ESET MOBILE SECURITY

PARA ANDROID

Manual de instalación y Guía del usuario

Haga clic aquí para descargar la versión más reciente de este documento

Contenido

ESET **MOBILE SECURITY**

Servicio de atención al cliente: www.eset.com/support

REV. 25. 4. 2012

1. Instalación de ESET Mobile Security

Para instalar ESET Mobile Security en Android, el dispositivo móvil debe cumplir los siguientes requisitos del sistema:

	Requisitos mínimos del sistema
Sistema operativo	Android 2.0/2.1 (Éclair) y posterior
CPU	600 MHz
RAM	256 MB
Espacio libre para almacenamiento interno	5 MB

NOTA: algunas funciones (p. ej., Antispam y Anti-Theft) no están disponibles en tablets Android 3.0 que no admiten llamadas ni mensajes. Puede encontrar más información en este artículo de la base de conocimientos (puede que no esté disponible en su idioma).

1.1 Instalación

Para instalar ESET Mobile Security, realice una de las siguientes acciones:

- busque ESET Mobile Security (o simplemente Eset) en la aplicación Google Play Store de su dispositivo Android. ESET Mobile Security aparece en **Aplicaciones** > **Herramientas**. De forma alternativa, puede instalar el programa escaneando el código QR siguiente con el dispositivo móvil y una aplicación del tipo QR Droid o Barcode Scanner.

- Descargue el ESET Mobile Security archivo de instalación *(ems.apk)* desde el sitio web de ESET escaneando el código QR siguiente.

- Descargue el archivo *ems.apk* en su equipo desde el sitio web de ESET. Copie el archivo en su dispositivo por Bluetooth o USB. Toque en el icono de inicio en la pantalla de inicio de Android (o vaya a **Inicio** > **Menú**), toque en **Ajustes** > **Aplicaciones** y asegúrese de que la opción **Orígenes desconocidos** esté seleccionada. Localice el archivo *ems.apk* mediante una aplicación similar a ASTRO File Manager o ES File Explorer. Abra el archivo y toque en **Instalar**. Una vez instalada la aplicación, toque en **Abrir**.

Advertencia: ESET Mobile Security debe instalarse en el almacenamiento interno del dispositivo. Algunos teléfonos cometen el error de permitir que los usuarios instalen aplicaciones en la tarjeta SD. Si instala ESET Mobile Security en la tarjeta SD, no funcionarán Protección en tiempo real, Antispam ni Anti-Theft.

Una vez que la instalación se ha realizado correctamente, active ESET Mobile Security siguiendo los pasos que se describen en la sección Activación del producto 4.

1.2 Desinstalación

Si desea desinstalar ESET Mobile Security del dispositivo, utilice el **Asistente de desinstalación** al que se puede acceder desde la pantalla principal de ESET Mobile Security o siga los siguientes pasos:

1. Toque en el icono de inicio en la pantalla de inicio de Android (o vaya a **Inicio** > **Menú**) y toque en **Ajustes** > **Ubicación y seguridad** > **Seleccionar administradores del dispositivo**, anule la selección de **Seguridad de ESET** y toque **Desactivar**. Cuando se le solicite, escriba su contraseña de ESET Mobile Security. (Si no ha establecido ESET Mobile Security como Administrador de dispositivos, omita este paso.)
2. Vuelva a **Ajustes** y toque en **Aplicaciones** > **Administrar aplicaciones** > **ESET Security** > **Desinstalar**.

ESET Mobile Security y la carpeta de cuarentena se eliminarán definitivamente del dispositivo móvil.

2. Activación del producto

Una vez que la instalación se ha realizado correctamente, es necesario activar ESET Mobile Security. Toque en **Activar ahora** en la pantalla principal de ESET Mobile Security.

Los métodos de activación varían en función de si se ha descargado ESET Mobile Security del sitio web de ESET o de Google Play.

