye la licencia de pago gratuita durante 30 días.

Cada vez que comparta un código de referencia recibirá una licencia de pago gratuita durante 30 días y un trofeo virtual que le ayudará a mantener un control de los códigos que ha compartido y recibido. Cada trofeo virtual representa una licencia de pago gratuita durante 30 días. Puede compartir hasta 12 códigos de referencia para recibir licencias gratuitas. Una vez haya recibido los 12 trofeos virtuales, podrá seguir compartiendo su código con sus amigos, quienes seguirán recibiendo licencias de pago gratuitas durante 30 días, pero usted no recibirá licencias gratuitas adicionales.



Recomendar a un amigo

Si desea compartir ESET Mobile Security y ayudar a su amigo a estar protegido, pulse el icono **Menú principal**  y seleccione **Recomendar a un amigo**.


Pulse el botón **Compartir**.

Seleccione el método para compartir que desee, y comparta el código de referencia con sus amigos.

Canjear código

La primera vez que recibe un código de referencia de un amigo, puede canjearlo para recibir una licencia de la versión Premium gratuita durante 30 días para usted y su amigo. El código de referencia solo puede utilizarse una vez para recibir una licencia de pago gratuita durante 30 días.

Para utilizar un código que ha recibido:

1. Diríjase al **Menú principal** .
2. Seleccione **Canjear código**.

Escriba en el campo de texto el código de referencia que ha recibido de su amigo y pulse **Intro**.

Tanto usted como el amigo que le envió el código recibirán una confirmación en sus dispositivos correspondientes.

Si dispone de más códigos (que no sean códigos de referencia), pulse **Desbloquear otro mes**.

Configuración

Para acceder a la configuración del programa, pulse **Menú**  en la pantalla principal de ESET Mobile Security (o pulse el botón Menú de su dispositivo) y pulse **Configuración**.

Hacer copia de seguridad y restaurar

ESET Mobile Security le permite crear un archivo de copia de seguridad que contiene su configuración de ESET Mobile Security. Puede descargar este archivo en un dispositivo externo y usarlo para restaurar la configuración de ESET Mobile Security.

Idioma

De forma predeterminada, ESET Mobile Security se instala en el idioma establecido como valor predeterminado del sistema en su dispositivo (en la configuración de Teclado e idioma del SO Android). Si desea cambiar el idioma de la interfaz de usuario de la aplicación, pulse **Idioma** y seleccione el idioma que quiera.

Notificación permanente

(Esta opción solo está disponible en Android 7 y versiones posteriores)

ESET Mobile Security mostrará una notificación en la parte inferior de la barra de notificaciones de Android. Si no desea que se muestre la notificación, anule la selección de Notificación permanente y pulse Desactivar.

Consentimiento del usuario

- **Permitir ESET LiveGrid®:** para obtener más información sobre el sistema de respuesta ESET LiveGrid®, visite la [sección Configuración avanzada](#).
- **Permitir que los análisis nos ayuden a mejorar nuestros productos:** ESET Mobile Security enviará información anónima sobre la aplicación (rendimiento, estadísticas operativas) que nos ayudará a mejorar nuestra aplicación y nuestros servicios. Para obtener más información sobre la información que recopilamos, visite el [capítulo Política de privacidad](#).
- **Permitir el uso de datos con fines de marketing**
- **Permitir que ESET envíe descuentos promocionales y noticias sobre productos:** se mostrarán en el producto noticias y las ofertas más recientes de ESET.

Actualización

Para disfrutar de la máxima protección es importante usar la versión más reciente de ESET Mobile Security. Pulse **Actualizar** para ver si hay una versión más reciente disponible para su descarga desde el sitio web de ESET. Esta opción no está disponible si se realizó la descarga de ESET Mobile Security desde Google Play; en este caso, la actualización del producto se realiza desde Google Play.

Desinstalar

La ejecución del asistente de desinstalación quitará ESET Mobile Security del dispositivo de forma permanente. Si la protección Antirrobo está activada, se le pedirá que introduzca su PIN/patrón de seguridad de ESET Mobile Security o su huella dactilar. Para desinstalar el producto manualmente, siga [los pasos descritos en esta sección](#).



Protección contra desinstalación

La opción Desinstalar protección no está activa en las versiones de Android 7.0 y posteriores.


Atención al cliente

Los especialistas de atención al cliente de ESET están disponibles para prestar ayuda administrativa y ofrecer soporte técnico relacionado con ESET Mobile Security o cualquier otro producto de ESET.



[Póngase en contacto con el Servicio de atención al cliente de ESET](#)

Si desea enviar una solicitud de soporte técnico directamente desde su dispositivo:

1. Pulse Menú  en la pantalla principal de ESET Mobile Security (o pulse el botón Menú de su dispositivo).
2. Pulse **Atención al cliente**.
3. Pulse **Atención al cliente** para crear una solicitud de soporte técnico.
4. Rellene todos los campos obligatorios. ESET Mobile Security incluye funciones de registro avanzado para ayudarle a diagnosticar posibles problemas técnicos.
5. Para ofrecer a ESET un registro detallado de la aplicación, asegúrese de que esté seleccionada la opción

Enviar registro de la aplicación (predeterminado).

6. Pulse **Enviar** para enviar su solicitud.

7. Un especialista del Servicio de atención al cliente de ESET se pondrá en contacto con usted en la dirección de correo electrónico que haya facilitado.

Los registros de diagnóstico se han eliminado si ha desinstalado y vuelto a instalar ESET Mobile Security para resolver problemas. Se recomienda replicar el problema de nuevo y enviar los registros después.

La aplicación no se puede abrir o no responde



Para enviar una solicitud de soporte a ESET si ESET Mobile Security no responde o no puede abrirlo, diríjase a **Configuración > Aplicaciones > ESET Mobile Security > Almacenamiento > Gestionar almacenamiento**. Haga clic en **Atención al cliente** y cumplimente los campos necesarios.

Acuerdo de licencia para el usuario final

Fecha de entrada en vigor: 19 de octubre de 2021.

IMPORTANTE: Lea los términos y condiciones de la aplicación del producto que se detallan a continuación antes de descargarlo, instalarlo, copiarlo o utilizarlo. **LA DESCARGA, LA INSTALACIÓN, LA COPIA O LA UTILIZACIÓN DEL SOFTWARE IMPLICAN SU ACEPTACIÓN DE ESTOS TÉRMINOS Y CONDICIONES Y DE LA [POLÍTICA DE PRIVACIDAD](#).**

Acuerdo de licencia para el usuario final

En virtud de los términos de este Acuerdo de licencia para el usuario final ("Acuerdo"), firmado por ESET, spol. s r. o., con domicilio social en Einsteinova 24, 85101 Bratislava, Slovak Republic, empresa inscrita en el Registro Mercantil administrado por el tribunal de distrito de Bratislava I, sección Sro, número de entrada 3586/B, número de registro comercial 31333532 ("ESET" o "el Proveedor") y usted, una persona física o jurídica ("Usted" o el "Usuario final"), tiene derecho a utilizar el Software definido en el artículo 1 del presente Acuerdo. El Software definido en el artículo 1 del presente Acuerdo puede almacenarse en un soporte de datos, enviarse por correo electrónico, descargarse de Internet, descargarse de los servidores del Proveedor u obtenerse de otras fuentes en virtud de los términos y condiciones especificados a continuación.

