ESET Mobile Security

Windows Mobile

Manual de instalación y guía para el usuario

ESET Mobile Security

Atención al cliente en todo el mundo: www.eset.eu/support
Atención al cliente en América del Norte: www.eset.com/support

REV. 10/28/2010

Contenido

1. Instalación de ESET Mobile Security

1.1 Requisitos mínimos del sistema

Para instalar ESET Mobile Security para Windows Mobile, su dispositivo móvil debe cumplir los siguientes requisitos del sistema:

	Requisitos mínimos del sistema
Sistema operativo	Windows Mobile 5.0 y posterior
Procesador	200 MHz
Memoria	16 MB
Espacio libre en disco	2,5 MB

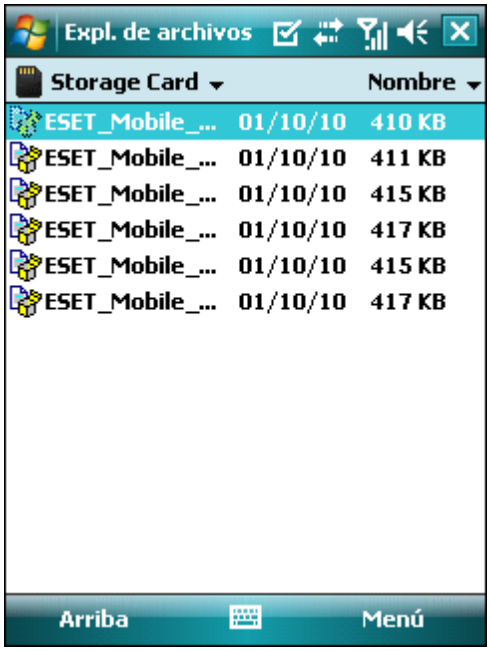
1.2 Instalación

Guarde todos los documentos abiertos y cierre todas las aplicaciones activas antes de instalar el producto. Puede instalar ESET Mobile Security directamente en el dispositivo o desde su equipo.

Luego de la instalación correcta, active ESET Mobile Security siguiendo los pasos que se detallan en la sección Activación del producto 5.

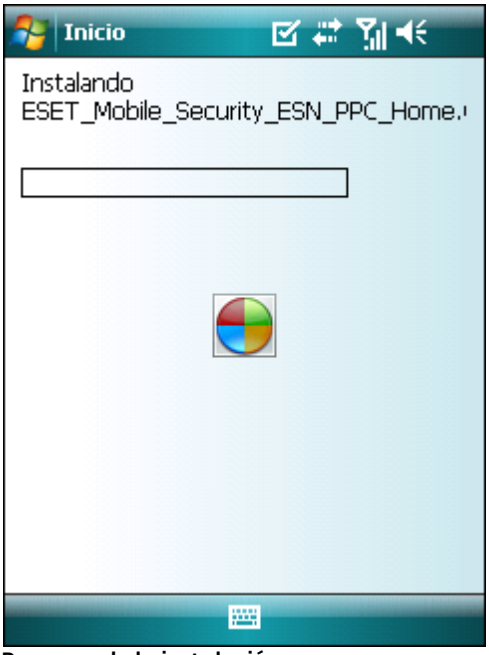
1.2.1 Instalación en el dispositivo

Para instalar ESET Mobile Security directamente en el dispositivo, descargue el archivo de instalación *.CAB* al dispositivo a través de Wi-Fi, transferencia de archivos por bluetooth o como archivo adjunto en un correo electrónico. Para encontrar el archivo, vaya a **Inicio > Programas > Exploración de archivos**. Presione el archivo para iniciar el programa de instalación y luego siga las indicaciones del asistente de instalación.



Instalación en curso de ESET Mobile Security

NOTA: La interfaz del usuario de Windows Mobile varía según el modelo del dispositivo. En su dispositivo, el archivo de instalación puede aparecer en un menú o una carpeta diferentes.

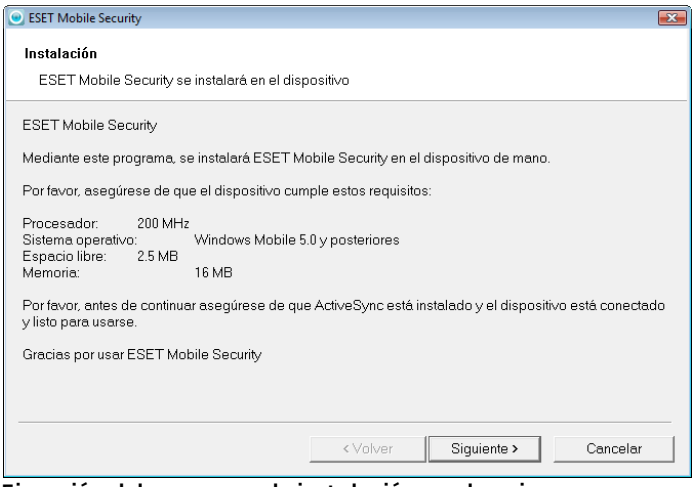


Progreso de la instalación

Luego de la instalación, puede modificar la configuración del programa. Sin embargo, la configuración predeterminada provee el máximo nivel de protección ante programas maliciosos.

1.2.2 Instalación desde el equipo

Para instalar ESET Mobile Security desde su equipo, conecte el dispositivo móvil al equipo a través de ActiveSync (en Windows XP) o Windows Mobile Device Center (en Windows 7 y Vista). Luego del reconocimiento del dispositivo, ejecute el paquete de instalación descargado (archivo *.EXE*) y siga las instrucciones del asistente de instalación.



Ejecución del programa de instalación en el equipo

Luego siga las indicaciones en el dispositivo móvil.

1.3 Desinstalación

Para desinstalar ESET Mobile Security del dispositivo móvil, presione **Inicio > Configuración**, presione la pestaña **Sistema** y luego **Eliminar programas**.

NOTA: La interfaz del usuario de Windows Mobile varía según el modelo del dispositivo. Estas opciones pueden presentar ligeras variaciones en su dispositivo.

Eliminación de ESET Mobile Security

Seleccione ESET Mobile Security y presione **Eliminar**. Presione **Sí** cuando el programa le solicite confirmar la desinstalación.

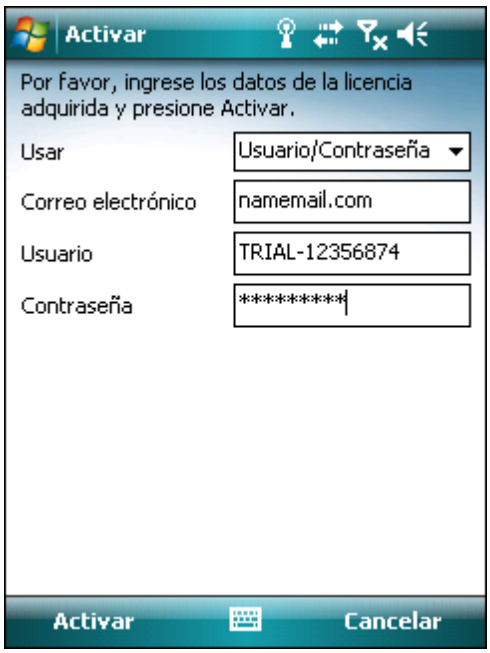
Eliminación de ESET Mobile Security

2. Activación del producto

La ventana principal de ESET Mobile Security (**Inicio > Programas > ESET Mobile Security**) es el punto de partida para todas las instrucciones de este manual.