- **Activar versión de prueba**: seleccione esta opción si no tiene una licencia y desea evaluar ESET Mobile Security antes de comprarlo. Escriba su dirección de **Email** para activar ESET Mobile Security durante un período de tiempo limitado. Tras la activación correcta del producto, recibirá un correo electrónico de confirmación. Las licencias de prueba solo se pueden activar una vez por dispositivo móvil.
- **Activar mediante una clave de activación**: (esta opción no estará disponible si ha realizado la instalación de ESET Mobile Security desde Google Play) si ha adquirido el programa con un nuevo dispositivo (o como un producto en caja física), con su compra recibirá una clave de activación. Escriba la información que haya recibido en el campo **Clave de activación** y la dirección de contacto actual en el campo **Email**. Los nuevos datos de autenticación (Nombre de usuario y Contraseña) sustituirán automáticamente a la clave de activación y se enviarán a la dirección de correo electrónico que haya especificado.
- **Activar mediante el nombre de usuario y la contraseña**: (esta opción no estará disponible si ha realizado la instalación de ESET Mobile Security desde Google Play) si ha adquirido el producto en un distribuidor, habrá recibido un nombre de usuario y una contraseña con la compra. Escriba la información que haya recibido en los campos **Nombre de usuario** y **Contraseña**. Escriba la dirección de contacto en el campo **Email**.
- **Renovar la licencia**: seleccione esta opción si la licencia actual va a expirar pronto. Introduzca su **nombre de usuario** y su **contraseña** (datos que se le proporcionaron en el momento de la adquisición de la licencia actual) en los campos correspondientes.
- **Cargar datos de licencia**: (esta opción no estará disponible si la descarga de ESET Mobile Security se ha realizado desde el sitio web de ESET) utilice esta opción si ya ha adquirido el programa con esta cuenta. ESET Mobile Security se activará cargando sus datos de licencia desde el servidor de ESET.
- **Comprar ahora**: seleccione esta opción si no tiene una licencia y le gustaría adquirir una.

Cada activación es válida durante un período de tiempo fijo. Una vez la activación expire, se le pedirá que renueve la licencia del programa (el programa le informará al respecto de forma anticipada).

NOTA: durante la activación, el dispositivo debe estar conectado a Internet ya que se descargará una pequeña cantidad de datos.

De forma predeterminada, ESET Mobile Security se instala con el idioma que su teléfono tiene establecido como configuración regional del sistema (dentro de la configuración del idioma y del teclado). Si desea cambiar el idioma de toda la interfaz de usuario de la aplicación, toque en **Idioma** en la pantalla principal de ESET Mobile Security y seleccione el idioma que desee.

3. Antivirus

Analizar dispositivo

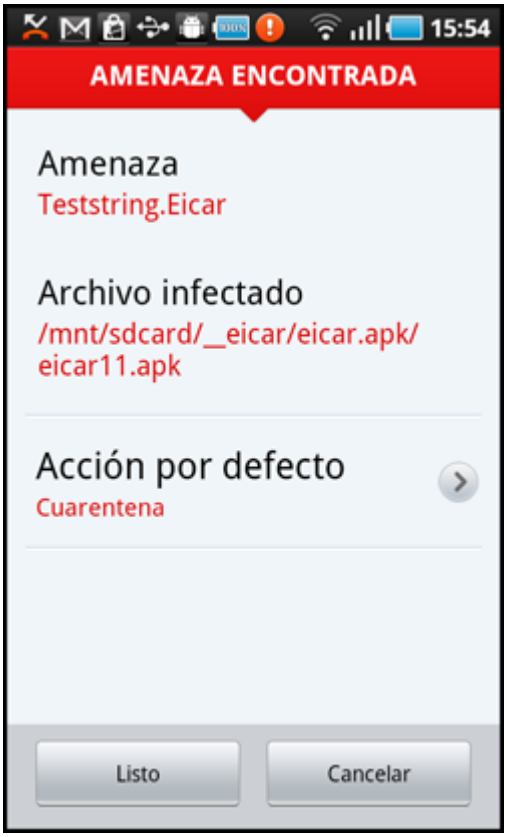
La opción **Analizar dispositivo** se puede utilizar para comprobar si hay amenazas en su dispositivo móvil.