ESTO NO ES UN CONTRATO DE VENTA, SINO UN ACUERDO SOBRE LOS DERECHOS DEL USUARIO FINAL. El proveedor sigue siendo el propietario de la copia del software y del soporte físico incluidos en el paquete de venta, así como de todas las copias que el usuario final pueda realizar en virtud de este acuerdo.

Al hacer clic en las opciones "Acepto" o "Acepto..." durante la instalación, la descarga, la copia o la utilización del Software, expresa su aceptación de los términos y condiciones de este Acuerdo y acepta la Política de Privacidad. Si no acepta todos los términos y condiciones de este Acuerdo o la Política de Privacidad, haga clic en la opción de cancelación, cancele la instalación o descarga o destruya o devuelva el Software, el soporte de instalación, la documentación adjunta y el recibo de compra al Proveedor o al lugar donde haya adquirido el Software.

USTED ACEPTA QUE SU UTILIZACIÓN DEL SOFTWARE INDICA QUE HA LEÍDO ESTE ACUERDO, QUE LO COMPRENDE Y QUE ACEPTA SU SUJECCIÓN A LOS TÉRMINOS Y CONDICIONES.

1. Software. En este acuerdo, el término "Software" se refiere a: (i) el programa informático que acompaña a este Acuerdo y todos sus componentes; (ii) todo el contenido de los discos, CD-ROM, DVD, mensajes de correo electrónico y documentos adjuntos, o cualquier otro soporte que esté vinculado a este Acuerdo, incluido el código objeto del Software proporcionado en un soporte de datos, por correo electrónico o descargado de

Internet; (iii) todas las instrucciones escritas y toda la documentación relacionada con el Software, especialmente todas las descripciones del mismo, sus especificaciones, todas las descripciones de las propiedades o el funcionamiento del Software, todas las descripciones del entorno operativo donde se utiliza, las instrucciones de uso o instalación del software o todas las descripciones de uso del mismo ("Documentación"); (iv) copias, reparaciones de posibles errores, adiciones, extensiones y versiones modificadas del software, así como actualizaciones de sus componentes, si las hay, para las que el Proveedor le haya concedido una licencia en virtud del artículo 3 de este Acuerdo. El Software se proporciona únicamente en forma de código objeto ejecutable.

2. Instalación, Ordenador y una Clave de licencia. El Software suministrado en un soporte de datos, enviado por correo electrónico, descargado de Internet, descargado de los servidores del Proveedor u obtenido de otras fuentes requiere instalación. Debe instalar el Software en un Ordenador correctamente configurado que cumpla, como mínimo, los requisitos especificados en la Documentación. El método de instalación se describe en la Documentación. No puede haber programas informáticos o hardware que puedan afectar negativamente al Software instalados en el Ordenador donde instale el Software. Ordenador significa hardware, lo que incluye, entre otros elementos, ordenadores personales, portátiles, estaciones de trabajo, ordenadores de bolsillo, smartphones, dispositivos electrónicos de mano u otros dispositivos electrónicos para los que esté diseñado el Software, en el que se instale o utilice. Clave de licencia significa la secuencia exclusiva de símbolos, letras, números o signos especiales facilitada al Usuario final para permitir el uso legal del Software, su versión específica o la ampliación de la validez de la Licencia de conformidad con este Acuerdo.

3. Licencia. Siempre que haya aceptado los términos de este Acuerdo y cumpla con todos los términos y condiciones aquí especificados, el Proveedor le concederá los siguientes derechos (la "Licencia"):

a) **Instalación y uso.** Tendrá el derecho no exclusivo e intransferible de instalar el Software en el disco duro de un ordenador u otro soporte permanente para el almacenamiento de datos, de instalar y almacenar el Software en la memoria de un sistema informático y de implementar, almacenar y mostrar el Software.

b) **Estipulación del número de licencias.** El derecho de uso del software está sujeto a un número de usuarios finales. La expresión "un usuario final" se utilizará cuando se haga referencia a lo siguiente: (i) la instalación del software en un sistema informático o (ii) un usuario informático que acepta correo electrónico a través de un Agente de usuario de correo ("un AUC") cuando el alcance de una licencia esté vinculado al número de buzones de correo. Si el AUC acepta correo electrónico y, posteriormente, lo distribuye de forma automática a varios usuarios, el número de usuarios finales se determinará según el número real de usuarios para los que se distribuyó el correo electrónico. Si un servidor de correo realiza la función de una pasarela de correo, el número de usuarios finales será equivalente al número de usuarios de servidor de correo a los que dicha pasarela preste servicios. Si se envía un número indefinido de direcciones de correo electrónico a un usuario, que las acepta (por ejemplo, mediante alias), y el cliente no distribuye los mensajes automáticamente a más usuarios, se necesita una licencia para un ordenador. No utilice la misma licencia en varios ordenadores de forma simultánea. El Usuario final tiene derecho a introducir la Clave de licencia en el Software si tiene derecho a utilizar el Software de acuerdo con la limitación derivada del número de licencias otorgadas por el Proveedor. La Clave de licencia se considera confidencial: no debe compartir la Licencia con terceros ni permitir que terceros utilicen la Clave de licencia, a menos que lo permitan este Acuerdo o el Proveedor. Si su Clave de licencia se ve expuesta, notifíquesele inmediatamente al Proveedor.

c) **Home Edition o Business Edition.** La versión Home Edition del Software se utilizará exclusivamente en entornos privados o no comerciales para uso doméstico y familiar. Debe obtener una versión Business Edition del Software para poder utilizarlo en entornos comerciales y en servidores de correo, relays de correo, puertas de enlace de correo o puertas de enlace a Internet.

d) **Vigencia de la licencia.** Tiene derecho a utilizar el Software durante un período de tiempo limitado.

e) **Software OEM.** El Software clasificado como "OEM" solo se puede utilizar en el equipo con el que lo haya

obtenido. No se puede transferir a otro ordenador.

f) **Software de prueba y NFR.** El Software cuya venta esté prohibida o de prueba no se puede pagar, y únicamente se debe utilizar para demostraciones o para probar las características del Software.

g) **Terminación de la licencia.** La licencia se terminará automáticamente cuando concluya su período de vigencia. Si no cumple algunas de las disposiciones de este acuerdo, el proveedor podrá cancelarlo sin perjuicio de los derechos o soluciones legales que tenga a su disposición para estos casos. En caso de cancelación de la Licencia, Usted debe eliminar, destruir o devolver (a sus expensas) el Software y todas las copias de seguridad del mismo a ESET o a la tienda donde lo haya adquirido. Tras la terminación de la Licencia, el Proveedor estará autorizado a cancelar el derecho que tiene el Usuario final para utilizar las funciones del Software que requieren conexión a los servidores del Proveedor o de terceros.

