Documento de ayuda para la aplicación Segurmática Seguridad Móvil.

ÍNDICE

1. Segurmática Seguridad Móvil

Segurmática Seguridad Móvil es un producto orientado a la detección de aplicaciones malignas en dispositivos móviles con sistema operativo Android, entre sus principales características está el bajo consumo de recursos, que no necesita privilegios de root para ejecutarse y la posibilidad de ejecutar varios análisis simultáneamente.

2. Requerimientos de instalación

- Versiones de Android a partir de la 4.2
- Arquitecturas ARM y x86.

3. Interfaz.

3.1 Pantalla Principal

La pantalla principal o portada de la aplicación (Figura 1.) cuenta con un diseño acorde a los estigmas de *Material Design*, con un menú de navegación inferior para acceder a las funciones principales de la aplicación. En su parte superior derecha se encuentran las 2 acciones fundamentales que son Analizar todas las aplicaciones y Actualizar (Figura 2.), así como el botón de configuración (Figura 3.) El cual mostrara un menú flotante (Figura 4.) con acceso a las diferentes configuraciones de la aplicación, así como la información de la licencia y la ayuda del producto.

Una vez instalada la aplicación si el dispositivo tiene una tarjeta SD, el sistema le pedirá que le de acceso a la misma para poder escanear y/o eliminar programas malignos guardados en esta. Siga las indicaciones, seleccionando la misma como se muestra en la (Figura 5.)

Figura 1. Pantalla Principal.

Figura 2. Botón Analizar todas las aplicaciones y botón Actualizar, respectivamente.

Figura 3. Botón Configuración.

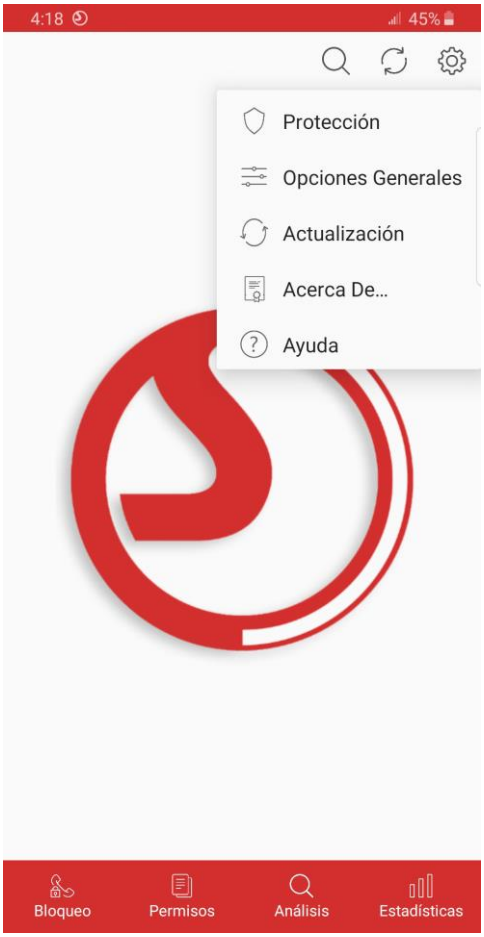

Figura 4. Menú Configuración.

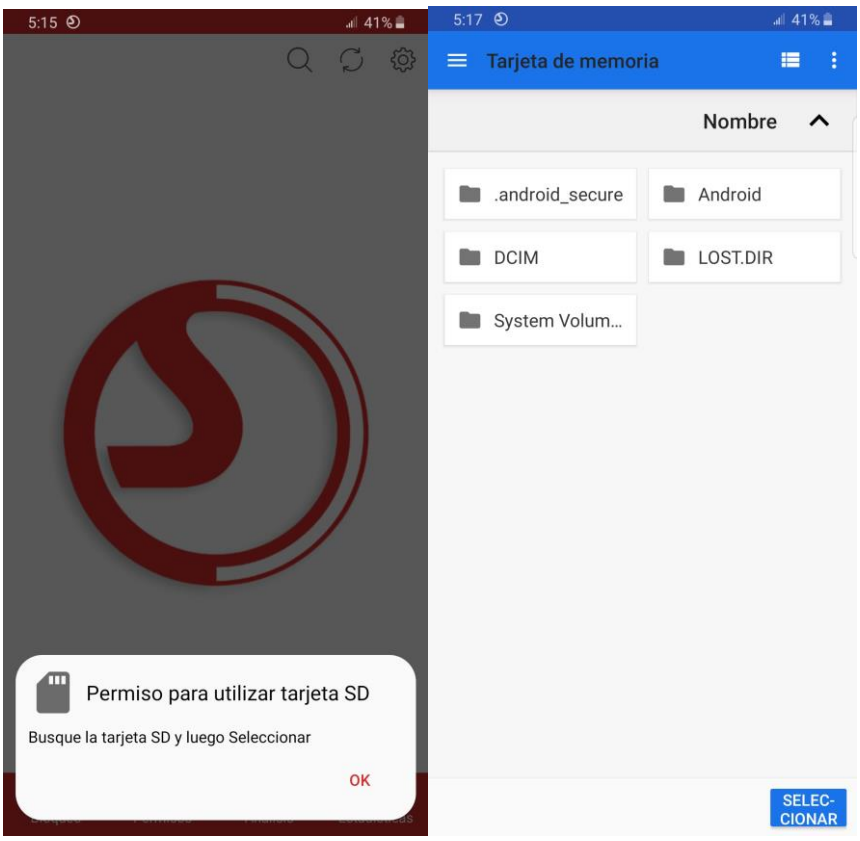

Figura 5. Solicitud de Permiso para dispositivos con Tarjeta SD.

Cada vez que el usuario inicie la aplicación, se verifica que la versión de la misma instalada en el dispositivo sea la última versión liberada, y en caso de no serlo le mostrará un mensaje de alerta recomendándole que descargue la nueva versión (Figura 6.). Si el usuario selecciona la opción “Descargar Nueva versión” la aplicación se conectará al sitio web de la empresa e iniciará la descarga de la misma. (Para esto el dispositivo tiene que estar conectado a una red Wi-Fi o a los datos móviles).

Figura 6. Mensaje de Alerta. Nueva Versión Disponible.

3.1.1 Botón Analizar todas las aplicaciones

El Botón *Analizar todas las aplicaciones* (Figura 7.) se encuentra en la parte superior derecha de la aplicación y tiene como objetivo que los usuarios puedan iniciar un análisis de todas las aplicaciones instaladas en el dispositivo directamente sin tener que acceder a la pantalla análisis.

Figura 7. Botón Analizar todas las aplicaciones.

Seleccionando este botón se inicia un análisis como su nombre indica de todas las aplicaciones instaladas en el dispositivo, el usuario puede observar el progreso del mismo tanto en la barra de notificaciones (Figura 8.) como en el centro de la pantalla de la aplicación (Figura 9.). Durante el proceso de análisis el botón cambia al estado de procesando y adopta una forma diferente para identificar que está en uso además se muestra el porcentaje analizado justo debajo, en el momento en el que el usuario desee cancelar el análisis en curso solo debe presionar sobre esta nueva forma y el botón regresará a su estado principal, permitiéndole volver a iniciar otro análisis. Tanto en el caso de que el usuario detenga en el análisis (Figura 10.) como cuando este termine con éxito (Figura 11.) el resultado se mostrará en la barra de notificaciones.

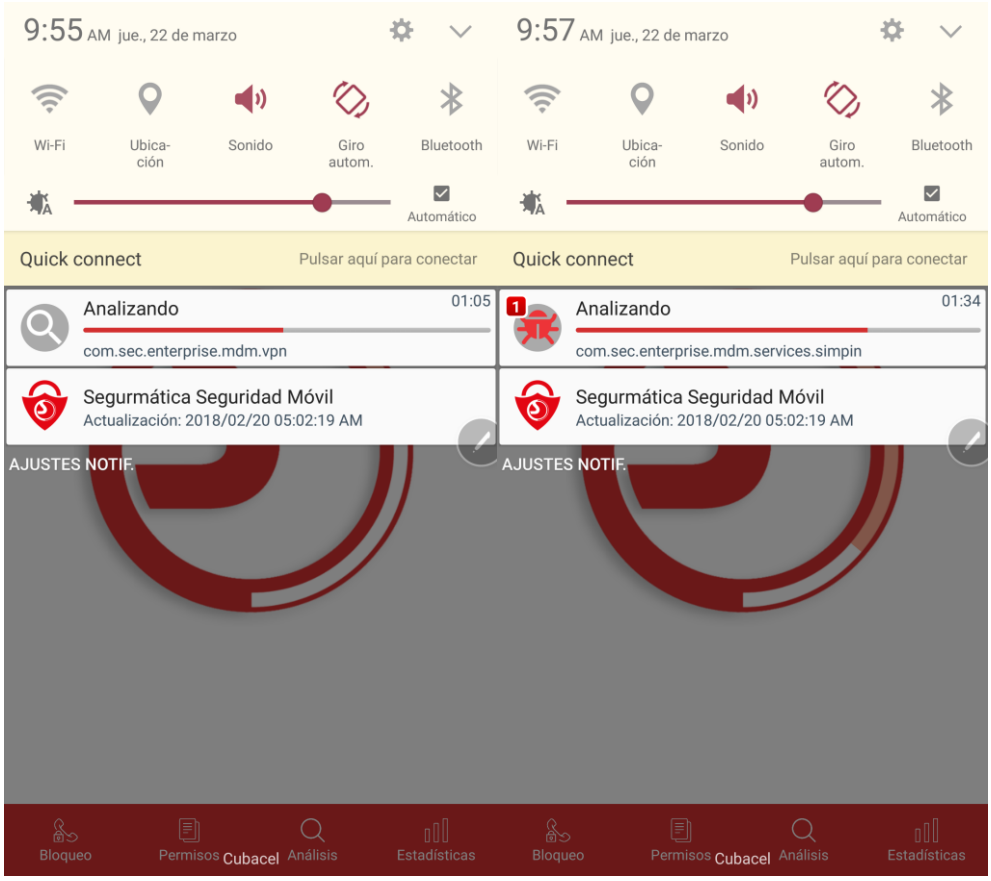

Figura 8. Barra de Notificaciones. Progreso del análisis en curso.

Figura 9. Pantalla principal. Progreso del análisis en curso.

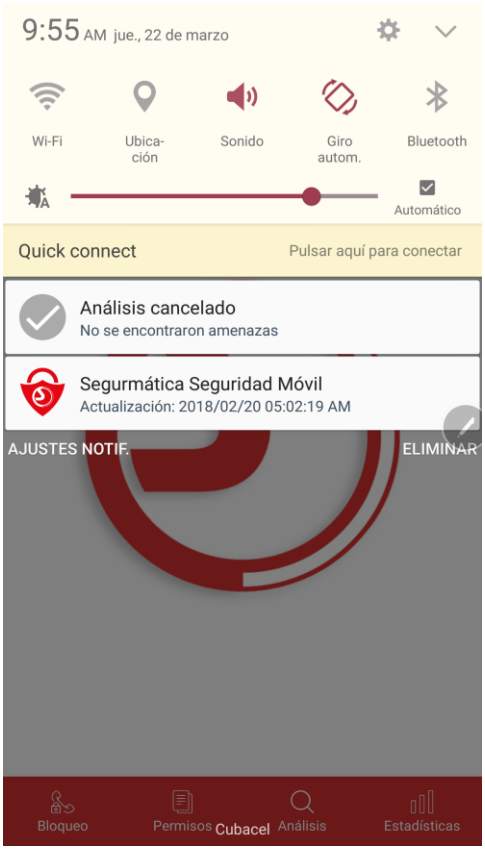

Figura 10. Barra de Notificaciones. Análisis cancelado.

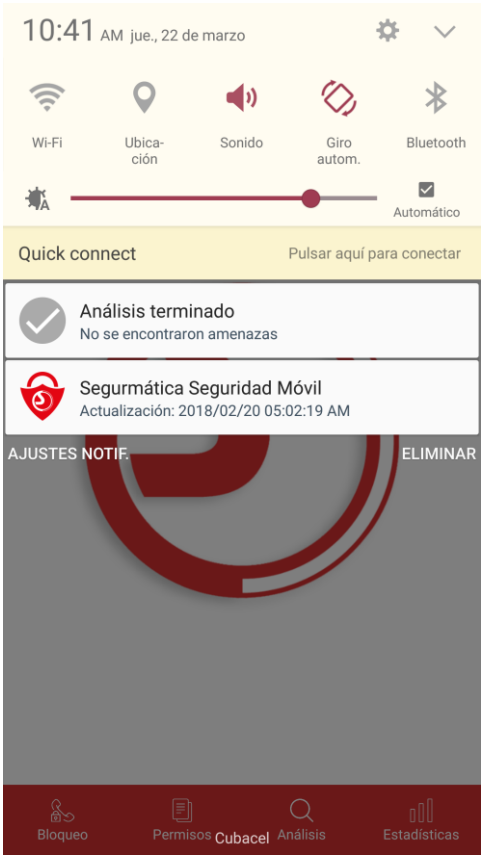

Figura 11. Barra de Notificaciones. Análisis terminado.