Ventana principal de ESET Mobile Security

Luego de una instalación correcta, es necesario activar ESET Mobile Security. Si el programa no le indica que active el producto, presione **Menú > Activar**.



Activación del programa

Existen dos métodos de activación; el suyo dependerá de la forma en que haya adquirido el producto ESET Mobile Security.

2.1 Activación mediante un nombre de usuario y una contraseña

Si usted adquirió el producto por medio de un distribuidor, habrá recibido un nombre de usuario y una contraseña junto con su compra. Seleccione la opción **Usuario/Contraseña** y complete los campos **Usuario** y **Contraseña** con la información recibida. Ingrese su dirección de correo electrónico actual en el campo **Correo electrónico**. Presione **Activar** para completar la activación.

2.2 Activación mediante una clave de registro

Si usted adquirió ESET Mobile Security junto a un nuevo dispositivo (o como parte de un producto en caja), habrá recibido una clave de registro con su compra. Seleccione la opción **Clave de registro**, ingrese la información recibida en el campo **Clave** y su dirección de correo electrónico actual en el campo **Correo electrónico**. Presione **Activar** para completar la activación. Sus nuevos datos de autenticación (el nombre de usuario y la contraseña) reemplazarán automáticamente la clave de registro y serán enviados a la dirección de correo electrónico especificada.

En ambos casos recibirá un mensaje de correo electrónico de confirmación indicando la activación correcta del producto.

Cada activación tiene validez durante un período fijo de tiempo. Cuando vence la activación, es necesario renovar la licencia del programa (el programa se lo notificará con anticipación).

NOTA: Durante la activación, el dispositivo debe permanecer conectado a Internet. Se descargará una cantidad de datos reducida. Estas transferencias se cobrarán según el acuerdo de servicio pactado con el proveedor del dispositivo móvil.

3. Actualización

En forma predeterminada, ESET Mobile Security se instala con una tarea de actualización para asegurar que el programa se actualice con regularidad. También existe la posibilidad de realizar actualizaciones en forma manual.

Luego de la instalación, se recomienda ejecutar la primera actualización manualmente. Para realizarla, presione **Acción > Actualizar**.

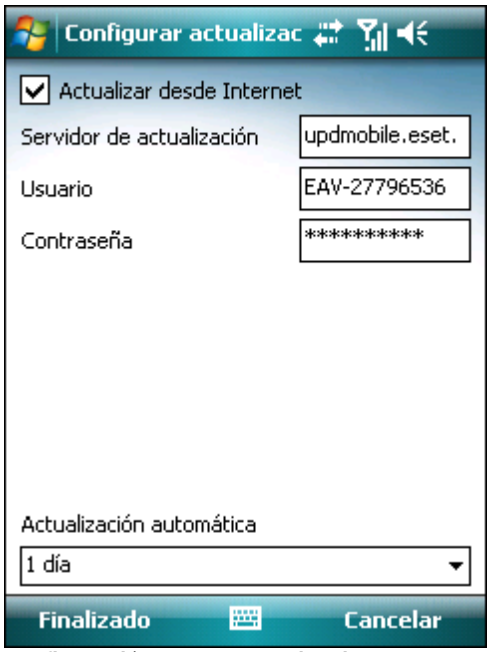
3.1 Configuración

Para configurar las opciones de actualización, presione **Menú > Configuración > Actualizar.**

La opción **Actualizar desde Internet** permite habilitar o deshabilitar las actualizaciones automáticas.

Puede especificar el **Servidor de actualización** desde el cual se descargan las actualizaciones (se recomienda dejar la configuración predeterminada: *updmobile.eset.com*).

Para establecer el intervalo de tiempo entre las actualizaciones automáticas, use la opción **Actualización automática**.



Configuración de las actualizaciones

NOTA: Para evitar el uso innecesario de ancho de banda, las actualizaciones de las bases de datos de firmas de virus se publican solo cuando son necesarias, al agregar una nueva amenaza. Si bien las actualizaciones de bases de datos de firmas de virus son gratuitas para las licencias activas, es posible que el proveedor del servicio móvil le cobre por la transferencia de datos.

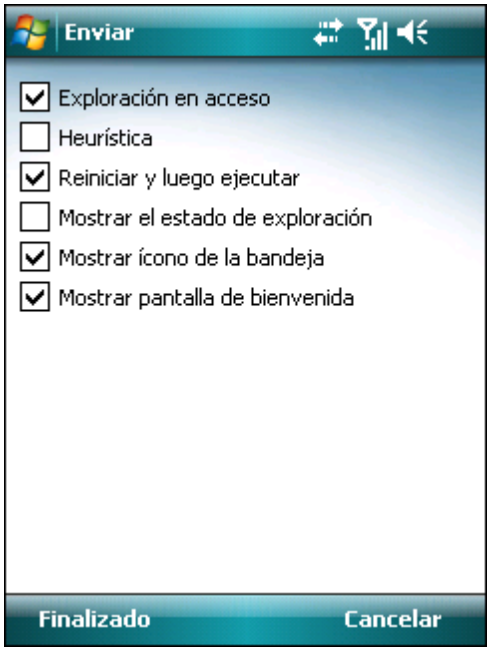
4. Exploración en acceso

La exploración en acceso verifica los archivos con los que usted interactúa en todo momento. Cuando un archivo se ejecuta, abre o guarda, el programa automáticamente los analiza en búsqueda de amenazas. La exploración se lleva a cabo antes de realizar cualquier acción con el archivo, lo que asegura la máxima protección con la configuración predeterminada. La exploración en acceso se activa en forma automática cuando se inicia el sistema.

4.1 Configuración

Presione **Menú > Configuración > En acceso** para habilitar o deshabilitar las siguientes opciones:

- **Exploración en acceso**: si está habilitada, el análisis se ejecuta en tiempo real y en segundo plano.
- **Heurística**: seleccione esta opción para aplicar las técnicas heurísticas de exploración. La heurística identifica en forma proactiva los nuevos códigos maliciosos todavía no detectados por las bases de datos de firmas de virus, ya que explora el código y reconoce la conducta típica de los virus. Su desventaja es que se requiere tiempo adicional para completar el análisis.
- **Reiniciar y luego ejecutar**: si esta opción está seleccionada, la exploración en acceso se iniciará en forma automática tras reiniciar el dispositivo.
- **Mostrar el estado de exploración**: seleccione esta opción para que se muestre el estado de exploración en la esquina inferior derecha mientras la exploración está en curso.
- **Mostrar ícono de la bandeja**: muestra el ícono de inicio rápido de la configuración en acceso (en la esquina inferior derecha de la pantalla de inicio de Windows Mobile).
- **Mostrar pantalla de bienvenida**: esta opción permite desactivar la pantalla de bienvenida de ESET Mobile Security que se muestra cuando se inicia el dispositivo.



Configuración de la exploración en acceso

5. Exploración bajo demanda

Use el análisis bajo demanda para verificar que su dispositivo móvil no contenga infiltraciones. Algunos tipos de archivos predefinidos se exploran en forma predeterminada.