4. **Funciones con requisitos de recopilación de datos y conexión a Internet.** El Software necesita conexión a Internet para funcionar correctamente, y debe conectarse periódicamente a los servidores del Proveedor o a servidores de terceros; además, se recopilarán datos de acuerdo con la Política de Privacidad. La conexión a Internet y la recopilación de datos son necesarias para las siguientes funciones del Software:

a) **Actualizaciones del software.** El Proveedor podrá publicar actualizaciones del Software ("Actualizaciones") cuando lo estime oportuno, aunque no está obligado a proporcionarlas. Esta función se activa en la sección de configuración estándar del software y las actualizaciones se instalan automáticamente, a menos que el usuario final haya desactivado la instalación automática de actualizaciones. Para proporcionar Actualizaciones, es necesario verificar la autenticidad de la licencia, lo que incluye información sobre el ordenador o la plataforma en los que está instalado el Software, de acuerdo con la Política de Privacidad.

La Política de final de la vida útil ("Política de final de la vida útil"), disponible en https://go.eset.com/eol_home, puede regir la forma de proporcionar las Actualizaciones. No se proporcionarán Actualizaciones después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil.

b) **Envío de amenazas e información al proveedor.** El software incluye funciones que recogen muestras de virus informáticos y otros programas informáticos maliciosos, así como objetos sospechosos, problemáticos, potencialmente indeseables o potencialmente inseguros como archivos, direcciones URL, paquetes de IP y tramas Ethernet ("amenazas") y posteriormente las envía al Proveedor, incluida, a título enunciativo pero no limitativo, información sobre el proceso de instalación, el Ordenador o la plataforma en la que el Software está instalado e información sobre las operaciones y las funciones del Software ("Información"). La Información y las Amenazas pueden contener datos (incluidos datos personales obtenidos de forma aleatoria o accidental) sobre el Usuario final u otros usuarios del ordenador en el que el Software está instalado, así como los archivos afectados por las Amenazas junto con los metadatos asociados.

La información y las amenazas pueden recogerse mediante las siguientes funciones del software:

i. La función del sistema de reputación LiveGrid incluye la recopilación y el envío al proveedor de algoritmos hash unidireccionales relacionados con las amenazas. Esta función se activa en la sección de configuración estándar del software.

ii. La función del Sistema de Respuesta LiveGrid incluye la recopilación y el envío al Proveedor de las Amenazas con los metadatos y la Información asociados. Esta función la puede activar el Usuario final durante el proceso de instalación del Software.

El Proveedor solo podrá utilizar la Información y las Amenazas recibidas con fines de análisis e investigación de las Amenazas y mejora de la verificación de la autenticidad del Software y de la Licencia, y deberá tomar las medidas pertinentes para garantizar la seguridad de las Amenazas y la Información recibidas. Si se activa esta función del

Software, el Proveedor podrá recopilar y procesar las Amenazas y la Información como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. Estas funciones se pueden desactivar en cualquier momento.

A los efectos de este Acuerdo, es necesario recopilar, procesar y almacenar datos que permitan al Proveedor identificarle, de acuerdo con la Política de Privacidad. Acepta que el Proveedor puede comprobar por sus propios medios si está utilizando el Software de conformidad con las disposiciones de este Acuerdo. Acepta que, a los efectos de este Acuerdo, es necesaria la transferencia de sus datos, durante la comunicación entre el Software y los sistemas informáticos del Proveedor o sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, para garantizar la funcionalidad del Software y la autorización para utilizar el Software y proteger los derechos del Proveedor.

Tras la terminación de este Acuerdo, el Proveedor y sus socios comerciales, como parte de la red de distribución y asistencia técnica del Proveedor, estarán autorizados a transferir, procesar y almacenar sus datos identificativos fundamentales para fines relacionados con la facturación, la ejecución del Acuerdo y la transmisión de notificaciones en su Ordenador.

En la Política de Privacidad, disponible en el sitio web del Proveedor y accesible directamente desde el proceso de instalación, pueden encontrarse detalles sobre privacidad, protección de datos personales y Sus derechos como persona interesada. También puede visitarla desde la sección de ayuda del Software.

5. Ejercicio de los derechos de usuario final. Debe ejercer los derechos del Usuario final en persona o a través de sus empleados. Tiene derecho a utilizar el Software solamente para asegurar sus operaciones y proteger los Ordenadores o los sistemas informáticos para los que ha obtenido una Licencia.

6. Restricciones de los derechos. No puede copiar, distribuir, extraer componentes ni crear versiones derivadas del software. El uso del software está sujeto a las siguientes restricciones:

- a) Puede realizar una copia del software en un soporte de almacenamiento permanente, a modo de copia de seguridad para el archivo, siempre que esta no se instale o utilice en otro ordenador. La creación de más copias del software constituirá una infracción de este acuerdo.
- b) No puede utilizar, modificar, traducir ni reproducir el software, ni transferir los derechos de uso del software o copias del mismo de ninguna forma que no se haya establecido expresamente en este acuerdo.
- c) No puede vender, conceder bajo licencia, alquilar, arrendar ni prestar el software, ni utilizarlo para prestar servicios comerciales.
- d) No puede aplicar la ingeniería inversa, descompilar ni desmontar el software, ni intentar obtener de otra manera su código fuente, salvo que la ley prohíba expresamente esta restricción.
- e) Acepta que el uso del software se realizará de conformidad con la legislación aplicable en la jurisdicción donde se utilice, y que respetará las restricciones aplicables a los derechos de copyright y otros derechos de propiedad intelectual.
- f) Usted manifiesta estar de acuerdo en usar el software y sus funciones únicamente de manera tal que no se vean limitadas las posibilidades del usuario final de acceder a tales servicios. El proveedor se reserva el derecho de limitar el alcance de los servicios proporcionados a ciertos usuarios finales, a fin de permitir que la máxima cantidad posible de usuarios finales pueda hacer uso de esos servicios. El hecho de limitar el alcance de los servicios también significará la total anulación de la posibilidad de usar cualquiera de las funciones del software y la eliminación de los datos y la información que haya en los servidores del proveedor o de terceros en relación con una función específica del software.

g) Se compromete a no realizar actividades que impliquen el uso de la Clave de licencia en contra de los términos de este Acuerdo o que signifiquen facilitar la Clave de licencia a personas no autorizadas a utilizar el Software, como transferir la Clave de licencia utilizada o sin utilizar de cualquier forma, así como la reproducción no autorizada, la distribución de Claves de licencia duplicadas o generadas o el uso del Software como resultado del uso de una Clave de licencia obtenida de fuentes distintas al Proveedor.