Algunos tipos de archivos predefinidos se analizan de forma predeterminada. Un análisis completo del dispositivo comprueba la memoria, los procesos en ejecución, sus bibliotecas de vínculos dinámicos dependientes y los archivos que forman parte del almacenamiento interno y extraíble. Finalizado el análisis se muestra un resumen corto de los resultados (número de archivos infectados, número de archivos analizados, duración del análisis, etc.).

Si desea anular un análisis en curso, toque en **Cancelar**.

Analizar carpeta

Para analizar determinadas carpetas del dispositivo, toque en **Analizar carpeta**. Busque las carpetas que desee analizar, toque en sus casillas de verificación en la columna derecha y toque en **Analizar**.



Amenaza detectada por ESET Mobile Security

Analizar registros

La sección **Analizar registros** contiene registros que proporcionan información completa acerca de las tareas de análisis realizadas. Los registros se crean después de cada análisis activado manualmente (a petición) o cuando se detecta una amenaza durante el análisis en tiempo real.

Cada registro contiene:

- fecha y hora del suceso.
- número de archivos analizados.
- número de archivos infectados.
- nombre de la ruta de acceso completa de los archivos infectados.
- duración del análisis.
- acción realizada o errores detectados durante el análisis.

Cuarentena

La tarea principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Mobile Security los detecta incorrectamente como infectados.

Los archivos almacenados en la cuarentena se pueden ver en un registro que muestra el nombre y la ubicación original del archivo infectado, así como la fecha y la hora de la cuarentena.

Si desea restaurar un archivo en cuarentena a su ubicación original, toque en el archivo y seleccione **Restaurar**. No se recomienda esta opción.

Para eliminar definitivamente un archivo en cuarentena del dispositivo, toque en el archivo y seleccione **Eliminar**. Para eliminar todos los archivos almacenados en la cuarentena, pulse el botón **MENÚ** y toque en **Quitar todo**.

Configuración

La opción **A petición** le permite modificar los parámetros de análisis de un análisis activado manualmente (a petición).

La opción **Mostrar aviso de alerta** muestra las notificaciones de alerta de amenaza cada vez que el análisis a petición detecta una nueva amenaza.

Si desea analizar todas las aplicaciones (archivos *.apk*) instaladas en el dispositivo, seleccione la opción **Analizar aplicaciones**.

Protección proactiva es un método de detección basado en algoritmos que analiza el código y busca comportamientos habituales de los virus. Su ventaja principal es la capacidad de identificar software malicioso sin reconocer aún en la base de datos actual de firmas de virus. Si está activada la protección proactiva, se necesitará tiempo adicional para realizar el análisis.

La opción **Profundidad del análisis de archivos** le permite especificar la profundidad de los archivos anidados (archivos *.zip*) que se van a analizar. Cuanto más alto es el número, más profundo es el análisis.

La opción **Registros almacenados** le permite definir el número máximo de registros que se almacenarán en la sección **Analizar registros** 5.

Puede especificar una **Acción por defecto** que se realice automáticamente cuando se detecten archivos infectados. Puede elegir las siguientes opciones:

- **Ignorar**: no se realizará acción alguna sobre el archivo infectado (no se recomienda esta opción).
- **Eliminar**: el archivo infectado se eliminará.
- **Cuarentena**: (por defecto) el archivo infectado se moverá a la **Cuarentena** 5.

La opción **Extensiones** muestra los tipos de archivos más comunes expuestos a amenazas en la plataforma Android. Seleccione los tipos de archivos que desea analizar o anule la selección de la extensiones para excluirlos del análisis. Esta configuración se aplica tanto al análisis a petición como al análisis en tiempo real:

- **Sensible a las extensiones**: si anula la selección de esta opción, se analizarán todos los tipos de archivos. También se comprobará si los archivos no están disfrazados de otro tipo de archivo. Como resultado, el tiempo de análisis se prolonga.
- **DEX (archivo de código de aplicaciones)**: formato de archivo ejecutable que contiene código compilado escrito para el sistema operativo Android.
- **SO (bibliotecas)**: bibliotecas compartidas guardadas en lugares designados en el sistema de archivos y vinculadas mediante programas que requieren sus funciones.
- **Archivos (archivos comprimidos)**: archivos comprimidos con la compresión Zip.
- **Otros**: otros tipos de archivos conocidos.