5.1 Exploración completa del dispositivo

La exploración completa del dispositivo verifica la memoria, los procesos activos, sus bibliotecas de enlaces dinámicos dependientes (DLL) y los archivos que forman parte del almacenamiento interno y en medios extraíbles.

Para ejecutar una exploración completa del dispositivo, presione **Acción > Explorar > Dispositivo completo**.

NOTA: La exploración de la memoria no se realiza en forma predeterminada. Puede habilitarla desde **Menú > Configuración > General**.

Exploración completa del dispositivo

El programa primero explora la memoria del sistema (incluyendo los procesos activos y sus DLL dependientes) y luego explora los archivos y las carpetas. Se mostrarán brevemente la ruta completa y el nombre de cada archivo explorado.

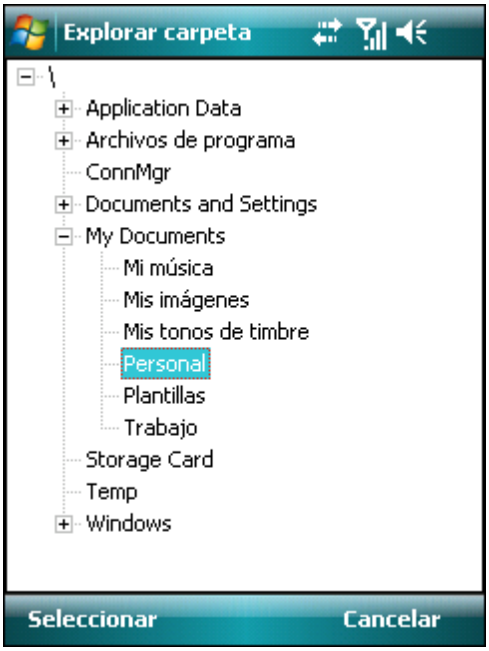
NOTA: Para cancelar una exploración en curso, presione **Acción > Explorar > Detener análisis.**

5.2 Exploración de una carpeta

Para explorar una carpeta específica del dispositivo, presione **Acción > Explorar > Carpeta**.

Exploración de una carpeta

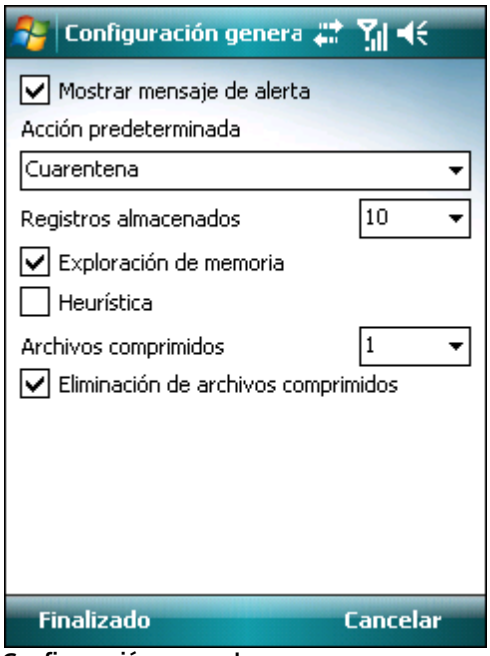
Presione la carpeta que desea explorar y luego presione **Seleccionar**.



Selección de una carpeta para su exploración

5.3 Configuración general

Para modificar los parámetros de la exploración, presione **Menú > Configuración > General.**



Configuración general

Seleccione la opción **Mostrar mensaje de alerta** para mostrar las notificaciones de alerta por amenazas.

Se puede especificar una acción predeterminada para que se realice automáticamente cuando se detecten archivos infectados. Puede elegir entre las siguientes opciones:

- **Cuarentena**
- **Eliminar**
- **Sin acción (no recomendado).**

La opción **Registros almacenados** permite definir la cantidad máxima de registros que se guardarán en la sección **Menú > Registros > Explorar**.

Si se encuentra habilitada la opción **Exploración de memoria**, se explorará la memoria del dispositivo automáticamente en busca de programas maliciosos antes de realizar la exploración de los archivos.

Si se encuentra habilitada la opción **Heurística**, ESET Mobile Security usará las técnicas heurísticas. La heurística consiste en un método de detección basado en algoritmos que analiza el código buscando conductas típicas de los virus. Su ventaja principal radica en la habilidad de detectar programas maliciosos aún no identificados por la actual base de datos de firmas de virus. Su desventaja es que se requiere tiempo adicional para completar la exploración.

La opción **Archivos comprimidos** permite determinar con qué profundidad se explorarán los archivos comprimidos anidados. (Cuanto mayor es el número, más profunda es la exploración).

Si se encuentra habilitada la opción **Borrar archivo compr.**, los archivos comprimidos (. *ZIP*, *.RAR* y *.JAR*) que contengan objetos infectados se eliminarán en forma automática.

5.4 Configuración de las extensiones

Para especificar los tipos de archivos que desea explorar en el dispositivo móvil, presione **Menú > Configuración > Extensiones.**

Se abrirá la ventana **Extensiones**, donde se mostrarán los tipos de archivos más comunes expuestos a infiltraciones. Seleccione los tipos de archivos que desea explorar y no seleccione las extensiones que desea excluir de la exploración. Si habilita la opción **Archivos comprimidos**, se explorarán todos los archivos comprimidos soportados (*.ZIP*, *.RAR* y *.JAR*).

Para explorar todos los archivos, quite la selección de la casilla de verificación **Respetar extensiones**.

Configuración de las extensiones

6. Amenaza detectada

Si se detecta una amenaza, ESET Mobile Security le solicitará que elija una acción.

Mensaje de alerta por amenaza

Se recomienda seleccionar **Eliminar**. Si selecciona **Cuarentena**, el archivo será enviado a cuarentena desde su ubicación original. Si selecciona **Ignorar**, no se realizará ninguna acción y el archivo infectado permanecerá en el dispositivo móvil.

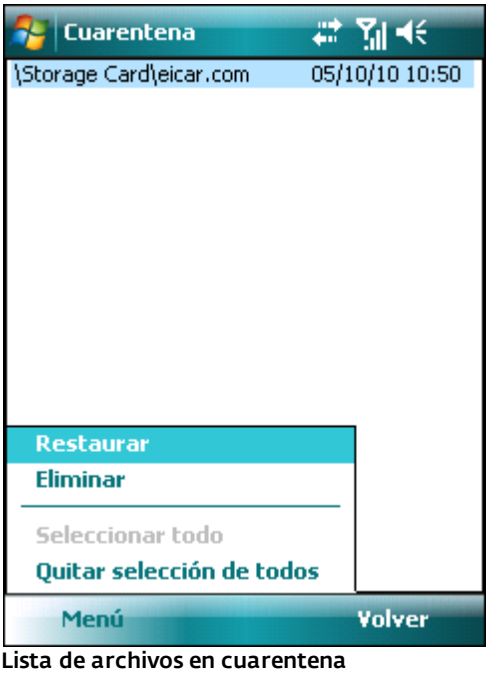
Si se detecta una infiltración en un archivo comprimido (por ej., en un archivo *.ZIP*), se encuentra disponible la opción **Eliminar archivo comprimido** en la ventana de alerta. Seleccione esta opción junto con la opción **Eliminar** para eliminar todos los archivos incluidos en el archivo comprimido.