7. Copyright. El software y todos los derechos, incluidos, entre otros, los derechos propietarios y de propiedad intelectual, son propiedad de ESET y/o sus proveedores de licencias. Los propietarios están protegidos por disposiciones de tratados internacionales y por todas las demás leyes aplicables del país en el que se utiliza el software. La estructura, la organización y el código del software son secretos comerciales e información confidencial de ESET y/o sus proveedores de licencias. Solo puede copiar el software según lo estipulado en el artículo 6 (a). Todas las copias autorizadas en virtud de este acuerdo deben contener los mismos avisos de copyright y de propiedad que aparecen en el software. Por el presente acepta que, si aplica técnicas de ingeniería inversa al código fuente del software, lo descompila, lo desmonta o intenta descubrirlo de alguna otra manera que infrinja las disposiciones de este acuerdo, se considerará de forma automática e irrevocable que la totalidad de la información así obtenida se deberá transferir al proveedor y que este será su propietario a partir del momento en que dicha información exista, sin perjuicio de los derechos del proveedor con respecto a la infracción de este acuerdo.

8. Reserva de derechos. Por este medio, el Proveedor se reserva todos los derechos del Software, excepto por los derechos concedidos expresamente bajo los términos de este Acuerdo a Usted como el Usuario final del Software.

9. Versiones en varios idiomas, software en soporte dual, varias copias. Si el software es compatible con varias plataformas o idiomas, o si recibe varias copias del software, solo puede utilizar el software para el número de sistemas informáticos y para las versiones para los que haya obtenido una licencia. No puede vender, arrendar, alquilar, sublicenciar, prestar o transferir ninguna versión o copias del Software no utilizado por Usted.

10. Comienzo y rescisión del Acuerdo. Este acuerdo es efectivo a partir de la fecha en que acepte sus términos. Puede terminar este acuerdo en cualquier momento mediante la desinstalación, destrucción o devolución (a sus expensas) del software, todas las copias de seguridad y todo el material relacionado que le hayan suministrado el proveedor o sus socios comerciales. Su derecho a usar el Software y sus funciones puede estar sujeto a la Política de final de la vida útil. Cuando el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil, dejará de tener derecho a utilizar el Software. Independientemente del modo de terminación de este acuerdo, las disposiciones de los artículos 7, 8, 11, 13, 19 y 21 seguirán en vigor de forma ilimitada.

11. DECLARACIONES DEL USUARIO FINAL. COMO USUARIO FINAL, USTED RECONOCE QUE EL SOFTWARE SE SUMINISTRA "TAL CUAL", SIN GARANTÍA EXPRESA O IMPLÍCITA DE NINGÚN TIPO Y DENTRO DEL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE. NI EL PROVEEDOR, SUS PROVEEDORES DE LICENCIAS O SUS AFILIADOS NI LOS TITULARES DEL COPYRIGHT OFRECEN NINGUNA GARANTÍA O DECLARACIÓN, EXPRESA O IMPLÍCITA; EN PARTICULAR, NINGUNA GARANTÍA DE VENTAS O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA O GARANTÍAS DE QUE EL SOFTWARE NO INFRINJA UNA PATENTE, DERECHOS DE PROPIEDAD INTELECTUAL, MARCAS COMERCIALES U OTROS DERECHOS DE TERCEROS. NI EL PROVEEDOR NI NINGUNA OTRA PARTE GARANTIZAN QUE LAS FUNCIONES CONTENIDAS EN EL SOFTWARE SATISFAGAN SUS REQUISITOS O QUE EL SOFTWARE FUNCIONE SIN INTERRUPCIONES NI ERRORES. ASUME TODOS LOS RIESGOS Y RESPONSABILIDAD DE LA SELECCIÓN DEL SOFTWARE PARA CONSEGUIR LOS RESULTADOS QUE DESEA Y DE LA INSTALACIÓN, EL USO Y LOS RESULTADOS OBTENIDOS.

12. Ninguna obligación adicional. Este Acuerdo no crea obligaciones del lado del Proveedor y sus licenciataria, excepto las obligaciones específicamente indicadas en este Acuerdo.

13. LIMITACIÓN DE RESPONSABILIDAD. HASTA EL ALCANCE MÁXIMO PERMITIDO POR LA LEGISLACIÓN APLICABLE, EN NINGÚN CASO EL PROVEEDOR, SUS EMPLEADOS O SUS PROVEEDORES DE LICENCIAS SERÁN RESPONSABLES DE PÉRDIDAS DE BENEFICIOS, DE INGRESOS, DE VENTAS O DE DATOS NI DE COSTES DERIVADOS DE LA OBTENCIÓN DE PRODUCTOS O SERVICIOS DE SUSTITUCIÓN, DE DAÑOS A LA PROPIEDAD, DE DAÑOS PERSONALES, DE LA INTERRUPCIÓN DEL NEGOCIO, DE LA PÉRDIDA DE INFORMACIÓN COMERCIAL O DE DAÑOS ESPECIALES, DIRECTOS, INDIRECTOS, ACCIDENTALES, ECONÓMICOS, DE COBERTURA, CRIMINALES O SUCESIVOS, CAUSADOS DE CUALQUIER MODO, YA SEA A CAUSA DE UN CONTRATO, UNA CONDUCTA INADECUADA INTENCIONADA, UNA NEGLIGENCIA U OTRO HECHO QUE ESTABLEZCA RESPONSABILIDAD, DERIVADOS DE LA INSTALACIÓN, EL USO O LA INCAPACIDAD DE USO DEL SOFTWARE, INCLUSO EN EL CASO DE QUE AL PROVEEDOR O A SUS PROVEEDORES DE LICENCIAS O FILIALES SE LES HAYA NOTIFICADO LA POSIBILIDAD DE DICHOS DAÑOS. DADO QUE DETERMINADOS PAÍSES Y JURISDICCIONES NO PERMITEN LA EXCLUSIÓN DE RESPONSABILIDAD, PERO PUEDEN PERMITIR LA LIMITACIÓN DE RESPONSABILIDAD, EN DICHOS CASOS, LA RESPONSABILIDAD DEL PROVEEDOR, SUS EMPLEADOS, LICENCIATARIOS O AFILIADOS SE LIMITARÁ AL PRECIO QUE USTED PAGÓ POR LA LICENCIA.

14. Ninguna de las disposiciones de este acuerdo se establece en perjuicio de los derechos estatutarios de una parte que actúe como consumidor en contra de lo aquí dispuesto.