En la opción **Tiempo real**, puede configurar los parámetros de análisis del análisis al acceder. El análisis al acceder comprueba los archivos con los que interactúa en tiempo real. Analiza automáticamente la carpeta *Descarga* en la tarjeta SD, los archivos de los archivos de instalación *.apk* y los archivos de la tarjeta SD una vez conectada (si está activada la opción **Analizar tarjeta SD conectada**). El análisis al acceder se inicia automáticamente al inicio del sistema.

- **Protección en tiempo real**: si está activada (por defecto), el análisis al acceder se ejecuta en segundo plano.
- **Mostrar aviso de alerta**: muestra las notificaciones de alerta de amenaza cada vez que el análisis al acceder detecta una nueva amenaza.
- **Analizar tarjeta SD conectada**: analiza los archivos antes de abrirlos o guardarlos en la tarjeta SD.
- **Protección proactiva**: seleccione esta opción para aplicar técnicas de análisis heurísticas. La heurística identifica de forma proactiva nuevo malware no detectado aún por la base de datos de firmas de virus mediante el análisis del código y el reconocimiento del comportamiento habitual de los virus. Si está activada la protección proactiva, se necesitará tiempo adicional para realizar el análisis.
- **Profundidad del análisis de archivos**: esta opción le permite especificar la profundidad de los archivos anidados (archivos *.zip*) que se van a analizar. Cuanto más alto es el número, más profundo es el análisis.

- **Acción por defecto**: puede especificar una acción por defecto que se realice automáticamente cuando el análisis al acceder detecte archivos infectados. Si selecciona **Ignorar**, no se realizará acción alguna sobre el archivo infectado (no se recomienda esta opción). Si selecciona **Eliminar**, el archivo infectado se eliminará. Si seleccionaCuarentena, el archivo infectado se moverá a la Cuarentena 5.

ESET Mobile Security muestra su icono de notificación en la esquina superior izquierda de la pantalla (barra de estado de Android). Si no desea que se muestre este icono, vaya a la pantalla principal de ESET Mobile Security, pulse el botón **MENÚ**, toque en **Notificaciones** y anule la selección de la opción **Mostrar icono de la notificación**. Tenga en cuenta que esto no desactivará un icono de advertencia rojo con un signo de exclamación que informa acerca de un riesgo para la seguridad (p. ej., Análisis de virus en tiempo real desactivado, Comprobación de SIM desactivada, etc.).

4. Antispam

El módulo **Antispam** bloquea los mensajes SMS/MMS entrantes y las llamadas entrantes y salientes de acuerdo con unas reglas especificadas.

Los mensajes no solicitados incluyen anuncios de los proveedores de servicios de telefonía móvil o mensajes procedentes de usuarios desconocidos o sin especificar. El término *bloquear contactos* hace referencia a mover automáticamente un mensaje entrante a la sección Registros de spam 7. Cuando se bloquea un mensaje entrante, no se muestra notificación alguna. Esto tiene como ventaja que no se le molestará con información no solicitada, pero siempre puede comprobar los registros para ver si hay mensajes que se puedan haber bloqueado por error.

Para agregar una nueva regla de antispam, toque en **Lista de reglas de llamadas y SMS** > **Agregar nueva**. Escriba el número de teléfono que desea bloquear o toque en el botón **+** para elegir el número de la lista de contactos. Personalice la regla permitiendo o bloqueando los mensajes y las llamadas y toque en **Listo**.

Para editar o eliminar una entrada de regla existente, toque y mantenga presionada la entrada y, a continuación, elija la acción deseada. Si desea eliminar todas las reglas de antispam, pulse el botón **MENÚ** y toque en **Quitar todo**.