Una vez finalizado un análisis en el cual se encontraron amenazas (Figura 12.), el usuario debe seleccionar la notificación que muestra este resultado y de esta forma se abrirá la pantalla *Resultados del Análisis* (Figura 13.) que le va a permitir al usuario desinstalar la aplicación o aplicaciones malignas encontradas o si lo desea ignorar la misma y mantenerla en el dispositivo.

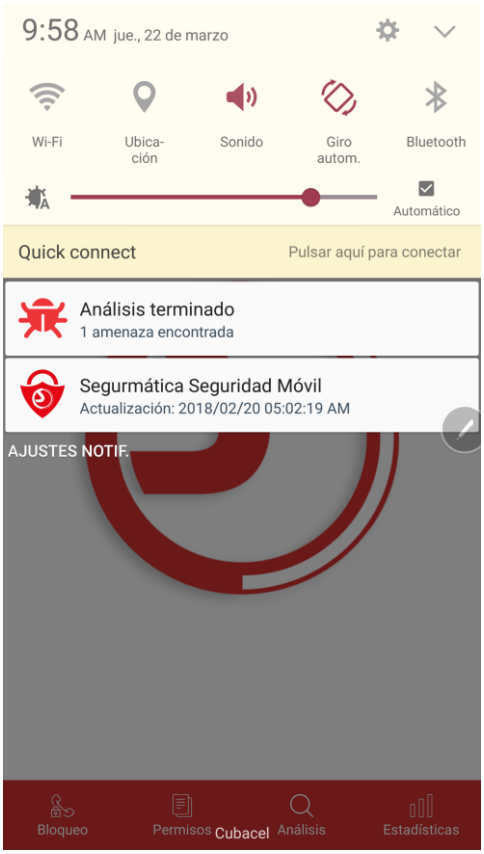

Figura 12. Barra de Notificaciones. Análisis terminado.

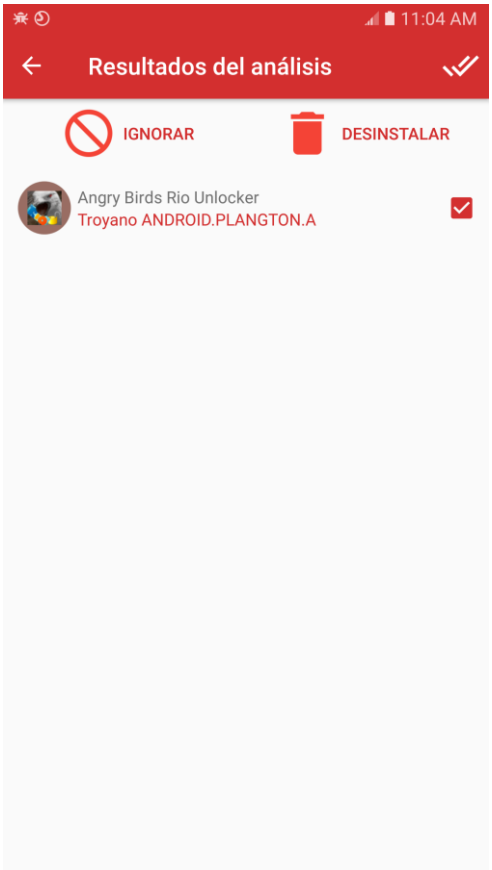

Figura 13. Pantalla Resultado del Análisis. Aplicación maligna detectada.

3.1.2 Botón Actualizar

Como su nombre indica con el botón *Actualizar* (Figura 14.) el usuario podrá iniciar la actualización del sistema. Cuando el usuario inicia una actualización el botón cambia de forma y muestra el porcentaje de actualización justo debajo.

Para actualizar la aplicación es necesario tener una licencia válida o estar conectado a una red de Etecsa, ya sea por datos o por WI-FI. Puede agregar una licencia desde el menú *Configuración,* apartado "*Acerca De…"* (Figura 15.).

El usuario puede acceder a las opciones de actualización desde el menú *Configuración* apartado "*Actualización*" (Figura 16.), donde podrá definir el origen y la frecuencia de la misma. Una vez terminada la actualización, o en el caso de que no se pueda actualizar por alguna razón, la aplicación muestra un mensaje indicando que la aplicación se actualizó correctamente o que no pudo actualizarse y el motivo. (Figura 17.).

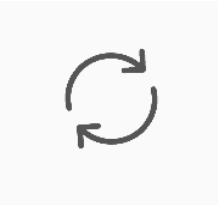

Figura 14. Botón Actualizar.

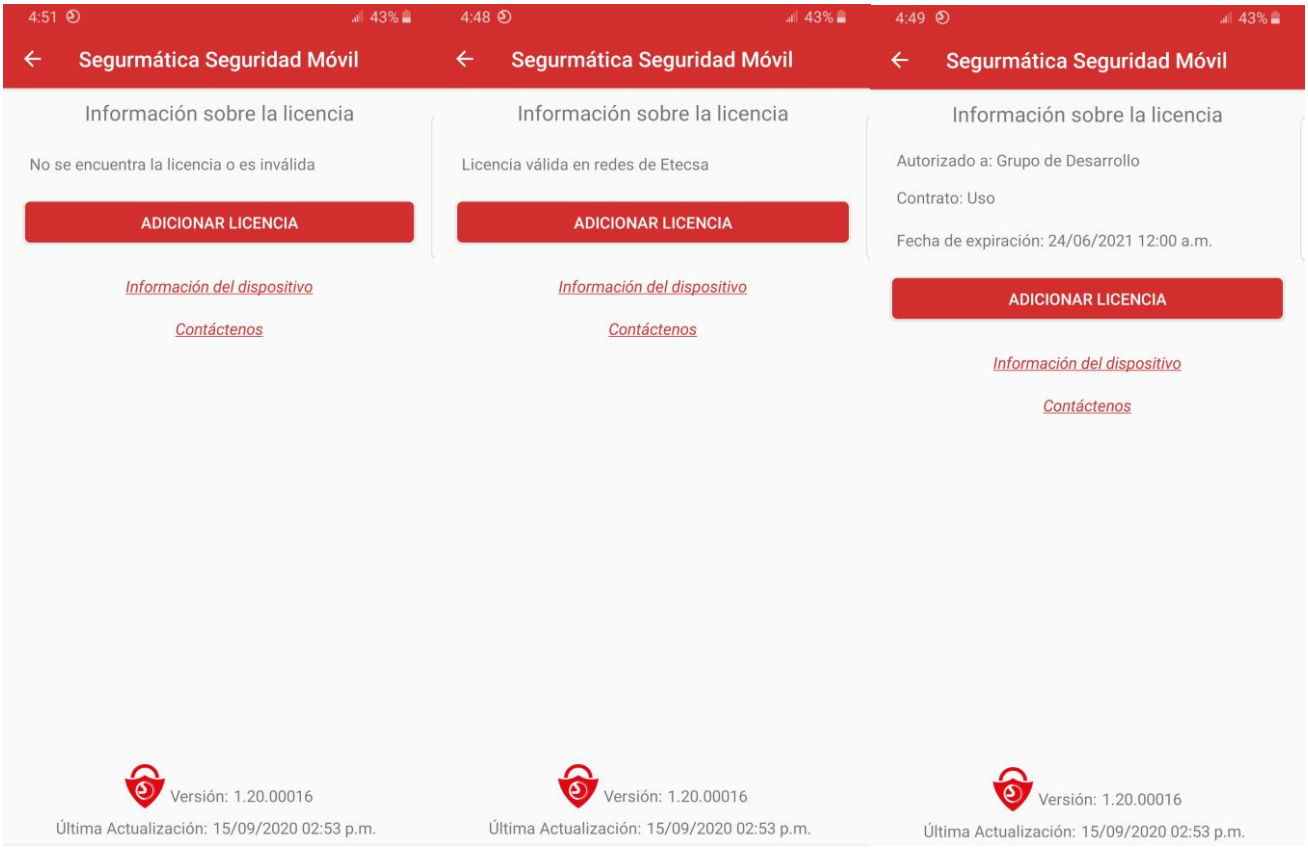

Figura 15. Pantalla "Acerca De…".

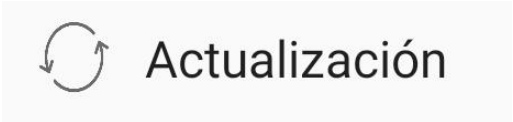

Figura 16. Apartado Actualización.

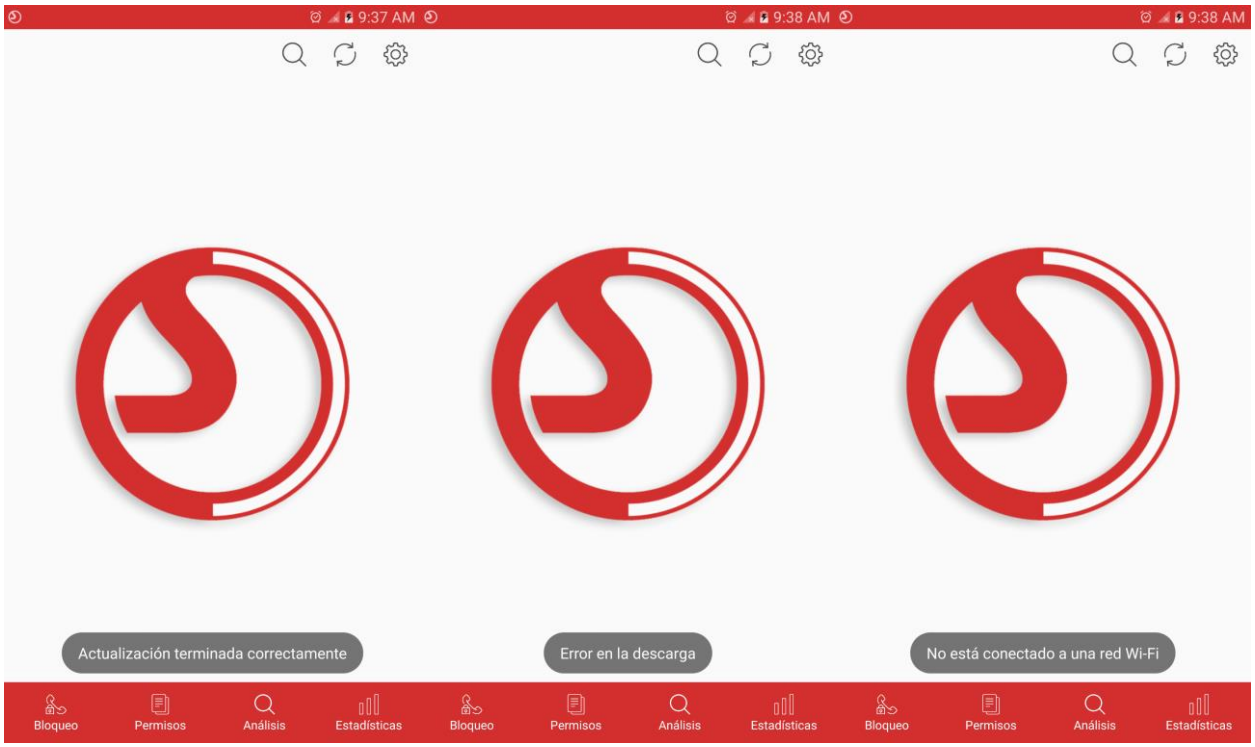

Figura 17. Pantalla "Resultado Actualización…".

3.1.3 Menú Configuración

El usuario puede acceder al menú configuración (Figura 4.) como se había mencionado previamente, a través de botón Configuración (Figura 3.) en la parte superior derecha de la pantalla principal. El mismo es un menú flotante con una serie de apartados que nos van a permitir configurar las diferentes opciones de la aplicación y acceder a la ayuda *online*.

- **Apartado Protección:**

Seleccionando este apartado el usuario puede acceder a la pantalla *Configurar Protección* (Figura 18.) Donde encontrará dos opciones de protección, la primera opción es para habilitar o no el análisis en demanda de las nuevas aplicaciones que se instalen o actualicen en el dispositivo (**Analizar nuevas instalaciones**).
Teniendo activada esta opción, cada vez que el usuario instale o actualice una aplicación el sistema analiza de manera inmediata y automática dicha aplicación y en caso de que la misma sea riesgosa para la seguridad de su dispositivo le muestra una ventana de alerta (Figura 19.), que le da la opción de desinstalar o ignorar la aplicación en cuestión.