15. Soporte técnico. ESET y los terceros contratados por ESET proporcionarán soporte técnico, a su discreción, sin ningún tipo de garantía o declaración. No se proporcionará soporte técnico después de que el Software o cualquiera de sus funciones lleguen a la fecha de final de la vida útil definida en la Política de final de la vida útil. El usuario final debe realizar una copia de seguridad de todos los datos, aplicaciones de software y programas almacenados en el ordenador antes de recibir soporte técnico. ESET y/o los terceros contratados por ESET no se hacen responsables de los daños, las pérdidas de datos, elementos en propiedad, software o hardware ni las pérdidas de ingresos a causa de la prestación del servicio de soporte técnico. ESET y/o los terceros contratados por ESET se reservan el derecho de determinar que la solución de un problema no entra dentro del ámbito de soporte técnico. ESET se reserva el derecho de rechazar, anular o terminar, a su discreción, la disposición de servicio técnico. Pueden ser necesarios los datos de Licencia, la Información y otros datos de acuerdo con la Política de Privacidad para prestar soporte técnico.

16. Transferencia de la licencia. El software se puede transferir de un sistema informático a otro, a no ser que se indique lo contrario en los términos del acuerdo. Si no se infringen los términos del acuerdo, el usuario solo puede transferir la licencia y todos los derechos derivados de este acuerdo a otro usuario final de forma permanente con el consentimiento del proveedor, y con sujeción a las siguientes condiciones: (i) el usuario final original no conserva ninguna copia del software; (ii) la transferencia de derechos es directa, es decir, del usuario final original al nuevo usuario final; (iii) el nuevo usuario final asume todos los derechos y obligaciones correspondientes al usuario final original en virtud de los términos de este acuerdo; (iv) el usuario final original proporciona al nuevo usuario final la documentación necesaria para verificar la autenticidad del software, tal como se especifica en el artículo 17.

17. Verificación de la autenticidad del Software. El Usuario final puede demostrar su derecho a utilizar el Software de las siguientes maneras: (i) mediante un certificado de licencia emitido por el Proveedor o un tercero designado por el Proveedor; (ii) mediante un acuerdo de licencia por escrito, si se ha celebrado dicho acuerdo; (iii) mediante el envío de un mensaje de correo electrónico enviado por el Proveedor con la información de la licencia (nombre de usuario y contraseña). Pueden ser necesarios los datos de Licencia y de identificación del Usuario final de acuerdo con la Política de Privacidad para verificar la autenticidad del Software.

18. Licencia para organismos públicos y gubernamentales de EE.UU.. El software se proporcionará a los organismos públicos, incluido el gobierno de Estados Unidos, con los derechos y las restricciones de licencia descritos en este acuerdo.

19. Cumplimiento de las normas de control comercial.

a) No puede exportar, reexportar, transferir ni poner el Software a disposición de ninguna persona de alguna otra forma, ni directa ni indirectamente, ni usarlo de ninguna forma ni participar en ninguna acción si ello puede tener como resultado que ESET o su grupo, sus filiales o las filiales de cualquier empresa del grupo, así como las entidades controladas por dicho grupo ("Filiales"), incumplan las Leyes de control comercial o sufran consecuencias negativas debido a dichas Leyes, entre las que se incluyen

i. cualquier ley que controle, restrinja o imponga requisitos de licencia en relación con la exportación, la reexportación o la transferencia de bienes, software, tecnología o servicios, publicada oficialmente o adoptada por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen y

ii. cualesquier sanciones, restricciones, embargos o prohibiciones de importación o exportación, de transferencia de fondos o activos o de prestación de servicios, todo ello en los ámbitos económico, financiero y comercial o en cualquier otro ámbito, o cualquier medida equivalente, impuestos por cualquier autoridad gubernamental, estatal o reguladora de los Estados Unidos de América, Singapur, el Reino Unido, la Unión Europea o cualquiera de sus Estados miembros o cualquier país en el que deban cumplirse obligaciones en virtud del Acuerdo o en el que ESET o cualquiera de sus Filiales estén registradas u operen.

(los actos jurídicos a los que se hace referencia en los puntos i e ii. anteriores se denominan, conjuntamente, "Leyes de control comercial").

b) ESET tiene derecho a suspender las obligaciones adquiridas en virtud de estos Términos o a rescindir los Términos con efecto inmediato en el caso de que:

i. con una base razonable para fundamentar su opinión, ESET determine que el Usuario ha incumplido o es probable que incumpla lo dispuesto en el Artículo 19 a) del Acuerdo; o

ii. el Usuario final o el Software queden sujetos a las Leyes de control comercial y, como resultado, con una base razonable para fundamentar su opinión, ESET determine que continuar cumpliendo las obligaciones adquiridas en virtud del Acuerdo podría causar que ESET o sus Filiales incumplieran las Leyes de control comercial o sufrieran consecuencias negativas debido a dichas Leyes.

c) Ninguna disposición del Acuerdo tiene por objeto inducir u obligar a ninguna de las partes a actuar o dejar de actuar (ni a aceptar actuar o dejar de actuar) de forma incompatible con las Leyes de control comercial aplicables o de forma penalizada o prohibida por dichas Leyes, y ninguna disposición del Acuerdo debe interpretarse en ese sentido.

20. Avisos. Los avisos y las devoluciones del Software y la Documentación deben enviarse a ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, sin perjuicio del derecho de ESET a comunicarle los cambios que se produzcan en este Acuerdo, en las Políticas de privacidad, en la Política de final de la vida útil y en la Documentación de conformidad con el art. 22 del Acuerdo. ESET puede enviarle correos electrónicos y notificaciones en la aplicación a través del Software o publicar la comunicación en su sitio web. Acepta recibir comunicaciones legales de ESET en formato electrónico, lo que incluye cualquier comunicación sobre cambios en los Términos, los Términos especiales o las Políticas de privacidad, cualquier propuesta o aceptación de contrato o invitación para negociar, avisos u otras comunicaciones legales. Dicha comunicación electrónica se considerará recibida por escrito, a menos que la legislación aplicable requiera específicamente una forma de comunicación diferente.

21. Legislación aplicable. Este acuerdo se registrará e interpretará de conformidad con la legislación eslovaca. El usuario final y el proveedor aceptan que los principios del conflicto entre las leyes y la Convención de las Naciones Unidas para la Venta Internacional de Bienes no serán de aplicación. Acepta expresamente que las disputas o reclamaciones derivadas de este acuerdo y relacionadas con el proveedor, así como las disputas o reclamaciones

relacionadas con el uso del software, se resolverán en el Tribunal del Distrito de Bratislava I. Acepta expresamente la jurisdicción de dicho tribunal.

22. Disposiciones generales. El hecho de que alguna de las disposiciones de este acuerdo no sea válida o aplicable no afectará a la validez de las demás disposiciones del acuerdo, que seguirán siendo válidas y aplicables de conformidad con las condiciones aquí estipuladas. Este Acuerdo se ha formalizado en inglés. Si se realiza una traducción del Acuerdo por motivos de comodidad o por cualquier otro motivo, o en caso de discrepancia entre las versiones de este Acuerdo en diferentes idiomas, prevalecerá la versión en inglés.