Si deshabilita la opción **Mostrar mensaje de alerta**, no se mostrarán mensajes de alerta durante la exploración en curso (para deshabilitar las alertas para todas las exploraciones futuras, consulte la sección Configuración general 9).

6.1 Cuarentena

La tarea principal de la cuarentena consiste en almacenar los archivos infectados en forma segura. Los archivos deben ponerse en cuarentena cuando no se pueden limpiar, cuando no es seguro o recomendable eliminarlos o en caso de que ESET Mobile Security los haya detectado erróneamente

Los archivos almacenados en la carpeta de cuarentena pueden visualizarse en un registro que muestra la fecha y la hora del envío a cuarentena y la ubicación original del archivo infectado. Para abrir la carpeta de cuarentena, presione **Menú > Ver > Cuarentena**.



Lista de archivos en cuarentena

Se pueden restaurar los archivos en cuarentena presionando **Menú > Restaurar** (cada archivo será restaurado a su ubicación original). Si desea eliminar los archivos en forma permanente, presione **Menú > Eliminar**.

7. Anti-Theft

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

Si usted pierde el teléfono o alguien se lo roba y reemplaza la tarjeta SIM existente por una nueva (no confiable), se enviará un mensaje SMS de alerta en forma secreta a un número telefónico (o a varios) definido previamente por el usuario. En el mensaje se incluirá el número telefónico de la tarjeta SIM insertada, el código IMSI (Identidad Internacional del Abonado a un Móvil, por sus siglas en inglés) de la tarjeta y el código IMEI (Identidad Internacional del Equipo Móvil, por sus siglas en inglés) del teléfono. El usuario no autorizado no tendrá conocimiento del mensaje enviado, ya que se eliminará automáticamente de la carpeta Enviados.

Para eliminar todos los datos (contactos, mensajes, aplicaciones) almacenados en el dispositivo y en todos los medios de almacenamiento portátiles conectados a él, envíe un mensaje SMS de borrado remoto al número de teléfono móvil del usuario no autorizado de la siguiente forma:
#RC# DS contraseña
Donde *contraseña* es la contraseña que usted había establecido en **Menú > Configuración > Contraseña**.

7.1 Configuración

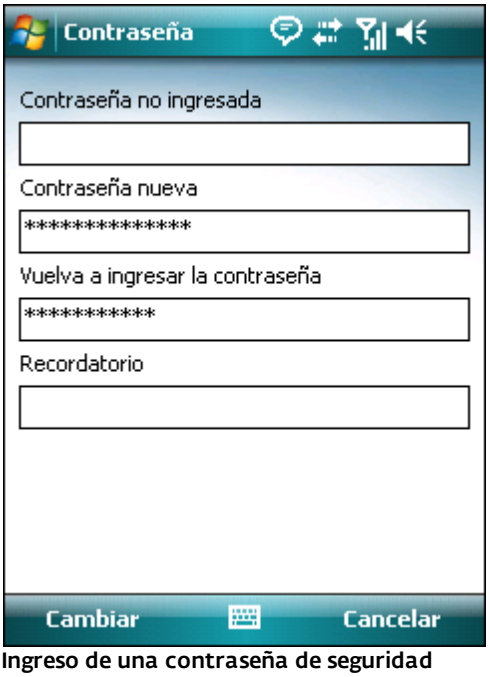
En primer lugar, establezca su contraseña en **Menú > Configuración > Contraseña**. Esta contraseña será necesaria para:

- enviar un mensaje SMS de borrado remoto al dispositivo
- acceder a la configuración de Anti-Theft del dispositivo
- desinstalar ESET Mobile Security del dispositivo.

Para establecer una nueva contraseña, ingrese su contraseña en los campos **Contraseña nueva** y **Reingrese contraseña**. La opción **Recordatorio** (si fue completada) le mostrará una pista en caso de que se olvide la contraseña.

Para modificar la contraseña actual, primero ingrese la contraseña en **Ingresar contraseña actual** y luego ingrese la nueva contraseña.

IMPORTANTE: Recuerde elegir cuidadosamente la contraseña, ya que será necesaria para desinstalar ESET Mobile Security del dispositivo.



Ingreso de una contraseña de seguridad

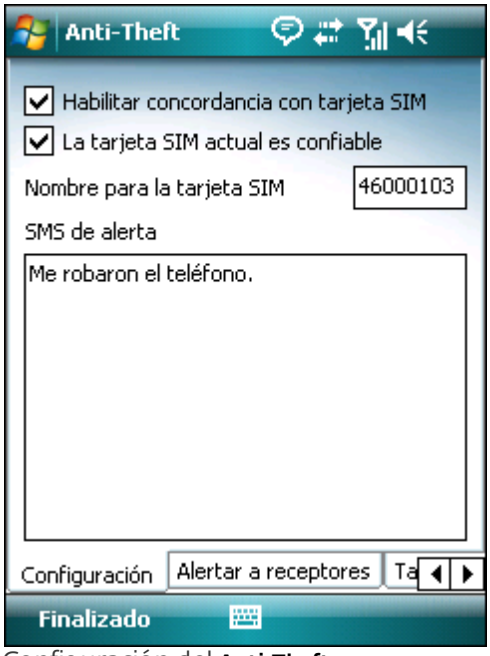
Para acceder a la configuración del Anti-Theft, presione **Menú > Configuración > Anti-Theft** e ingrese su contraseña.

Para deshabilitar la verificación automática de la tarjeta SIM insertada (y el posible envío de mensajes SMS de alerta), no seleccione la opción **Habilitar concordancia con tarjeta SIM**.

Si la tarjeta SIM insertada actualmente en el dispositivo móvil es la que desea guardar como confiable, seleccione la casilla de verificación **La tarjeta SIM actual es confiable** y la tarjeta SIM se guardará en la lista de tarjetas SIM confiables (pestaña **Tarjeta SIM confiable**). El campo de texto **Nombre para la tarjeta SIM** se completará automáticamente con el código IMSI.

Si usted usa más de una tarjeta SIM, es posible que prefiera distinguirlas modificando el **Nombre para la tarjeta SIM** (por ej., *Oficina*, *Hogar*, etc.).

En **SMS de alerta**, puede modificar el mensaje de texto que será enviado al número o números predefinidos cuando se inserte una tarjeta SIM no confiable en el dispositivo.



Configuración del **Anti-Theft**

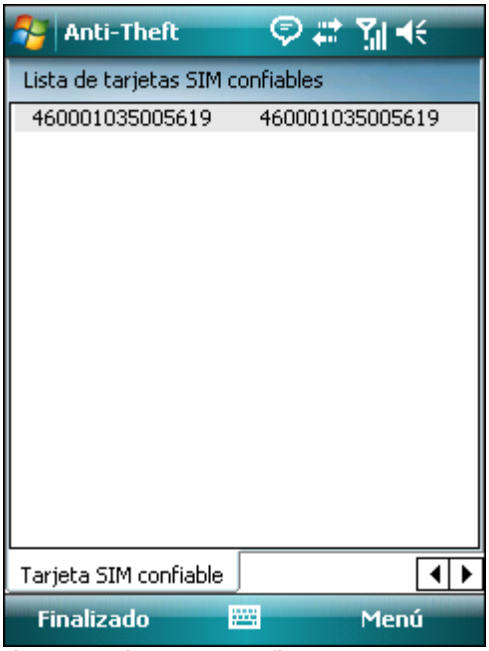
La pestaña **Alertar a receptores** muestra la lista de números predefinidos que recibirán un mensaje SMS de alerta cuando se inserte una tarjeta SIM no confiable en su dispositivo. Para agregar un nuevo número, presione **Menu > Add**. Para agregar un número desde la lista de contactos, presione **Menú > Agregar contacto**.