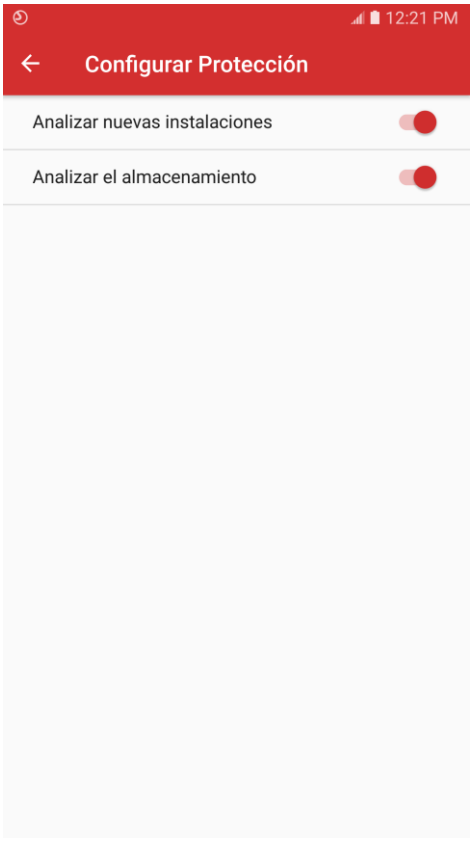

Figura 18. Pantalla Configurar Protección. Apartado Protección.

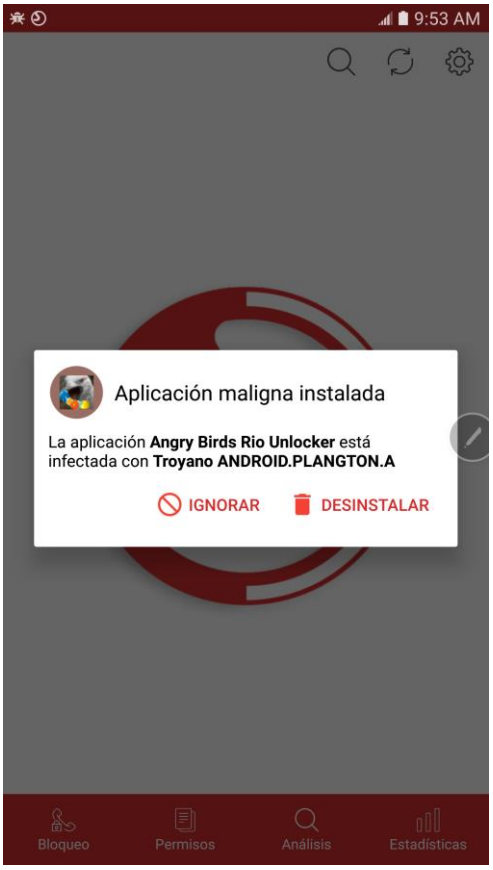

Figura 19. Ventana de Alerta. Aplicación maligna Detectada.

En el caso de la segunda opción (**Analizar el almacenamiento**), cuando está habilitada el sistema revisa automáticamente todo el trabajo que se realice con el almacenamiento del dispositivo, es decir copia de ficheros o aplicaciones desde una PC, copia de archivos por Zapya o Bluetooth, etc.
De igual forma en caso de que el sistema encuentre algún fichero maligno el sistema muestra una ventana de alerta (Figura 20.), que le da la opción de eliminar el fichero o ignorar el mismo.
Existen algunos dispositivos para los cuales el análisis automático del almacenamiento no funciona correctamente debido a errores internos del sistema dependiendo del fabricante y la versión de Android.
Ver más detalles sobre este problema en:
https://code.google.com/p/android/issues/detail?id=189231

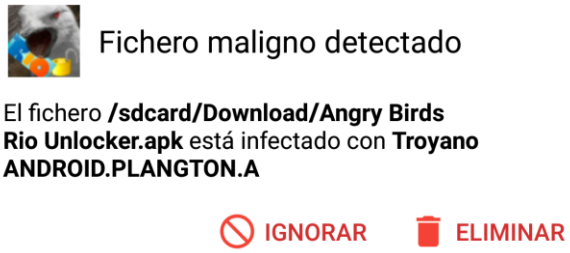

Figura 20. Ventana de Alerta. Fichero maligno Detectado.

Aclarar que para el caso de sistemas Android 4.4 no es posible eliminar el contenido del almacenamiento (memoria interna y tarjeta SD) del dispositivo a no ser que sea una aplicación interna del teléfono, por lo tanto, esta funcionalidad no estará disponible para los dispositivos con este sistema. La variante que proponemos es que el usuario elimine manualmente el fichero en la dirección especificada utilizando el administrador de archivos del sistema.
Ver más detalles sobre este problema en:
https://developer.android.com/about/versions/android-4.4.html
https://developer.android.com/guide/topics/data/data-storage.html

- **Apartado Opciones Generales:**

En el apartado Opciones Generales permite acceder a la pantalla de este mismo nombre (Figura 21.) el usuario tiene la posibilidad de habilitar o deshabilitar las opciones “Mostrar notificación principal”, “Mostrar notificación de bloqueo”, “Sonido” y “Ayudar a mejorar el producto”, así como la opción de introducir el número de días que desea permanezcan almacenadas las estadísticas.

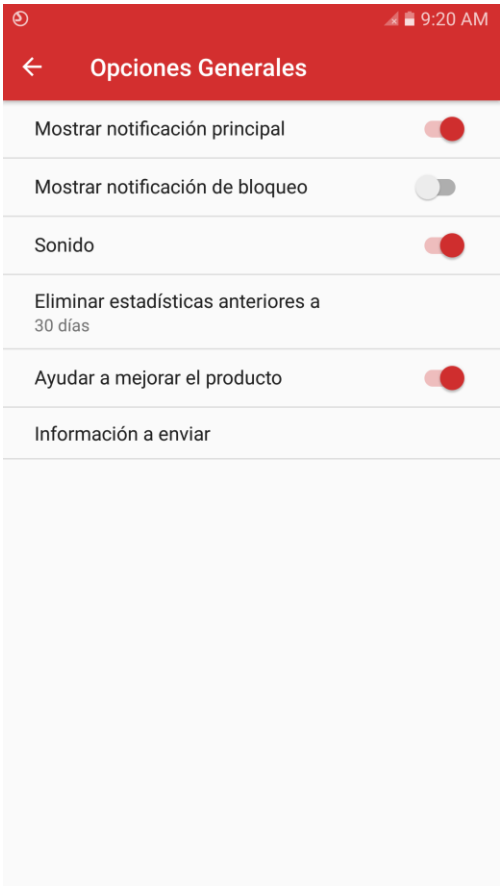

Figura 21. Pantalla Opciones Generales. Apartado Opciones Generales.

Cuando está habilitada la opción "Mostrar notificación principal" nos permite tener siempre visible el ícono de la aplicación, con la fecha de la última actualización, en la barra de notificaciones (Figura 22).

Figura 22. Barra de notificaciones. Ícono Segurmática Seguridad Móvil.

Habilitando la opción "Mostrar notificación de bloqueo" la aplicación creará una notificación cada vez que una llamada sea bloqueada por la misma la cual se mostrará en la barra de notificaciones (Figura 23).

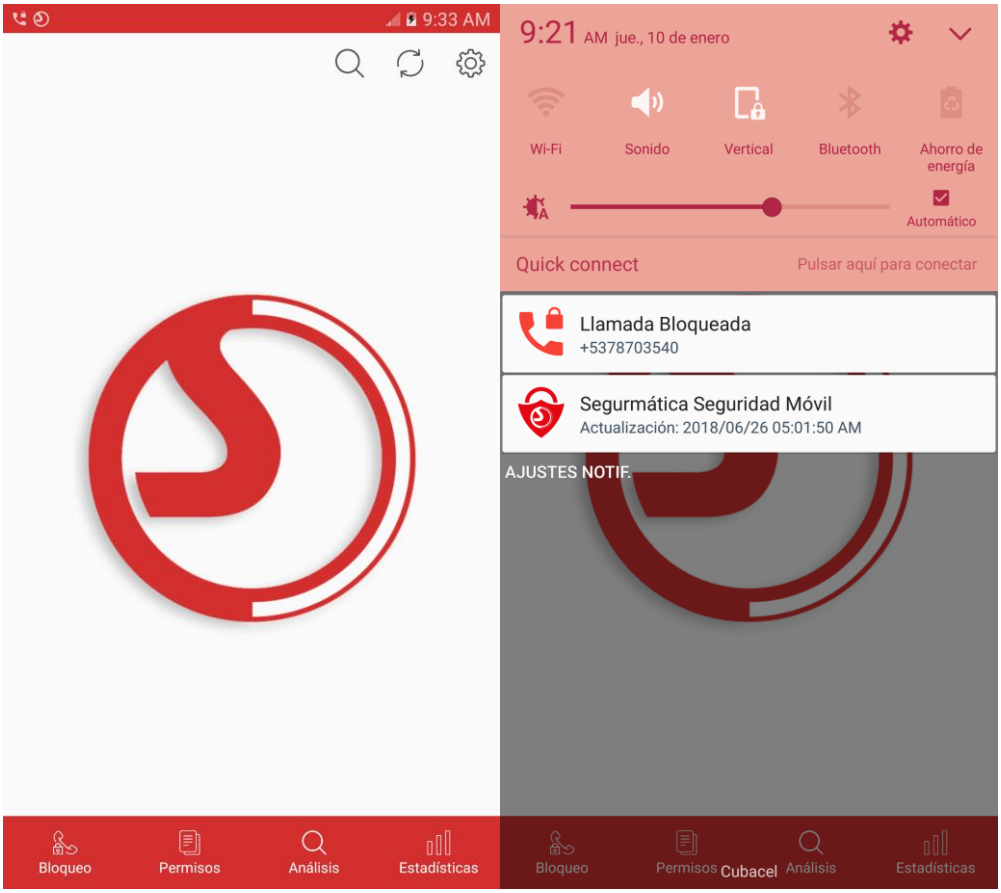

Figura 23. Barra de notificaciones. Notificación de Llamada Bloqueada.

En el caso de la opción "Sonido", cuando esta se encuentra habilitada el sistema reproduce un sonido cada vez que se completa un análisis, de manera que el usuario no tenga que estar pendiente del avance del mismo, además lo reproduce cuando el sistema detecta la instalación de una aplicación maligna y muestra la ventana de alerta (Figura 19) o la ventana de alerta (Figura 20.) para el caso de ficheros malignos.

La opción "Eliminar estadísticas anteriores a", le permite seleccionar el número de días que desea que permanezcan almacenadas las estadísticas, es decir las estadísticas cuya fecha sobrepase este número serán eliminadas automáticamente.

Habilitando la opción "Ayuda a mejorar el producto" (Figura 23.), se muestra la pestaña "Información a enviar", en la cual el usuario podrá seleccionar la información que desea que la aplicación envíe a nuestro sistema (Figura 24.) para ayudarnos a mejorar la calidad del producto.

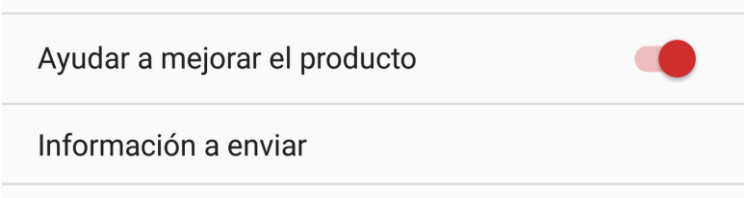

Figura 23. Pantalla Opciones Generales. Ayudar a mejorar el producto.

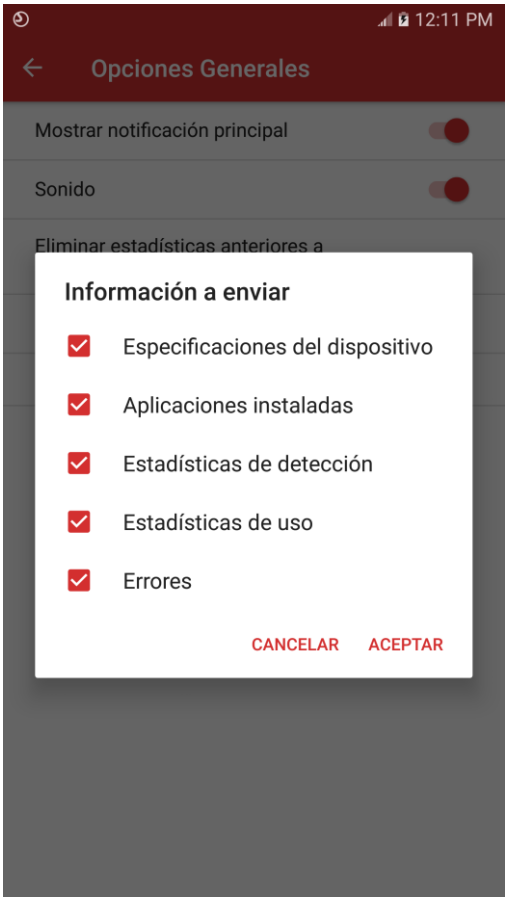

Figura 24. Pantalla Opciones Generales. Información a enviar.