ESET se reserva el derecho a realizar cambios en el Software y a modificar los términos de este Acuerdo, sus Anexos, la Política de Privacidad, la Política de final de la vida útil y la Documentación, o de cualquier parte de lo anterior, en cualquier momento mediante la actualización del documento pertinente (i) para reflejar los cambios del Software o en la forma en la que ESET desarrolla su actividad, (ii) por motivos legales, de legislación o de seguridad, o (iii) para evitar un uso inadecuado o perjuicios. Se le notificará cualquier modificación del Acuerdo por correo electrónico, mediante una notificación en la aplicación o a través de otros medios electrónicos. Si no está de acuerdo con los cambios propuestos para el Acuerdo, puede rescindir el acuerdo con el art. 10 en el plazo de 30 días después de recibir un aviso del cambio. A menos que rescinda el Acuerdo dentro de este límite de tiempo, los cambios propuestos se considerarán aceptados y estarán vigentes para Usted a partir de la fecha en que reciba un aviso del cambio.

Este es el Acuerdo completo entre el Proveedor y Usted en relación con el Software y sustituye cualquier otra representación, debate, compromiso, comunicación o publicidad previas relacionadas con el Software.

ANEXO AL ACUERDO

Evaluación de seguridad de los dispositivos conectados a la red. A la evaluación de seguridad de los dispositivos conectados a la red se le aplican las siguientes disposiciones adicionales:

El Software incluye una función destinada a comprobar la seguridad de la red local del Usuario final y la seguridad de los dispositivos de la red local. Esta función necesita el nombre de la red local e información sobre los dispositivos de la red local, como presencia, tipo, nombre, dirección IP y dirección MAC del dispositivo en la red local en conexión con la información de la licencia. La información también incluye el tipo de seguridad inalámbrica y el tipo de cifrado inalámbrico de los routers. Esta función también puede proporcionar información sobre la disponibilidad de una solución de software de seguridad destinada a proteger los dispositivos de la red local.

Protección contra el mal uso de los datos. A la protección contra el mal uso de los datos se le aplican las siguientes disposiciones adicionales:

El Software incluye una función que impide la pérdida o el uso indebido de datos esenciales en conexión directa con el robo de un Ordenador. Esta función está desactivada en la configuración predeterminada del Software. Se debe crear la Cuenta de ESET HOME para poder activarla; la función activa la recopilación de datos a través de esa cuenta en caso de producirse un robo del ordenador. Si activa esta función del Software, se recopilarán datos sobre el Ordenador robado y se enviarán al Proveedor; podrán incluirse datos sobre la ubicación de red del Ordenador, datos sobre el contenido mostrado en la pantalla del Ordenador, datos sobre la configuración del Ordenador o datos grabados por una cámara conectada al Ordenador (en adelante denominados "Datos"). El Usuario final solo tendrá derecho a utilizar los Datos obtenidos por esta función y facilitados a través de la Cuenta de ESET HOME para rectificar una situación adversa causada por el robo de un Ordenador. Únicamente a los efectos de esta función, el Proveedor procesa los Datos como se especifica en la Política de Privacidad y de acuerdo con la normativa legal relevante. El Proveedor permitirá al Usuario final acceder a los Datos durante el periodo necesario para alcanzar el fin con el que se obtuvieron los datos, que no debe superar el periodo de retención especificado en la Política de Privacidad. La protección contra el uso indebido de datos solo se utilizará con Ordenadores y cuentas a los que el Usuario final tenga acceso legítimo. Cualquier uso ilegal se denunciará

ante la autoridad competente. El Proveedor cumplirá las leyes pertinentes y colaborará con las autoridades encargadas del cumplimiento de las leyes en caso de uso indebido. Reconoce y acepta que es responsable de salvaguardar la contraseña para acceder a la Cuenta de ESET HOME y que no debe revelar su contraseña a terceros. El Usuario final es responsable de cualquier actividad que se realice utilizando la función de protección contra el uso indebido de datos y la Cuenta de ESET HOME, esté autorizada o no dicha actividad. Si su Cuenta de ESET HOME se ve expuesta, notifíquesele inmediatamente al Proveedor.

Códigos. A los códigos se les aplican las siguientes disposiciones adicionales:

ESET podrá crear y proporcionar códigos de referencia y otros códigos con fines promocionales o de marketing (de aquí en adelante, "códigos") según su propio criterio. Podrá canjear el código para prolongar la duración de la licencia en virtud de este acuerdo. ESET se reserva el derecho de desactivar el código en cualquier momento si dicho código se obtiene o utiliza de una forma que no cumpla con este acuerdo, o en caso de existir datos fehacientes que lleven a pensar que existe algún tipo de error, fraude o actividad ilegal asociados. Está obligado a cumplir las siguientes restricciones:

- i. No podrá canjear el código más de una vez.
- ii. No podrá vender, arrendar o alquilar el código ni utilizarlo para proporcionar servicios comerciales.
- iii. Acepta que ESET podrá desactivar el suministro o el uso del código en cualquier momento sin responsabilidad alguna para ESET.
- iv. Acepta que el código no se pueda cambiar por dinero en efectivo ni ninguna otra compensación.
- v. Acepta que el código o el uso del mismo pueden estar sujetos a condiciones especiales impuestas por ESET para la campaña de referencia, promocional o marketing concreta.

EULAID: EULA-PRODUCT-LG-EMS; 3537.0

Política de privacidad

La protección de los datos personales es muy importante para ESET, spol. s r. o., con domicilio social en Einsteinova 24, 851 01 Bratislava, Slovak Republic, registrada en el Registro Mercantil administrado por el Tribunal de Distrito de Bratislava I, Sección Sro, n.º de entrada 3586/B, n.º de registro de la empresa: 31333532 como Responsable del tratamiento ("ESET"). Cumplimos con el requisito de transparencia que se estipula en el Reglamento general de protección de datos de la UE ("RGPD"). Para lograr este objetivo, publicamos esta Política de privacidad con el único fin de informar a nuestros clientes ("Usuario final" o "Usted") sobre los siguientes temas de protección de datos personales:

- Fundamento jurídico del tratamiento de datos personales
- Intercambio y confidencialidad de datos
- Seguridad de datos
- Sus derechos como interesado
- Tratamiento de sus datos personales
- Información de contacto.