NOTA: el número telefónico debe incluir el prefijo telefónico internacional seguido del número (por ej., *+16105552000*).

Lista de números telefónicos predefinidos

La pestaña **Tarjeta SIM confiable** muestra la lista de tarjetas SIM confiables. Cada entrada está compuesta por el nombre elegido para la tarjeta SIM (columna izquierda) y el código IMSI (columna derecha).

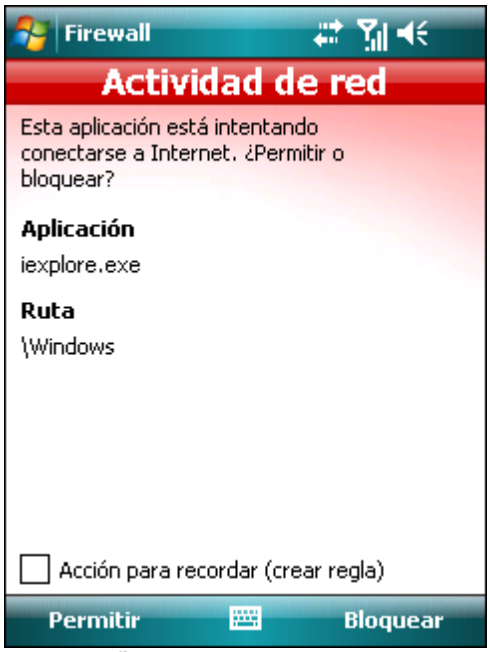
Para eliminar una tarjeta SIM de la lista, seleccione la tarjeta y presione **Menú > Eliminar**.



Lista de tarjetas SIM confiables

8. Firewall

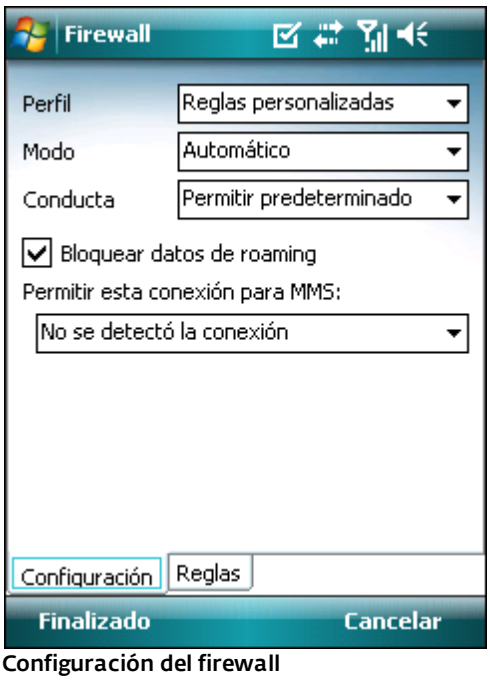
El firewall controla todo el tráfico de entrada y salida a través de la red permitiendo o rechazando conexiones individuales según las reglas de filtrado.



Alerta del firewall

8.1 Configuración

Para modificar la configuración del firewall, presione **Menú > Configuración > Firewall**.



Configuración del firewall

Puede elegir entre los siguientes perfiles:

- **Permitir todos**: permite todo el tráfico de red
- **Bloquear todos**: bloquea todo el tráfico de red
- **Reglas personalizadas**: le permite definir sus propias reglas de filtrado.

En el perfil de **Reglas personalizadas**, puede elegir entre dos modos de filtrado:

- **Automático**: adecuado para los usuarios que prefieren un uso sencillo y conveniente del firewall sin la necesidad de definir reglas. Este modo permite todo el tráfico de salida. Para el tráfico de entrada, puede establecer una acción predeterminada (**Permitir predeterminado** o **Bloqueo predeterminado**) en la opción **Conducta**.
- **Interactivo**: le permite modificar en detalle las opciones de su firewall personal. Cuando se detecta una comunicación sin ninguna regla asociada, se muestra una ventana de diálogo donde se informa sobre la conexión desconocida. La ventana de diálogo ofrece la opción de permitir la comunicación o de bloquearla y de crear una regla. Si elige crear una regla, todas las conexiones futuras del mismo tipo serán permitidas o bloqueadas de acuerdo con la regla. Si se ha modificado una aplicación que tiene asociada una regla existente, aparecerá una ventana de diálogo con la opción de aceptar o rechazar dicho cambio. La regla existente se modificará según su respuesta.

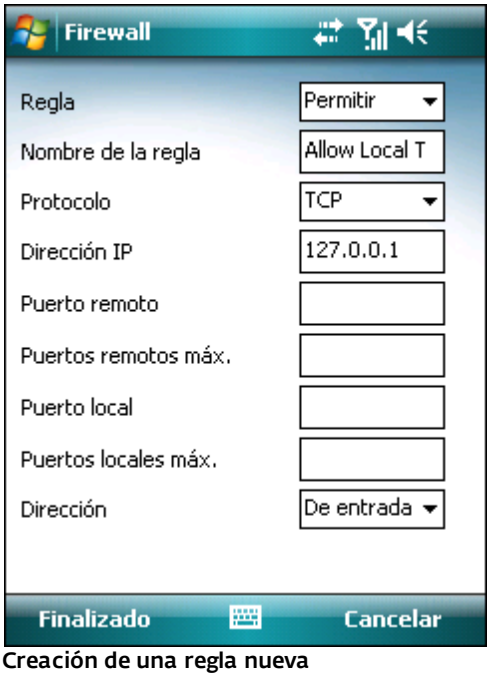
Bloquear datos de roaming: si esta opción se encuentra habilitada, ESET Mobile Security detectará automáticamente si el dispositivo está conectado a una red de roaming y bloqueará tanto los datos de entrada como los de salida. Esta opción no bloquea los datos recibidos a través de Wi-Fi o GPRS.

Permitir esta conexión para MMS: elija una conexión para recibir mensajes MMS en una red de roaming. Los mensajes MMS provenientes de otras conexiones serán bloqueados por ESET Mobile Security.

En la pestaña **Reglas**, se pueden editar o quitar las reglas existentes del firewall.

Lista de reglas del firewall

Para crear una regla nueva, presione **Menú > Agregar**, complete todos los campos requeridos y presione **Finalizado**.

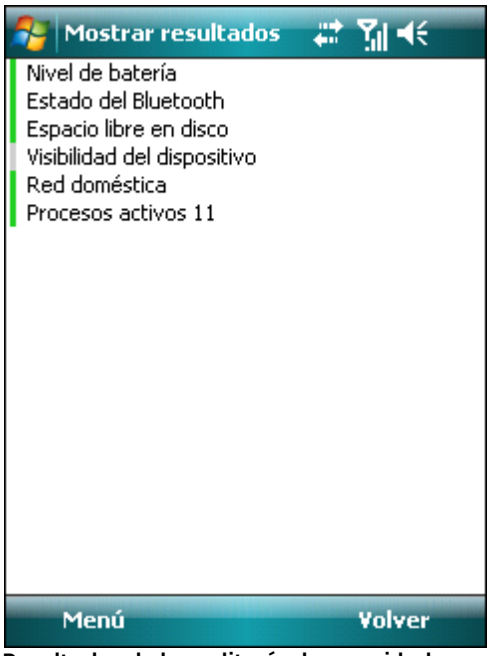


Creación de una regla nueva

9. Auditoría de seguridad

La auditoría de seguridad verifica el estado del teléfono en lo que respecta al nivel de batería, el estado del bluetooth, el espacio libre en disco, etc.

Para ejecutar una auditoría de seguridad en forma manual, presione **Acción > Auditoría de seguridad**. Se mostrará un informe detallado.

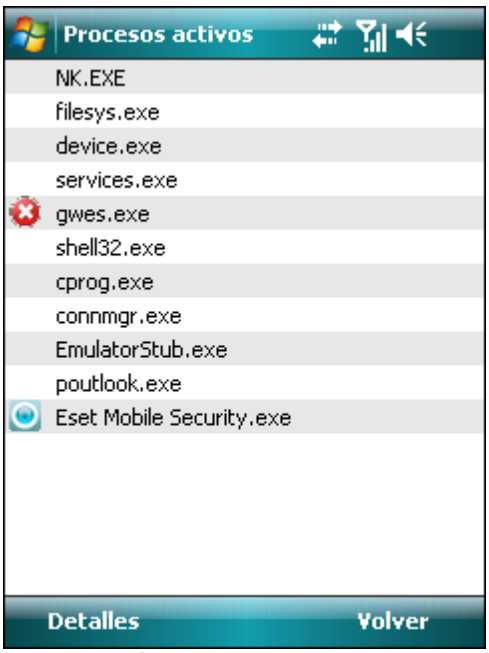


Resultados de la auditoría de seguridad

El color verde junto a cada elemento indica que el valor se encuentra por sobre el límite o que el elemento no representa un riesgo en seguridad. El color rojo significa que el valor se encuentra por debajo del límite o que el elemento representa un riesgo potencial en seguridad.

Si el **Estado del bluetooth** o la **Visibilidad del dispositivo** están resaltados en rojo, puede desactivar su estado seleccionando el elemento y presionando **Menú > Reparar**.

Para ver los detalles de cada elemento, seleccione el elemento y presione **Menú > Detalles**.



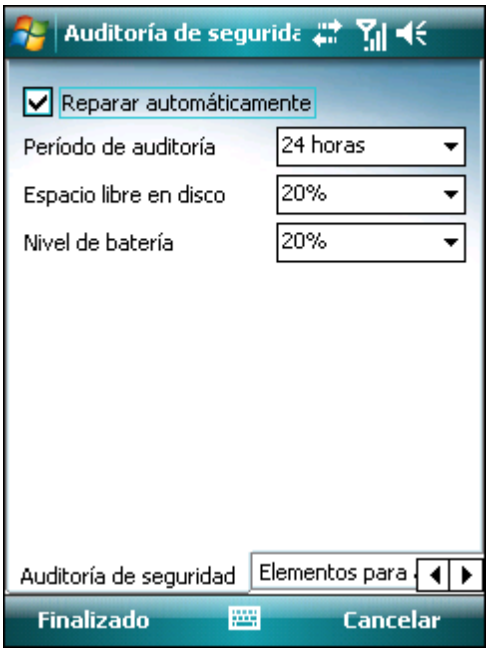
Procesos activos

La opción de **Procesos activos** muestra la lista de todos los procesos activos en el dispositivo.

Para ver los detalles de los procesos (la ruta completa y el uso de memoria), seleccione el proceso y presione **Detalles.**

9.1 Configuración

Para modificar los parámetros de la auditoría de seguridad, presione **Menú > Configuración > Auditoría de seguridad**.



Security audit settings

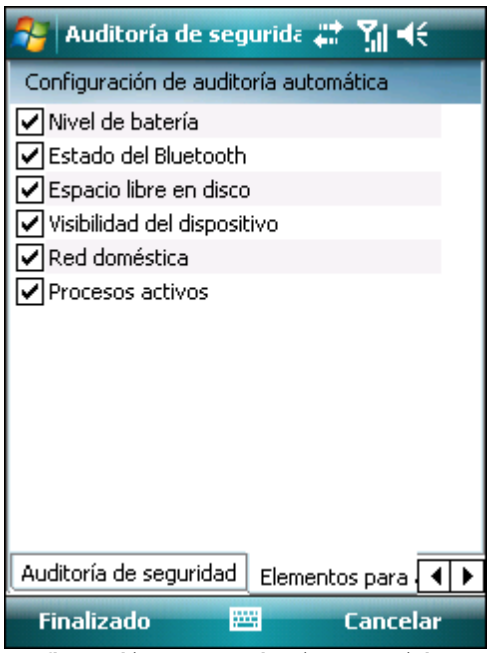
Si la opción **Reparar automáticamente** se encuentra habilitada,ESET Mobile Security intentará reparar los elementos en riesgo (por ej., el estado del bluetooth, la visibilidad del dispositivo) en forma automática sin la

intervención del usuario. Esta configuración solo se aplica a la auditoría automática (programada).

La opción **Período de auditoría** permite elegir la frecuencia con la que se realizará la auditoría automática. Si desea deshabilitar la auditoría automática, seleccione **Nunca**.

Puede ajustar el valor límite en el cual el **Espacio libre en disco** y el **Nivel de batería** se considerarán bajos.

En la pestaña **Elementos para auditar** puede seleccionar los elementos para explorar durante la auditoría de seguridad automática (programada).



Configuración de la auditoría automática

10. Antispam

El antispam bloquea los mensajes SMS y MMS no deseados, enviados al dispositivo móvil.

Los mensajes no deseados suelen incluir publicidades de proveedores de servicios para telefonía móvil o mensajes provenientes de usuarios desconocidos o no especificados.

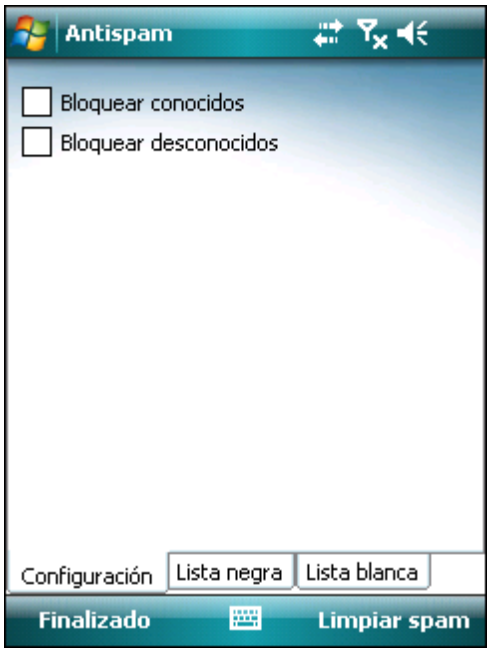
10.1 Configuración

Presione **Menú > Ver > Estadísticas** para ver la información estadística sobre los mensajes recibidos y bloqueados.

En la configuración del antispam (**Menú > Configuración > Antispam**), se encuentran disponibles los siguientes modos de filtrado:

- **Bloquear desconocidos**: habilite esta opción para aceptar solamente los mensajes provenientes de contactos que figuran en su libreta de direcciones.
- **Bloquear conocidos**: habilite esta opción para recibir solamente los mensajes provenientes de remitentes que no figuran en su libreta de direcciones.
- Habilite tanto **Bloquear desconocidos** como **Bloquear conocidos** para bloquear automáticamente todos los mensajes de entrada.
- Deshabilite tanto **Bloquear desconocidos** como **Bloquear conocidos** para desactivar el antispam. Se aceptarán todos los mensajes de entrada.

NOTA: as entradas de la lista blanca y la lista negra rigen por sobre estas opciones (consulte la sección Lista blanca / lista negra 17).



Configuración del antispam

10.2 Lista blanca / lista negra

La **Lista negra** es una lista de números telefónicos cuyos mensajes son bloqueados. Las entradas incluidas en esta lista rigen por sobre todas las opciones de la configuración antispam (pestaña (**Configuración**).

La **Lista blanca** es una lista de números telefónicos cuyos mensajes son aceptados. Las entradas incluidas en esta lista rigen por sobre todas las opciones de la configuración antispam (pestaña (**Configuración**).

Lista negra

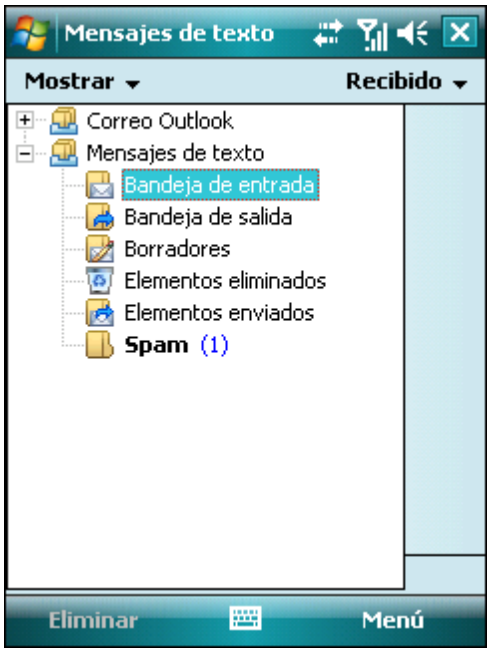
Para agregar un número nuevo en la lista blanca / lista negra, seleccione la pestaña correspondiente a la lista que desea modificar y presione **Menú > Agregar**. Para agregar un número desde la lista de contactos, presione **Menú > Agregar contacto**.

Advertencia: Cuando se agrega un número o contacto a la lista negra, los mensajes de dicho remitente se envían en forma automática y discreta a la carpeta **Spam**.

10.3 Búsqueda de los mensajes de spam

La carpeta **Spam** se usa para almacenar los mensajes bloqueados que se identificaron como spam según la configuración antispam. La carpeta se crea automáticamente al recibir el primer mensaje de spam. Para encontrar la carpeta **Spam** y revisar los mensajes bloqueados, siga los pasos detallados a continuación:

1. Abra el programa de mensajería que usa en su dispositivo, por ej. **Mensajería** del menú **Inicio**.
2. Presione **Mensajes de texto** (o **MMS** si desea encontrar la carpeta de spam para MMS).
3. Presione **Menú > Ir a > Carpetas** (o **Menú > Carpetas** en los teléfonos inteligentes).
4. Seleccione la carpeta **Spam**.

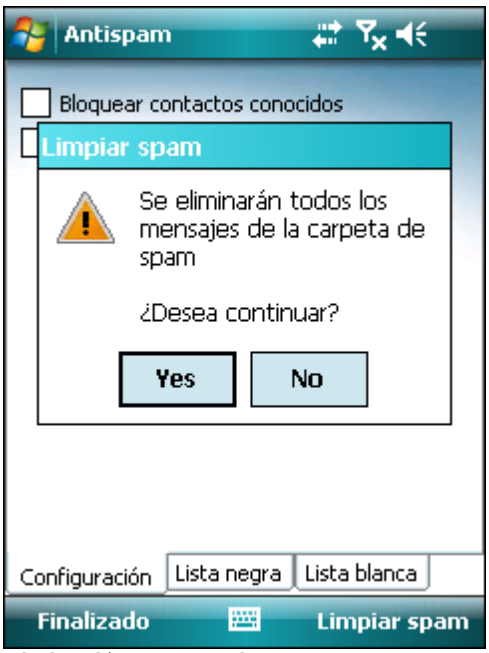


Carpeta de spam

10.4 Eliminación de los mensajes de spam

Para eliminar los mensajes de spam del dispositivo móvil, siga los pasos detallados a continuación:

1. Presione **Menú > Configuración > Antispam** en la ventana principal de ESET Mobile Security
2. Presione **Limpiar spam**
3. Presione **Sí** para confirmar la eliminación de todos los mensajes de spam.



Eliminación de mensajes de spam

11. Visualización de registros y estadísticas

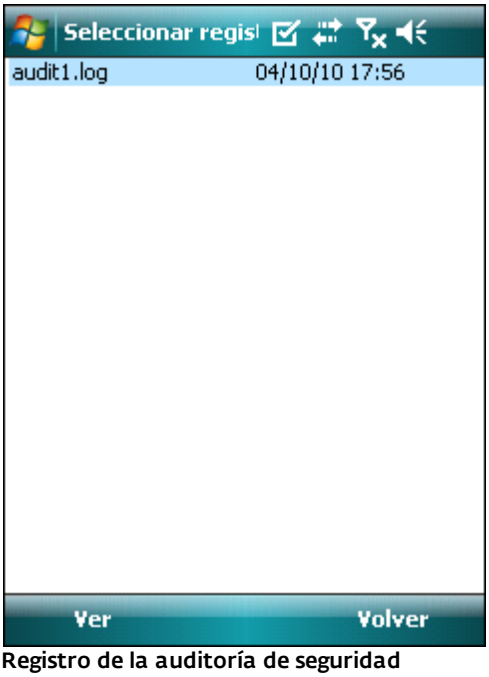
La opción **Registro de exploración** (**Menú > Registros > Explorar**) contiene registros que proporcionan datos detallados sobre las tareas de exploración completadas. Los registros se crean cada vez que la exploración bajo demanda finaliza con éxito o cuando la exploración en acceso detecta una infiltración. Todos los archivos infectados se resaltan en rojo. Al final de cada entrada de registro se explica por qué se incluyó el archivo en el registro.

Los Registros de exploración contienen:
- el nombre del archivo de registro (en general en la forma *Número.de.Exploración.log*)
- la fecha y la hora del evento
- la lista de archivos explorados
- las acciones realizadas o los errores encontrados durante la exploración.

Registro de exploración

La sección **Registro de la auditoría de seguridad** (**Menú > Registros > Auditoría de seguridad**) almacena todos los resultados de las auditorías de seguridad, tanto de las automáticas (programadas) como de las ejecutadas manualmente.

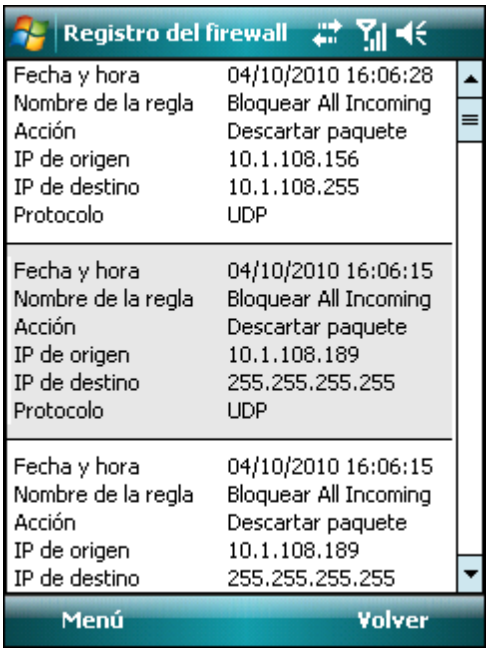
Los registros de la auditoría de seguridad contienen:
- el nombre del archivo de registro (en la forma *NúmeroDeAuditoría.log*)
- la fecha y la hora de la auditoría
- los resultados detallados.



Registro de la auditoría de seguridad

El **Registro del firewall** (**Menú > Registros > Firewall**) contiene información sobre los eventos de firewall bloqueados por ESET Mobile Security. El registro se actualiza luego de cada comunicación realizada a través del firewall. Los eventos nuevos aparecen al comienzo del registro.

El Registro del firewall contiene:
- la fecha y la hora del evento
- el nombre de la regla utilizada
- la acción realizada (basada en la configuración de la regla)
- la dirección IP de origen
- la dirección IP de destino
- el protocolo utilizado.



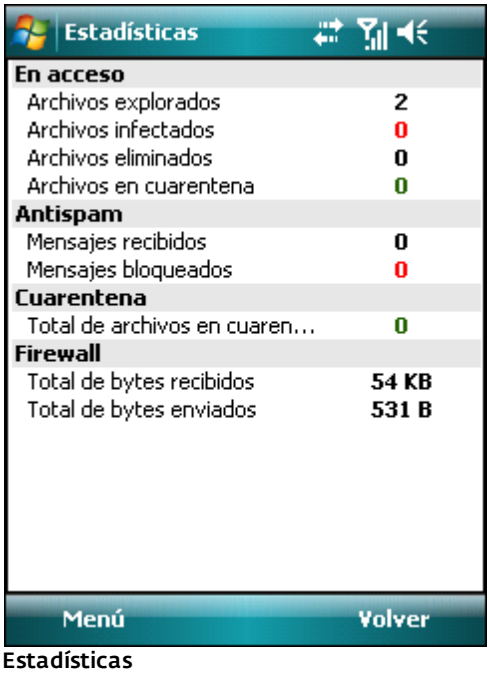
Registro del firewall

La pantalla **Estadísticas** (**Menú > Ver > Estadísticas**) muestra un resumen de:

- los archivos explorados por la exploración en acceso
- los mensajes recibidos y bloqueados
- los archivos en cuarentena
- los datos recibidos y enviados a través del firewall.

Si desea poner en cero las estadísticas actuales, presione **Menú > Reiniciar contadores**.

NOTA: Todos los datos estadísticos se calculan a partir de la última vez que se reinició el dispositivo.

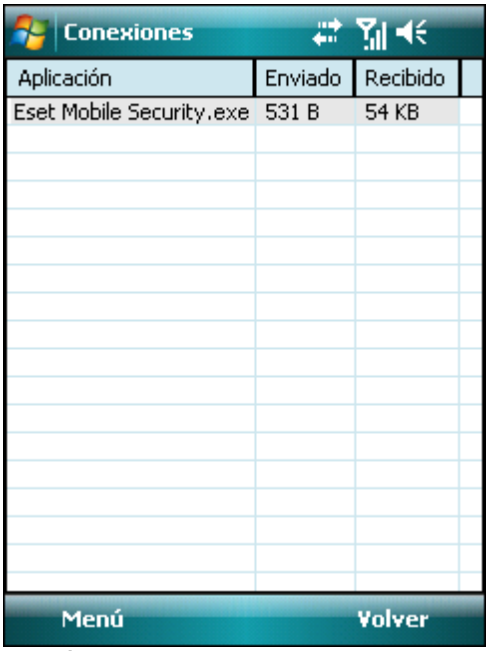


Estadísticas

La sección **Conexiones** (**Menú > Ver > Conexiones**) muestra las aplicaciones usadas para enviar y recibir datos.

La información incluye:

- el nombre del proceso
- la cantidad de datos enviados
- la cantidad de datos recibidos.



Conexiones

12. Solución de problemas y soporte

12.1 Solución de problemas

En esta sección encontrará soluciones a preguntas comunes relacionadas con ESET Mobile Security.

12.1.1 Instalación sin éxito

La causa más común de la aparición de un mensaje de error durante la instalación es que se ha instalado la versión incorrecta de ESET Mobile Security en el dispositivo. Al descargar el archivo de instalación del *ESET website*, asegúrese de que la versión del producto sea la correcta para su dispositivo.

12.1.2 Falla de la conexión con el servidor de actualización

Este mensaje de error se muestra luego de un intento de actualización sin éxito cuando el programa no consigue establecer contacto con los servidores de actualización.

Pruebe las siguientes soluciones:

1. Verifique su conexión a Internet: abra el explorador de Internet e ingrese a *http://www.eset.com* para corroborar que está conectado a Internet.
2. Verifique que el programa está usando el servidor de actualización correcto: presione **Menú > Configuración > Actualizar** y corrobore que aparezca el servidor *updmobile.eset.com* en el campo **Update Server**.

12.1.3 Tiempo de espera excedido al descargar archivo

La conexión a Internet se interrumpió o su velocidad se redujo en forma inesperada durante la actualización. Intente volver a ejecutar la actualización más tarde.

12.1.4 Falta el archivo de actualización

Si está intentando instalar una nueva base de datos de firmas de virus desde el archivo de actualización (*esetav_wm.upd*), el archivo debe estar guardado en la carpeta de instalación de ESET Mobile Security (*\Archivos de programa\ESET\ESET Mobile Security*).

12.1.5 El archivo de la base de datos está dañado

El archivo de actualización de la base de datos de firmas de virus (*esetav_wm.upd*) está dañado. Es necesario reemplazar el archivo y volver a ejecutar la actualización.

12.2 Soporte técnico

En caso de que necesite asistencia administrativa o soporte técnico relacionado con ESET Mobile Security o con cualquier otro producto de seguridad de ESET, nuestros especialistas de Atención al cliente se encuentran disponibles para ayudarlo. Para encontrar la solución a un problema de soporte técnico, puede elegir entre las siguientes opciones:

Para encontrar las respuestas a las preguntas más frecuentes, acceda a ESET Knowledgebase, la Base de conocimiento de ESET en español en:
http://kb.eset-la.com

La Base de conocimiento contiene una gran cantidad de información útil para resolver los problemas más comunes, donde se puede buscar por categorías y por búsqueda avanzada.

Para contactarse con el servicio de Atención al cliente de ESET, use el formulario de solicitud de soporte disponible en:
http://www.eset-la.com/support/contact.php