NOTA: el número de teléfono debe incluir el código de marcado internacional seguido del número real (p. ej., +16101001000).

Lista de reglas del antispam

Configuración

Bloquear llamadas anónimas: active esta opción si desea bloquear a las personas que llaman cuyo número de teléfono se haya ocultado intencionadamente a través del servicio de restricción de identificación del número llamante (CLIR, Calling Line Identification Restriction).

Bloquear contactos conocidos: utilice esta opción para bloquear los mensajes y las llamadas de los contactos incluidos en la lista de contactos.

Bloquear contactos desconocidos: bloquea los mensajes y las llamadas de los contactos no incluidos en la lista de contactos. Puede utilizar esta opción para bloquear las llamadas telefónicas indeseadas (p. ej., "llamadas de venta") o para evitar que los niños marquen números desconocidos (para ello, se recomienda proteger con contraseña 10 la configuración del antispam).

En la sección **Registros de spam**, puede ver las llamadas y los mensajes bloqueados por el módulo Antispam. Cada registro contiene el nombre del evento, el número de teléfono correspondiente y la fecha y hora del evento. Los mensajes SMS bloqueados también contienen el cuerpo del mensaje.

5. Anti-Theft

La característica **Anti-Theft** protege el teléfono móvil del acceso no autorizado.

Si pierde el teléfono o alguien se lo roba y sustituye la tarjeta SIM por una nueva (que no sea de confianza), ESET Mobile Security bloqueará el teléfono automáticamente. Se enviará un SMS de alerta de forma secreta a los números de teléfono definidos por el usuario. Este mensaje incluirá el número de teléfono de la tarjeta SIM actualmente insertada, el número IMSI (International Mobile Subscriber Identity) y el número de IMEI (International Mobile Equipment Identity) del teléfono. El usuario no autorizado no sabrá que este mensaje se ha enviado, puesto que se eliminará automáticamente de los hilos de **Mensajes**. Además, también puede solicitar las coordenadas GPS del teléfono móvil perdido o borrar de forma remota todos los datos almacenados en el dispositivo.

Tarjetas SIM de confianza

Si la tarjeta SIM actualmente insertada en el teléfono móvil es la que desea guardar como de confianza, toque en **Agregar**. Si utiliza más de una tarjeta SIM, puede que desee distinguirlas modificando su **Alias para la tarjeta SIM** (p. ej., *Trabajo*, *Casa* etc.).

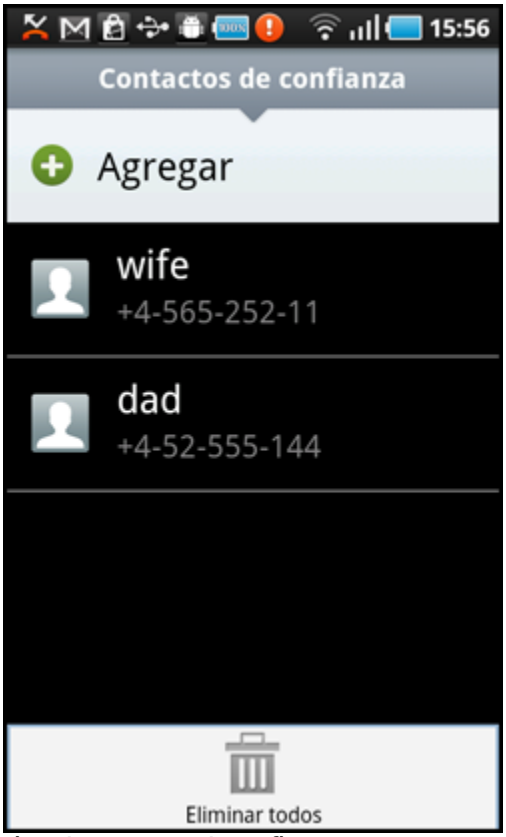
Para editar o quitar una entrada de SIM existente, toque y mantenga presionada la entrada y, a continuación, elija **Editar** o **Quitar**. Si desea eliminar todas las entradas de la lista, pulse el botón **MENÚ** y toque en **Quitar todo**.

Contactos de confianza

En la lista **Contactos de confianza**, toque en **Agregar** para agregar los números de teléfono que recibirán un SMS de alerta cuando se inserte en el dispositivo una tarjeta SIM que no sea de confianza. Escriba un nombre en el campo **Nombre del contacto** y su número de teléfono en el campo **Número de teléfono** o toque en el botón **+** para seleccionar el contacto de la lista de contactos. Si el contacto contiene más de un número de teléfono, se enviará un SMS de alerta a todos esos números.

Para editar o quitar una entrada existente, toque y mantenga presionada la entrada y, a continuación, elija **Editar** o **Quitar**. Si desea eliminar todas las entradas de la lista, pulse el botón **MENÚ** y toque en **Quitar todo**.

NOTA: el número de teléfono debe incluir el código de marcado internacional seguido del número real (p. ej., +16101001OO).



Lista de contactos de confianza

Configuración

Si tiene un dispositivo sin tarjeta SIM (p. ej., un tablet o un teléfono CDMA), seleccione la opción **Ignorar comprobación de la SIM**. Esto desactivará las advertencias rojas *¡Riesgo de seguridad!* (*La comprobación de la SIM está desactivada* y *No se ha definido ninguna tarjeta SIM de confianza*) en la pantalla principal de ESET Mobile Security. (Tenga en cuenta que en los dispositivos CDMA la opción Ignorar comprobación de la SIM aparecerá atenuada.)

Para activar la comprobación automática de la tarjeta SIM insertada (y el envío de SMS de alerta), seleccione la opción **Activar la comprobación de la SIM**.

En el campo **Texto de alerta SMS** puede modificar el mensaje de texto que se enviará a los números de teléfono predefinidos tras insertarse en el dispositivo una tarjeta SIM que no sea de confianza. Si ha adquirido ESET Mobile Security desde Google Play, automáticamente se introduce una dirección de correo electrónico desde su cuenta de Google. También puede introducir otra cuenta de correo o bien un número de contacto alternativo.

Comandos SMS

Los comandos SMS remotos (wipe, lock y find) solo funcionan si está seleccionada la opción **Activar comandos SMS**.

La opción **Activar el reinicio de contraseña vía SMS** le permite restablecer la contraseña de seguridad

mediante el envío de un mensaje SMS desde el móvil guardado en los **Contactos de confianza** a su número de móvil. Este SMS debe tener el siguiente formato:
eset remote reset

Si pierde el teléfono y le gustaría bloquearlo, envíe un SMS de bloqueo remoto desde cualquier dispositivo móvil a su número de teléfono en el siguiente formato:
eset lock contraseña
Sustituya *contraseña* por su propia contraseña definida en la sección **Contraseña** 10. Los usuarios no autorizados no podrán usar su teléfono dado que se les pedirá que escriban su contraseña.

Si desea solicitar las coordenadas GPS de su teléfono móvil, envíe un SMS de búsqueda remota a su número de móvil o al número de móvil del usuario no autorizado (según si la tarjeta SIM ya se ha sustituido):
eset find contraseña
Recibirá un SMS con las coordenadas GPS junto con un vínculo a los mapas de Google con la ubicación exacta de su teléfono móvil. Tenga en cuenta que para recibir las coordenadas GPS, el módulo GPS del teléfono tiene que estar activado de forma anticipada.

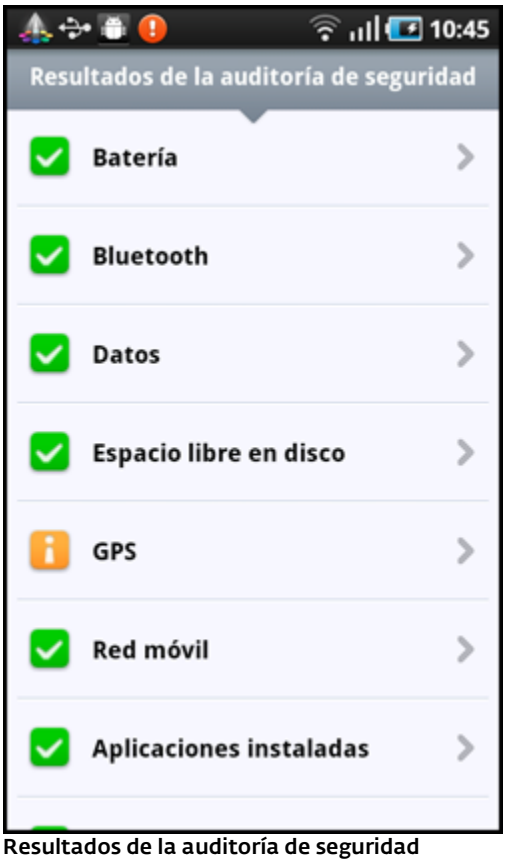
Si desea borrar todos los datos almacenados en el dispositivo y todos los soportes extraíbles actualmente insertados, envíe un SMS de borrado remoto:
eset wipe contraseña
Todos los contactos, mensajes, correos electrónicos, aplicaciones instaladas, su cuenta de Google y el contenido de la tarjeta SD se eliminarán definitivamente del dispositivo. Si ESET Mobile Security no está establecido como Administrador de dispositivos, solo se borrarán los contactos, los mensajes y el contenido de la tarjeta SD.

NOTA: la contraseña distingue entre mayúsculas y minúsculas. Asegúrese de escribir la contraseña exactamente como la ha definido en la sección Contraseña.

6. Auditoría de seguridad

La **Auditoría de seguridad** comprueba el estado del teléfono respecto a nivel de batería, estado de Bluetooth, espacio libre en disco, etc.

Para ejecutar la auditoría de seguridad manualmente, toque en **Auditar**. Se muestra un informe detallado.



Resultados de la auditoría de seguridad

Una marca de verificación verde junto a cada elemento indica que el valor se encuentra por encima del umbral o que el elemento no representa un riesgo para la seguridad.

Un icono amarillo significa que al menos uno de los elementos se encuentra por debajo del umbral o que el elemento puede representar un posible riesgo para la seguridad. Toque en el elemento para ver detalles de los resultados.

Un signo de exclamación rojo indica que el elemento está por debajo del umbral o que el elemento representa un riesgo para la seguridad y debe repararse.

Si desea corregir el estado del elemento resaltado en rojo, toque en el elemento y confirme tocando en **Sí**.

Configuración

Por defecto, la auditoría de seguridad está programada para ejecutarse periódicamente cada 24 horas. Si desea desactivar la auditoría periódica, anule la selección de la opción **Auditar periódicamente**.

Si la opción **Corregir automáticamente** está activada, ESET Mobile Security intentará corregir automáticamente los elementos en riesgo (p. ej., el estado de bluetooth) sin la intervención del usuario. Esta opción solo se aplica a una auditoría periódica (programada).

La opción **Registros almacenados** le permite definir el número máximo de registros que se almacenarán en la sección **Registros de auditoría**.

La opción **Período de auditoría** le permite definir la frecuencia con que se realizará la auditoría periódica (programada).

Para ajustar el valor del umbral en el que el espacio en disco disponible y el nivel de batería se consideran bajos, utilice las opciones **Límite de espacio libre en disco** y **Límite del nivel de batería**.

En la pestaña **Elementos que auditar**, seleccione los elementos que se comprobarán durante la auditoría periódica (programada).

La sección **Registros de auditoría** contiene registros que proporcionan información completa acerca de las auditorías activadas manualmente y periódicas realizadas. Cada registro contiene la fecha y la hora del suceso y resultados detallados de cada elemento.

El **Administrador de tareas** proporciona una visión general de todos los procesos, servicios y tareas que se ejecutan en su dispositivo. ESET Mobile Security le permite detener los procesos, servicios y tareas que no ejecute el sistema. Estos se indica con un icono rojo (**x**).

7. Actualización

Por defecto, ESET Mobile Security se instala con una tarea de actualización para garantizar que el programa se actualice periódicamente. Para ejecutar la actualización manualmente, toque en **Actualizar ahora**.

Configuración

La opción **Actualización automática** le permite definir el intervalo de tiempo para la descarga automática de las actualizaciones de la base de datos de virus.

NOTA: para evitar el uso innecesario de ancho de banda, las actualizaciones se emiten en caso necesario, cuando se agrega una nueva amenaza. Aunque las actualizaciones se incluyen de forma gratuita con la licencia activa, puede que el proveedor de servicios de telefonía móvil le cobre las transferencias de datos.

8. Contraseña

La contraseña de seguridad protege la configuración frente a los cambios no autorizados. La contraseña es necesaria en los siguientes casos:

- Para acceder a características protegidas con contraseña ESET Mobile Security (Antivirus, Antispam, Anti-Theft y Auditoría de seguridad).
- Para acceder al teléfono cuando está bloqueado.
- Para enviar comandos SMS al dispositivo.
- Desinstalar ESET Mobile Security.

NOTA: La protección frente a la desinstalación solo está disponible en Android 2.2 y posterior.

Para definir una nueva contraseña de seguridad, escríbala en los campos **Contraseña** y **Vuelva a escribir la contraseña**. La opción **Frase recordatoria** (si está establecida) muestra una sugerencia en caso de que no recuerde la contraseña.

IMPORTANTE: Proceda con cuidado cuando elija su contraseña ya que se le pedirá para desbloquear el dispositivo o desinstalar ESET Mobile Security.

En la pestaña **Aplicar a**, puede especificar los módulos que estarán protegidos por la contraseña.

Si olvida la contraseña, puede enviar un SMS desde el número de móvil guardado en la lista **Contactos de confianza** a su número de móvil. Este SMS debe tener el siguiente formato:
eset remote reset
Se restablecerá su contraseña.

9. Resolución de problemas y asistencia técnica

9.1 Resolución de problemas

ESET Mobile Security proporciona una funcionalidad de inicio de sesión avanzada que ayuda a diagnosticar posibles problemas técnicos. Antes de ponerse en contacto con el servicio de atención al cliente de ESET, le recomendamos encarecidamente que busque una posible solución a su problema en la base de conocimientos de ESET. Si aun así necesita ponerse en contacto, siga los pasos siguientes:

1. Vaya a la pantalla principal de ESET Mobile Security, pulse el botón **MENÚ** y toque en **Configuración de inicio de sesión**.
2. Seleccione un componente de programa adecuado con el que esté relacionado el problema.
3. Reproduzca el problema. La información se debe escribir dentro de un archivo de registro de la aplicación.
4. Vaya a la pantalla principal de ESET Mobile Security, pulse el botón **MENÚ** y toque en **Atención al cliente**.
5. Si no encuentra una solución en nuestra base de conocimientos, toque en **Continuar**.
6. Rellene toda la información y pulse **Enviar** en la parte inferior de la pantalla. Asegúrese de que la opción **Registro de la aplicación** esté seleccionada (lo está de forma predeterminada).

9.2 Asistencia técnica

Si necesita ayuda con aspectos administrativos o asistencia técnica relacionada con ESET Mobile Security o con cualquier otro producto de seguridad de ESET, nuestros especialistas del servicio de atención al cliente están disponibles para ayudarle.

Para encontrar respuestas a las preguntas más frecuentes, acceda a la base de conocimientos de ESET en:
http://kb.eset.com/android

La base de conocimientos contiene abundante información útil para resolver la mayoría de los problemas más comunes, con acceso fácil por categorías o mediante una herramienta de búsqueda avanzada.

Para ponerse en contacto con el servicio de atención al cliente de ESET, utilice el formulario de solicitud de asistencia disponible en:
http://eset.com/support/contact

Para solicitar asistencia directamente desde el teléfono móvil, vaya a la pantalla principal de ESET Mobile Security, pulse el botón **MENÚ** y toque en **Atención al cliente**. Rellene todos los campos obligatorios. Para incluir un **registro de la aplicación** completo, siga los pasos que se describen en la secciónResolución de problemas 11.