Fundamento jurídico del tratamiento de datos personales

Solo hay varias disposiciones jurídicas para el tratamiento de datos que usamos de acuerdo con el marco jurídico aplicable a la protección de los datos personales. El tratamiento de los datos personales en ESET es necesario para

la ejecución del [Acuerdo de licencia para el usuario final](#) ("EULA") con el Usuario final (artículo 6 1] b] del RGPD), que se aplica a la prestación de servicios o productos de ESET a menos que se indique explícitamente lo contrario, por ejemplo:

- El fundamento jurídico de interés legítimo (artículo 6 1] b] del RGPD), que nos permite tratar los datos sobre el uso que los clientes hacen de nuestros Servicios y su satisfacción para ofrecer a los usuarios los mejores niveles de protección, asistencia y experiencia que sea posible. Incluso el marketing es reconocido por la legislación aplicable como un interés legítimo, por lo que nos basamos en ese concepto para las comunicaciones de marketing con nuestros clientes.
- El consentimiento (artículo 6 1] b] del RGPD), que podemos solicitarle en situaciones concretas en las que consideramos que este fundamento jurídico es el más adecuado o si la ley lo requiere.
- El cumplimiento de una obligación legal (artículo 6 1] b] del RGPD), por ejemplo, estipulando los requisitos de comunicación electrónica o retención de facturas o documentos de facturación.

Intercambio y confidencialidad de datos

No compartimos sus datos con terceros. Sin embargo, ESET es una empresa que opera en todo el mundo a través de empresas o socios que forman parte de su red de ventas, servicio y asistencia. La información de licencias, facturación y asistencia técnica tratada por ESET puede transferirse entre filiales o socios para cumplir el EULA en aspectos como la prestación de servicios o la asistencia.

ESET prefiere procesar sus datos en la Unión Europea (UE). No obstante, en función de su ubicación (uso de nuestros productos o servicios fuera de la UE) o el servicio que elija, puede que sea necesario transferir sus datos a un país fuera de la UE. Por ejemplo, utilizamos servicios de terceros para prestar servicios de informática en la nube. En estos casos, seleccionamos cuidadosamente a los proveedores de servicios y ofrecemos un nivel adecuado de protección de los datos mediante medidas contractuales, técnicas y organizativas. Por lo general, aceptamos las cláusulas contractuales tipo de la UE con la normativa contractual aplicable si es necesario.

En algunos países de fuera de la UE, como el Reino Unido y Suiza, la UE ya ha determinado un nivel de protección de datos comparable. Gracias al nivel de protección de datos, la transferencia de datos a estos países no requiere ninguna autorización o acuerdo especial.

Seguridad de datos

ESET implementa medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado para los posibles riesgos. Hacemos todo lo posible para garantizar la confidencialidad, la integridad, la disponibilidad y la resistencia de los sistemas y los servicios de procesamiento. En caso de filtración de datos que pongan en peligro sus derechos y libertades, estamos preparados para notificárselo a la autoridad supervisora correspondiente y a los usuarios finales en calidad de interesados.

Derechos del titular de los datos.

Los derechos de los usuarios finales son importantes para nosotros, sean de un país de la UE o de fuera de la UE. Por lo tanto, en ESET les garantizamos los derechos siguientes. Para ejercer los derechos de los interesados, puede ponerse en contacto con nosotros a través del formulario de asistencia o por correo electrónico en la dirección dpo@eset.sk. Le pediremos la información siguiente con fines de identificación: Nombre, dirección de correo electrónico y, si procede, clave de licencia o número de cliente y empresa. No nos envíe otros datos personales, como la fecha de nacimiento. Cabe destacar que trataremos sus datos personales con fines de identificación y procesamiento de solicitudes.

Derecho a retirar el consentimiento. El derecho a retirar el consentimiento solo se aplica si se tratan los datos

con su consentimiento previo. Si nos da su consentimiento para tratar sus datos personales, podrá retirarlo en cualquier momento sin explicar los motivos. La retirada del consentimiento solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite.

Derecho de objeción. El derecho a oponerse al tratamiento se aplica si el tratamiento se basa en el interés legítimo de ESET o terceros. Si tratamos sus datos personales para proteger un interés legítimo, puede oponerse a dicho interés legítimo y al tratamiento de sus datos personales en cualquier momento. La oposición solo se aplicará en el futuro y no afectará a la legalidad de los datos tratados antes de la fecha en que se solicite. Si tratamos sus datos personales con fines de marketing directo, no es necesario explicar los motivos por los que se opone. Esto también se aplica a la creación de perfiles, ya que está relacionada con el marketing directo. En el resto de casos, debe enviarnos las quejas que tenga en relación con el interés legítimo de ESET para tratar sus datos personales.

En algunos casos, a pesar de su consentimiento, podemos seguir tratando sus datos personales sobre la base de otro fundamento jurídico (como la ejecución de un contrato).

Derecho de acceso. Como interesado, puede solicitar información sobre los datos personales que ESET almacena en cualquier momento sin coste alguno.

Derecho de rectificación. Si tratamos datos personales incorrectos de manera involuntaria, puede pedir que se corrija esta información.

Derecho a eliminar y restringir el tratamiento de datos personales. Como interesado, puede solicitar la eliminación o restricción del tratamiento de sus datos personales. Por ejemplo, si tratamos datos personales con su consentimiento y lo retira sin otro fundamento jurídico (como un contrato), eliminaremos sus datos personales de inmediato. Sus datos personales también se eliminarán cuando dejen de ser necesarios para los fines indicados al finalizar el periodo de retención.

Si solo utilizamos sus datos personales con fines de marketing directo y revoca su consentimiento o se opone al interés legítimo de ESET, restringiremos el tratamiento una vez que incluyamos sus datos de contacto en nuestra lista negra interna para evitar el contacto no solicitado. De lo contrario, sus datos personales se eliminarán.

Puede que estemos obligados a almacenar sus datos hasta que expiren las obligaciones de retención y los periodos emitidos por el organismo de legislación o las autoridades supervisoras. También pueden surgir periodos u obligaciones de retención porque la legislación eslovaca así lo exija. En ese caso, los datos correspondientes se eliminarán de forma rutinaria a partir de ese momento.

Derecho a la portabilidad de datos. Dado que es un interesado, le proporcionamos los datos personales que trata ESET en formato XLS.

Derecho a presentar una queja. Como interesado, puede presentar una reclamación ante una autoridad supervisora en cualquier momento. ESET se rige por la legislación de Eslovaquia y, al ser parte de la Unión Europea, en este país se debe cumplir la correspondiente legislación sobre protección de datos. La autoridad supervisora que gestiona cuestiones de datos es la Oficina de protección de datos personales de Eslovaquia, situada en Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Tratamiento de sus datos personales

Los servicios de ESET que se hayan implementado en nuestros productos se prestan en virtud de las condiciones de [EULA](#), pero algunos pueden requerir atención especial. Queremos proporcionarle más detalles sobre la recopilación de datos relacionada con la prestación de nuestros servicios. Prestamos distintos servicios descritos en el EULA y la documentación del [documentación](#). Para que todo funcione, debemos recopilar la siguiente

información:

Datos de licencias y facturación. ESET recopila y trata el nombre, la dirección de correo electrónico, la clave de licencia y, si procede, la dirección, la afiliación y los pagos de la empresa para facilitar la activación de la licencia, la entrega de la clave de licencia, los recordatorios de caducidad, las solicitudes de asistencia, la verificación de autenticidad de la licencia, la prestación de nuestros servicios y otras notificaciones (como mensajes de marketing) en virtud de la legislación aplicable o su consentimiento. Aunque ESET debe retener la información de facturación durante un periodo de 10 años, la información de la licencia se anonimizará en un plazo máximo de 12 meses una vez que la licencia caduque.