- **Apartado Actualización:**

En el apartado actualización el usuario accede a la pantalla Opciones de Actualización (Figura 25.) donde debe definir los datos necesarios para que el sistema acceda al directorio de actualización, así como la frecuencia de las próximas actualizaciones. La fecha y hora definida se puede observar en la parte inferior de la misma.

Cuando seleccionamos la opción *Origen* accedemos a la pantalla Configurar Actualización (Figura 26.) y dentro de esta como primer apartado los diferentes orígenes que puede definir el usuario para actualizar la aplicación (Figura 27.).

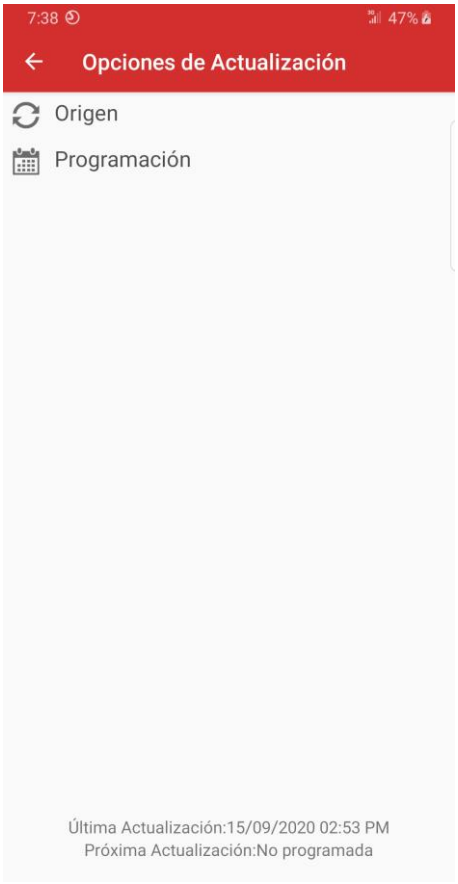

Figura 25. Pantalla Opciones de Actualización.

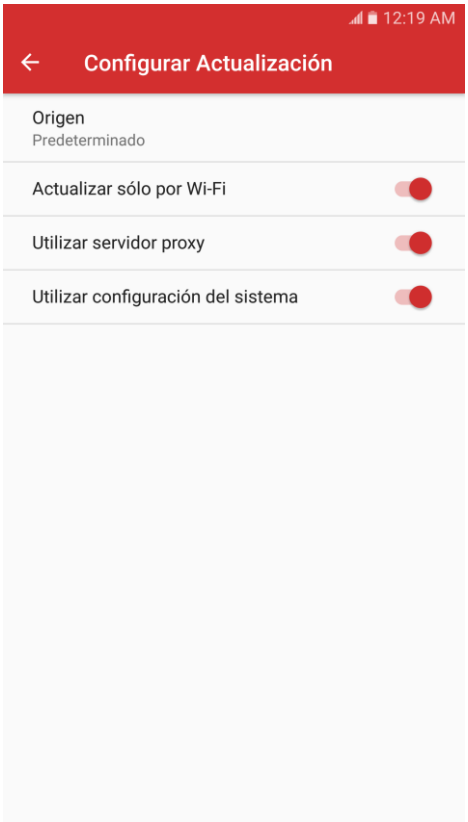

Figura 26. Pantalla Configurar Actualización.

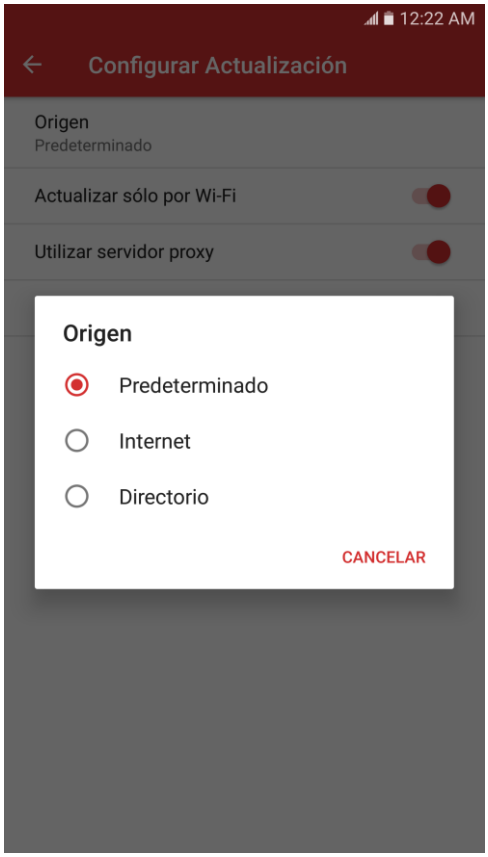

Figura 27. Pantalla Configurar Actualización. Origen.

1. **Origen Predeterminado**

   Es la opción que tiene la aplicación seleccionada por defecto y con ella el sistema se conecta automáticamente al servidor de Segurmática para descargar la actualización. Muestra como opciones además las pestañas “Actualizar solo por Wi-Fi” y “Utilizar servidor proxy” (Figura 28.).

   Cuando la opción “Actualizar solo por Wi-Fi” está habilitada el sistema ejecutará las actualizaciones programadas siempre y cuando el dispositivo se encuentre conectado a una red Wi-Fi.
   En el caso de la pestaña “Utilizar servidor proxy” al habilitarla se muestra la pestaña “Utilizar configuración del sistema” que aparece por defecto habilitada de manera tal que se conecte al proxy con la configuración que ya tiene el dispositivo.

   En caso de que desee conectarse con otra configuración debe deshabilitar esta opción, con lo cual se mostraran nuevas pestañas con datos a introducir para configurar el servidor proxy.

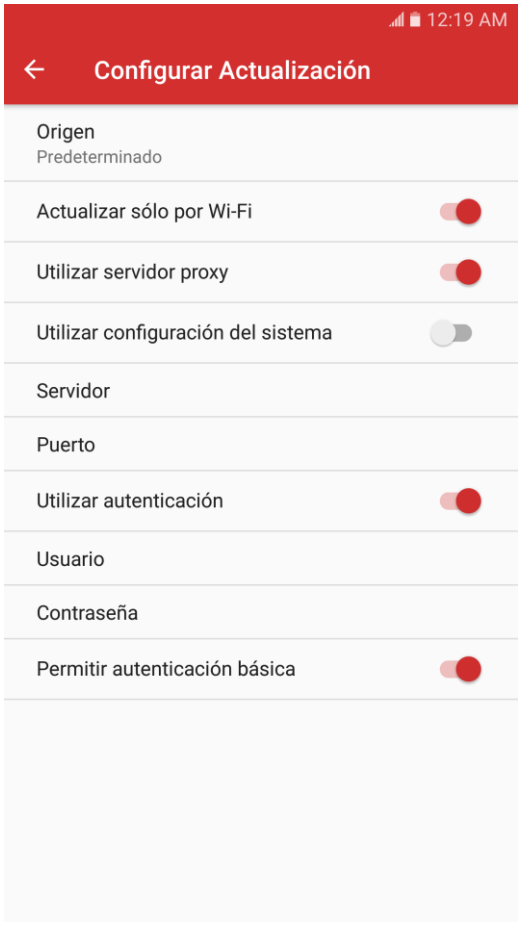

Figura 28. Pantalla Configurar Actualización. Origen Predeterminado.

La pestaña "Utilizar autenticación" por defecto se encuentra deshabilitada, no obstante, en caso de que el servidor requiera autenticación al habilitar la misma se muestran los datos necesarios a introducir, resaltando en este caso la pestaña "Permitir autenticación básica" que da la opción de enviar los datos en texto claro (sin cifrar) por lo que se recomienda mantenerla deshabilitada.
Aclarar en este punto que el producto no soporta autenticación NTLM.

2. Origen Internet

Cuando se selecciona como origen la opción internet se le habilitan una serie de pestañas (Figura 29.) en el caso de la pestaña "URL" como su nombre lo indica le permite al usuario introducir la dirección url a la que desea acceder. La pestaña "Actualizar solo por Wi-Fi", "Utiliza servidor proxy" y "Utilizar configuración del sistema" tiene las mismas opciones y funcionamiento que se explicaron en el apartado anterior.

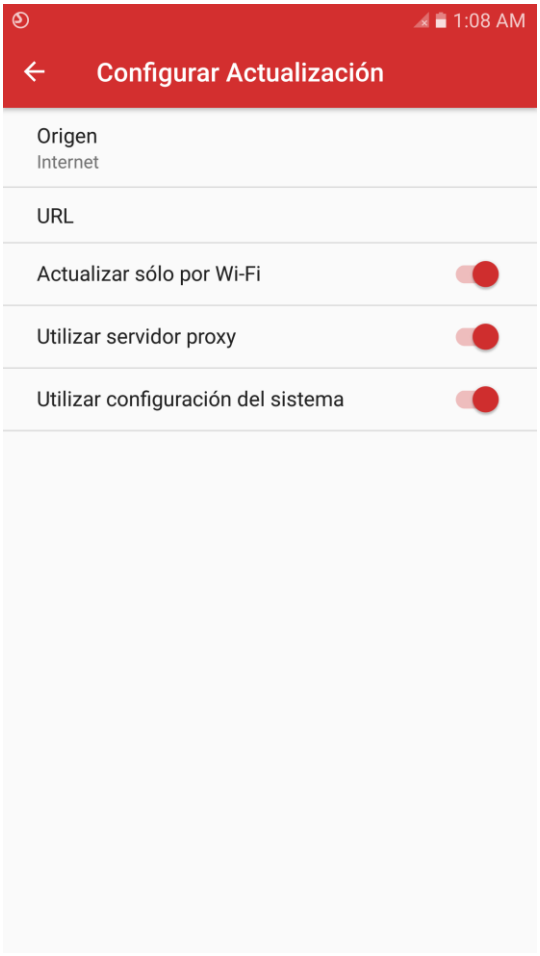

Figura 29. Pantalla Configurar Actualización. Origen Internet.

3. Origen Directorio

Cuando se selecciona como origen la opción directorio (Figura 30.) el usuario debe seleccionar la ubicación de este directorio dentro del dispositivo, para esto cuando el usuario accede a la pestaña “Ubicación” el sistema abre el explorador de archivos (Figura 31.) a través del cual el usuario puede navegar hasta encontrar la ruta deseada y seleccionarla. Para actualizar desde un directorio es obligatorio que la aplicación tenga agregada una licencia válida, ya que la licencia de Etecsa solo funciona para los orígenes anteriores.

Figura 30. Pantalla Configurar Actualización. Origen Directorio.

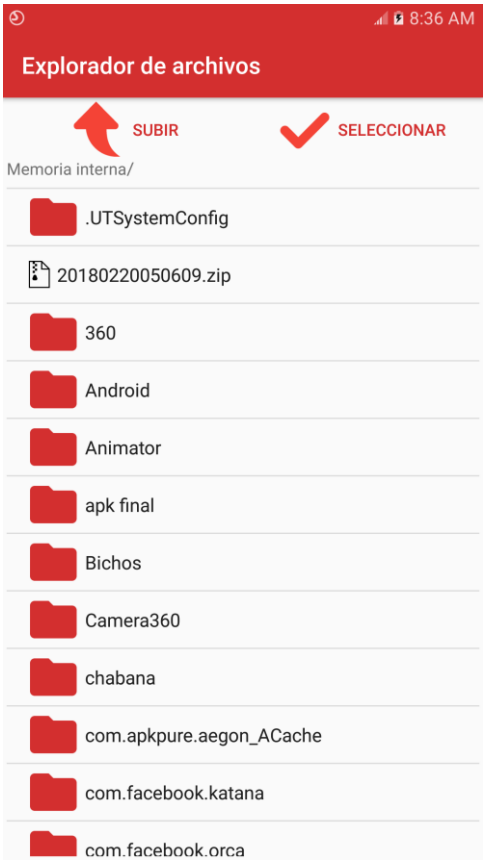

Figura 31. Explorador de Archivos.

Regresando a la pantalla Opciones de Actualización (Figura 25.) Cuando seleccionamos la opción ***Programación*** accedemos a la pantalla Configurar Actualización con las opciones para definir la frecuencia de la próxima actualización automática (Figura 32.).

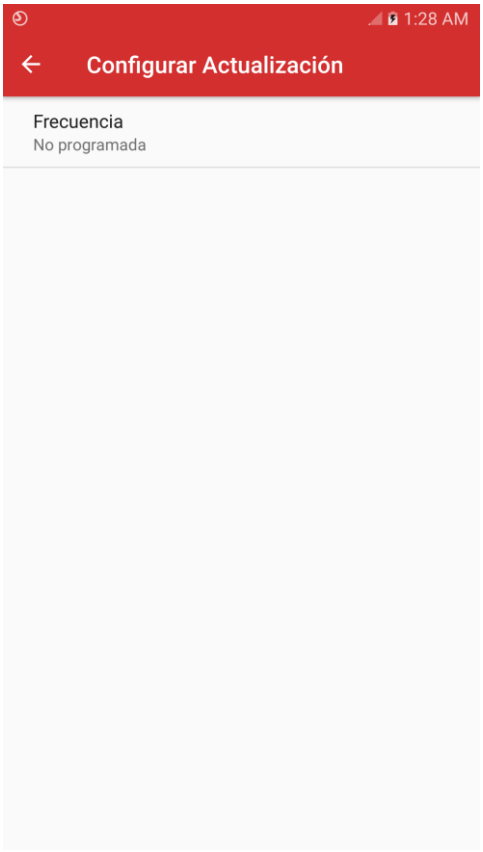

Figura 32. Pantalla Configurar Actualización. Frecuencia No Programada.

El sistema cuenta con 4 opciones de frecuencia:

1. No programada
   Como su nombre indica, no se define una fecha de actualización automática.
2. Horaria
   Cuando se selecciona esta frecuencia se muestran dos pestañas (Figura 33.) en las cuales el usuario puede definir cada cuantas horas y minutos desea se inicie el proceso de actualización de manera automática.

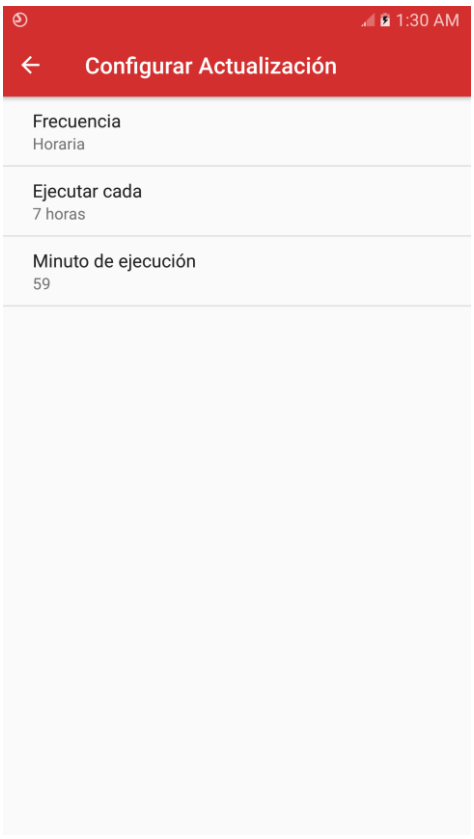

Figura 33. Pantalla Configurar Actualización. Frecuencia Horaria.

3. Diaria

   Para el caso de la frecuencia diaria se muestran las pestañas (Figura 34.) En las cuales el usuario puede definir cada cuántos días y la hora del día en que comenzará el proceso de actualización.

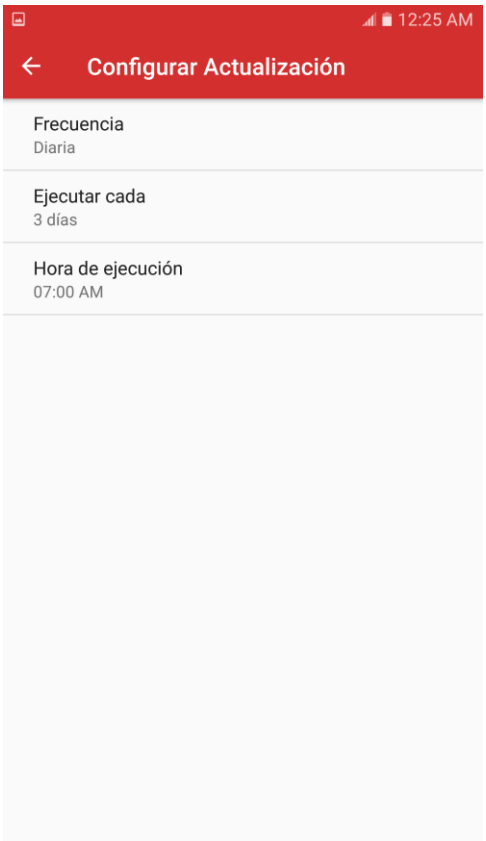

Figura 34. Pantalla Configurar Actualización. Frecuencia Diaria.

4. Semanal

La frecuencia semanal por su parte muestra las pestañas (Figura 35.) En las cuales el usuario puede definir los días de la semana, así como la hora de ejecución del proceso automático de actualización.

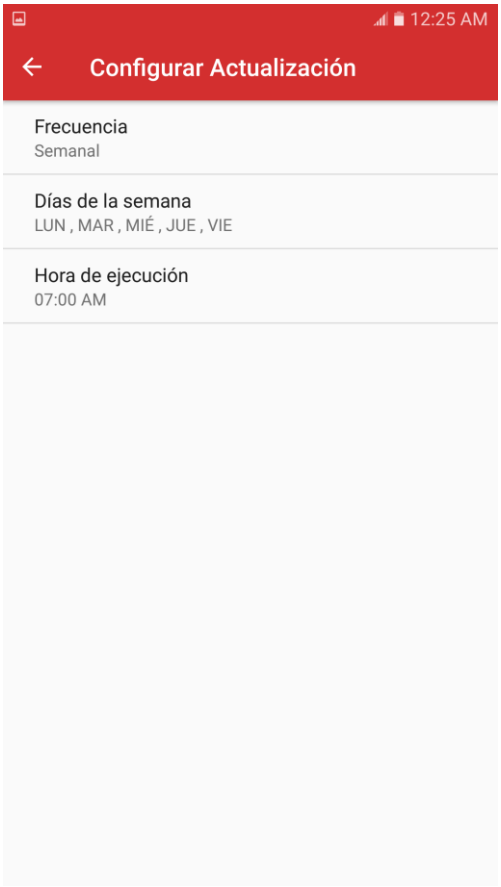

Figura 35. Pantalla Configurar Actualización. Frecuencia Semanal.

- **Apartado Acerca De…:**

En el apartado *Acerca De…* el usuario accede a la pantalla que contiene información relevante sobre el producto, la licencia y otras informaciones de interés (Figura 15.). En la parte inferior de esta pantalla podemos encontrar además datos de la aplicación *Segurmática Seguridad Móvil* tales como la versión, la fecha de la actualización que está utilizando.

Principales informaciones y funcionalidades de esta pantalla:

Información sobre la Licencia: Datos referentes a las características de la licencia que está utilizando, así como un botón (Figura 36.) para seleccionar dentro del dispositivo el archivo licencia.

Figura 36. Apartado Acerca De…. Botón Adicionar Licencia.

Información del dispositivo: Seleccionando el enlace (Figura 37.) el usuario puede observar el modelo y la versión Android del dispositivo actual (Figura 38.).

Figura 37. Apartado Acerca De…. Información del dispositivo.

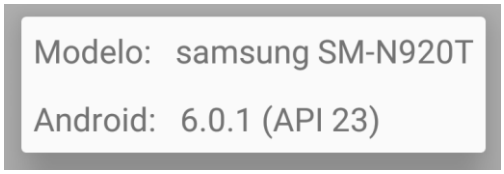

Figura 38. Apartado Acerca De…Información del dispositivo.

Contáctenos: Seleccionando el enlace (Figura 39.) el usuario puede observar los datos de contacto de nuestra entidad Segurmática (Figura 40.)

Figura 39. Apartado Acerca De…. Contáctenos.

Figura 40. Apartado Acerca De…. Contactos Segurmática.

- **Apartado Ayuda:**

Seleccionando este apartado en el menú configuración (Figura 4.). El sistema lo re-direcciona directamente al documento de ayuda de la aplicación, que se encuentra en el sitio web de nuestra empresa.
(Para poder acceder a la ayuda es necesario que el dispositivo se encuentre conectado a internet).

3.2 Menú Inferior de Navegación

Este menú como su nombre indica se encuentra en la parte inferior de la pantalla principal o portada de la aplicación (Figura 1.) y a través de sus diferentes botones el usuario puede acceder a las principales pantallas de la aplicación.

3.2.1 Bloqueo de Llamadas

A través del botón *Bloqueo* (Figura 41.) el usuario accede a la pantalla *Bloqueo de Llamadas* (Figura 42.). En esta pantalla tendrá la posibilidad de configurar las reglas de bloqueo, las excepciones y visualizar las diferentes llamadas que ha realizado y recibido, incluyendo aquellas que hayan sido bloqueadas, las cuales no podrá visualizar en el registro de llamadas del dispositivo.

Figura 41. Menú inferior de navegación. Botón Bloqueo.

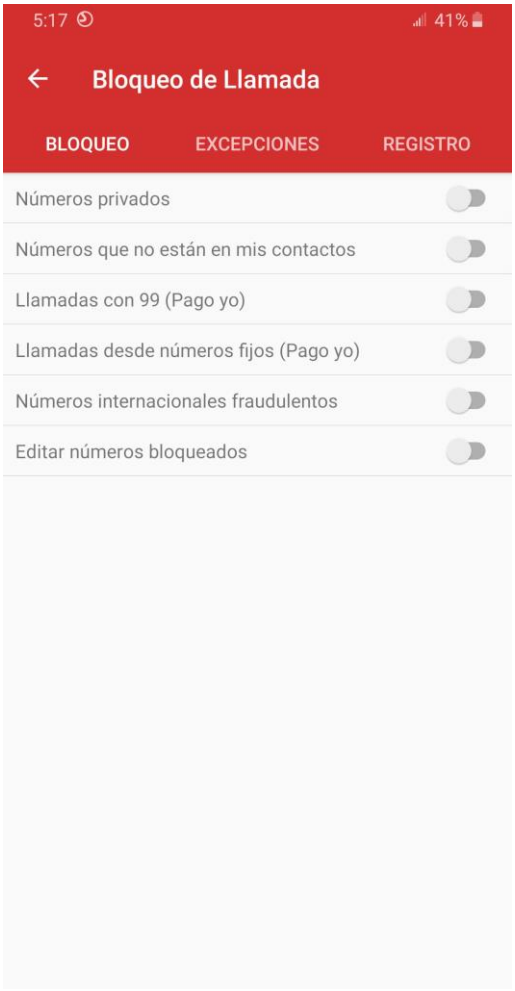

Figura 42. Pantalla Bloqueo de Llamadas.

Reglas de Bloqueo

El usuario tiene diferentes reglas de bloqueo predefinidas y personalizadas para nuestro país como se puede ver en la figura anterior (Figura 42.) y tiene además la opción de editar los números que tiene ya bloqueados o agregar nuevos números a la lista, ya sea eligiéndolo de su lista de contactos, eligiéndolo del registro de llamadas recientes o entrando el número directamente (Figura 43.). También se muestra la cantidad de números bloqueados (Figura 44.).

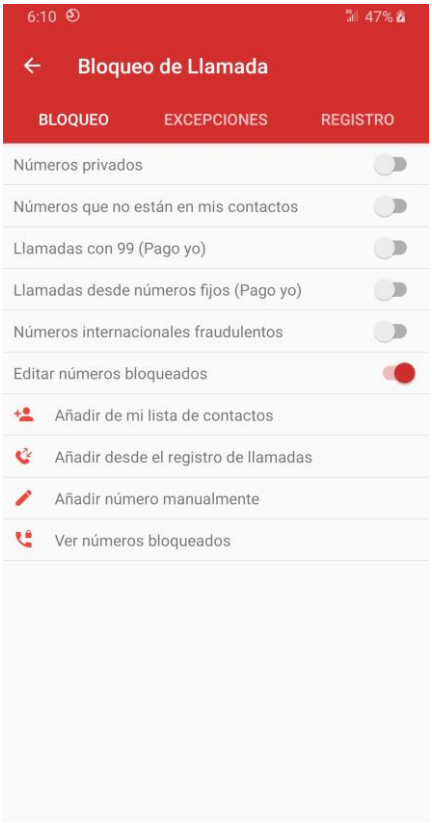

Figura 43. Pantalla Bloqueo de Llamadas. Editar números bloqueados.

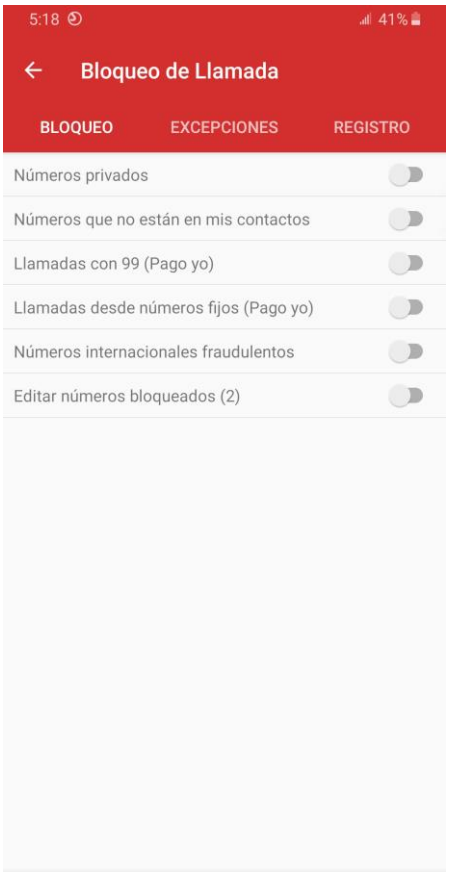

Figura 44. Pantalla Bloqueo de Llamadas. Cantidad de números bloqueados.

Excepciones

Una vez que el usuario define las reglas de bloqueo, puede agregar contactos a la lista de excepciones, que serán aquellos contactos que, aunque cumplan alguna de estas reglas el usuario no desea que sean bloqueados.

Ejemplo práctico:

Activo la regla de bloqueo “Llamadas con 99 (Pago yo)”, esto bloquea todas las llamadas que reciba el dispositivo que hayan sido realizadas con *99.

Yo deseo que algunos miembros de mi familia puedan llamarme con *99. ¿Qué hago?

Voy a excepciones (Figura 45.). Y agrego los números de los familiares que deseo eximir de las reglas de bloqueo, ya sea importando el número de mi lista de contactos o desde el registro de llamadas recientes, o adicionándolo manualmente. También muestra la cantidad de Excepciones (Figura 46.).

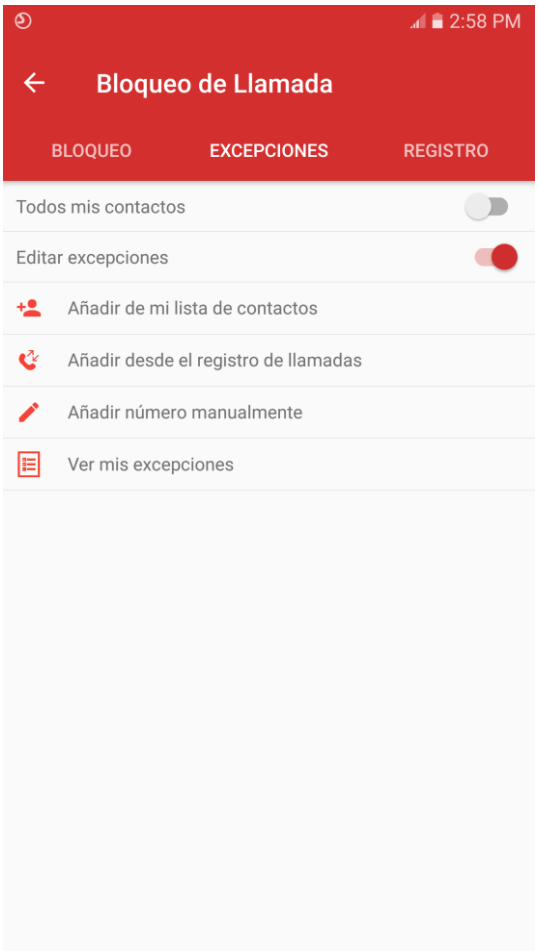

Figura 45. Pantalla Bloqueo de Llamadas. Excepciones.

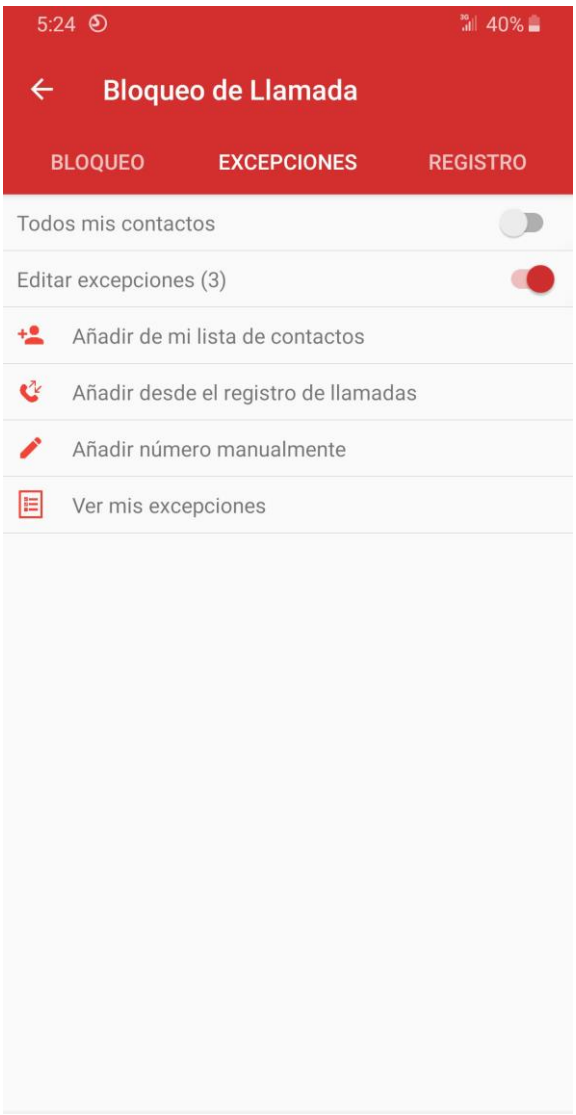

Figura 46. Pantalla Bloqueo de Llamadas. Cantidad de Excepciones.

Registro de Llamadas

En el caso del registro de llamadas el usuario puede observar las llamadas entrantes y salientes del dispositivo (Figura 47.), incluyendo las llamadas que fueron bloqueadas por la aplicación, las cuales no son mostradas en el registro de llamadas del dispositivo y se pueden identificar por el ícono de bloqueo en el registro.

Directamente desde el registro el usuario tiene la opción de bloquear un número o bien eliminarlo de la lista de bloqueo (Figura 48.), solo debe dejar presionado por un segundo el registro del contacto que desee Bloquear o Eliminar bloqueo. Haciendo esta misma operación podrá además agregar este número a las Excepciones, iniciar una llamada o copiarlo al portapapeles.

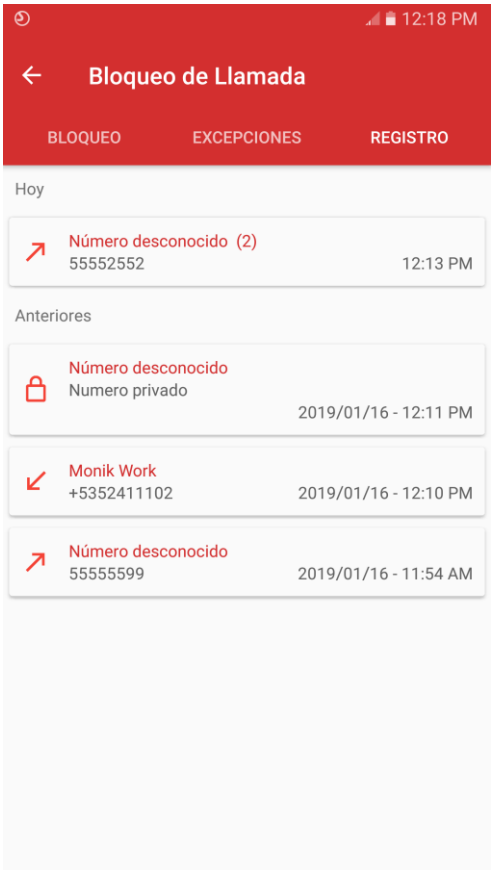

Figura 47. Pantalla Bloqueo de Llamadas. Registro de Llamadas.

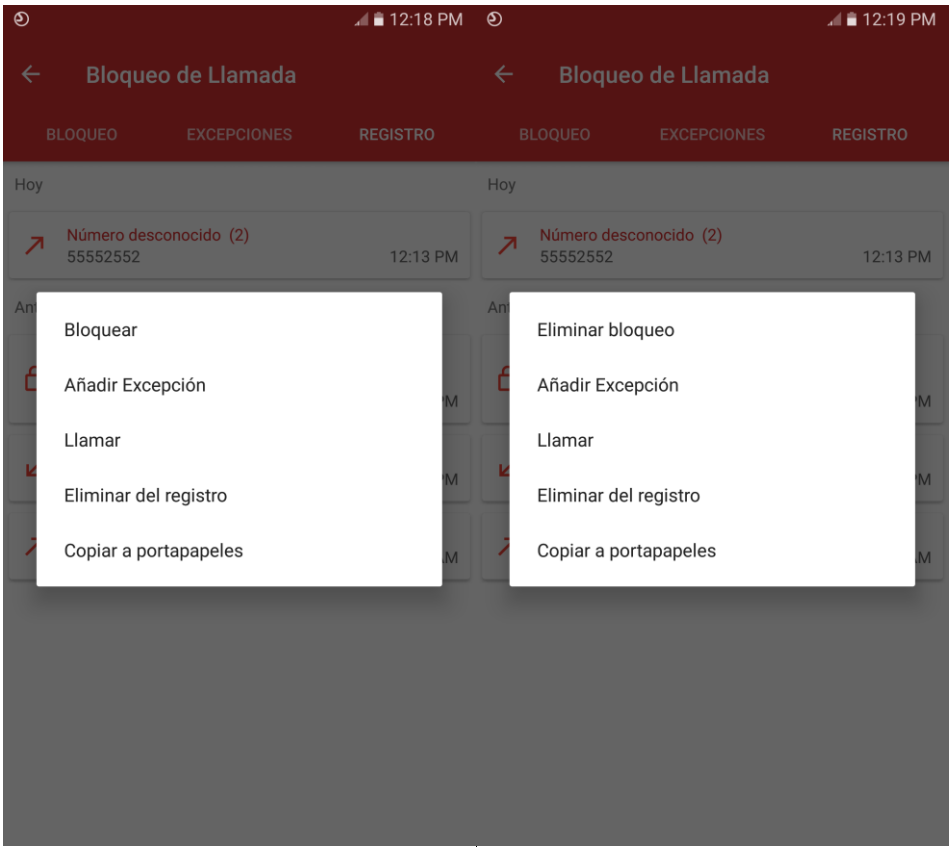

Figura 48. Pantalla Bloqueo de Llamadas. Registro. Bloquear/Desbloquear.

El usuario también tiene la opción de eliminar alguno de los registros en el caso en el que un mismo número tiene varias entradas (Figura 49.) con diferentes fechas y horarios. Seleccionando el registro se abrirá una pantalla (Figura 50.) que le permitirá ver en detalle cada una de las entradas y eliminar aquellas que desee.

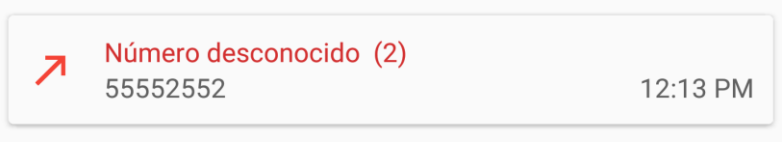

Figura 49. Pantalla Bloqueo de Llamadas. Registro.

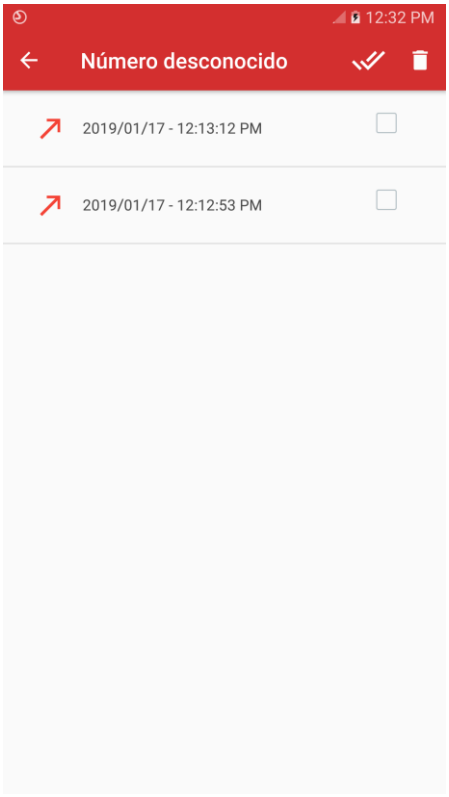

Figura 50. Pantalla Bloqueo de Llamadas. Registro. Eliminar registro.

3.2.2 Permisos

A través del botón *Permisos* (Figura 51.) el usuario accede a la pantalla de este mismo nombre (Figura 52.). El objetivo de esta es permitirle al usuario conocer de las aplicaciones que tiene instaladas en su dispositivo aquellas que requieren permisos que predominan en las aplicaciones malignas.

Figura 51. Menú inferior de navegación. Botón Permisos.

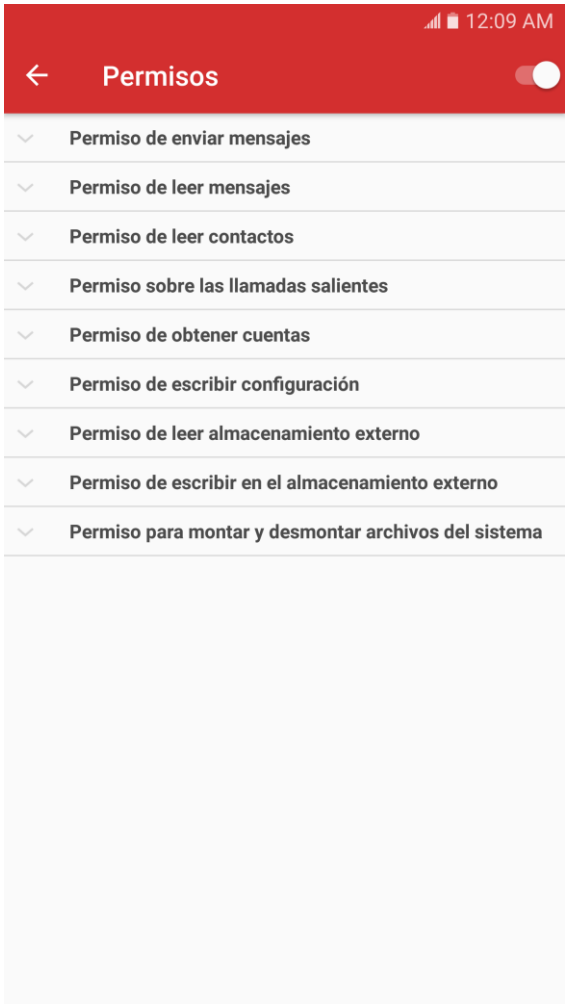

Figura 52. Pantalla Permisos.

Muestra un listado con 10 permisos riesgosos para la seguridad de su dispositivo, seleccionando cada uno de estos se despliega un sub-listado (Figura 53.) con las aplicaciones que tienen otorgado este permiso en su dispositivo.

Habilitando la opción que se encuentra en la parte superior derecha, el sistema oculta de la lista las aplicaciones del sistema, de igual forma si los deshabilita estas se mostraran al igual que el resto.

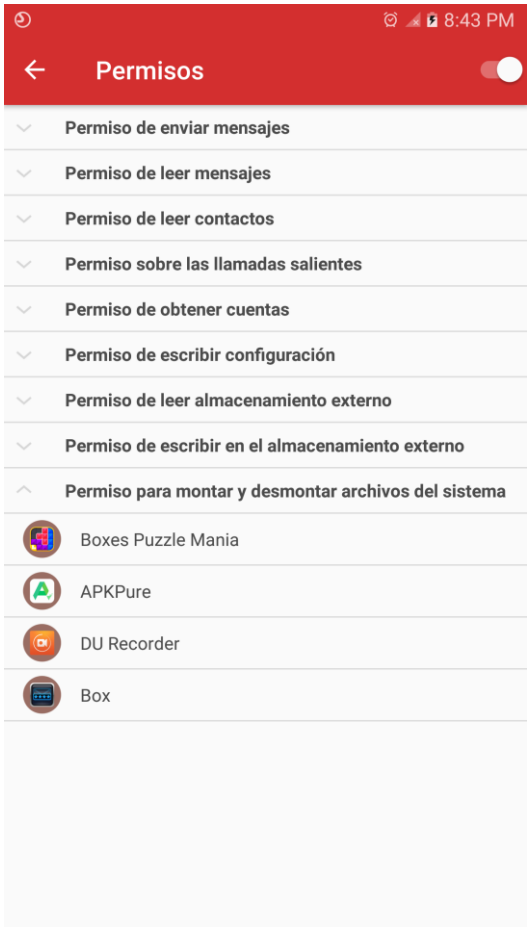

Figura 53. Pantalla Permisos. Sub-listado Permiso para montar y desmontar archivos del sistema.

Por cada una de estas aplicaciones el usuario tiene la opción de iniciar un análisis o ir a la información de la aplicación en el sistema (Figura 54.) solo debe seleccionar la aplicación del listado.

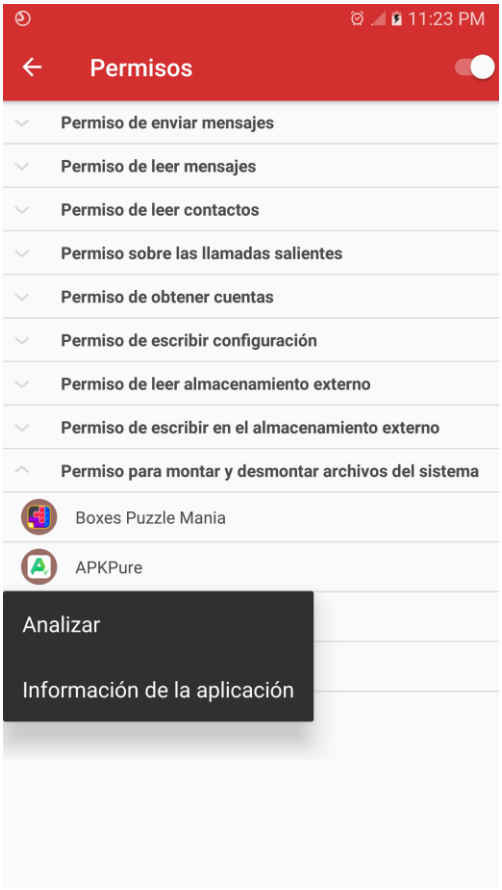

Figura 54. Pantalla Permisos. Iniciar análisis directo.

3.2.3 Análisis

El botón *Análisis* (Figura 55.) le permite al usuario acceder a la pantalla *Analizar* (Figura 56.). En la cual podrá encontrar las diferentes opciones de análisis en demanda que brinda la aplicación.

Figura 55. Menú inferior de navegación. Botón Análisis.

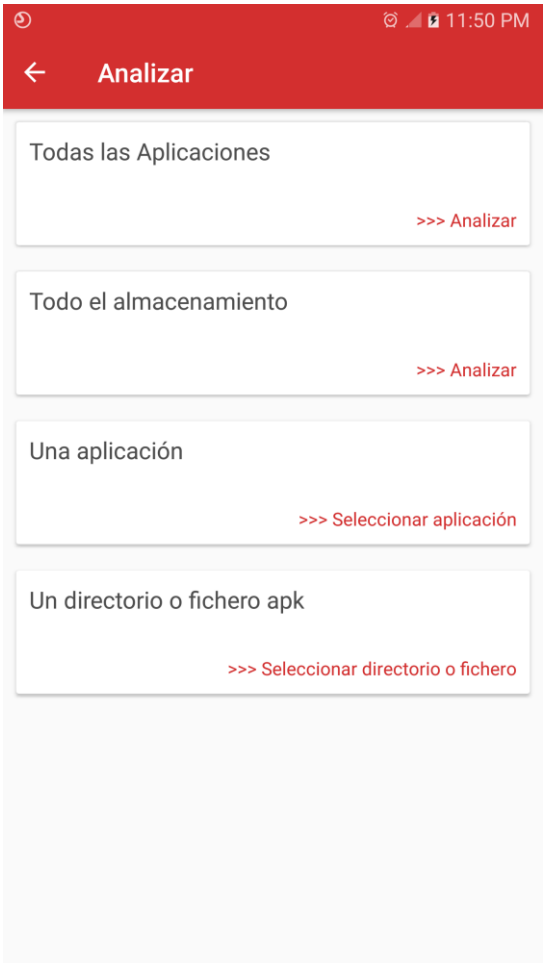

Figura 56. Pantalla Análisis.

Las opciones de análisis que abarca la aplicación son las siguientes:

- Análisis en demanda de todas las aplicaciones instaladas.
  El usuario puede analizar todas las aplicaciones instaladas en el dispositivo seleccionando el botón analizar (Figura 57.) el proceso de análisis puede verse tanto en la propia pantalla como en la barra de notificaciones (Figura 58.)

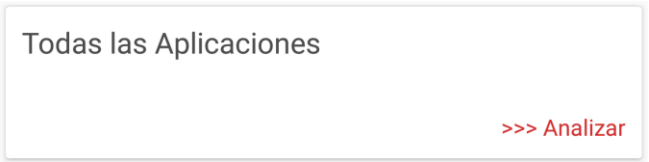

Figura 57. Botón Analizar Aplicaciones.

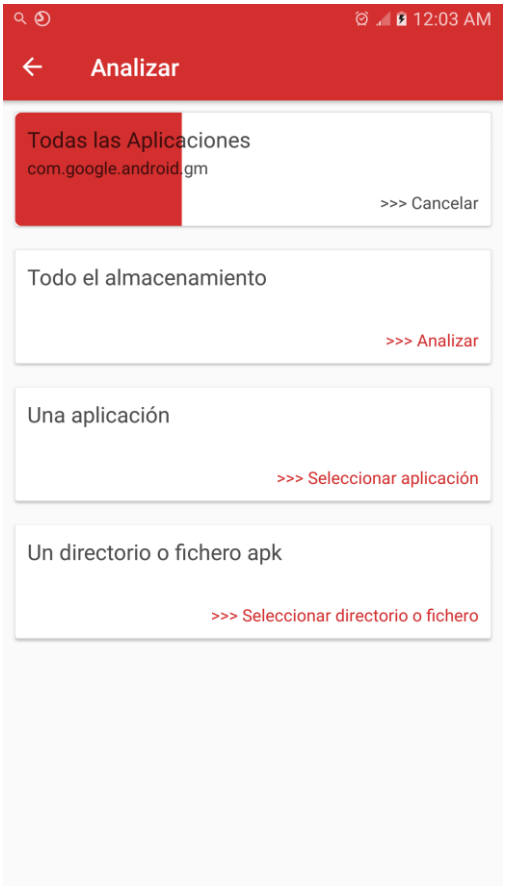

Figura 58. Botón Analizar Todas las Aplicaciones. Análisis en curso.

Una vez finalizado un análisis cuando una amenaza fue detectada el usuario puede seleccionar la notificación que muestra este resultado en la barra de notificaciones o bien seleccionar la opción ver amenazas detectadas (Figura 59.), de esta forma se abrirá la pantalla *Resultados del Análisis* (Figura 13.) que le va a permitir al usuario desinstalar la aplicación o aplicaciones malignas encontradas o si lo desea ignorar la misma y mantenerla en el dispositivo.

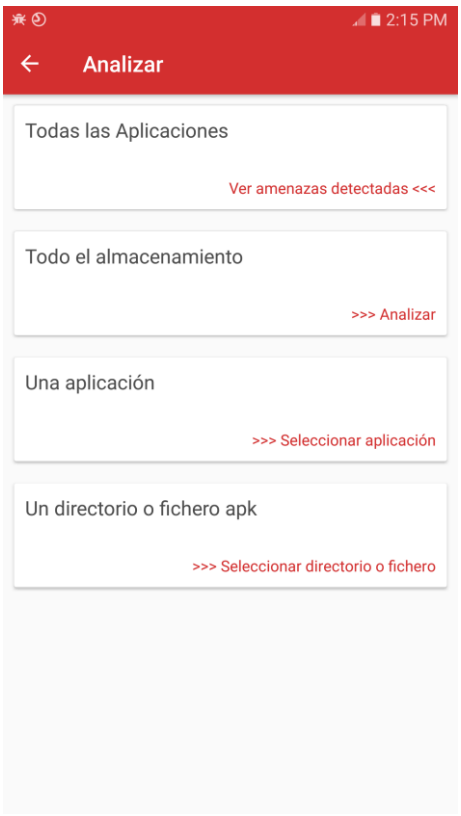

Figura 59. Pantalla Análisis. Análisis terminado. Amenazas detectadas.

- Análisis en demanda de todo el almacenamiento (la memoria interna y la tarjeta micro SD).

  El usuario puede analizar el almacenamiento de su dispositivo seleccionando el botón analizar (Figura 60.) el proceso de análisis puede verse tanto en la propia pantalla como en la barra de notificaciones (Figura 61.)

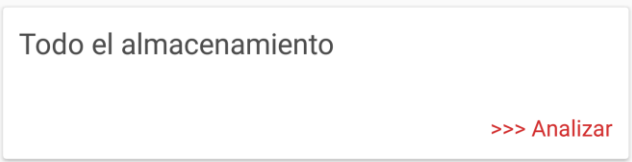

Figura 60. Botón Analizar Almacenamiento.

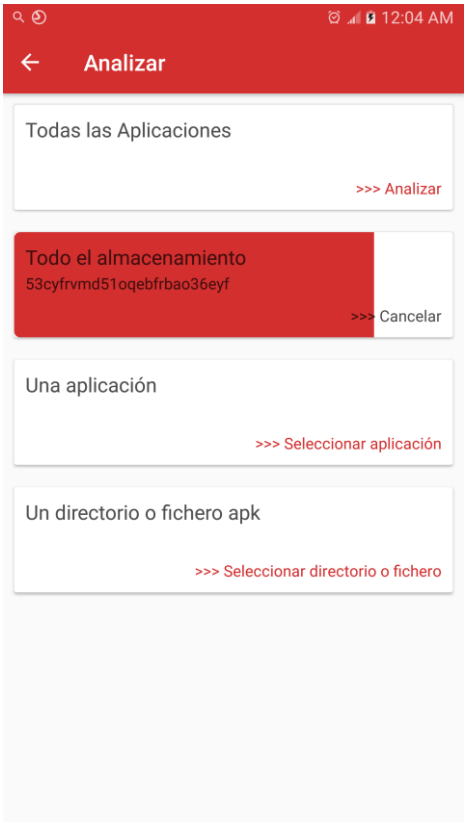

Figura 61. Botón Analizar Todo el almacenamiento. Análisis en curso.

Una vez finalizado un análisis cuando una amenaza fue detectada el usuario al igual que en el caso anterior puede seleccionar la notificación que muestra este resultado en la barra de notificaciones o bien seleccionar la opción ver amenazas detectadas (Figura 62.), de esta forma se abrirá la pantalla *Resultados del Análisis* (Figura 63.) que le va a permitir eliminar el o los ficheros malignos detectados o si lo desea también puede ignorarlos y mantenerlos en el dispositivo.

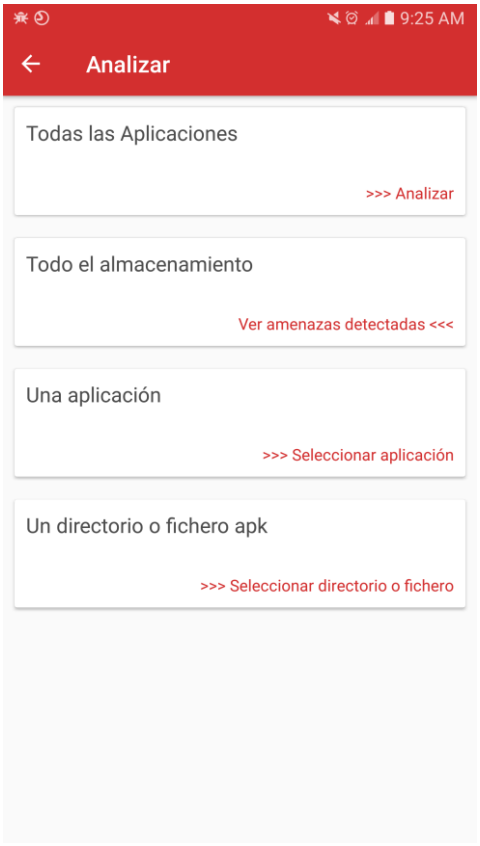

Figura 62. Pantalla Análisis. Análisis terminado. Amenazas detectadas.

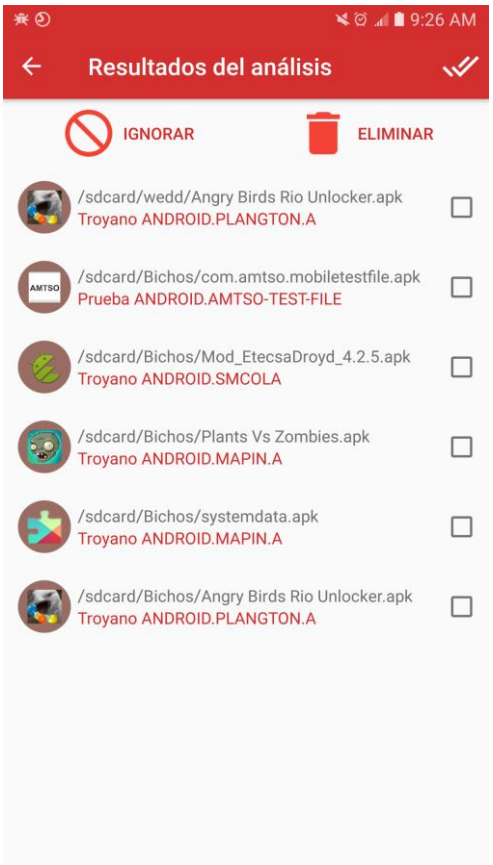

Figura 63. Pantalla Resultado del Análisis. Ficheros Malignos detectados.

- Análisis de una aplicación seleccionada por el usuario de la lista de aplicaciones instaladas.
  En la pantalla Análisis cuando se selecciona el botón analizar una aplicación (Figura 64.) el sistema muestra una nueva pantalla con la lista de todas las aplicaciones instaladas en el dispositivo (Figura 65.) donde podrá seleccionar la aplicación que desee analizar.

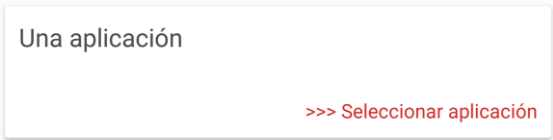

Figura 64. Botón Analizar una Aplicación.

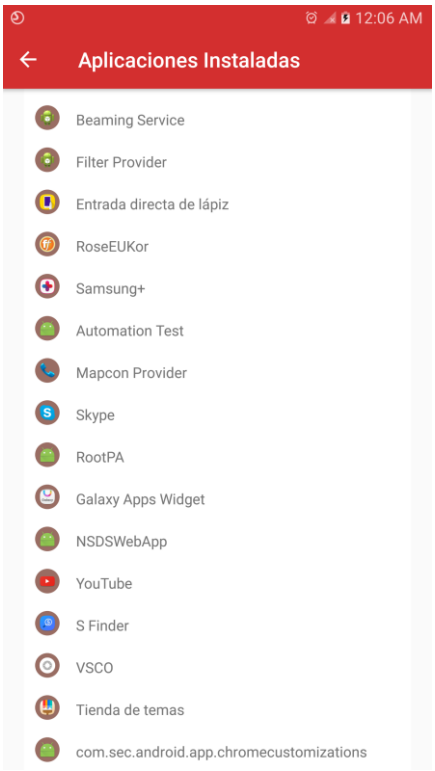

Figura 65. Lista de aplicaciones instaladas en el dispositivo.

- Análisis de un directorio seleccionado por el usuario.
  En la pantalla Análisis cuando el usuario selecciona el botón analizar un directorio (Figura 66.) el sistema muestra un explorador de archivos (Figura 31.) que le permite navegar a través de su dispositivo y seleccionar el directorio deseado.

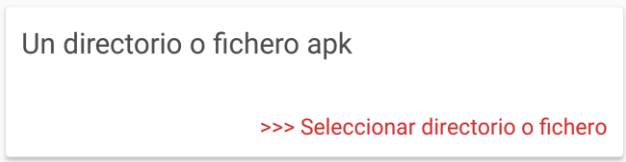

Figura 66. Botón Analizar un Directorio o Fichero.

Amenazas encontradas.

Cuando al terminar un análisis si el sistema ha detectado amenazas el usuario puede visualizar estos resultados seleccionando el botón detalles que se encuentra en cada uno

de los análisis terminados con amenazas detectadas, de esta forma se muestra la pantalla Resultados del análisis que varía en dependencia de la amenaza encontrada, podemos observar un listado de aplicaciones instaladas en nuestro dispositivo dándonos la posibilidad de desinstalarlas o bien un listado de ficheros malignos (.apk) dándonos la posibilidad de eliminarlos. En ambos casos el usuario tendrá la opción de ignorar estos resultados.

3.2.4 Estadísticas

El botón *Estadísticas* (Figura 67.) le permite al usuario acceder a la pantalla *Estadísticas* (Figura 68.). En la cual podrá encontrar las estadísticas de funcionamiento y de códigos malignos.

Figura 67. Menú inferior de navegación. Botón Estadísticas.

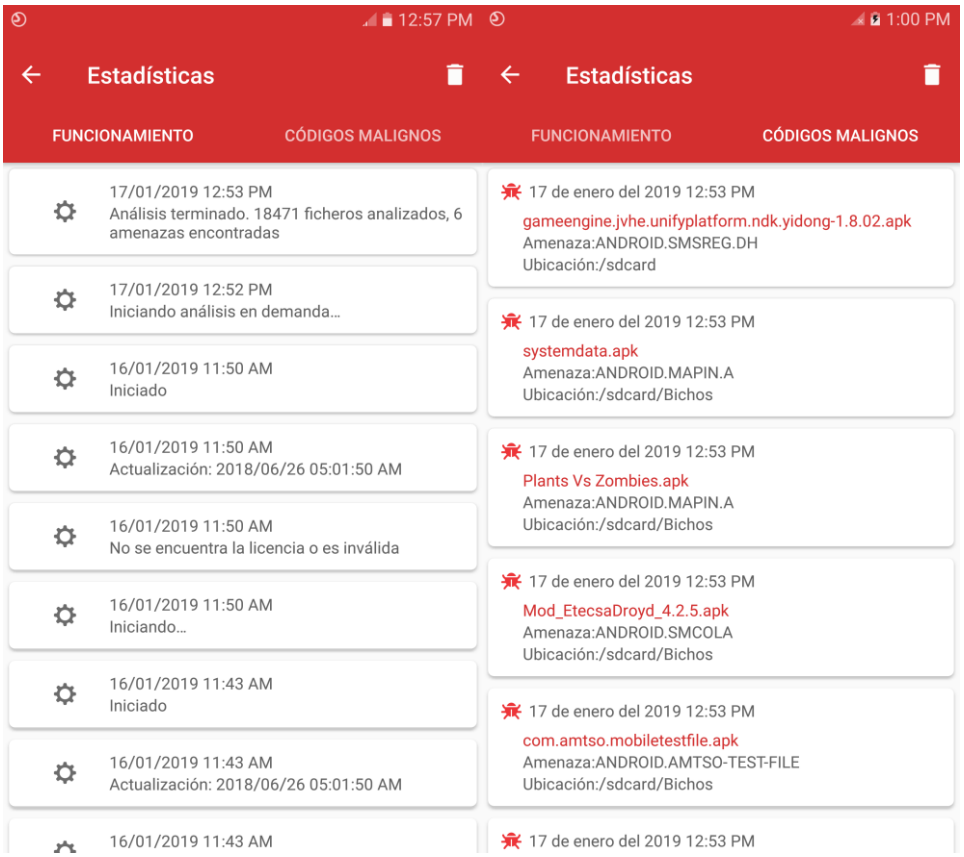

Figura 68. Pantalla Estadísticas. Funcionamiento/Códigos Malignos.

Como se aprecia en la figura anterior las estadísticas de funcionamiento muestran toda la actividad de la aplicación, los análisis realizados, las actualizaciones, etc. Y en el caso de los códigos malignos va a mostrar todos los códigos malignos detectados por la aplicación con su fecha de detección y ubicación dentro del dispositivo.

En caso de que se deseen eliminar las estadísticas debe seleccionar el botón que aparece en la esquina superior derecha y se mostrarán las opciones de eliminación (Figura 69.).

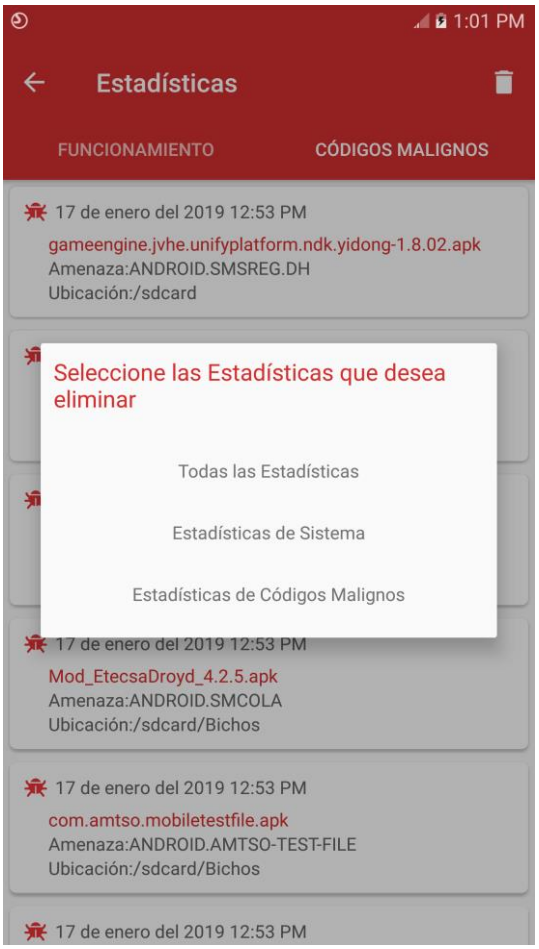

Figura 69. Pantalla Estadísticas. Opciones de eliminación.

4. Contactos

Empresa de Consultoría y Seguridad Informática. Segurmática

Soporte Técnico

Dirección: Zanja No. 651 esquina a Soledad, Centro Habana, Ciudad de La Habana, Cuba.

Teléfonos: +53(7) 878 2665 y 870 3536 al 38.

Telefax: +53(7) 8735965.

Email: soporte@segurmatica.cu.

Para la recepción de errores, inconformidades o sugerencias enviar correo con la plantilla de inconformidades, que puede descargar en el sitio de la entidad, y como asunto: “Aplicación Android”.

Internet: http://www.segurmatica.cu.