Actualizaciones y otras estadísticas. Los datos tratados abarcan información relativa al proceso de instalación y a su ordenador, incluidas la plataforma en la que está instalado nuestro producto e información sobre las operaciones y la funcionalidad de nuestros productos (como el sistema operativo, información sobre el hardware, identificadores de instalación, identificadores de licencias, dirección IP, dirección MAC o ajustes de configuración del producto). Todo ello se trata en el marco de los servicios de actualización con fines de mantenimiento, seguridad y mejora de la infraestructura de backend.

Estos datos se retienen junto con la información de identificación necesaria para las licencias y la facturación, ya que no es necesario identificar al Usuario final. El periodo de retención asciende a cuatro años.

Sistema de Reputación ESET LiveGrid®. Trata algoritmos hash unidireccionales relativos a infiltraciones para ejecutar el Sistema de Reputación ESET LiveGrid®, lo que mejora la eficiencia de nuestras soluciones antimalware mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube. Durante este proceso no se identifica al Usuario final.

Sistema de Respuesta ESET LiveGrid®. Muestras sospechosas y metadatos que forman parte del sistema de respuesta ESET LiveGrid®, lo que permite a ESET reaccionar inmediatamente ante las necesidades de los usuarios finales y responder a las amenazas más recientes. Dependemos de que Usted nos envíe

- Infiltraciones como posibles muestras de virus y otros programas malintencionados y sospechosos; objetos problemáticos, potencialmente no deseados o potencialmente peligrosos, como archivos ejecutables, mensajes de correo electrónico marcados por Usted como spam o marcados por nuestro producto;
- Información relativa al uso de Internet, como dirección IP e información geográfica, paquetes de IP, URL y marcos de Ethernet;
- Archivos de volcado de memoria y la información contenida en ellos.

No deseamos recopilar sus datos más allá de este ámbito, pero en ocasiones es imposible evitarlo. Los datos recopilados accidentalmente pueden estar incluidos en malware (recopilados sin su conocimiento o aprobación) o formar parte de nombres de archivos o URL, y no pretendemos que formen parte de nuestros sistemas ni tratarlos con el objetivo declarado en esta Política de privacidad.

La información obtenida y tratada con el Sistema de Respuesta ESET LiveGrid® se debe utilizar sin identificar al Usuario final.

Evaluación de seguridad de los dispositivos conectados a la red. Para ofrecer la función de evaluación de seguridad tratamos el nombre de la red local y la información sobre los dispositivos de dicha red (como presencia, tipo, nombre, dirección IP y dirección MAC del dispositivo en la red local) en relación con la información de la licencia. La información también incluye el tipo de seguridad inalámbrica y el tipo de cifrado inalámbrico de los routers. La información de licencia que identifique al Usuario final se anonimizará en un plazo máximo de 12 meses una vez que la licencia caduque.

Soporte técnico. La información de contacto o licencia y los datos contenidos en sus solicitudes de asistencia pueden ser necesarios para el servicio de soporte. Según el canal que elija para ponerse en contacto con

nosotros, podemos recopilar datos como su dirección de correo electrónico, su número de teléfono, información sobre licencias, datos del producto y descripción de su caso de asistencia. Podemos pedirle que nos facilite otra información para facilitar el servicio de asistencia. Los datos tratados para ofrecer asistencia técnica se almacenan durante cuatro años.

Protección contra el mal uso de los datos. Si crea la cuenta de ESET HOME en <https://home.eset.com> y marca su dispositivo como perdido con la función Antirrobo, se recopilará y tratará la siguiente información: datos de ubicación, capturas de pantalla, datos sobre la configuración de un ordenador y datos registrados por la cámara de un ordenador. Los datos recopilados se almacenan en nuestros servidores o los de nuestros proveedores de servicios, con un periodo de retención de 3 meses.

Análisis de uso y bloqueo. Siempre que nos dé su consentimiento, recopilaremos y analizaremos datos relacionados con el uso de nuestros productos para probar su rendimiento y mejorarlos para nuestros usuarios. Los datos recopilados pueden incluir diferentes acciones y eventos del usuario en el producto (por ejemplo, el inicio de la aplicación, la actualización de la aplicación, la duración de la sesión o las compras dentro de la aplicación), información sobre un dispositivo, plataforma o sistema operativo utilizado, así como datos relacionados con su edad, sexo, ubicación e intereses, que pueden estar asociados con distintos identificadores (por ejemplo, ID de instalación). También trataremos datos técnicos relacionados con los bloqueos de la aplicación (como información del dispositivo, identificador de instalación, seguimientos de bloqueo o minidump de bloqueo) para obtener información sobre los bloqueos o sus causas y garantizar que el producto esté totalmente operativo. A fin de recopilar y analizar esos datos, utilizamos nuestro Programa de mejora de la experiencia del cliente (en el que solo se tratan datos de telemetría anónimos) y los servicios de Google para obtener información más detallada. Para obtener más información sobre el tratamiento de sus datos por parte de Google, consulte la [Política de privacidad de Google](#) pertinente.

Tratamiento con fines de marketing. Si decide darnos su consentimiento para el tratamiento con fines de marketing, tanto nosotros como nuestros socios de marketing utilizaremos los datos sobre el uso que haga de nuestro producto para evaluar el rendimiento de nuestras actividades de marketing en línea, comprender mejor sus intereses y mostrarle anuncios en línea más relevantes para usted. Los datos recopilados pueden incluir diferentes acciones y eventos del usuario en el producto (por ejemplo, el inicio de la aplicación, la actualización de la aplicación, la duración de la sesión o las compras dentro de la aplicación), información sobre un dispositivo, plataforma o sistema operativo utilizado, así como datos relacionados con su edad, sexo, ubicación e intereses, que pueden estar asociados con distintos identificadores (ID de instalación, ID de anuncio móvil). Usamos Google para recopilar y analizar esos datos. Para obtener más información sobre el tratamiento de sus datos por parte de Google, consulte la [Política de privacidad de Google](#) pertinente.

Si la persona que utiliza nuestros productos o servicios no es el Usuario final que ha adquirido el producto o servicio ni ejecutado el EULA con ESET (como un empleado o familiar del Usuario final o una persona autorizada por este para utilizar el producto o servicio en virtud del EULA, el tratamiento de los datos se llevará a cabo según el interés legítimo de ESET conforme al artículo 6 1) f) del RGPD. De este modo, la persona autorizada por el Usuario final podrá utilizar nuestros productos y servicios en virtud del EULA.

Información de contacto

Si desea ejercer sus derechos como titular de los datos o tiene preguntas o dudas, envíenos un mensaje a:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk