**PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR SEDE ESMERALDAS**

**CARRERA:**

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

**INFORME ESTUDIO DE CASO:**

MALWARE EN ANDROID Y MEDIDAS DE PREVENCIÓN

**LÍNEA DE INVESTIGACIÓN:**

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

**PREVIO A LA OBTENCIÓN DEL TITULO DE:**

INGENIERIO DE SISTEMAS Y COMPUTACIÓN

**AUTOR:**

VIVAS PINCAY CARLOS FRANCISCO

**ASESOR:**

MGT. XAVIER QUIÑÓNEZ KU

**ESMERALDAS – MAYO 2023**

Disertación Aprobada luego de haber dado cumplimiento de los requisitos exigidos por el reglamento de Grado de la Pontificia Universidad Católica del Ecuador Sede en Esmeraldas, previa la obtención del Título de Ingeniería de Sistemas y Computación.

## TRIBUNAL DE GRADUACIÓN

**Título**: MALWARE EN ANDROID Y MEDIDAS DE PREVENCIÓN

**Autor:** CARLOS FRANCISCO VIVAS PINCAY

**Mgt. Xavier Quiñónez Ku** **f.- _____**

**ASESOR DE TESIS**

**Mgt. Jaime Sayago Heredia** **f.- _____**

**LECTOR 1**

**Mgt. José Luis Carvajal** **f.- _____**

**LECTOR 2**

**Mgt. Xavier Quiñónez Ku** **f.- _____**

**DIRECTOR DE ESCUELA**

Esmeraldas, Ecuador, 2023

# DECLARACIÓN AUTORÍA

Yo, **VIVAS PINCAY CARLOS FRANCISCO** portador de la cedula de identidad No. **080235854-9** declaro que los resultados obtenidos en la investigación que presento como estudio de caso previo a la obtención del título de **INGENIERÍA EN SISTEMAS Y COMPUTACIÓN** es absolutamente original, autentica y personal.

En virtud que el contenido de esta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCE Sede Esmeraldas.

_____

**CARLOS FRANCISCO VIVAS PINCAY**

**CI: 080235854-9**

# DEDICATORIA

Quiero dedicar este trabajo a las personas que han sido fundamentales en mi vida académica y personal. En primer lugar, a mis padres, Angela Pincay y Gustavo Vivas, cuyo apoyo incondicional ha sido una fuente constante de motivación para mí. También a mi esposa, Diana Espinoza, y mis hijos, Dylan, Joseph y Jaslene, quienes han sido el motor que ha impulsado mi espíritu de superación.

Además, quiero agradecer a todas aquellas personas que, de una u otra forma, han estado presentes en momentos clave para brindarme aliento y motivación en momentos de dificultad. Agradezco también a mis docentes de la universidad, quienes siempre estuvieron dispuestos a brindarme su ayuda y apoyo cuando lo necesitaba. A todos ellos, y muchos más que han contribuido a mi formación académica y personal, les estoy profundamente agradecido.

# AGRADECIMIENTO

Dios, por darme la oportunidad de culminar esta etapa universitaria y bendecirme con el don de la vida y la felicidad. A mis padres quienes estuvieron ahí desde que era tan solo un niño apoyándome en mi vida estudiantil. A mi esposa quien fue un pilar de motivación en mi formación universitaria, a mis hijos quienes me enseñaron a dar lo mejor de mí en momentos difíciles, a mis abuelas que ya no están en esta tierra que de una u otra manera contribuyeron también para la obtención de este título universitario. A todos ustedes gracias de corazón.

# INDICE GENERAL

# INDICE DE FIGURAS

# RESUMEN

Se realiza un estudio acerca de los malware en la plataforma Android, dicho tema ha llevado a los desarrolladores de software de la empresa Google a reflexionar sobre sus vulnerabilidades enfocado a la seguridad. La plataforma Android ha sido el objetivo para muchos desarrolladores de software malicioso, conocidos como cibercriminales quienes buscan elaborar y obtener beneficios económicos por medio de fraudes, extorciones, suplantación de identidad, robos a cuentas bancarias, comercio de datos, espionajes empresariales, con el único fin de hurtar la información y en muchos casos generar el mal funcionamiento de los dispositivos móviles. Se plantea un estudio de caso cualitativo y cuantitativo basados en métodos utilizados en investigación anteriores para la obtención de datos acerca de la detección de malware en un entorno virtual controlado. Posteriormente se realiza un test sobre las herramientas de prevención que existen en el medio, bajo una previa distinción, dicha prueba ayuda a identificar la eficacia o no en la detección, mitigar el malware en el dispositivo móvil, y el impacto sobre el rendimiento del mismo. Se realiza una selección de malware a evaluar en el entorno virtual controlado con el fin mitigar el riesgo en un dispositivo real. Se realizan pruebas correspondientes para identificar los malware detectados y como afectan al rendimiento tanto de CPU, RAM y batería del dispositivo, asimismo se presentan recomendaciones de buenas prácticas de seguridad a la hora de instalar apps y como mantener un correcto funcionamiento equilibrado del dispositivo móvil.

**Palabras claves:** Android, app, evaluación, malware, prevención

# ABSTRACT

A study about malware on the Android platform has led Google software developers to reflect on their vulnerabilities focused on security. The Android platform has been the target for many malware developers, known as cybercriminals who seek to develop and obtain economic benefits through fraud, extortion, identity theft, theft of bank accounts, data trading, corporate espionage, with the sole purpose of stealing information and in many cases generate reportmal function of mobile devices. A qualitative and quantitative case study is proposed based on methods used in previous research to obtain data about malware detection in a controlled virtual environment. Subsequently, a test is performed on the prevention tools that exist in the environment, under a previous distinction, this test helps to identify the effectiveness or not in the detection, mitigate the malware on the mobile device, and the impact on the performance of the same. A selection of malware to be evaluated in the controlled virtual environment is made in order to mitigate the risk in a real device. Corresponding tests are performed to identify the malware detected and how they affect the performance of both CPU, RAM and battery of the device, also recommendations of good security practices are presented when installing apps and how to maintain a proper balanced operation of the mobile device.



**Keywords:** Android, malware, test, prevention, app.

# INTRODUCCIÓN

Actualmente en todo el mundo se puede presenciar un ambiente de evolución tecnológica lo cual ha generado una revolución sin precedente, como consecuencia de la gran demanda de personas por adquirir equipos tecnológicos como dispositivos móviles, dejando a su paso una ardua tarea para los desarrolladores de software y hardware que día a día se ven en la necesidad de crear sistemas y dispositivos más robustos en cuanto a funcionalidad y seguridad se refiere.

Desde entonces las compañías tecnológicas han elaborado variedad de dispositivos inteligentes smartphone, lanzando al mercado una gran gama de teléfonos inteligentes para todos los gustos y nivel social. Sin embargo, estos dispositivos inteligentes no sirven de nada sin un sistema operativo y es cuando nace la plataforma Android, el cual dio su primer salto al mercado tecnológico en el 2003 de la mano de su fundador Andy Rubin quien luego vendió su compañía a una empresa dedicada al desarrollo de productos y servicios en internet, como lo es Google en el año 2005.

Gracias a la aceptación en el mercado tecnológico y la cantidad de información que se obtiene de los usuarios, la plataforma Android ha sido el objetivo de muchos desarrolladores de software malicioso, conocidos como cibercriminales quienes buscan elaborar y obtener beneficios económicos por medio de fraudes, extorciones, suplantación de identidad, robos a cuentas bancarias, comercio de datos, espionajes empresariales, con el único fin de hurtar la información y en muchos casos generar el mal funcionamiento en el rendimiento de los dispositivos móviles.

Para ello los desarrolladores de aplicaciones móviles como Google, Apple y Windows se han visto en la necesidad de crear medidas de prevención contra los malware, también conocidos como softwares maliciosos. Cabe indicar que los malware también pueden incidir en el rendimiento del dispositivo provocando un excesivo consumo de recursos físicos en los dispositivos móviles. El presente estudio de caso se enfoca en el sistema operativo Android 12, dado que, en la actualidad es una versión establecida e instalada en gran parte de dispositivos, además se describe la situación actual de los malware involucrados para dicha plataforma móvil. Para la detección del malware se utilizó un entorno virtual controlado para simular el ambiente de convivencia, para luego testear por medio de herramientas de prevención utilizadas en el medio de seguridad antimalware, previo a una rigurosa selección, todo esto se emplea para limitar al malware en un entorno

donde no pueda dañar el sistema operativo real de un dispositivo móvil donde la máquina virtual se ejecutará desde un estado conocido y libre.

Los resultados de las pruebas realizadas en el entorno virtual controlado sirven como referencia para proponer recomendaciones tecnológicas sobre prácticas de prevención contra los malware, la cual permitirá al usuario tomar las medidas de seguridad necesarias a la hora de adquirir una app para su dispositivo móvil, además se muestran las mejores herramientas de prevención para poder detectar y eliminar los malware en los smartphones.

# 1. OBJETIVOS

Evaluar las herramientas de prevención contra el malware para Android 12 existentes en el mercado mediante pruebas en un entorno virtual controlado para mostrar cómo afectan estas a los recursos físicos del dispositivo móvil.

## 1.1. Objetivos Específicos

**1.1.1.** Identificar las vulnerabilidades y mejoras en seguridad de la plataforma Android.

**1.1.2.** Seleccionar herramienta de prevención contra el malware existente en el mercado de seguridad móvil.

**1.1.3.** Elegir las muestras de malware a utilizar donde se infectará el sistema operativo Android.

**1.1.4.** Crear entorno virtual controlado con Android 12 para simular el comportamiento del malware en su entorno real.

**1.1.5.** Elaborar recomendaciones que ayuden a prevenir el ataque de malware en Android 12 de los dispositivos móviles.

# 2. INFORME DEL CASO

## 2.1. ANTECEDENTES

La investigación del presente estudio se llevó a cabo mediante una exploración de artículos científicos relacionados directamente con el objeto de estudio "Malware en Android y medidas prevención" que sirven como base de apoyo a nivel de conocimiento para realizar el análisis de las variables a estudiar, las cuales son: herramientas de efectividad y funcionalidad para dispositivos con sistemas operativo Android 12.

La información de la presente investigación fue recopilada de fuentes bibliográficas digitales, tales como ACM (Asociation for Computing Machinery), IEEE Xplore (Institute of Electrical and Electronics Engineers) y Scopus (base de datos sobre ciencia y tecnología), que fue de gran ayuda para recuperar información relacionada con el tema de estudio el cual titula "Malware en Android y medidas de prevención". Es así como se han recuperado cinco estudios que abarcan relación directa con los distintos métodos para la detección de malware en la plataforma Android. Estos estudios han sido publicados entre el periodo 2012-2022 y serán detallados a continuación.

La primera investigación denominada "Detección de vulnerabilidades en aplicaciones recientes de Androide: Un estudio empírico", que se realizó en Bangladés, consistió en la selección de varias herramientas para detectar las vulnerabilidades más comunes en algunas aplicaciones Android que son de uso gratuito, cabe recalcar que el estudio se realizó en dos partes, primero el análisis de algunas aplicaciones muy poco usadas en Latino América. Luego la observación estuvo dirigida a seis aplicaciones muy conocidas en Google Play Store entre las que se encuentran: Gmail, YouTube, Cam Scanner, Sound Cloud, Clean Master. La investigación en mención tiene mucha relación con este estudio, porque busca indagar si algunas herramientas son lo verdaderamente seguras o ponen en riesgo a los dispositivos móviles. En los resultados se encontró un índice alto de vulnerabilidad en algunas de las aplicaciones más usadas actualmente, lo que pone en riesgo la seguridad de muchos internautas [1].

La segunda investigación titula "Malware en Android y medidas de prevención", la cual tuvo como objetivo principal evaluar un conjunto de herramientas de prevención existentes en el mercado y determinar si son eficaces en la detección del malware, además se comprueba cómo afecta al rendimiento del dispositivo en cuanto a consumo de CPU, memoria y durabilidad de la batería. Para alcanzar el objetivo propuesto en la

investigación de realizó una exhaustiva búsqueda de información donde se identificó las herramientas de prevención existentes en el mercado para luego seleccionar de un sitio web quien otorga certificados de efectividad en lo referente a la detección del malware a las empresas que desarrollan app de seguridad, además un repositorio donde se almacenan muestras de malware con el fin investigativo para luego ser testeadas en un entorno de hardware / software virtualizado que reproduce la arquitectura y el comportamiento de la plataforma real de Android, donde se evidenció el comportamiento del malware frente a las herramientas de prevención. Además, desarrolla una serie de recomendaciones sobre buenas prácticas y medidas de prevención en ataques cibernéticos para usuarios con poco conocimiento. Esta investigación se relaciona con el tema de estudio ya que proporciona información sobre el método para la detección de malware en la plataforma Android, además evidencia el impacto que tienen las herramientas de prevención en los recurso lógicos y físicos del dispositivo móvil [2].

El tercer estudio titulado "*Seguridad en Android, análisis de vulnerabilidades y malware",* cuyo objetivo principal es el análisis de malware en dispositivos con sistema Android mediante el uso de diferentes pruebas y test. Esta investigación se centra en el análisis de un teléfono celular que ha sido infectado con malware para conocer su comportamiento, además, que proporciona una serie de consejos dirigidos a los usuarios a fin de evitar muchos problemas de vulnerabilidad. El estudio mencionado tiene muchos aportes que sirven de referencia para esta investigación, porque tiene una metodología muy parecida y busca proporcionar recomendaciones que eduquen a los usuarios de Android [3].

La cuarta investigación lleva por título "*Técnicas de Análisis de Malware en dispositivos móviles basados en Android".* Es una investigación que tiene como objetivo identificar el comportamiento e interacción del malware con el sistema operativo para móviles Android con el fin de generar un marco metodológico que sirva como referencia ante las nuevas y constantes mutaciones del malware, además emplea una metodología análisis teórico-práctico de aplicaciones disponibles en Google Play infectadas con malware para luego ser testeadas en un entorno virtual controlado permitiendo identificar el comportamiento real de los malware en Android [4].

El último trabajo investigativo se titula *"Análisis de las vulnerabilidades en dispositivos móviles con sistema operativo Android"* y fue realizada a nivel local, tiene como objetivo analizar las vulnerabilidades de los dispositivos móviles con sistema operativo Android y sugerir las mejores prácticas para salvaguardar la seguridad de este. En esta

investigación se utiliza un método deductivo, el cual provee estrategias de razonamiento de lo general a lo más específico, con el fin de investigar sobre lo macro en referencia a las vulnerabilidades para llegar a lo especifico que ayude al desarrollo de su investigación. La presente investigación evidencia las vulnerabilidades a las que están expuestas los dispositivos Android, mediante la búsqueda de información en la nube, seguido de la elaboración de un entorno virtual controlado donde se realiza ataques por medio del sistema Kali Linux a un dispositivo con sistemas operativo Android, con el objetivo de utilizar las vulnerabilidades para poder así exponer a usuarios de la plataforma Android. La relación que tiene con el estudio de caso es porque se utiliza un entorno virtual controlado donde se tomó la idea de observar el comportamiento del malware en su entorno real mediante la implementación de la máquina virtual y de esta manera no exponer al dispositivo móvil logrando realizar pruebas sin exponer el dispositivo móvil, puesto que se simula el comportamiento en su entorno real [5].

## 2.2. Presentación del Caso

### 2.2.1. Android

Se define a la plataforma Android, como un conjunto de herramientas de software para teléfonos móviles, creado por Google y la Open Handset Alliance. Está incorporado en millones de teléfonos celulares y otros dispositivos tecnológicos, como lo es el internet de las cosas, lo que hace de Android un sistema operativo importante para desarrolladores de aplicaciones [6].

El lanzamiento de Android como nueva plataforma para el desarrollo de aplicaciones móviles ha causado gran expectación y ha tenido una importante aceptación por parte de los usuarios y también de la industria. En la actualidad se ha convertido en la alternativa dominante frente a otras plataformas como iPhone o Windows Phone [7].

La plataforma Android se ha convertido en un sistema operativo para dispositivos móviles con más de un billón de usuarios activos a nivel mundial a diferencias de años anteriores donde apenas era conocido. La empresa de servicios de análisis web STATISTA analizó los sistemas operativos para smartphone con más aceptación a nivel mundial desde diciembre del 2012 a diciembre 2022, informando que Android se posiciona como el sistema operativo con más acogida a nivel mundial con un 70% por encima de su mayor competidor IOS con el 25% aceptación [8].

Además, la empresa stancounter quien también realiza análisis de tendencias en el mercado de sistemas operativos entre mayo del 2021 y mayo del 2022 informa que la tendencia de Android en el mercado es de 71,45% superior a iOS quienes se mantienen en un 27.83%, Samsung 0,41% y KaiOS 0.12%, mostrando que Android desde su aparición en el 2008 es el sistema operativo para dispositivos móviles más utilizado en el mundo, como se muestra en el Anexo 1 [9].

En el Ecuador existe un porcentaje alto en relación a la tendencia de sistemas operativos en el mercado mundial tecnológico con un 85.87% por encima de sus competidores directo como IOS con 13.69% y Samsung con un 0,37% de aceptación en el mercado nacional ecuatoriano [10]. En el Anexo 2 se puede observar el resultado de los datos obtenidos por el sitio análisis web.

Los resultados mencionados demuestran que en el medio existe una gran aceptación hacia la plataforma Android, por esa razón nace la idea de realizar un estudio de caso que ayude a los usuarios con dispositivos móviles a prevenir ataques por software malicioso, pues un estudio realizado por el sitio web "Security Report Latinoamérica" sobre vulnerabilidades en Android muestra que este sistema desde su aparición en 2009 ha sufrido más de 17400 incidencias. La mayor preocupación en materia de seguridad son los códigos maliciosos (64%), seguido del robo de información (60%) y accesos indebidos a los sistemas (56%) ratificando las amenazas a las cual están expuestos los usuarios finales [11].

### 2.2.2. Historia

Google adquiere Android Inc. en el año 2005. Se trataba de una pequeña compañía, recién creada, orientada a la producción de aplicaciones para terminales móviles. Ese mismo año empiezan a trabajar en la creación de una máquina virtual Java optimizada para móviles. En el año 2007 se crea el consorcio Open Handeser Allieance con el fin de establecer una serie de estándares abiertos para dispositivos móviles [7]. El consorcio cuenta con decenas de miembros que se pueden clasificar en varios tipos de empresas:

- Operadores de telefonía móvil.
- Fabricantes de dispositivos.
- Fabricantes de procesadores y microelectrónica.
- Compañías de software.

Después de esta colaboración y arduo trabajo en equipo en septiembre del 2008 se lanza Android, fecha que se conoce hasta hoy como el día oficial de su lanzamiento [12]. En el año 2010, Android se consolida como uno de los sistemas operativos más utilizados, en el 2011 se lanza la versión 3x. Para el 2012, Google cambia su estrategia en su tienda virtual reemplazando a Android Market por Google Play Store. En el 2014 se lanza la versión 5.0, mientras que en el 2016 la versión 6.0. La 8.0 aparece a finales del 2017 y la versión 9.0 llega al mercado en agosto del 2018 [7].

Este sistema operativo está basado en Linux una plataforma de código abierto, lo que permite a fabricantes, operadores y desarrolladores dar mayor funcionalidad a sus dispositivos móviles. Además Android es multiplataforma, lo cual permite que el sistema operativo pueda ser usado en distintos ambientes de desarrollo, y a su vez se pueda combinarse con el hardware y software usada para ejecutar aplicaciones [13].

### 2.2.3. Versiones de Android

Las versiones de Android reciben en inglés el nombre de postres a diferencia de la aparición desde las versiones 10, 11, 12 y en la actualidad 13, cada versión empieza por una letra distinta, conforme al orden alfabético, como se muestra en el Anexo 3 [14].

### 2.2.4. Arquitectura de Android

La arquitectura de Android es un sistema estratificado que conforma en sí una jerarquía, sus componentes son divididos en estratos, en donde los niveles más bajos agrupan componentes relacionados con la interacción del hardware del dispositivo, los estratos superiores corresponden a procesos de más alto nivel. En concreto los componentes de cada estracto brindan servicios a estractos inferiores y a la vez ofrecen servicios de capas superiores [15]. El Anexo 4 evidencia como está estructurada la arquitectura de Android.

### 2.2.5. Modelo de seguridad de Android

El modelo de seguridad de la plataforma de Android está distribuido a lo largo de toda la arquitectura. A continuación, se describen los aspectos más importantes:

**Application Sandbox**

Es una manera segura de obtener privacidad en Android, específicamente estas soluciones limitarán el intercambio de datos de usuario con terceros y operarán sin identificadores entre aplicaciones, incluido el ID de publicidad. Este tipo de aplicación brinda un camino claro para mejorar la privacidad del usuario sin poner en riesgo el acceso a contenido y servicios gratuitos [16].

**Permisos**

Android utiliza un proceso de aislamiento para las aplicaciones instaladas, conocido como Application SandBox. En Android se puede identificar dos clases de permisos, los definidos por la misma aplicación con el propósito de auto protección y los predefinidos por Android, los cuales controlan el acceso a recursos del sistema [17].

### 2.2.6. Versión de Android a utilizar

Se realizó una investigación para definir en qué versión de Android centrar el estudio de caso, mediante los resultados obtenidos se evidenció que la versión actual Android 13 podría traer inconvenientes a la hora de recolectar información. Según los resultados del equipo de análisis statcounter el sistema operativo con mayor aceptación es Android 11 con 33.04%, Android 10 con 22.56%, Android 12 con 14.67% y Android Pie con 11.33%, mostrando que la versión 11 de Android es la que encabeza la lista como se muestra en el Anexo 5 [15].

La empresa de seguridad Bitdefender, en uno de sus artículos menciona que el 35% de los teléfonos Android se volverán más vulnerables a los virus y hackers con 3 años de actualizaciones de seguridad para la mayoría de los dispositivos Android [18].

Los investigadores recuerdan que alrededor del 70% de los teléfonos inteligentes en el planeta funcionan con Android.

Entre todos estos usuarios de Android:

- El 36.47% viajaría en la versión Android 12
- El 29.15% se ejecutaría en Android 11
- Un 15.03% se ejecutaría en Android 10

A partir de septiembre de 2022, casi un tercio de los teléfonos inteligentes Android utilizarán un sistema operativo obsoleto y no compatible. Los dispositivos Android ocupan alrededor del 70% del mercado, pero muchos de estos dispositivos representan un riesgo de seguridad porque Google ya no los admite. Uno de los problemas con Android es la fragmentación del sistema operativo. Google ha lanzado muchas versiones de Android en los últimos 14 años. Solo las últimas tres versiones continúan recibiendo soporte, pero esto es bastante habitual. Es costumbre que las empresas abandonen el soporte después de un tiempo para productos específicos Android [18].

La versión 12 de Android es una versión que ya está establecida y aún está vigente y operativa por los usuarios, considerando que Android ofrece parches de seguridad a dispositivos que contengan las últimas tres versiones, Android 12 salió el 18 de febrero del 2021, además goza del 36.47% de aceptación en el mercado mundial. Así se constata en el Anexo 6.

### 2.2.7. Vulnerabilidades de Android 12

Android 12 es sin duda una de las versiones más estable en lo que va del año, ya que Android lanzó su actual versión 13 que en muchos de los dispositivos móviles no ha sido aun actualizados a la nueva versión por el tema adaptabilidad y usabilidad.

En esta sección se mencionan las vulnerabilidades de la versión 12 de Android que han tenido más impacto en lo que va desde su aparición, estos resultados son obtenidos gracias al sitio web CVE details la cual es una base de datos público que registra, identifica y clasifica cada vulnerabilidad, en la actualidad tiene más de 178.600 vulnerabilidades comunes de diferentes tipos. En el Anexo 7, se muestra el resumen global de las vulnerabilidades registradas por el sitio web mencionado [19].

**Vulnerabilidades frecuentes**

En el Anexo 8, se aprecia las vulnerabilidades más frecuentes en la línea del tiempo en lo que comprende 2009 y lo que va del año 2022; donde se muestra que en el 2020 fue el año con más incidencia en la plataforma Android con 859, seguido del 2017 con 840 incidencias, 609 incidencias en el 2018, 572 incidencias en el 2021, 500 incidencias en 2016 y 209 incidencias en lo que va del 2022 lo cual indica que existe una caída en las

vulnerabilidades para la plataforma Android, lo cual es favorable para el sistemas operativos [20].

**Vulnerabilidades según su tipo**

A lo largo de las primeras versiones de Android, se observan siete vulnerabilidades más explotadas por los ciberdelincuentes: Overflow (desbordamiento) con 672 incidencias, Execute Code (ejecución de código) con 714 incidencias, Gain Privilege (ganar privilegio) 311 incidencias, Grain information (ganar información) 428 incidencias, Bypass Something 388 incidencias y Denia of service 404 incidencias, Google Android, tal como se muestra en el Anexo 9.

Android 12 sin duda ha sido un sistema operativo que desde su aparición en el 2021 no ha tenido tantas incidencias de vulnerabilidades como las otras versiones, según el sitio web CVE details en el 2021 tuvo un total de 84 incidencias de vulnerabilidades y en lo que va del 2022 solo 187 lo que demuestra que a medida que va pasando el tiempo de operatividad del sistema operativo su seguridad va decayendo. Las incidencias con respecto a las vulnerabilidades que más impacto tienen en Android 12 son: la ejecución de código 34 incidencias, el omitir algo con 30 incidencias y problemas con el DoS con 20 incidencias según Google Android. La explicación detallada a todo lo mencionado se puede observar en el Anexo 10.

### 2.2.8. Detalle de las vulnerabilidades más frecuentes en Android

**Overflow (Desbordamiento)**

La vulnerabilidad de desbordamiento es ocasionada por un desperfecto o error en el sistema operativo, del cual los cibercriminales explotan para sobrescribir códigos y datos ejecutables en el dispositivo. *"La vulnerabilidad normalmente se encuentra en los buffers de stack/heap, que están destinados a limitar la cantidad de datos escritos en la memoria del dispositivo".* Cuando es atacado por los cibercriminales el buffer no alcanza a abarcar la cantidad de códigos generados, lo que desafortunadamente puede dejar vulnerable a otro código para ser manipulado, como resultado de este tipo de ataques el dispositivo puede presentar un comportamiento no esperado, generar perdida de datos, etc., es

importante destacar que los ataques de Overflow van acompañados de otros ataques como Denial of Service, Memory Corruption y/o Execute Code [5].

**Execute Code (Ejecución de código)**

Esta vulnerabilidad es generada por un error en el sistema operativo, el cual causa que el atacante ejecute código arbitrario en el dispositivo. Los "exploit de ejecución de código" son programas diseñados para explotar una vulnerabilidad y que esta concluya con una ejecución de código. Execute Code, le permite al hacker ejecutar de forma remota un comando específico en otro dispositivo destino, como, por ejemplo, descargar una parte de malware o enviar peticiones arbitrarias y ocasionar un ataque de servicio denegado. Execute Code es una de las vulnerabilidades más registradas en la plataforma CVE Details [5].

**Gain Privilege (Ganar privilegio)**

Gain Privileges es una vulnerabilidad que aprovecha una falla del sistema operativo para obtener un nivel de permiso elevado en el dispositivo. El ataque se puede realizar de distintas formas ya sea mediante una aplicación maliciosa, programas o por medio de una página web. "Los ataques de esta naturaleza generalmente resultan en la exfiltración de información de identificación personal del dispositivo a un pirata informático externo". Muchos de los ataques realizados de este tipo en los dispositivos móviles son el resultado de alguna vulnerabilidad que se está explotando, posteriormente, los datos y permisos del terminal se vuelven sensibles [5].

**Denegación de servicios (DoS)**

Una vulnerabilidad de denegación de servicio (DoS) se presenta dentro de un sistema operativo Apple o Android. Estos ataques se centran en hacer que un recurso no esté disponible para el propósito para el que fue diseñado [21].
Los dispositivos móviles también se pueden utilizar como 'bots' para perpetrar ataques DoS distribuidos (DDoS). Esto significa que muchos dispositivos infectados con el mismo malware se pueden usar juntos para generar un ataque DDoS en una entidad separada. Android estaba plagado de, un gran número de vulnerabilidades internas,

errores de alta gravedad que, junto con hacer que el dispositivo fuera susceptible a un ataque DoS, permitió a los atacantes remotos ejecutar código arbitrario y causar corrupción de memoria en año 2015 [21].

### 2.2.9. Mejoras de seguridad en Android 12

Se implementaron mejoras en la privacidad, seguridad y estabilidad de la cámara, nuevas APIs para desarrolladores, del mismo modo se aplicó el rediseño prácticamente de casi toda la totalidad de la interfaz de usuario del sistema, con un nuevo lenguaje visual, Material You, el cual otorga un control al usuario en cuanto la apariencia de la interfaz [22].

### 2.2.10. Análisis del modelo de seguridad de Android

**Programa de seguridad**

El equipo de Android contempló en su ciclo de desarrollo un programa de seguridad para abordar los puntos débiles de los sistemas operativos móviles. Las principales actividades de seguridad ejecutadas en el programa son:

**Revisión del diseño:** La seguridad en Android fue abordada desde una etapa temprana del ciclo de desarrollo con la creación y diseño de un modelo de seguridad robusto y configurable. Cada una de las características principales de la plataforma fue revisada para integrar los controles apropiados en la arquitectura del sistema.

**Pruebas de penetración y revisión del código:** Durante el desarrollo de la plataforma los componentes de Android y aquellos de licencia libre que utiliza pasaron por revisiones detalladas de seguridad. Estas revisiones fueron realizadas por el equipo de seguridad de Android, el equipo de seguridad de la información de Google y consultores de seguridad independientes. El objetivo fue identificar las posibles debilidades y vulnerabilidades mucho antes que la plataforma fuera utilizada y simular los tipos de análisis que llevarán a cabo expertos de seguridad externos después del lanzamiento de la misma [23].

**Revisión de la comunidad:** Dado que Android es un proyecto de código abierto, permite una amplia revisión de seguridad de cualquier parte interesada, lo que contribuye a la mejora de la plataforma.

**Respuesta a incidentes:** Con el fin de atender los problemas de seguridad en producción, Android creó un proceso integral que contempla dos aspectos, para dar respuestas de seguridad. Primero, hay una vigilancia constante por parte del equipo de seguridad de Android de los componentes del sistema y de la comunidad para identificar posibles vulnerabilidades. Segundo, una vez se descubren problemas, el equipo de seguridad tiene un proceso de respuesta que permite una rápida atención de las vulnerabilidades para que el riesgo potencial de los usuarios Android sea reducido al mínimo. Estas respuestas pueden incluir actualizaciones de la plataforma y la eliminación de aplicaciones de Google Play y de los dispositivos [23].

### 2.2.11. Malware

Malware proviene de un grupo de palabras malicious software, el cual es dañino para el equipo, se diseñó con el objetivo de insertar virus, gusanos, troyanos o spyware, regularmente son usados para recopilar información privada del usuario o del ordenador. En la actualidad se toma el nombre de malware, para definir en un amplio sentido de peligro, pero en el pasado la forma más común de nombrarlas era como virus informáticos [24].

### 2.2.12. Casos de Malware en Android

La última edición del Informe de Amenazas de ESET hace un recuento de los diversos ciberataques relacionados con la guerra en curso en Ucrania que los investigadores de ESET analizaron y ayudaron a mitigar. Esto incluye la resurrección del malware Industroyer, que intentaba atacar subestaciones eléctricas de alto voltaje.

La telemetría de ESET también ha visto muchas otras amenazas no relacionadas con la guerra entre Rusia y Ucrania. «*Podemos confirmar que Emotet el malware que se propaga principalmente a través del correo electrónico de spam está de vuelta después de los intentos de retirada del año 2021, y se ha disparado de nuevo en nuestra telemetría*», También revisa los hallazgos más importantes de la investigación

descubriendo: el abuso de las vulnerabilidades de los controladores del kernel; las vulnerabilidades UEFI de alto impacto; el malware de criptomoneda dirigido a dispositivos Android e iOS; una campaña aún no atribuida que despliega el malware DazzleSpy macOS; y las campañas de Mustang Panda, Donot Team, Winnti Group y el grupo TA410 APT [25].

Según informe elaborado por FortiGuard Labs, el laboratorio de inteligencia de amenazas de Fortinet, México fue el país que más intentos de ataques recibió (156 mil millones), seguido de Brasil (88,5 mil millones), Perú (11,5 mil millones) y Colombia (11,2 mil millones) en lo que respecta al continente americano [26].

El equipo de ciberseguridad de McAfee ha detectado la presencia de nuevo malware en Play Store. Curiosamente, son aplicaciones que se hacen pasar por escáneres de seguridad en Android, aunque son troyanos capaces de capturar las credenciales de bloqueo de pantalla para monitorizar la actividad del dispositivo e incluso robar claves bancarias. El malware se denomina BRATA y lleva en Android desde 2018 [27].

### 2.2.13. Clasificación del malware

**Virus**

Se trata de programas informáticos capaces de multiplicarse infectando los archivos. Llegan al computador de distintas formas especialmente en los correos electrónicos, tienen la capacidad de ocultarse hasta que se activa, sus daños van desde simples como pequeñas molestias hasta incapacitar completamente un ordenador [28].

**Gusanos**

Son programas que se auto-replican en todo el sistema y su comportamiento a diferencia de los virus, su labor no es infectar archivos existentes, si no que se instalan en la memoria RAM del dispositivo, donde utilizan la red para propagarse e infectar otros sistemas. Es capaz de consumir recursos de redes hasta saturarlos, regularmente se propagan mediante la libreta de direcciones [28].

**Troyanos**

Es una clase de virus que se oculta en programas que aparentemente se ven inofensivos para un usuario, donde esperan para ser ejecutados y lograr su objetivo de hurtar información o generar el mal funcionamiento del dispositivo móvil. Esta clase de virus puede clasificarse por el daño que ocasionan en los dispositivos móviles, como se mencionan a continuación.

- **Downloader:** descarga y ejecuta otros códigos maliciosos.
- **Banker:** posee como objetivo el robo de credencial de acceso financieras.
- **Dropper:** se ejecuta en paralelo con un programa legítimo.
- **Clicker:** busca beneficios económicos a través de clics en publicidad.
- **Keylogger:** registra las actividades que se realizan en el sistema.
- **Backdoor (Puerta trasera):** abre puertos en el sistema sin autorización.
- **Bot:** convierte el sistema en zombi.

**Spyware**

Es un tipo de software malicioso que envía información confidencial de la víctima a terceros para fines desconocidos. Se lo conoce como software espía por ser sigiloso mientras recopila información, es diferente a un virus porque no se replica, aunque su capacidad para monitorear la información lo vuelve peligroso [29].

**Rootkit**

Son ataques sofisticados que modifican ficheros o también llamadas librerías del sistema operativo, para ocultar su existencia de otros códigos maliciosos también pueden se puertas traseras para otros usuarios. El comportamiento de este malware puede ser de forma automática como también por parte de un atacante que puede instalar el programa una vez obtenido permiso de root (permite obtener el control de equipos) [2].

**Bot**

Un bot es un tipo de programa malicioso que permite a un atacante tomar control de equipo en cuestión infectado. A su vez, participa en un sistema de control a gran escala de máquinas víctima.

**Phishing**

Su función es recopilar información de autenticación de sitios web del usuario como: información de bancos, cuentas de correos u otras, a través de un archivo que es enviado por correo electrónico**,** el usuario pareciese que ingresara a un sitio web legítimo, pero está siendo direccionado a una web falsa [30].

**Adware**

Este tipo de virus se instala en el sistema operativo de Android sin que el usuario lo note. Su función es descargar y mostrar textos o imágenes de publicidad en la pantalla de la víctima. Este tipo de malware se aloja en las apps del mismo gestor de aplicaciones móviles como Google play store, generando para el usuario una molestia a la hora de navegar donde es afectado su tarifa de datos, rendimiento y su batería [31].

**Rouge**

Simula ser un programa de seguridad, o sitios web que garantiza eliminar falsas infecciones detectadas y al ser ejecutados por el usuario, instalan otro tipo de malware en el sistema informático infectado [30].

**Rooting**

Es considerada una aplicación de escalada de privilegios que enraíza el dispositivo. Existe una diferencia entre las aplicaciones de rooteo malicioso y las aplicaciones de Rooting no maliciosas. Las aplicaciones de Rooting no maliciosas permiten que el usuario sepa de antemano que van a rootear el dispositivo y no ejecutan otras acciones potencialmente dañinas que aplicar a otras categorías de PHA (Aplicaciones Potencialmente Peligrosas).

Las aplicaciones de Rooting malintencionadas no informan al usuario que van a rootear el dispositivo, o informan al usuario sobre el enraizamiento en avanzar, pero también ejecutar otras acciones que se apliquen a otras categorías de PHA [31].

## 2.3. Identificación del problema

Para muchos la palabra Android en la actualidad es sinónimo de avance tecnológico en teléfonos inteligentes también conocidos como smartphone, lo cual conlleva a una masiva adquisición de dispositivos móviles. Al ser una plataforma con gran aceptación en el medio es objeto de ataques por partes de cibercriminales considerados como hackers quienes han refinado sus intentos de propagar los malware en dispositivos móviles.

De acuerdo a Sánchez [32], existe una enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos, haciendo que estas sean más vulnerables a los posibles ataques cibernéticos y al fraude en la red. Además, menciona en su artículo que es fácil ingresar a internet, cualquier persona guardando su anonimato puede realizar acciones difíciles de asociar. Indica también que la red se ha convertido en medio ideal para que los delincuentes y terroristas lleven a cabo sus acciones y actividades, sin mencionar también a los Estados quienes utilizan este medio para atacar a sus enemigos. Considera también que el cibercrimen, el ciberterrorismo y la ciberguerra hayan pasado a ser tres de las más importantes amenazas que parecen acechar a las sociedades occidentales.

Android se puede considerar como una plataforma vulnerable por muchos ya que su sistema operativo es libre para desarrolladores que buscan en mucho de los casos personalizarla desvinculándose de la seguridad. En la plataforma Android un malware es fácil de instalar ya sea por medio de tiendas en líneas o sitios web con solo hacer clips en un anuncio lo cual conllevaría a la instalación de la app infectada, a diferencia de plataformas como iOS quienes si manejan políticas de firmas de seguridad a la hora de instalar una app.

El director de seguridad de Android indica que el objetivo es hacer de esta plataforma informática la más segura del mundo. De tal manera que invierten en tecnologías y servicios que fortalecen la seguridad de los dispositivos, las aplicaciones y el ecosistema global. Además, menciona que la seguridad de Android empieza en una capa que se encarga de la defensa contra el malware que está incorporado en la plataforma, amparado

en el aprendizaje automático del análisis diario de todas las aplicaciones en los dispositivos Android [32].

La falta de recomendaciones a los usuarios en cuanto a prevención de los malware es una de las causas por las cuales los usuarios estarían expuestos a infectarse con software maliciosos. Por lo expuesto con anterioridad existe una preocupación en el medio por el tema de los malware en los dispositivos móviles con sistemas operativos Android lo que conlleva a realizar un estudio acerca de la problemática para plantear medidas que puedan detectar y prevenir la propagación de esta app maliciosas.

Sin duda los smartphone o comúnmente denominados teléfonos inteligentes almacenan todo tipo de información confidencial de sus usuarios, quienes a lo largo de sus jornadas laborales o actividades diarias dependen mucho de la información alojada en sus teléfonos inteligentes, prueba de ello es las estadísticas que definen al sistema operativo Android como el software más aceptado a nivel mundial con un 70%, esto permite comprender por qué es el software con más ataques a su plataforma. Los malware considerados como más letales a la hora de contagio son: ransomware, troyanos bancarios y RAT (troyanos de accedo remoto).

## 2.4. METODOLOGÍA

De acuerdo con las características de la investigación se presenta una metodología científica basada en un estudio de caso, misma que según Soto & Escribano [33], es una de las estrategias investigativas más importante para realizar el diagnóstico de una situación particular, el estudio de caso demanda de un trabajo especializado y un sinnúmero de procesos durante un corto periodo de tiempo.

El principal método para usarse es el cualitativo porque se centra en un fenómeno específico del mundo real, tal es el caso de los malware en la plataforma Android. También está presente el método cuantitativo mediante el análisis de datos obtenidos de los resultados, de la técnica aplicada y lo relacionado a efectividad y rendimiento.

Dentro de la técnica de investigación se contempla la observación, que para Castellanos [34], es el registro exacto de todo lo que irá ocurriendo en el paso a paso a fin de analizar el fenómeno en su totalidad. La observación y evaluación mediante un test será primordial durante el proceso.

Se procederá a recolectar información y evaluar las herramientas de prevención antimalware que existen en mercado de app. El primer método para utilizar es un

emulador de Android Studio donde se desarrollarán las pruebas a las diferentes herramientas de prevención en el mercado, particularidad que impide medir como afecta al

funcionamiento del dispositivo. El segundo método permitirá evaluar los recursos que utiliza las herramientas de prevención sobre un dispositivo físico.

Existen dos metodologías que ya han sido utilizados en investigación anteriores como lo es la metodología de análisis de durabilidad de la batería y la metodología de efectividad y rendimiento, las cuales fueron utilizadas en el estudio de caso realizado por Villanova para obtener datos acerca de cómo evaluar las herramientas de prevención [2].

### 2.4.1. Metodología sobre Efectividad y Rendimiento

La metodología para evaluar la efectividad de las herramientas y el impacto que tiene sobre el dispositivo en cuanto al rendimiento es el siguiente según Villanova [2]. La metodología será modificada a situaciones actuales para obtener resultados acordes a la realidad.

**Descripción del Hardware utilizado:**

- Sistema Operativo Windows 11 Home Single Language 64 bits.
- Procesador Intel (R) Core (TM) I3 10th Gen CPU 1.20 GHz (4 CPUs)
- Memoria RAM: 8 GB
- Disco solido: 250 GB

**Descripción del Sistema operativo virtualizado**

- Sistema operativo Android 12.
  1. Crear un entorno virtual mediante el programa VirtualBox donde se monta el sistema operativo de Android 12 de x64 bits: Descripción máquina virtual:
     - Sistema operativo Android 12
     - Almacenamiento 32 GB
     - Procesador de 3 núcleos
     - RAM 4 GB

2. Instalar la app para medir el rendimiento como lo es 3C All-in.One ToolBox Pro versión 2.6.5b el cual permitirá analizar el consumo de la CPU y memoria RAM del entorno Android 12 ejecutado en la máquina virtual.
3. Instalar la app Anydesk que nos permitirá transferir las muestras de malware a testear entre la laptop y el sistema virtual.
4. Realizar una prueba de análisis de rendimiento con el sistema "limpio". Que posteriormente servirá de referencia por medio de la app 3C All-in.One ToolBox Pro.
5. Crear una máquina virtual desde esa plantilla clonando, definiéndolo como base para las pruebas posteriores.
6. Instalar una herramienta de prevención a testear del grupo seleccionado y actualizarla a la última versión si se lo amerita.
7. Iniciar grabación en la opción "**analizar**" en la app 3C All-in.One ToolBox Pro, donde se obtendrá valores consumidos por la CPU y RAM del dispositivo.
8. Utilizando la app Anydesk transferir los malware al dispositivo, es decir, transferir las muestras a testear entre el pc y el entorno virtual controlado.
9. Determinar si la herramienta de protección los detecta en tiempo real (cuando estos son almacenados en el dispositivo), o por el contrario hemos de forzar un análisis del sistema y comprobar cuántos detecta del conjunto.
10. Extraer los resultados de la monitorización del sistema en cuanto al rendimiento.
11. Suprimir la copia de la máquina virtual y volver al punto 5.

### 2.4.2. Metodología Análisis Consumo de Batería

Considerando que el entorno donde se realizarán las pruebas de efectividad de las herramientas de prevención y del rendimiento es virtual, el cual no permitirá realizar el test de durabilidad de la batería ya que no presenta los requerimientos para la medición. Se plantea una nueva manera de medir la durabilidad de la batería, esta se realizará por medio de un dispositivo móvil quien ayudará a la investigación. Este dispositivo físico presenta las siguientes características.

- Samsung Galaxy A9 (2018)
- RAM 5 GB
- Sistema operativo Android 12
- CPU Qualcomm Snapdragon 660
- Procesador Octa-core 1,84 GHz - 2.21 GHz

La metodología para evaluar a las herramientas de prevención es la siguiente según [2].

1. Tener el S.O. Android recién instalado.
2. Instalar la herramienta de análisis de batería. GSAM battery monitor PRO. Nos mostrará, desde la última carga en qué se ha usado la batería.
3. Cargar al 100% antes de instalar la app sobre el rendimiento de la batería.
4. Instalar herramienta prevención.
5. Generar actividad durante un tiempo (transferir ficheros, navegar, gestionar correo, etc.) simulando un funcionamiento habitual hasta que la batería se descargue hasta el 87% como mínimo, para que la herramienta de monitorización obtenga datos.
6. Recopilar resultados de GSAM battery monitor PRO.
7. Desinstalar herramienta prevención.
8. Si no es la última herramienta que evaluar. Volver al paso 3

### 2.4.3. Selección de las herramientas de prevención a evaluar

En la actualidad existe un gran número de aplicaciones antimalware que brindan al usuario una protección adicional a sus dispositivos móviles. El instituto de seguridad de investigación de antivirus AvTest The Independent IT-Security Institute, evaluó 51 aplicaciones de antivirus para el sistema operativo Android 12, donde utilizó el emulador conocido como Android Studio, que permite realizar test de efectividad, exponiendo a las aplicaciones de seguridad a un test de detección de malware. Considerando tres aspectos importantes a evaluar la protección, utilidad y funcionalidad que aportan a los sistemas Android (AV-T).

En el estudio de caso se enfocará la investigación en la protección y utilidad que los antimalware ofrecen a la plataforma Android, considerándolo como punto partida. A

continuación, se realiza una comparación de las herramientas de seguridad para Android disponibles en el mercado.

Solo 4 de los 21 antimalware analizados tenían una tasa de detección por debajo de los 86% indicando que las aplicaciones restantes estaban con una tasa de detección superior a los 93% indicando que son aplicaciones con un alto nivel de detección de malware. Estos resultados indican las herramientas evaluadas de prevención contra los malware son efectivas y van a la par. Sin embargo, se pretende realizar una evaluación sobre las herramientas antimalware que existen en la actualidad para demostrar si ofrecen a los usuarios la seguridad necesaria que evite el contagio y permita un buen aprovechamiento de los recursos del smartphone.

Se recoge información del laboratorio del Instituto Independiente de seguridad AV-Test, como referencia para analizar las apps disponibles en el mercado para la seguridad a los dispositivos móviles o smartphone [35]. Como se muestra en el Anexo 12.

De acuerdo con la información planteada en el Anexo 10 se procede a seleccionar diez de ellas para realizar las pruebas en el entorno virtual controlado. Dicha selección se realizó en base a dos organizaciones sin fines de lucro que realizan pruebas a productos de seguridad para plataformas como Android, estas empresas buscan demostrar si los productos antimalware que ofertan son eficaces a la hora de identificar y eliminar una app con código maliciosos. También se consideran algunas herramientas de prevención que están en boga y tienen nombre comercial conocidos por los usuarios. En el Anexo 11, se lista las herramientas de prevención a utilizar.

**Selección de Malware a Evaluar**

Las muestras de malware seleccionadas fueron extraídas de un repositorio llamado www.virusshare.com, es un sitio web que brinda a investigadores de seguridad y analistas de código malicioso ejecutables y apk para su posterior utilización. Al repositorio solo se puede acceder con una previa invitación del administrador del sitio web, donde la investigador o estudiante debe explicar las razones por las cuales desea tener acceso al sitio web.

En el Anexo 12 se muestran los malware con su respectiva familia donde se expone cómo funciona el malware en el smartphone. En caso de necesitar información detallada de la muestra de MD5 se sugiere copiar el código de la muestra y dirigirse al sitio web www.virustotal.com para realizar la búsqueda. Este sitio web Virus Total inspecciona elementos con más de 70 escáneres antivirus y servicios de listas negras de URL / dominio, además de una gran cantidad de herramientas para extraer señales del contenido estudiado [36].

## 2.5. DIAGNÓSTICO

**Resultados de evaluación**

En esta sección se presenta los resultados obtenidos de las pruebas en el entorno virtual controlado y en el dispositivo móvil. Cabe recalcar que las pruebas de herramientas de prevención se las realizó en un entorno virtual controlado para evitar el daño del dispositivo móvil y las pruebas para identificar el consumo de la batería se hicieron en un smartphone, donde se evidenció el impacto que tiene en el consumo de los recursos físicos del smartphone como CPU, memoria RAM y batería.

**Efectividad de Herramientas**

El test realizado a las herramientas de prevención consiste en evaluar en un entorno virtual las aplicaciones de los antimalware existentes en el mercado. En el Anexo 11 se muestran las herramientas de prevención seleccionadas para el test, donde cada una de estas apps son instaladas y ejecutadas en la proforma Android 12. Cada muestra de malware encontrada por las herramientas de prevención pasa a ejecutarse en el entorno virtual. Los archivos con el código malicioso son transferidos por AnyDesk que permite el acceso remoto, como el paso de archivos entre ordenadores. En el Anexo 12 se evidencia el nombre del malware y una pequeña descripción de lo potencial que puede ser el riesgo.

Los malware identificados por las herramientas de prevención instaladas en la máquina virtual garantizan que son muestras potencialmente dañinas para la plataforma Android. Sin embargo, no se puede dejar de lado que podrían existir falsos positivos, para ello se ha comprobado su validez haciendo uso del sitio web “virus total” donde han sido identificados por otros antimalware como código malicioso.

Para infectar a la máquina virtual con la muestra del malware se utilizó app AnyDesk la cual permite transferir archivos entre ordenadores, donde se evidenció que algunos antimalware no detectaban el malware en tiempo de real, AhnLab V3 Mobile Security 3.3, AVIRA, F-Secure, G DATA, Ikarus mobile securtity 2.0, Kaspersky, Line Antivirus y McAfee.

Muchas de las herramientas de prevención evaluadas tienen una versión gratuita, pero a la hora del análisis en su mayoría respondieron en promedio 78,91% en la detección de los malware.

Detalles de la prueba realizada a las herramientas de prevención:

- Mediante los resultados se evidencia que existen dos antimalware testeados en este estudio de caso que obtuvieron una tasa de detección del 100% de efectividad es Ikarus Mobile security 2.0 y McAfee Mobile Security, seguido la app de prevención como Line Antivirus con un 95%, G Data y Kaspersky con 83%, además se evidencia que SOPHOS INTERCEPT X for Mobile obtuvo una tasa de detenciones de 80%.
- Existe un promedio de detección de malware en un rango de 78% y 75% como la app Avast, AVG y Avira, como se muestra en la Figura 1.
- Se observa que dos apps antimalware coinciden en la detección realizadas con porcentajes iguales a 73% siendo los más bajos en diferencias a las otras apps como AhnLab V3 Mobile Security 3.3, F-Secure. En la Figura 1 se muestran la información de forma visual sobre los datos obtenidos en lo que concierne a la efectividad de la herramienta.

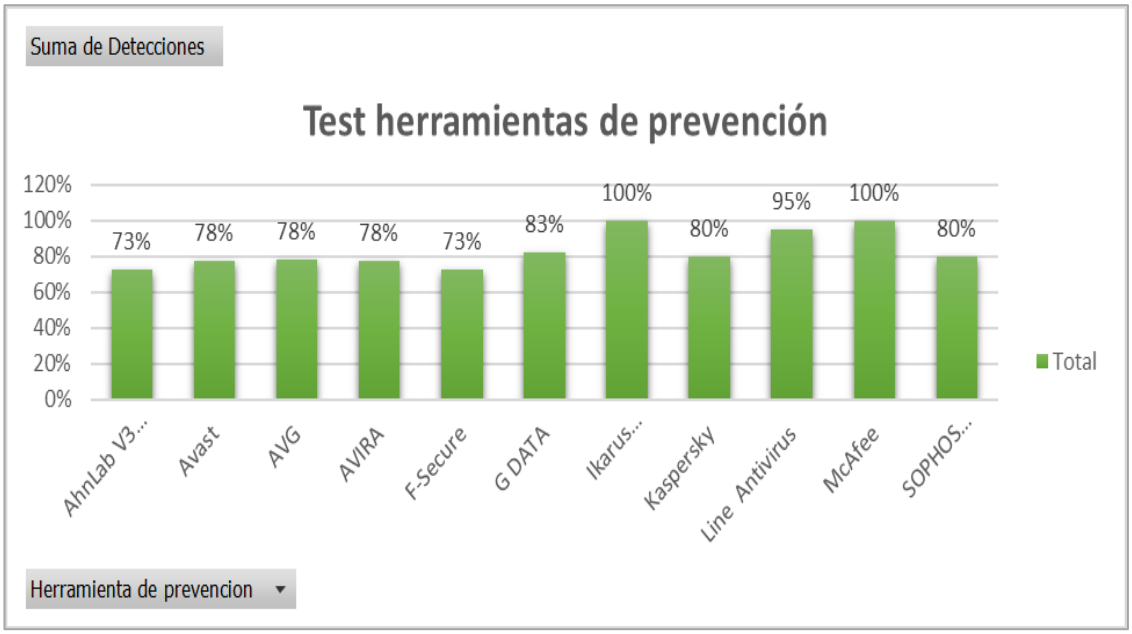



Figura 1. Test de efectividad en la detección del malware.

**Impacto en el Rendimiento del Sistema**

En esta sesión se detalla el impacto del rendimiento producido por las herramientas de prevención sobre el sistema basándose en aspectos como el consumo de la CPU, memoria RAM y el consumo de la batería. Como se había mencionado, las pruebas para medir el consumo de la batería se las realizó en un dispositivo móvil. Esta demás hay que indicar que se utilizó la herramienta 3C Tool Box Pro con el fin de poder medir el consumo de las variables a evaluar. A continuación, se muestran los resultados obtenidos del test de consumo de CPU y memoria RAM.

**Consumo CPU Y memoria RAM**

La imagen que se muestra es el resumen de los datos recogidos por la herramienta 3c Tool Box sobre el sistema desde que se arranca la máquina virtual, donde se detecta que el consumo de los recursos del sistema es bajo durante el inicio y en resumen de evidencia que los test realizados de forma manual si tiene un impacto no tan representativo que el sistema no pueda superar en los referentes al consumo de la CPU y Ram del entorno virtual controlado. A continuación, se muestra información obtenida de los test realizados a las diferentes herramientas de prevención.

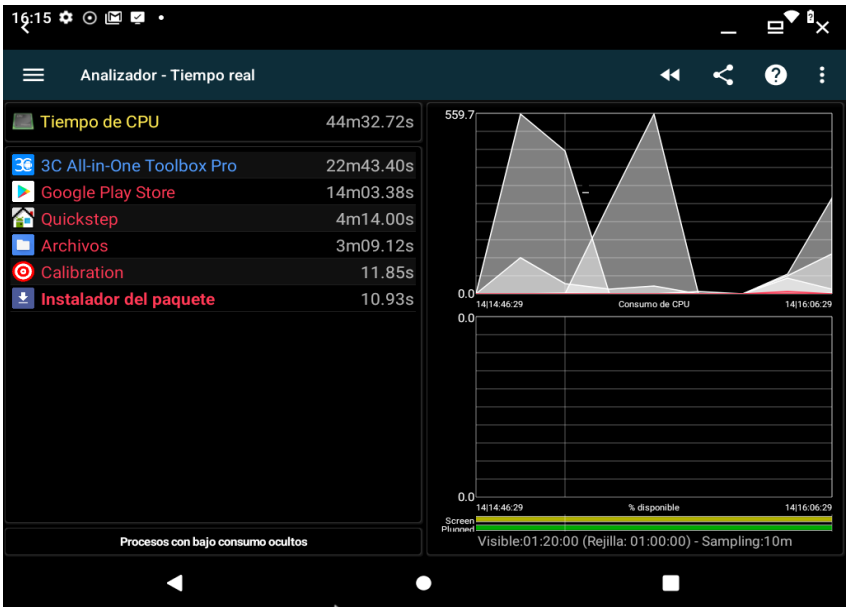



Figura 2. Consumo de CPU y RAM del sistema al iniciar máquina virtual

**Avast Mobile Security**

Los valores presentados en la Figura 3 muestra que la app tiene un almacenamiento de 60,37 MB y consumo inicial de memoria RAM de 25,38 MB el cual incrementa a 2,08 MB.

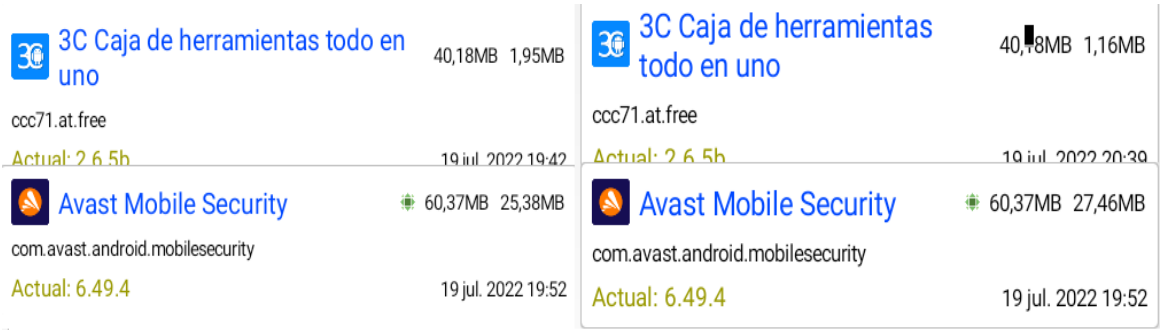



Figura 3. Consumo RAM Avast Mobile Security

La Figura 4, muestra el consumo inicial de la CPU utilizado por los procesos del sistema, los cuales oscilan en un tiempo de uso de 3m 03s y 4,8% del consumo de recursos de la CPU desde el inicio de la app antimalware.

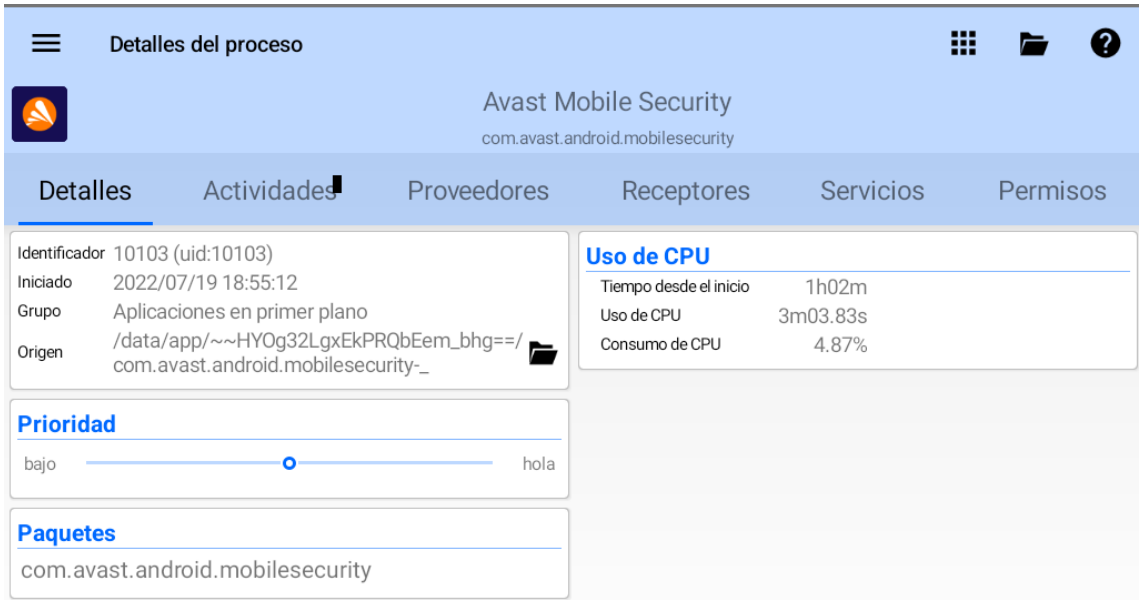



Figura 4. Consumo inicial CPU de la app Avast Mobile Security

En la Figura 5, se muestra el consumo de CPU generado durante el proceso de detección del malware, donde la app ocupa 9,03% mientras realizaba la detección antimalware con un tiempo de uso de 11m 10s.

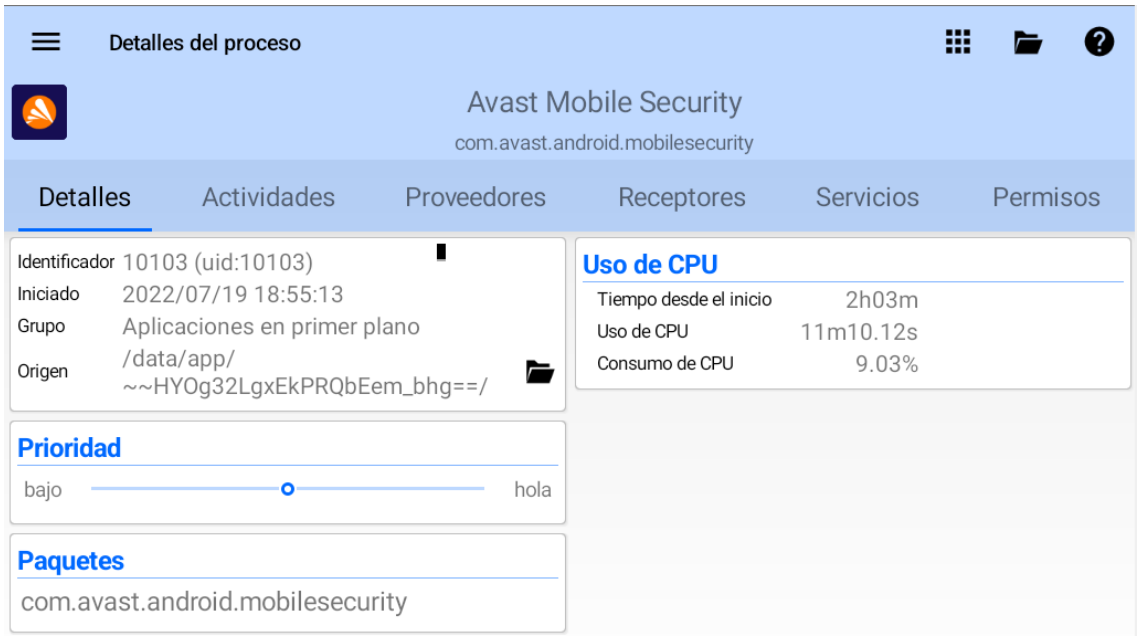



Figura 5. Consumo final CPU de la app Avast Mobile Security

### F. Secure Safe 19.60

En la Figura 6, se muestra los resultados obtenidos del test inicial del consumo de RAM 21,97 MB de la app F-Secure para ello se tomó estos valores antes de realizar el proceso de detección de la app antimalware.

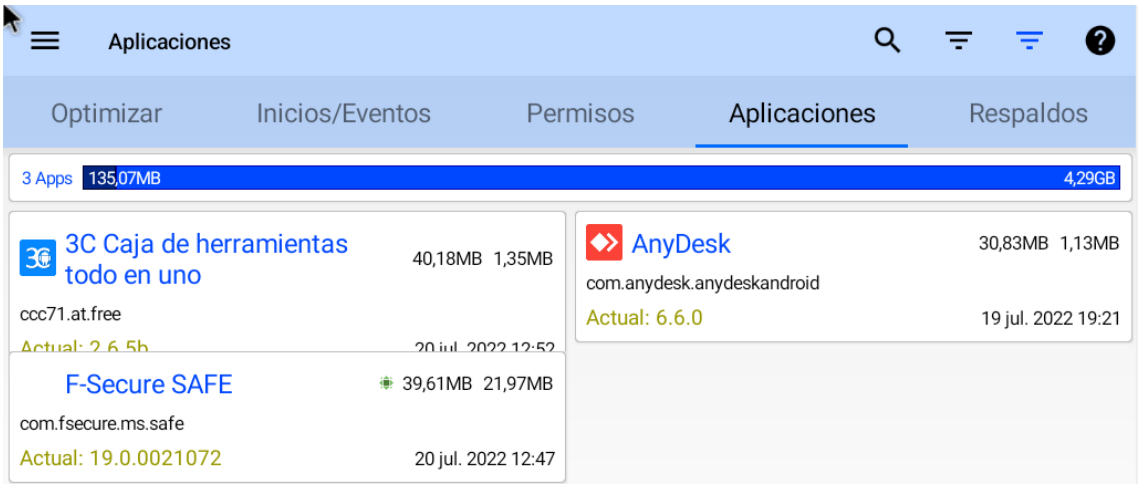



Figura 6. Consumo inicial app RAM F-Secure Safe 19.60

En la Figura 7, se muestra el consumo de RAM de la app F-Secure SAFE con un aumento de 0,57% durante el proceso de detección del malware en ejecución.

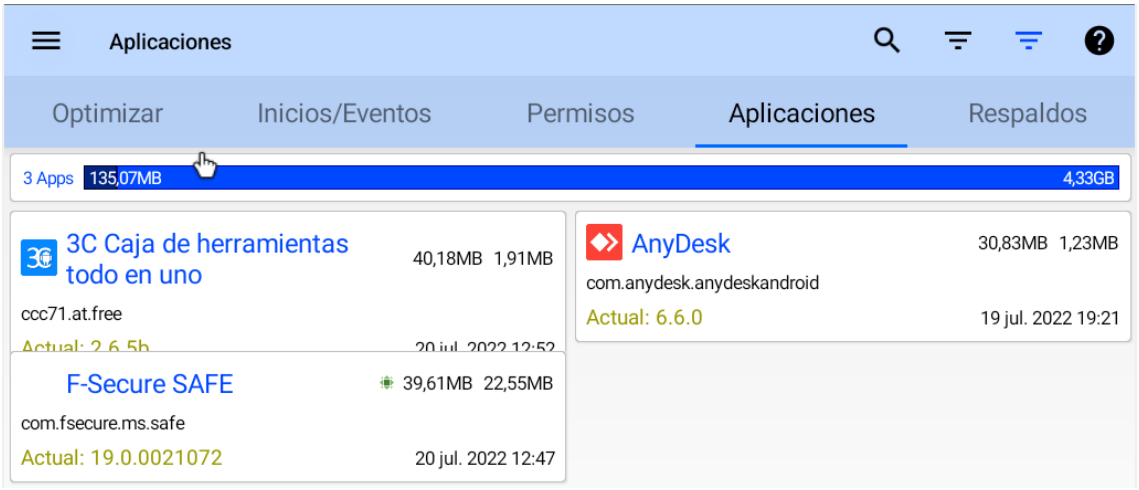



Figura 7. Consumo final RAM app RAM F-Secure Safe 19.60

En la Figura 8 los resultados de esta app F-Secure Safe se muestran durante la ejecución de inicio es de 3m 51s y un consumo de CPU del 0,35%.

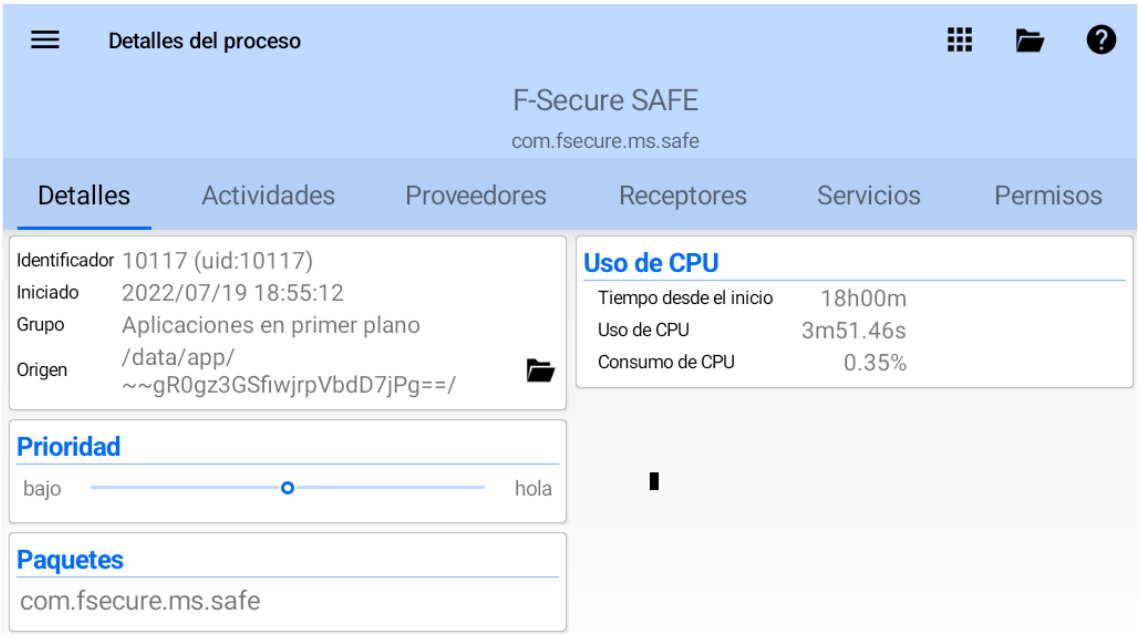



Figura 8. Consumo inicio de CPU de la app F-Secure Safe

En la Figura 9 se puede observar que existe un tiempo de 53m 14s un aumento de 4,64%.de consumo de CPU durante el tiempo de detección del malware en el dispositivo móvil.

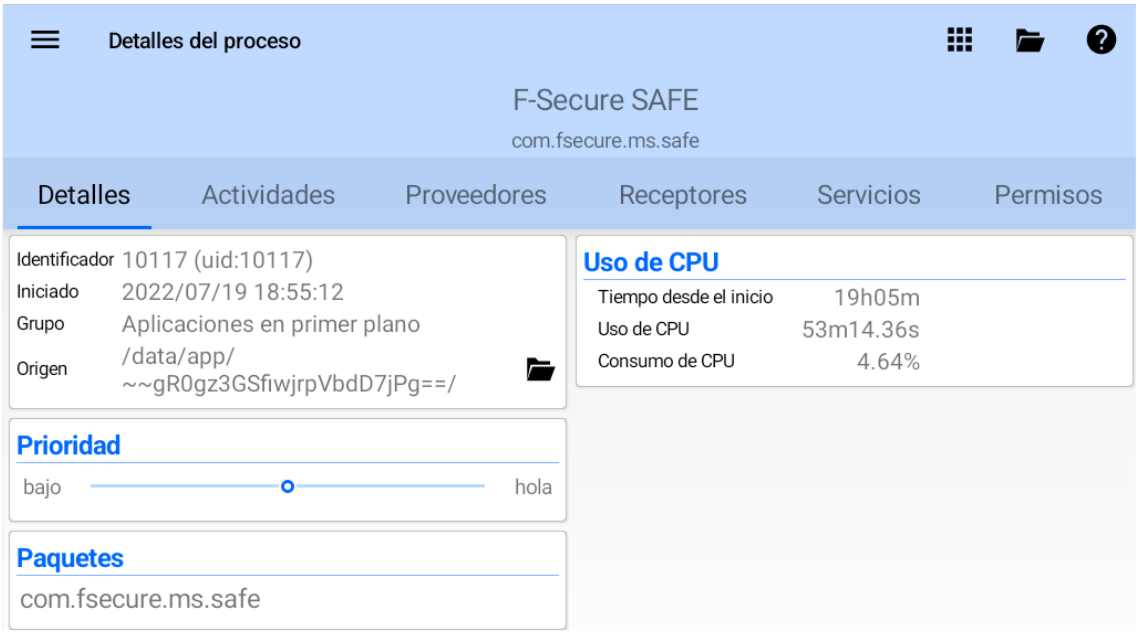



Figura 9. Consumo final de CPU de la app F-Secure Safe

### Ikarus Mobile Security

En la Figura 10**,** se muestran los resultados sobre la app Ikarus Mobile Security durante su ejecución inicial en el entorno virtual controlado con un consumo de 57,36 MB de RAM.

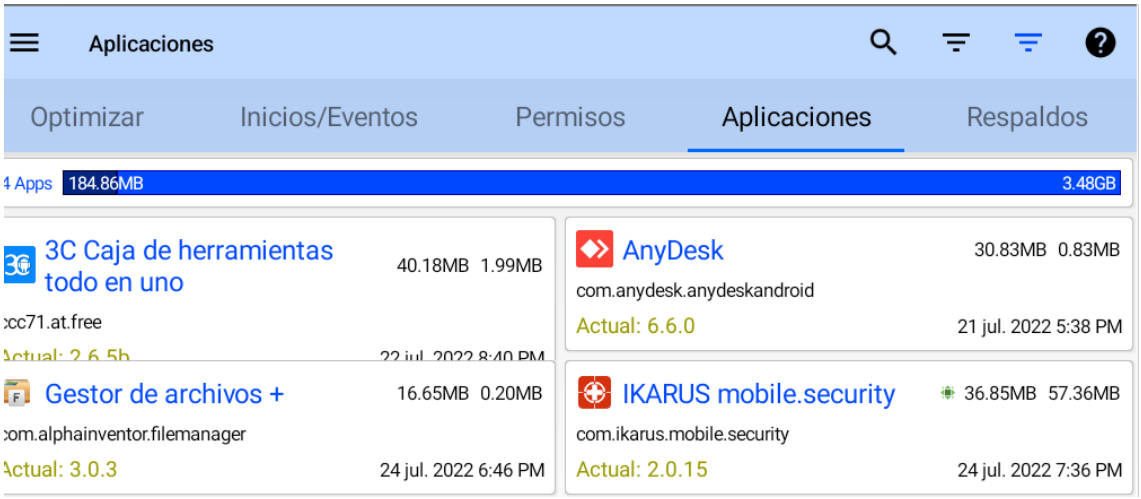



Figura 10. Consumo inicial de RAM de la app Ikarus Mobile Security

En la Figura 11 se muestra un almacenamiento de 36,85 MB, en el transcurso de ejecución del test el consumo de la RAM varia en 0,03% evidenciando que no existe mayor consumo durante el arranque de la app Ikarus Mobile Security.

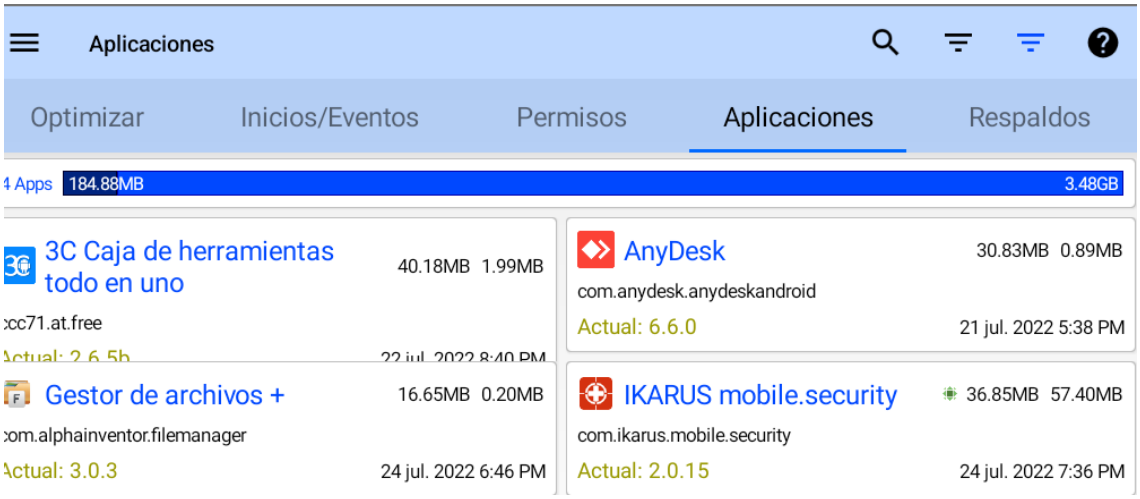



Figura 11. Consumo final de RAM de la app Ikarus Mobile Security

En la Figura 12 los resultados de esta app Ikarus mobile security muestran que un inicio existe un tiempo de uso 2m 58s y un consumo de CPU del 0,21%.

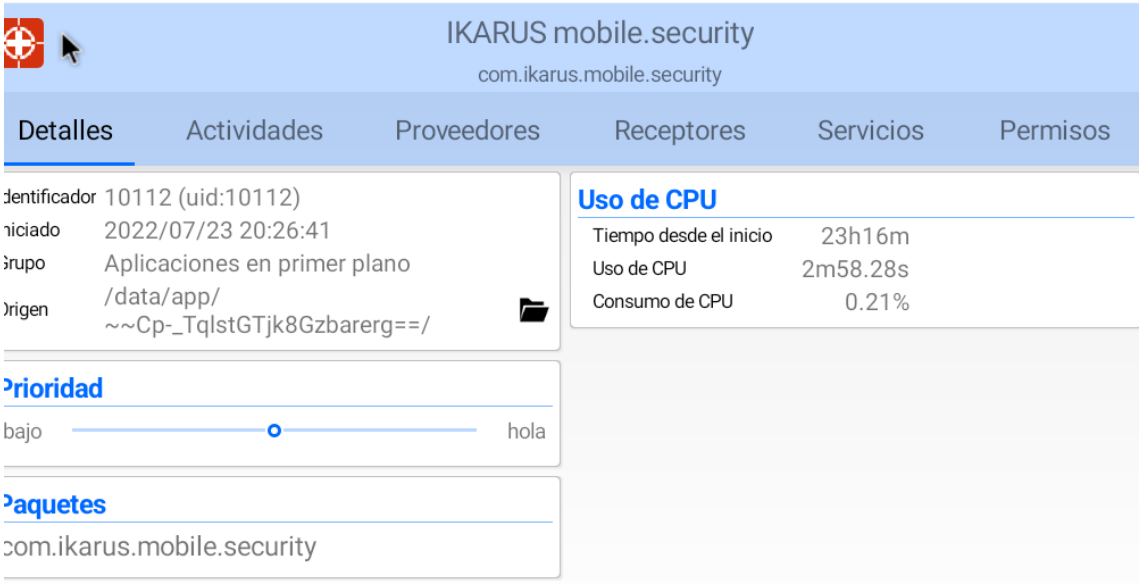



Figura 12. Consumo inicial de CPU de la app IKARUS Mobile Security

En la Figura 13 se puede observar que existe una variación en el uso de la CPU durante el transcurso de 13m 61s un aumento de 0,92% como resultado del proceso de búsqueda del malware.

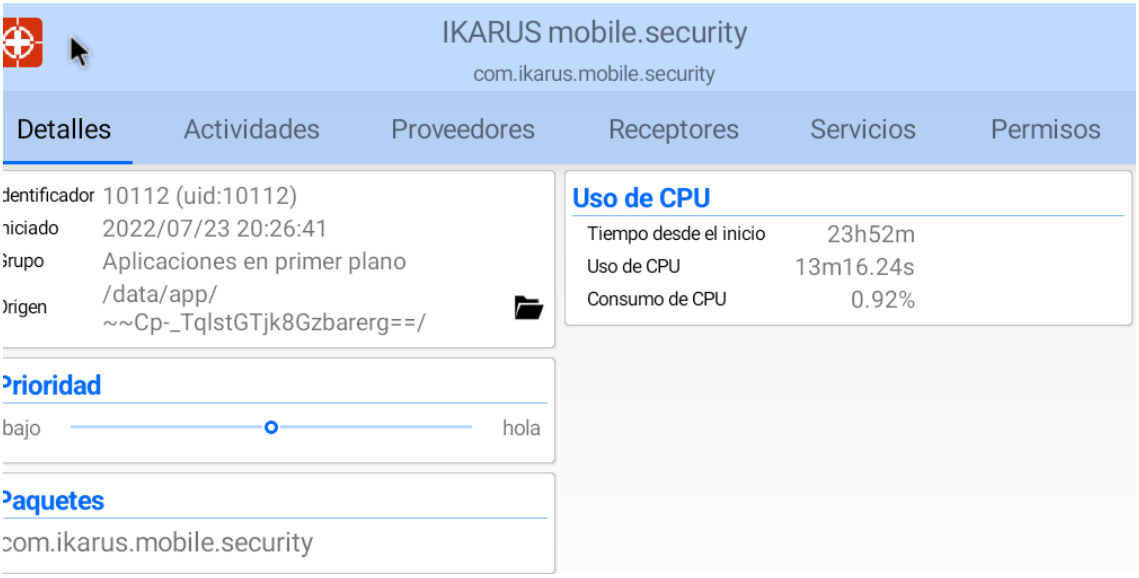



Figura 13. Consumo final de CPU de la app IKARUS Mobile Security

**Sophos Intercept X for Mobile 9.7**

En la Figura 14 se muestra que el espacio utilizado de almacenamiento en disco duro es 58.52MB y durante el proceso de ejecución inicial un espacio de RAM de 17.95MB.

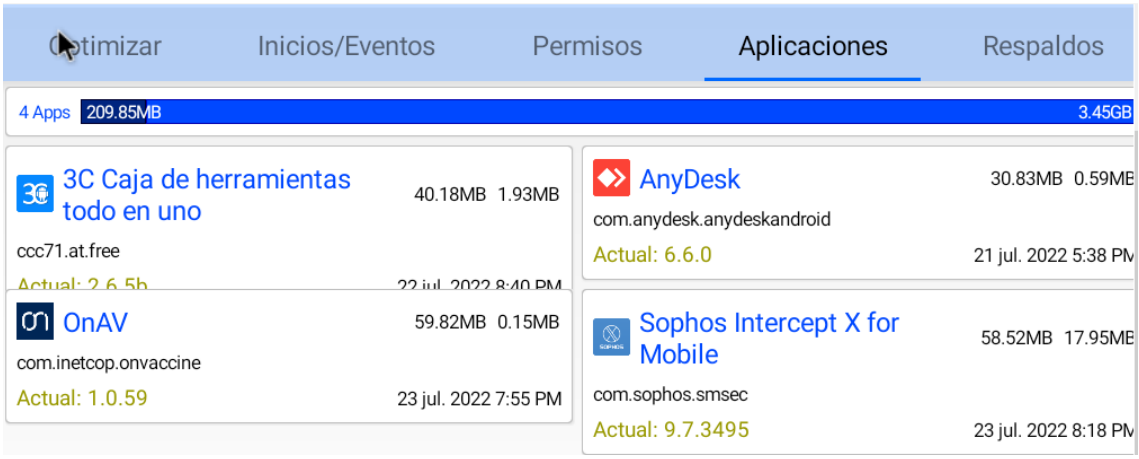



Figura 14. Consumo inicial de RAM Sophos Intercept X for Mobile 9.7

En la Figura 15, se muestra que durante el proceso de detección de malware existe un 17,97MB de consumo de RAM siendo este un incremento de 0,27% lo cual no repercute al funcionamiento del dispositivo móvil.

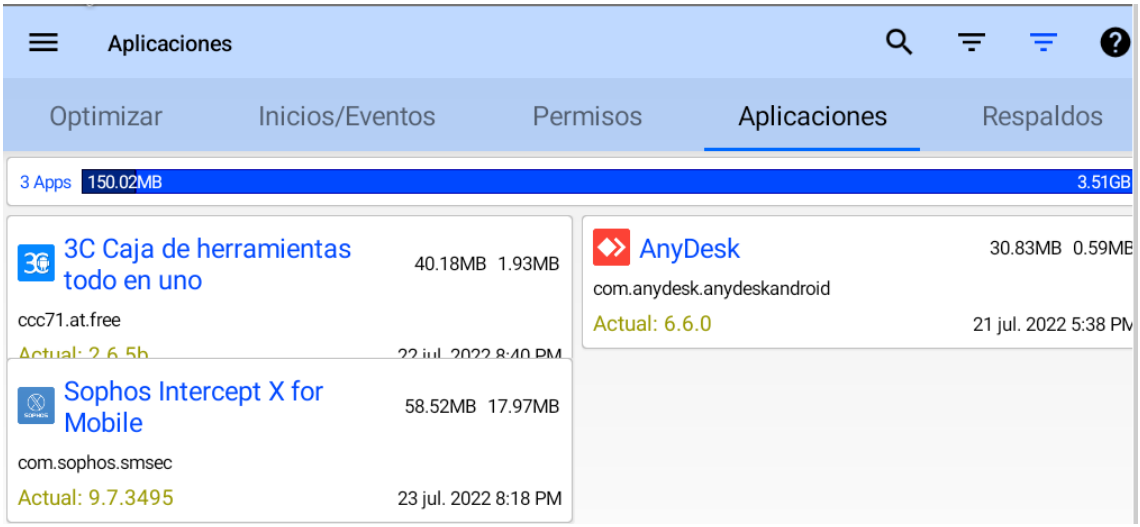



Figura 15. Consumo final de RAM Sophos Intercept X for Mobile 9.7

En la Figura 16, se muestra los resultados obtenidos de la app Sophos Intercept X for Mobile con un tiempo de inicio de consumo de CPU de 2h 1m y un consumo de recursos de CPU del 7,85% se puede evidenciar que tiene consumos alto.

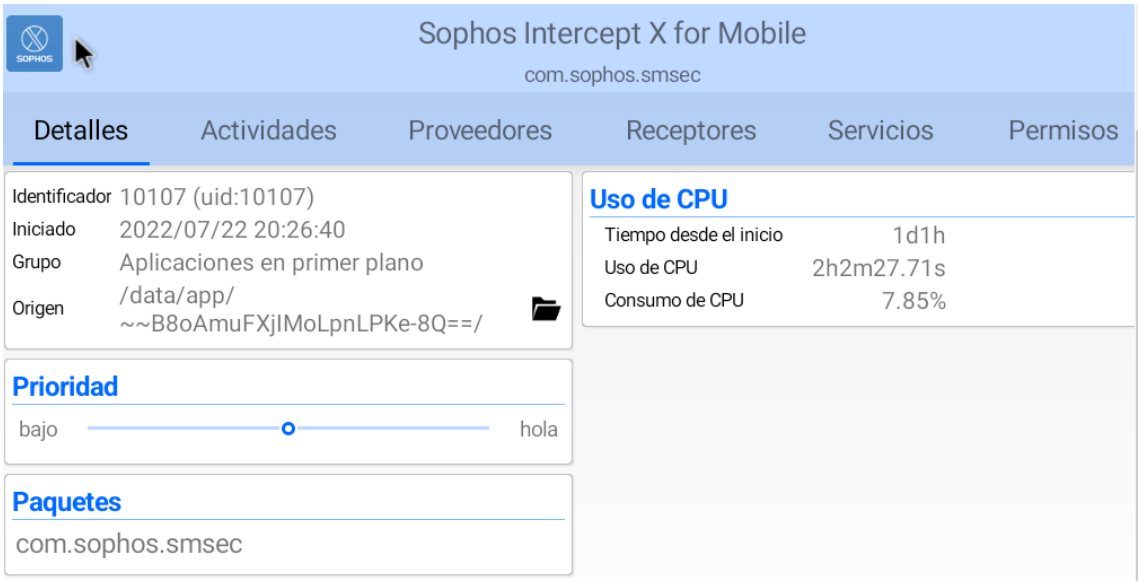



Figura 16. Consumo inicial de CPU Sophos Intercept X for Mobile 9.7

En la Figura 17, se muestra que existe una variación en el uso de CPU durante el tiempo de 2h 4m con un aumento en el consumo de los recursos de la CPU de 0,05% lo cual no es relevante para el proceso, siendo la app que menos recursos utilizo mediante la detección del malware.

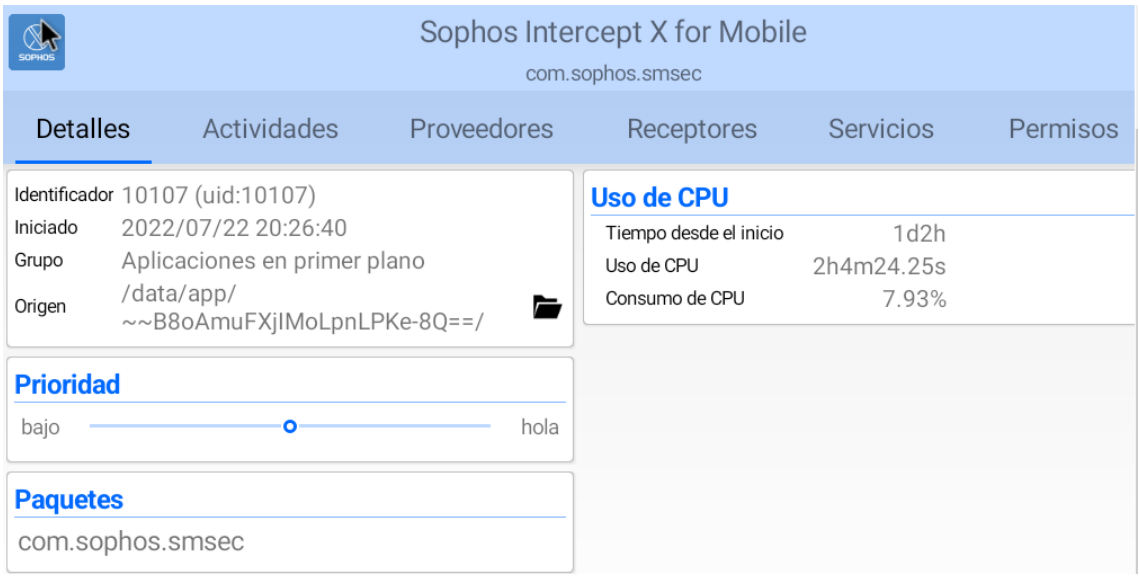



Figura 17. Consumo final de CPU Sophos Intercept X for Mobile 9.7

### AhnLab V3 Mobile Security 3.3

En la Figura 18 se muestra el consumo de recursos en el sistema provocado por la app AhnLab V3 Mobile Security con un almacenamiento en disco duro de 74,04MB y un consumo inicial de RAM de 20,01MB.

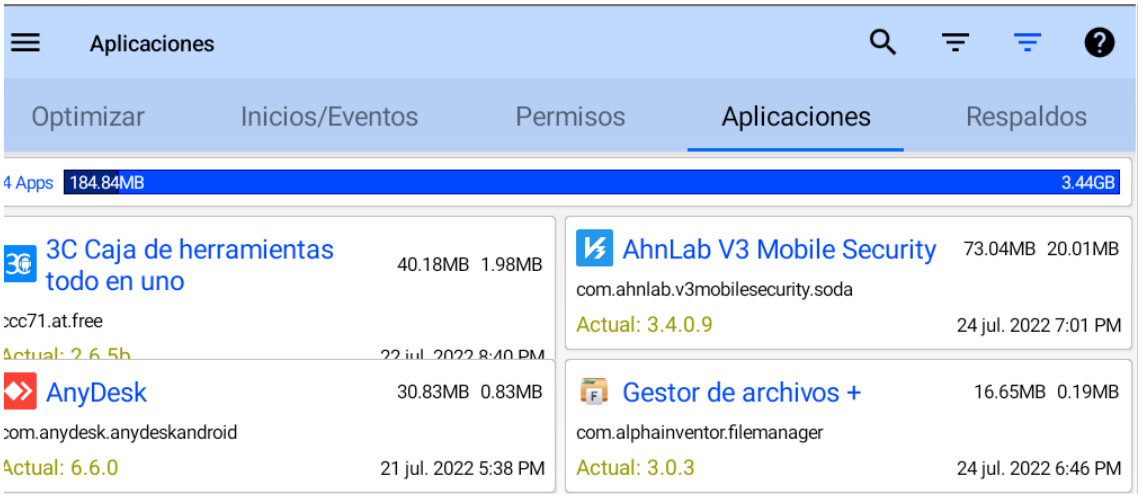



Figura 18. Consumo inicial de RAM app AhnLab V3 Mobile Security

En la Figura 19, se muestra el consumo de la RAM durante el tiempo de detección del malware con un consumo 21,19MB donde se puede evidenciar un aumento del 0,18 MB algo que si puede asumir el dispositivo móvil para su correcto funcionamiento.

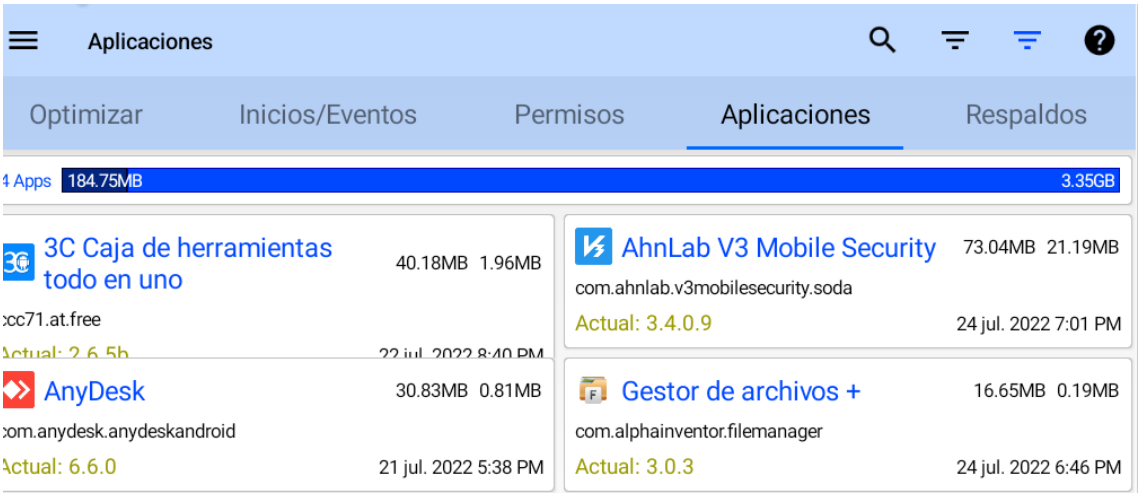



Figura 19. Consumo final de RAM app AhnLab V3 Mobile Security

En la Figura 20 se muestra el tiempo de uso inicial de CPU generado por la app AhnLab V3 en el arranque de la app antimalware oscilando el 3m 42m y 0,27% del consumo en porcentaje de la CPU.

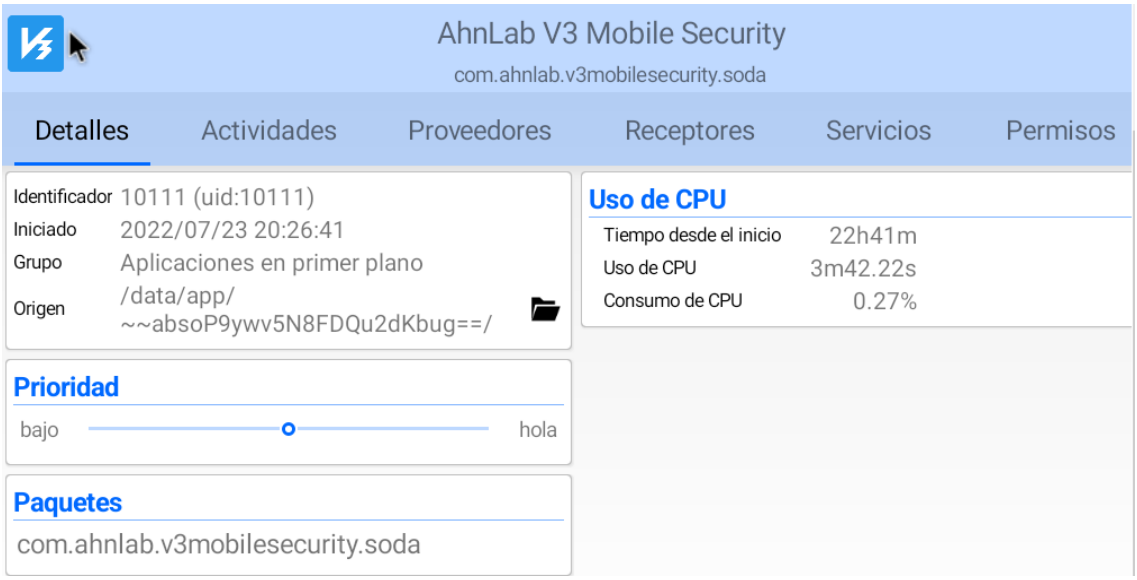



Figura 205. Consumo inicial de CPU AhnLab V3 mobile Security

En la figura 21, se muestra que existe una variación en el uso de CPU durante el tiempo de 24m 6s con un aumento en el consumo de los recursos de la CPU de 1,5% de un total de 1,77% existiendo un aumento significativo.

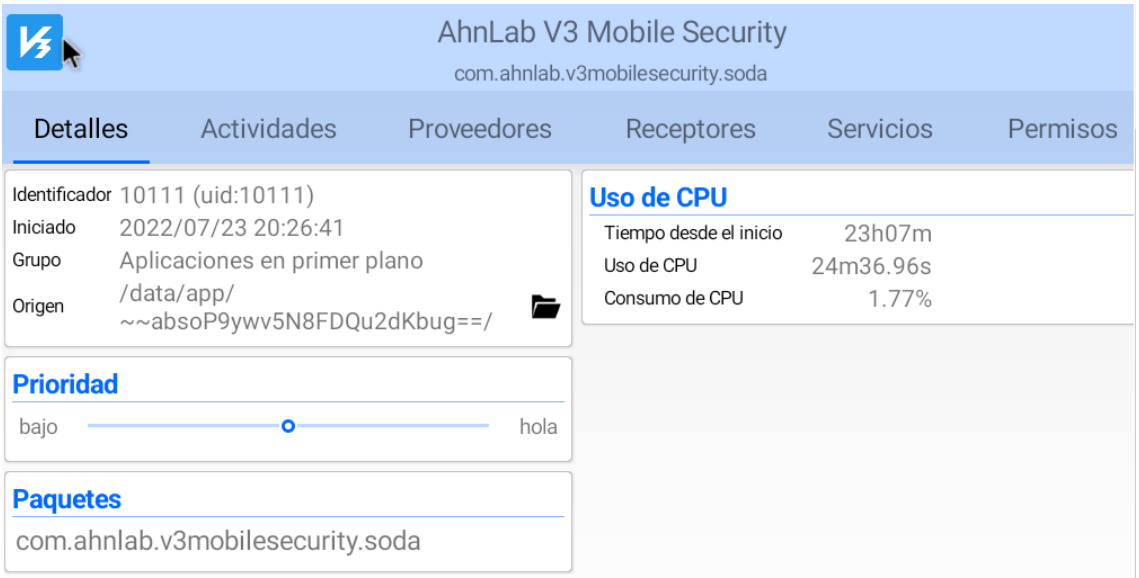



Figura 21. Consumo final de CPU AhnLab V3 mobile Security

**AVG Antivirus Free 6.48**

En la Figura 22 se muestra el consumo de recursos en el sistema provocado por la app AVG Antivirus Free 20,53 MB con un almacenamiento interno de 61,96 MB.

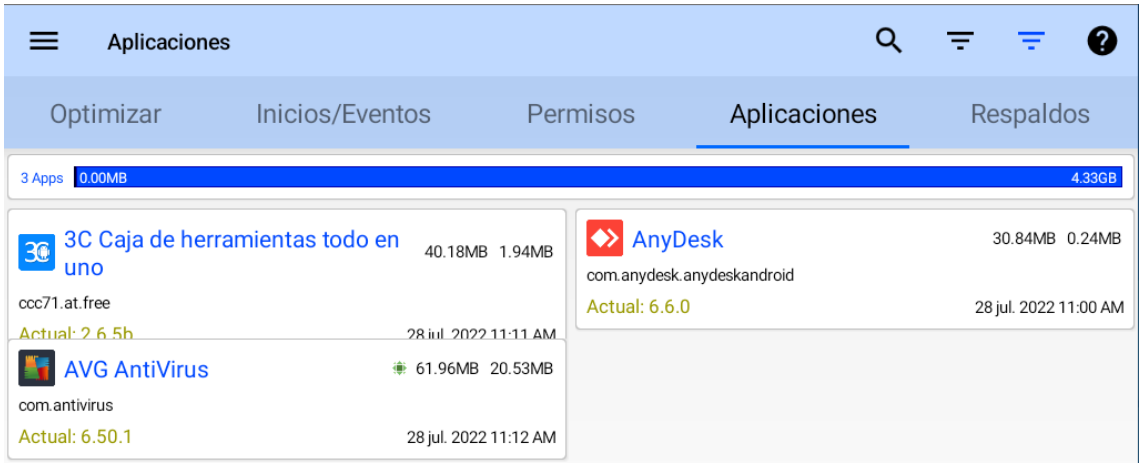



Figura 226. Consumo inicial de RAM AVG ANTIVIRUS FREE

En la Figura 23 se muestra un aumento del 2,73 MB de un total de 23,26 MB a diferencias de otras apps que el incremento fue bajo, pero esto es algo que si puede asumir el dispositivo móvil para su posterior procesamiento.

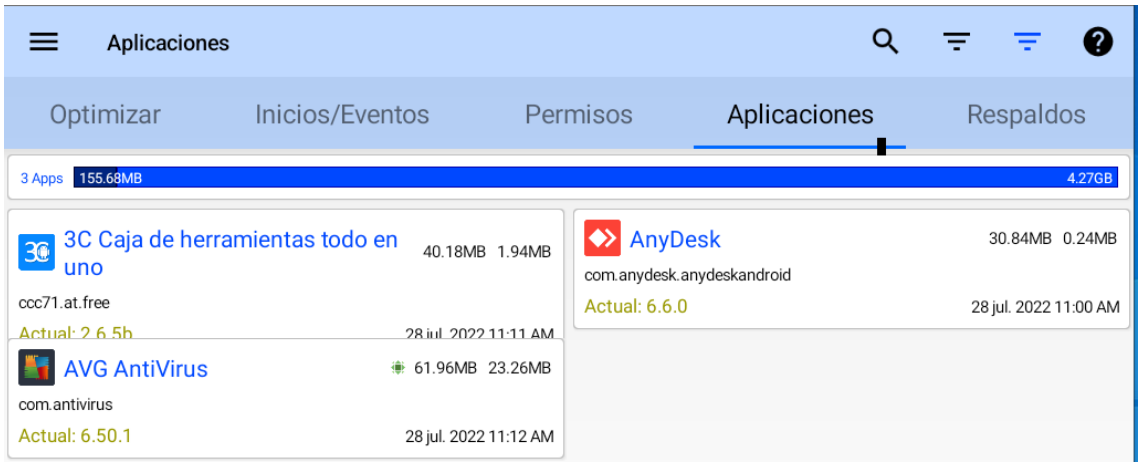



Figura 237. Consumo final de RAM AVG ANTIVIRUS FREE

En la Figura 24 se muestra el tiempo de uso de CPU generado por la app AVG Antivirus Free el cual es 1m 10s y 0,11% durante la ejecución de inicial de la app antimalware.

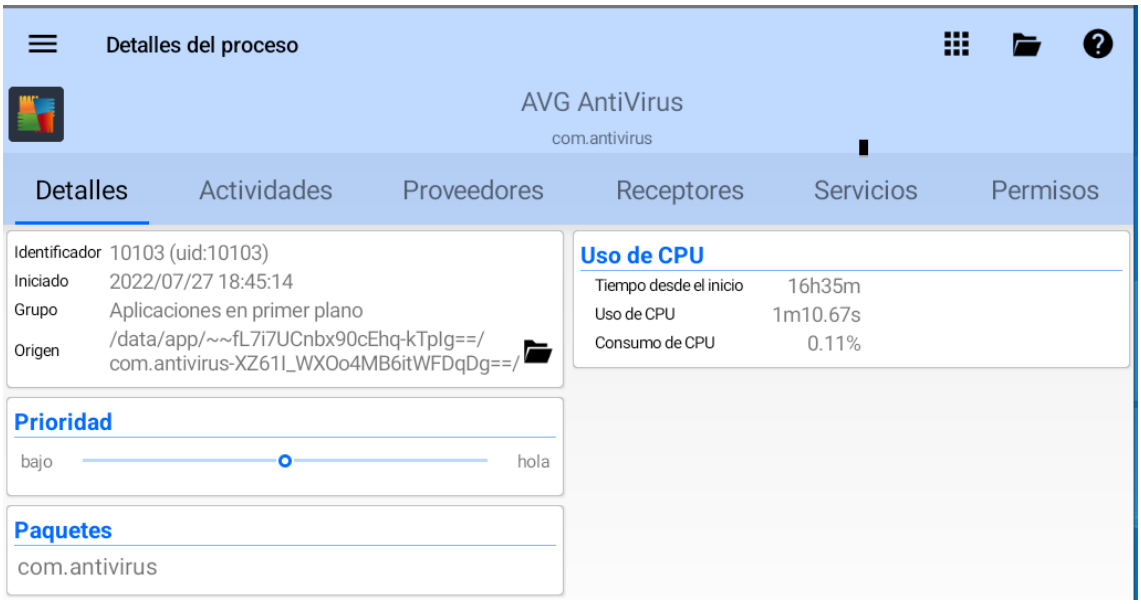



Figura 24. Consumo inicial de CPU AVG Antivirus Free

En la figura 25 se muestra el porcentaje que aumento la CPU, este valor es de 0,51% de un total de 0,62% siendo valores bajo los cuales no afectan al funcionamiento del dispositivo móvil.

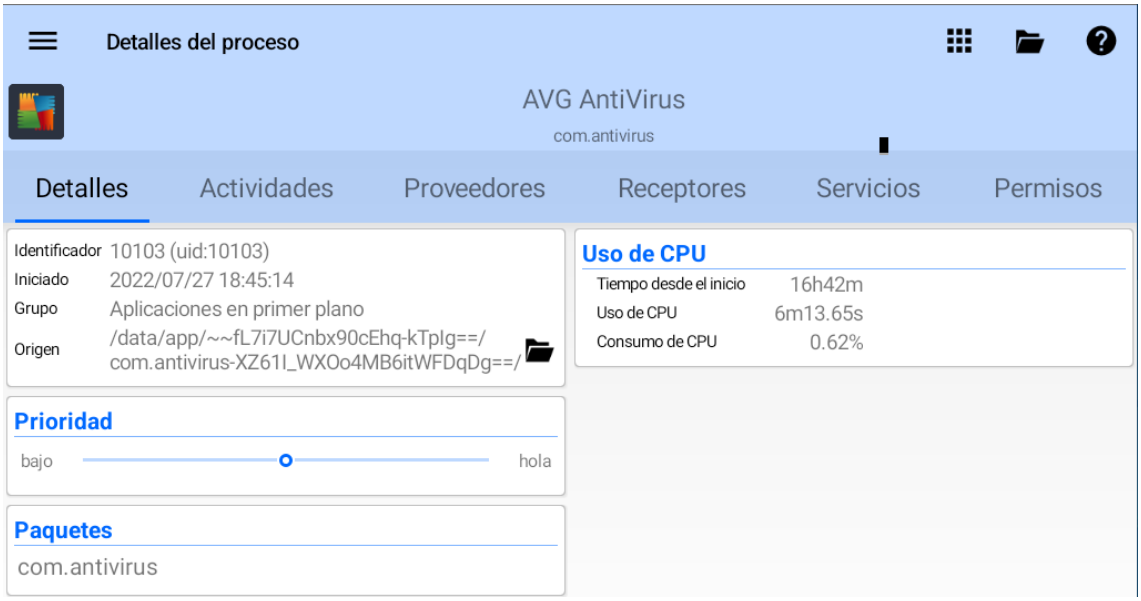



Figura 25. Consumo final de CPU AVG Antivirus Free

### Kaspersky Internet Security

En la Figura 26 se muestra el consumo de los recursos de la CPU en el sistema provocado por la app Kaspersky Internet Security con un consumo inicial de 381,13 MB con un almacenamiento interno de 134,75 MB.


Figura 26. Consumo inicial de RAM de la app Kaspersky Internet Security

En la Figura 27 se muestra el tiempo de uso de CPU generado por la app Kaspersky Internet Security desde su instalación fue 0,31% con un tiempo de uso de 1m10s considerando que no se realizaba aun el test de detección del malware.

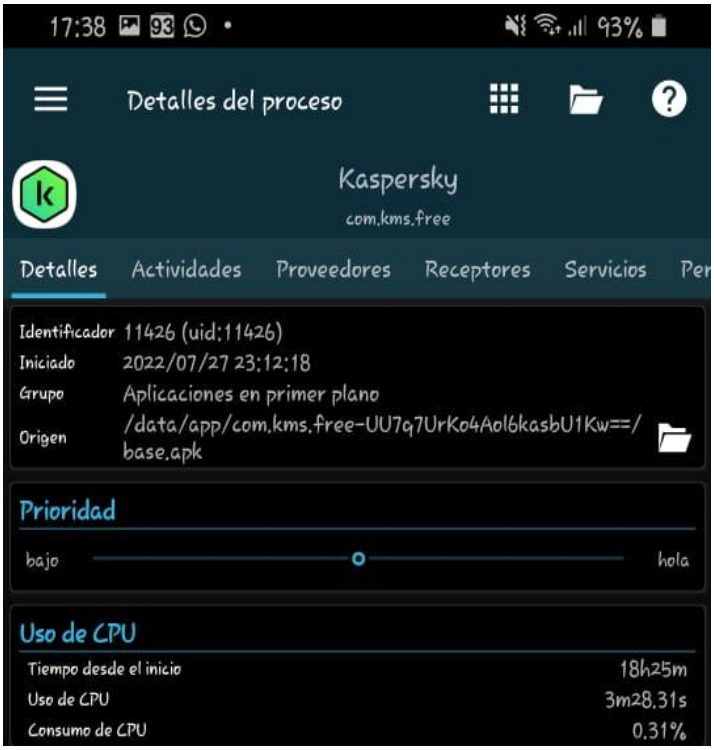



Figura 27. Consumo inicial de CPU KASPERSKY INTERNET SECURITY

En la Figura 28 se muestra que un aumento de 1,09% de un total de 1,40% durante el test realizado con un tiempo de 15m 59s sin dejar de lado la RAM que tuvo un aumento sorprendente.

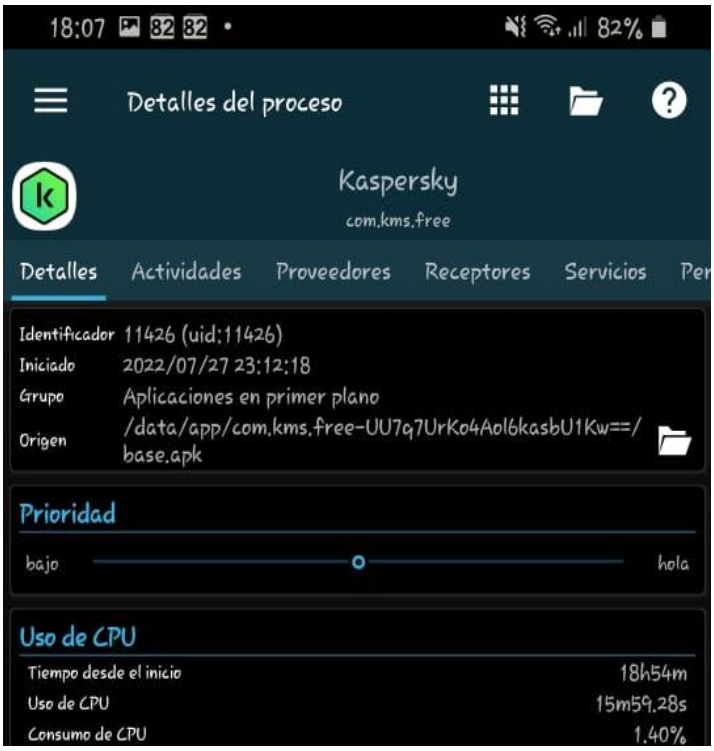



Figura 28. Consumo final de CPU KASPERSKY INTERNET SECURITY

**Bitdefender Mobile Security**

En la Figura 29 se muestra el consumo de recursos en el sistema provocado por la app Bitdefender con un almacenamiento de interno de 84,98 MB y un consumo inicial de RAM 6,87 MB.

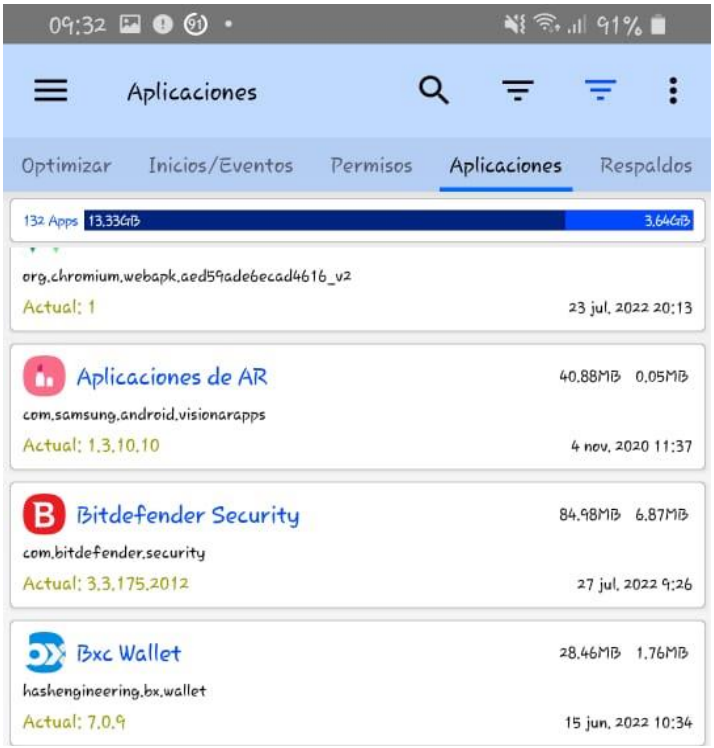



Figura 298. Consumo inicial de la RAM app Bitdefender Mobile Security

En la Figura 30 se muestra el aumento 0,67MB de un total de 7,43MB desde su ejecución inicial, siendo este un incremento bajo que no podría afectar al funcionamiento del dispositivo móvil.

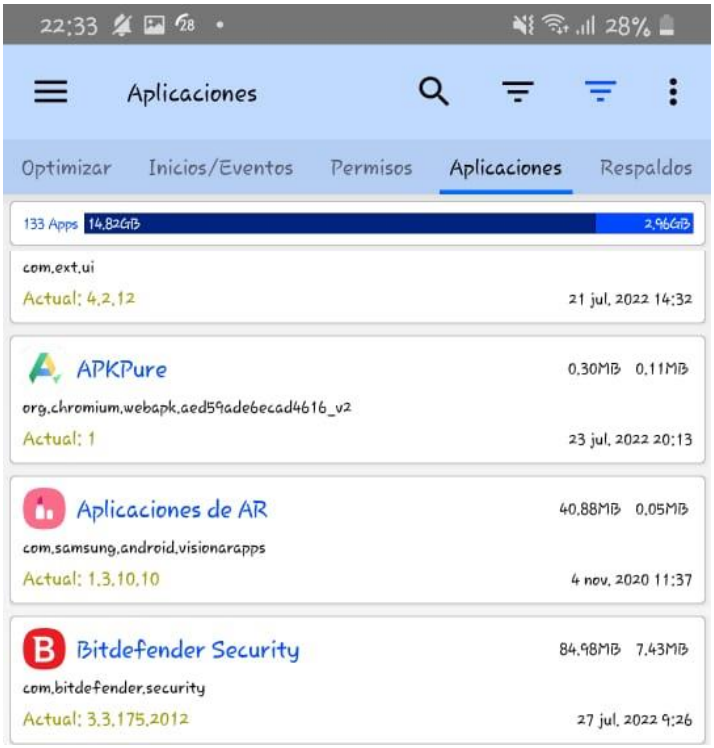



Figura 309. Consumo final de la RAM app Bitdefender Mobile Security

La Figura 31 se muestra el tiempo de uso de CPU generado por la app BITDEFENDER MOBILE SECURITY desde su instalación fue 0,54% con un tiempo de uso de 3m 21s.

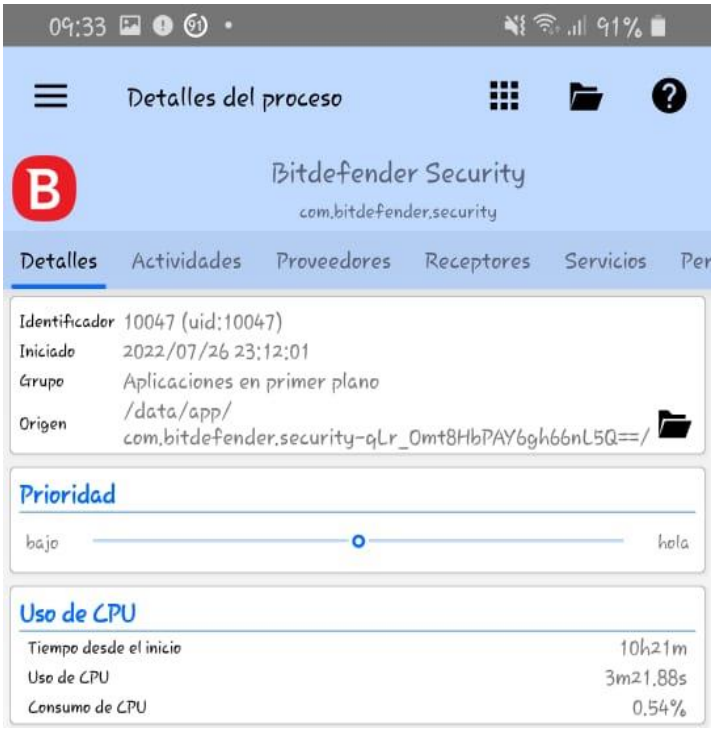



Figura 31. Consumo inicial de CPU app Bitdefender Mobile Security

En la Figura 32 se muestra el aumento de CPU por la app Bitdefender Security con un 1,13% de un total de 1,67% de consumo de durante el test realizado con un tiempo de 23m 28s.

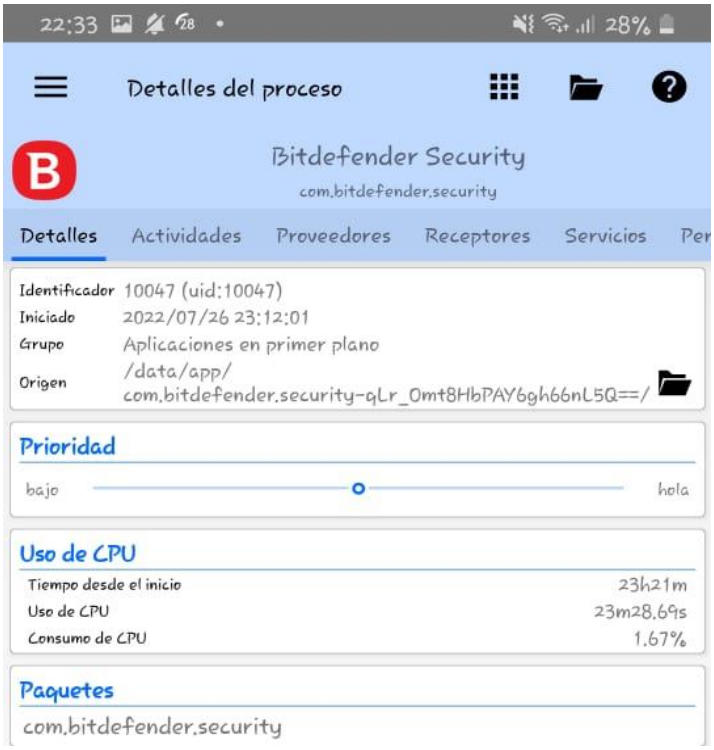


Figura 32. Consumo final de la CPU app Bitdefender Mobile Security

**G Data Mobile Security**

En la Figura 33 se muestra el consumo de recursos en el sistema provocado por la app G Data Mobile Security con un almacenamiento de interno de 34,42 MB y un consumo inicial de RAM 0,77 MB

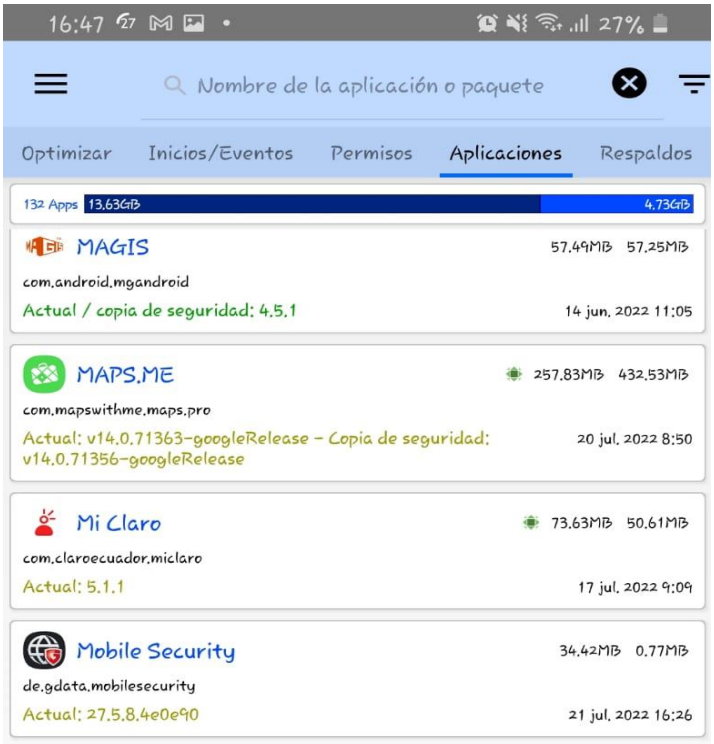



Figura 32. Consumo inicial de RAM G DATA MOBILE SECURITY

En la figura 33 se muestra que durante el tiempo de ejecución para la detección del malware la app aumento el consumo de RAM 1,18MB de un total de 1,95MD utilizado al final del test de detección de malware.

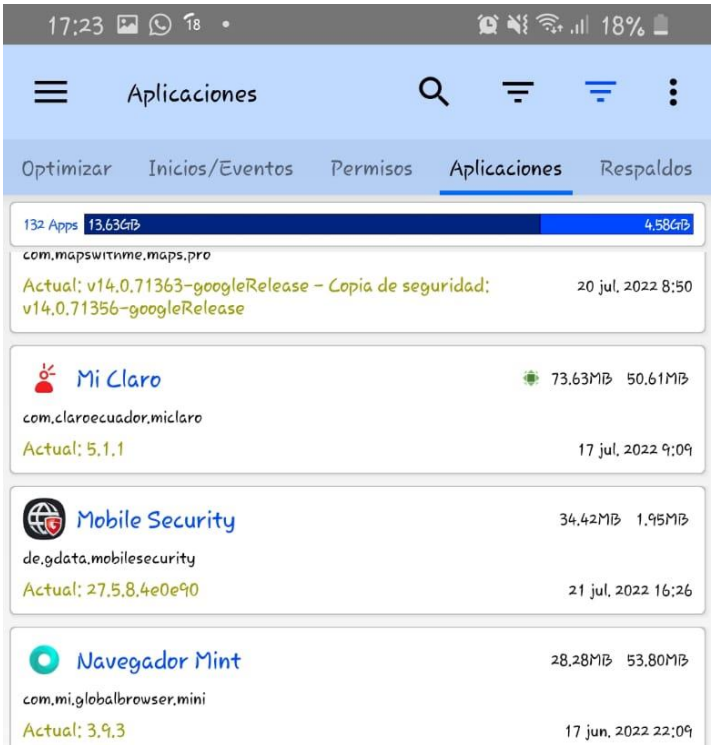



Figura 33. Consumo final de RAM de la app G Data Mobile Security

En la Figura 34 se muestra el tiempo de uso de CPU generado por la app G Data Mobile Security desde su instalación fue de 16m 15s y un consumo de CPU de 1,53% del consumo total.

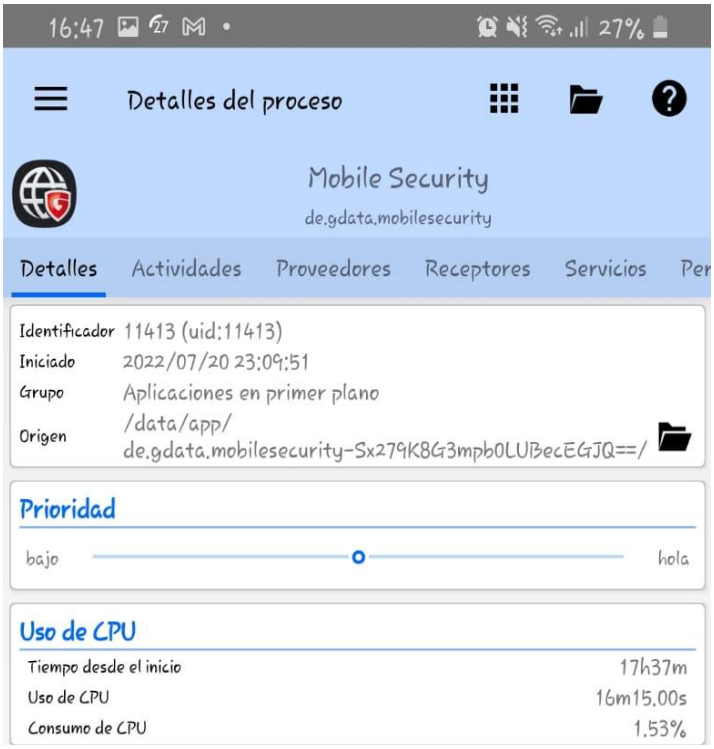



Figura 34. Consumo inicial de CPU de la app G Data Mobile Security

En la Figura 35 se muestra el consumo de CPU provocado por la app Mobile Security durante del proceso de detección de malware el cual fue de 2,33% y en un tiempo de 25m 30s como, siendo un aumento de 0,8% considerado como bajo.

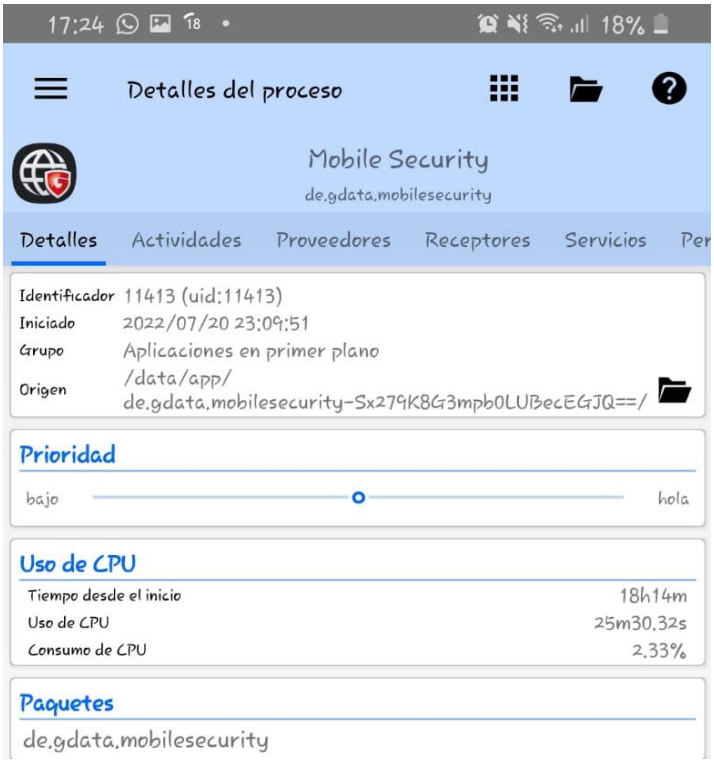



Figura 35. Consumo final de CPU de la app G Data Mobile Security

### Avira Antivirus Security

En la Figura 36 se muestra el consumo inicial del recurso en el sistema provocado por la app Avira Antivirus Security con un almacenamiento interno de 78,05 MB y una RAM ocupada de 12,39MB.

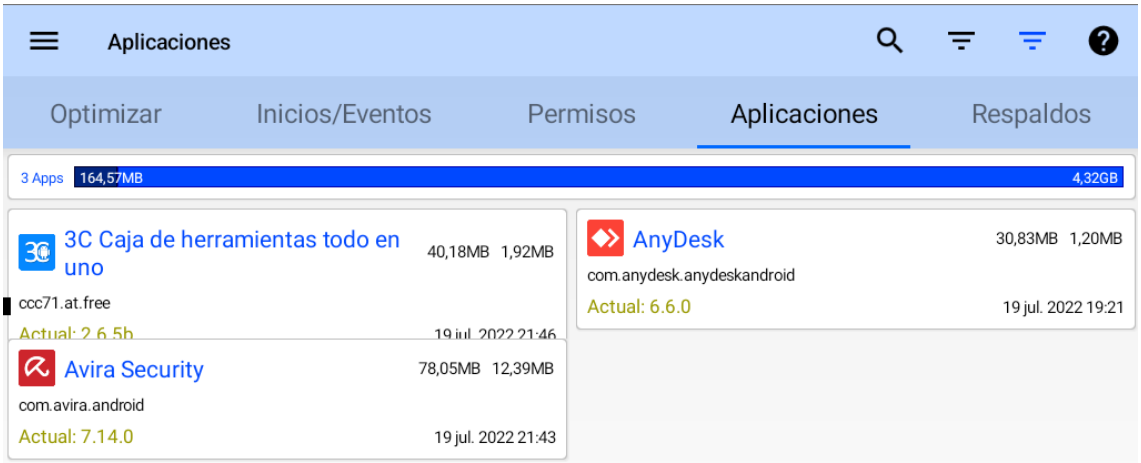



Figura 3610. Consumo inicial de RAM de la app Avira Antivirus Security

En la Figura 37 se muestra la RAM utilizada por la app Avira Security durante el proceso de detección de malware, donde se evidencio que existió un incremento leve de 0,44MB el cual no afecta al funcionamiento del dispositivo móvil.

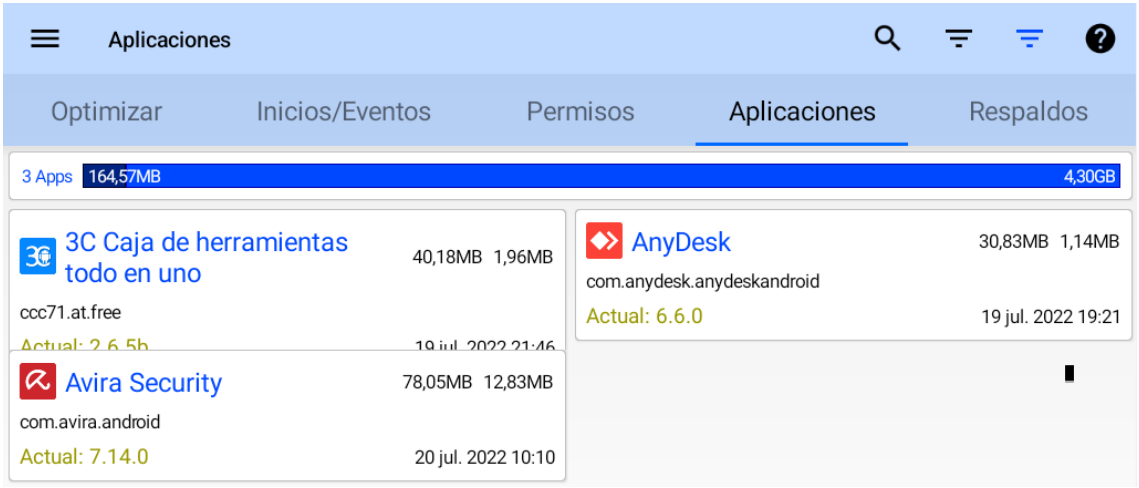



Figura 3711. Consumo final de RAM de la app Avira Antivirus Security

En la Figura 38 se muestra el tiempo de uso de CPU generado por la app Avira Antivirus Security desde su instalación fue 0,43% con un tiempo de uso de 30s durante la ejecución inicial de app.

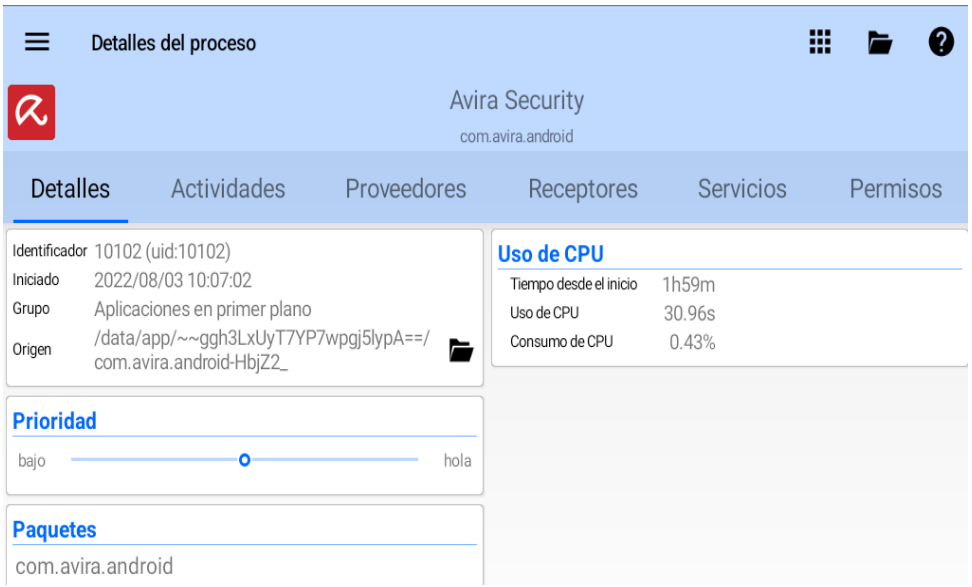


Figura 38. Consumo inicial de CPU app Avira Antivirus Security

En la Figura 39 se muestra el consumo de la CPU en 11,39% con un tiempo de uso de este de 15m 51s durante el test realizado para la detección del malware en android.

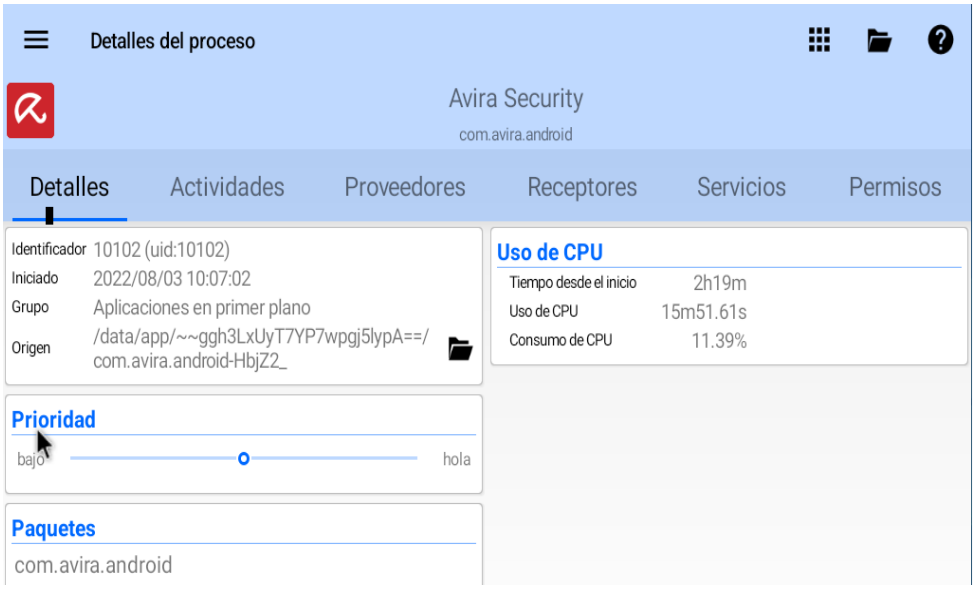



Figura 39. Consumo final de CPU de la app Avira Antivirus Security

**Naver Cloud Line Antivirus**

En la Figura 40 se muestra el consumo de recursos en el sistema provocado por la app Line Antivirus con un almacenamiento de interno de 22,66 MB y un consumo inicial de RAM de 1,41 MB.

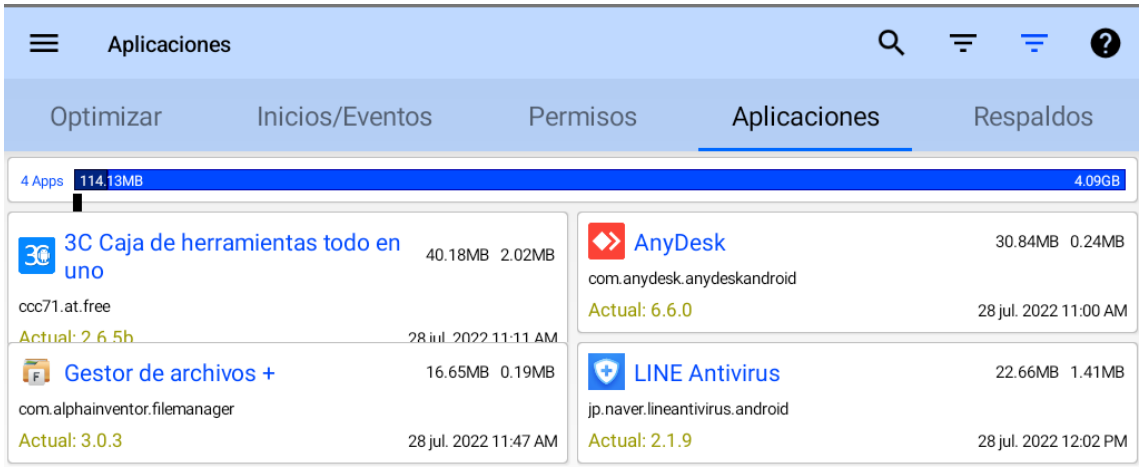


Figura 40. Consumo inicial de CPU de la app Naver Cloud Line Antivirus

En la Figura 41 se muestra la RAM utilizada por la app Naver Cloud Line Antivirus durante el proceso de detección de malware, donde se evidencio que existió un incremento leve de 0,09MB de un total de 1,50MB utilizado por la app, el cual no afecta al funcionamiento del dispositivo móvil.

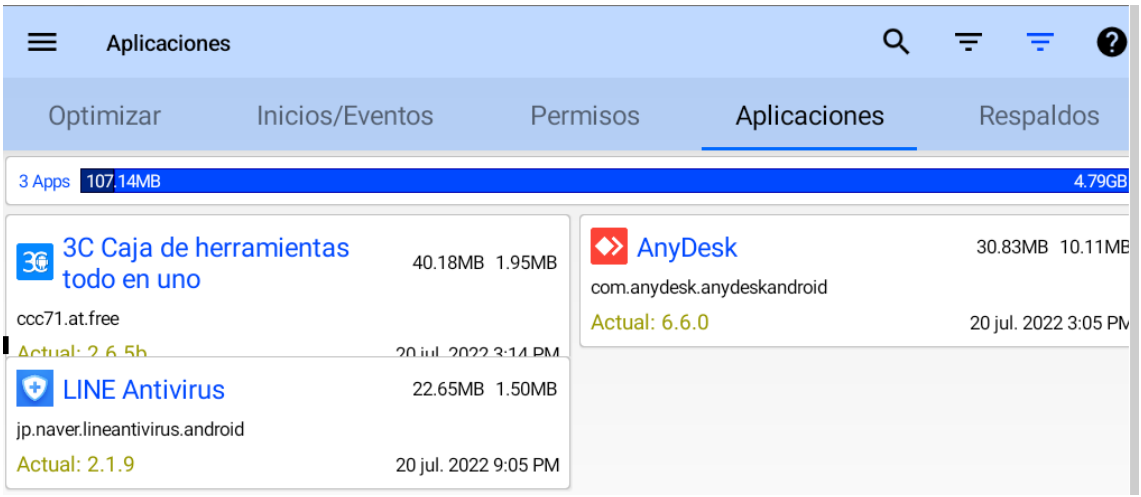



Figura 4112. Consumo final de CPU app Naver Cloud Line Antivirus

En la Figura 42 se muestra el tiempo de uso de CPU generado por la app Naver Cloud Line Antivirus desde su instalación fue 0,24% con un tiempo de uso de 2m 30s.

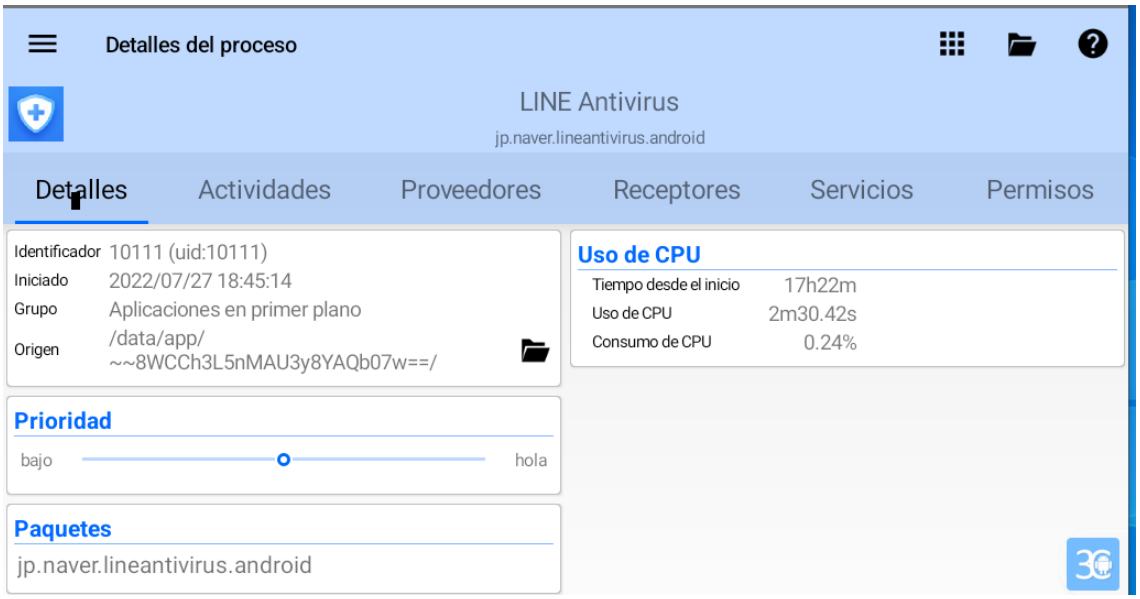


Figura 4213. Consumo de CPU app Naver Cloud Line Antivirus

En la Figura 43 se muestra el aumento de recursos de CPU 0,66% durante el test realizado con un tiempo de 6m58s, donde se puede presumir que es una app antimalware que no ocupa excesivos recursos de CPU.

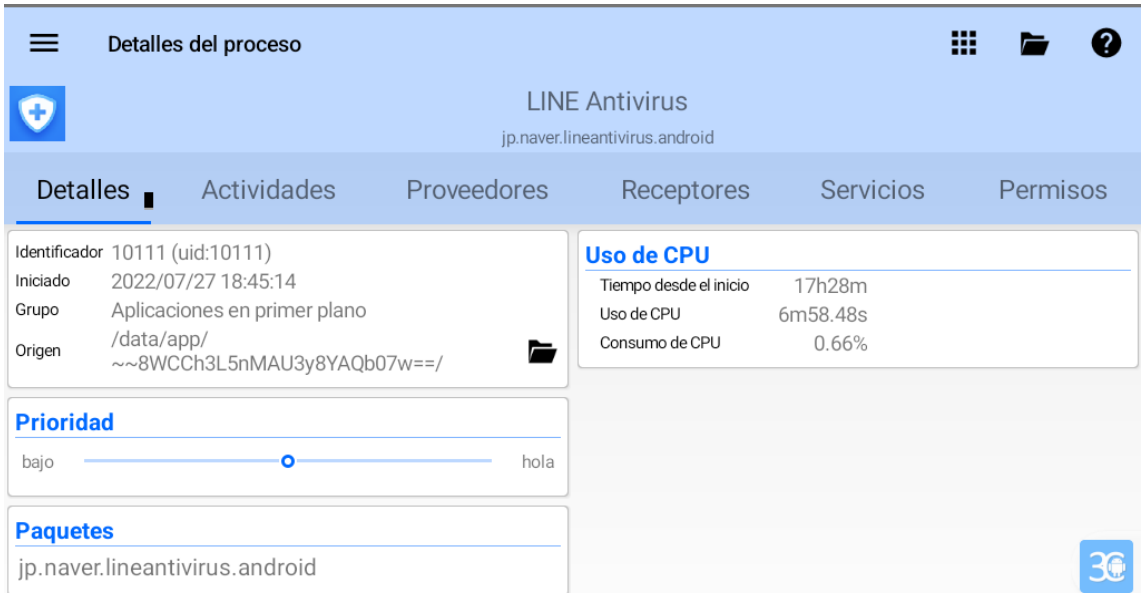



Figura 4314. Consumo final de CPU app Naver Cloud Line Antivirus

### McAfee Security

En la Figura 45 se muestra el consumo de recursos en el sistema provocado por la app McAfee Security con un almacenamiento de interno de 93,24 MB y un consumo inicial de RAM 44,41MB. Es importante mencionar que esta prueba fue realizada en un dispositivo móvil ya que el entorno virtual no lo permitió.

Figura 45. Consumo inicial de RAM de la app McAfee Security

En la Figura 46 se muestra el consumo de la RAM provocado por la app McAfee Security donde se tiene un aumento de 1,11MB de un total ocupado de 45,52MB.

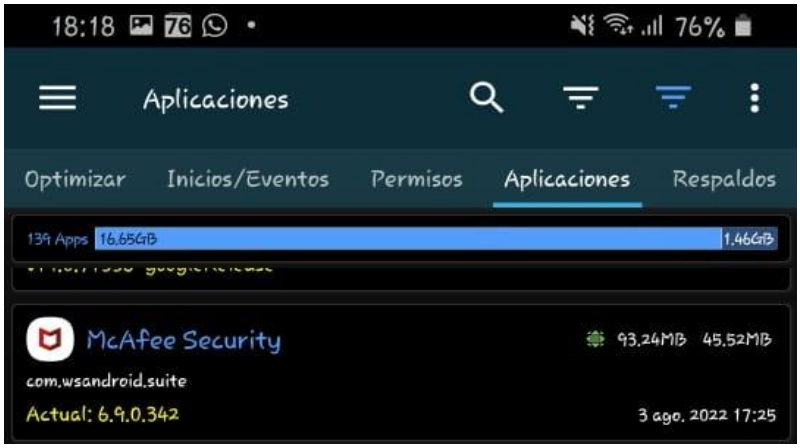



Figura 46. Consumo final de RAM de la app McAfee Security

En la Figura 47 se muestra el tiempo de uso de CPU generado por la app McAffe Security desde su instalación consumiendo 0,16% en un tiempo de 4m 07s.

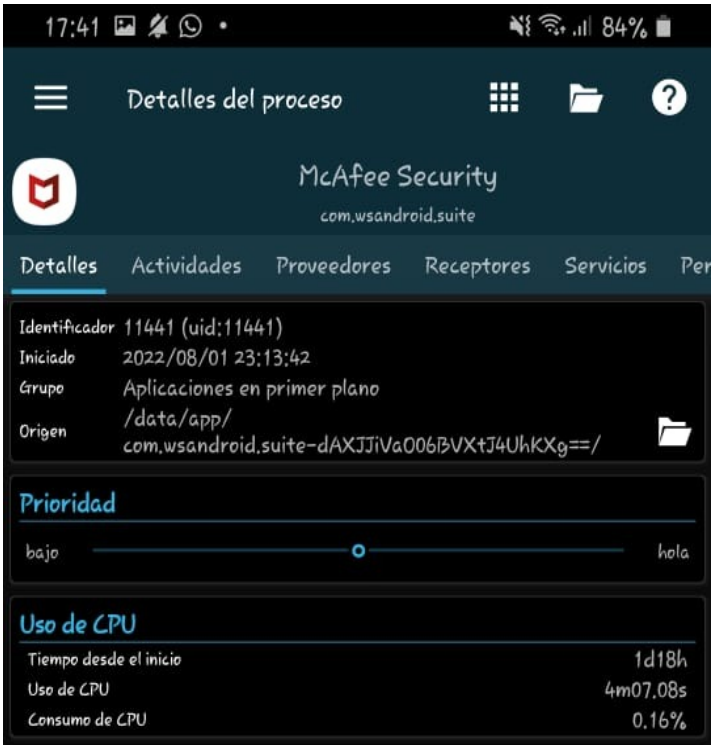


Figura 47. Consumo inicial de CPU de la app McAfee Security

En la Figura 48 se muestra el consumo de CPU  0,81% durante el test realizado con un tiempo de 20m58s como se muestra en la figura, siendo este un consumo bajo el cual no afectaría al funcionamiento del dispositivo móvil.

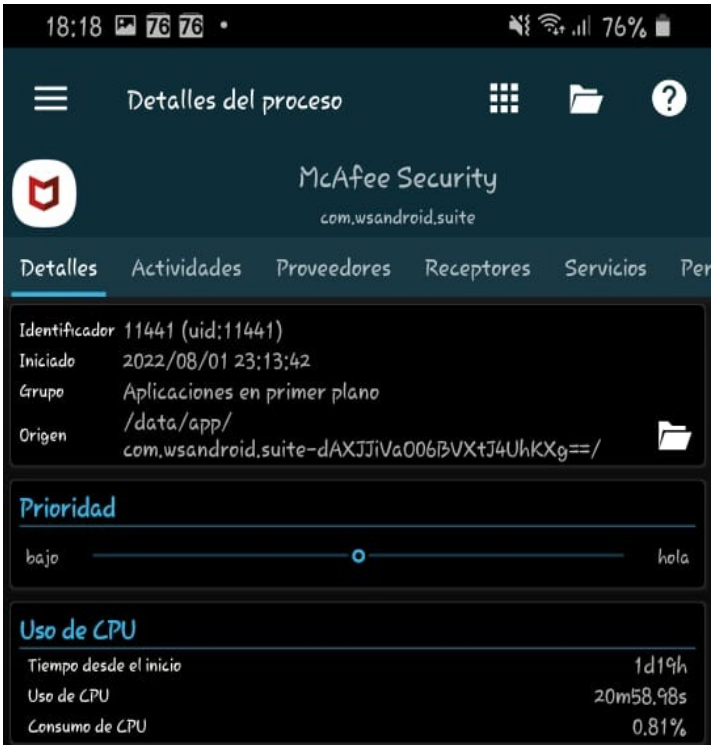



Figura 48. Consumo final de CPU de la app McAfee Security

**Consumo de Batería**

Para determinar el consumo de la batería del smartphone en cuestión se siguen los pasos establecidos en la metodología de análisis del consumo. Cabe indicar que las pruebas realizadas a las herramientas de prevención ya no son en el entorno virtual, ahora se toma un dispositivo móvil para realizar las pruebas de consumo de batería, utilizando una app que sirve para monitorear los procesos en ejecución, el cual se enfoca en el consumo de batería como lo es GsAM Battery Monitor Pro.  El proceso para evaluar las herramientas de prevención consiste en cargar de energía la batería en 100%, luego instalar la app de prevención y obtener los datos del consumo de batería utilizada en su ejecución inicial del dispositivo móvil. Luego se procede a utilizar el smartphone de manera cotidiana hasta alcanzar un 50% de batería para luego obtener la información de cuanta energía a

utilizado la herramienta en cuestión. En este periodo se realizarán dos análisis manuales para detectar malware. A continuación, se presentan los resultados:

**Avast Mobile Security**

En la Figura 49 se observa que el dispositivo móvil ha consumido una batería inicial de 5,3% realizando de entrada un test y después de transcurrir hasta niveles de batería de 90% el dispositivo móvil tiene un consumo total de 7,6 % estando en segundo plano, considerando que el consumo total del dispositivo de 60,7%.


Figura 49. Consumo batería de la app Avast Mobile Security.

**AVG mobile security**

En la Figura 50 se observa que el dispositivo móvil a utilizado un promedio de batería inicial de 61,1% del cual utilizó 2,6% la app AVG mobile security, llegando al nivel de batería de 88% el total de batería ocupada por el dispositivo es de 64,4% y la app AVG Mobile Security a utilizado 6,8 % de ello.

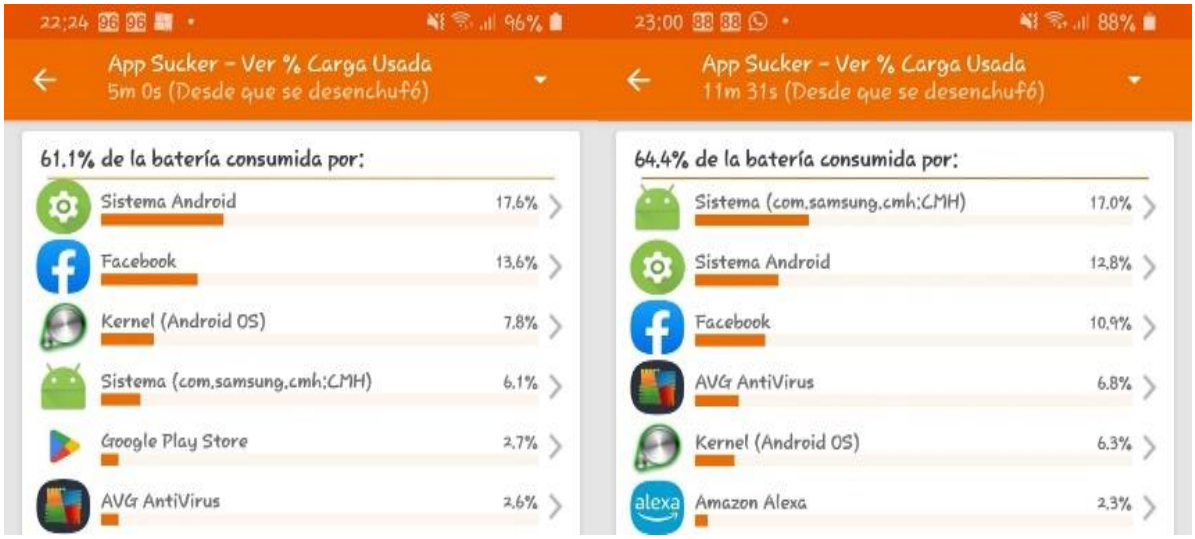


Figura 50. Consumo batería app AVG Mobile Security

**F-Secure Safe**

En la Figura 51 se observa que el dispositivo móvil a utilizado un promedio inicial de batería 61,9 % de los cuales al antimalware F-Secure Mobile Security a utilizado 5,5 %, con el transcurrir de los minutos llega el dispositivo a 90% de niveles de batería donde se empleó un total de 56,9% de los cuales 10,3% es de la app F-Secure SAFE.

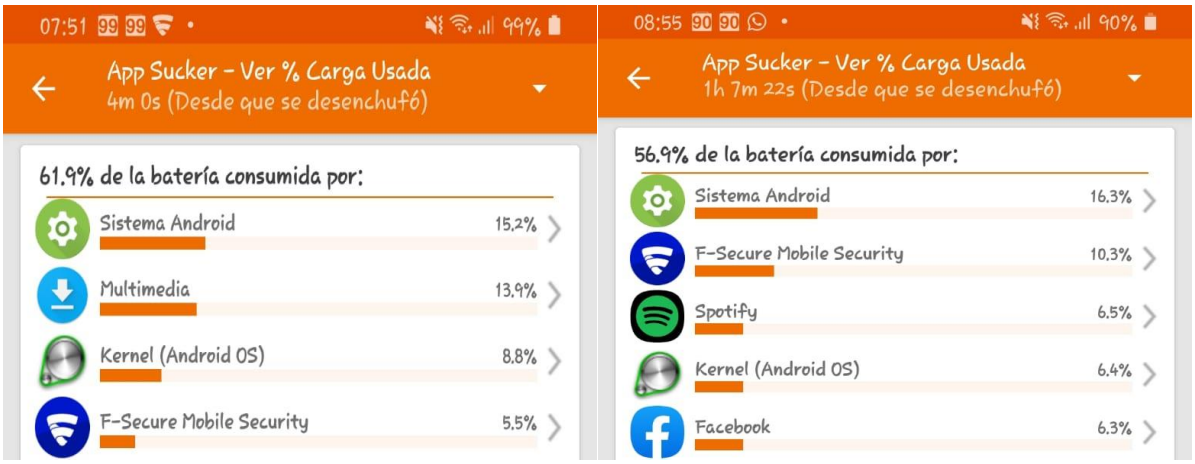



Figura 51. Consumo de batería de la app F-Secure SAFE.

**Avira Antivirus Security**

En la Figura 52 se observa que el dispositivo móvil a utilizado un promedio inicial de batería 62,2 % de los cuales al antimalware Avira Antivirus Security a utilizado 19,1 %, con el transcurrir de los minutos llega el dispositivo a 82% de niveles de batería donde se empleó un total de 71,6% de los cuales 6,5% es de la app disminuyendo desde el arranque del mismo donde realizó un análisis del dispositivo móvil para luego mantenerse en segundo plano donde no utilizo en exceso los recursos de batería.

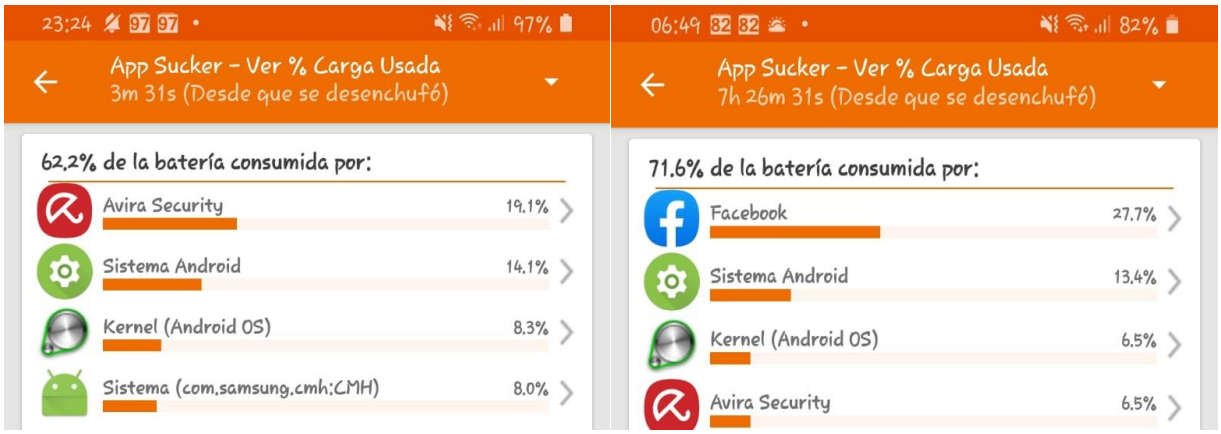



Figura 52. Consumo de batería de la app Avira Antivirus Security.

**Ikarus mobile security**

En la Figura 53 se observa que el dispositivo móvil a utilizado un promedio de batería de 61,3% de los cuales al antimalware Ikarus mobile security a utilizado 3,2% de ello, al llegar el dispositivo a un nivel de batería del 89% la app a consumido 24,8% de un total de 64,9% del consumo total del dispositivo.


Figura 53. Consumo de batería de la app Ikarus Mobile Security.

**SOPHOS INTERCEPT X for Mobile**

En la Figura 54 se observa que el dispositivo móvil a utilizado un promedio de batería de uso de 62,9% de los cuales al antimalware SOPHOS INTERCEPT X for Mobile a utilizado 0,2% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 88% la app a consumido 39,3% de un total de 78,7% del consumo total del dispositivo.

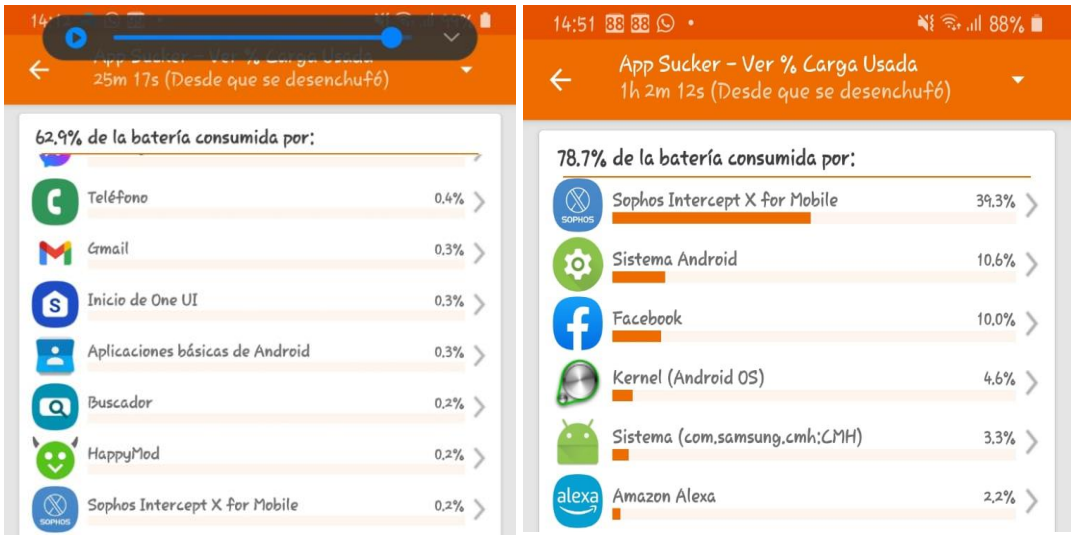



Figura 54. Consumo de batería de la app Sophos Intercept X for Mobile

**Bitdefender Mobile Security**

En la figura 55 se observa que el dispositivo móvil a utilizado un promedio de batería de uso de 65,8% de los cuales el antimalware Bitdefender Mobile Security a utilizado 2,1% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 88% la app a consumido 0,6% de un total de 64% del consumo total del dispositivo, esto podría ser causa de que la app no está realizando ningún proceso que incida en el consumo de la batería.

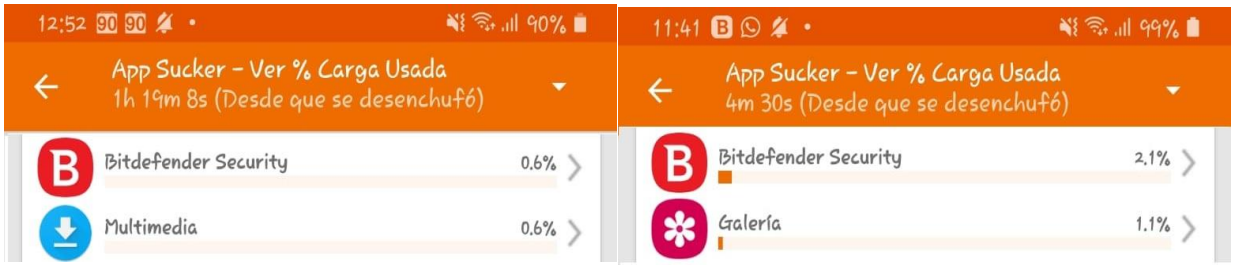



Figura 55. Consumo de batería de la app Bitdefender Mobile Security

**McAfee Security**

En la figura 56 se observa que el dispositivo móvil a utilizado un promedio de batería de uso de 62,3% de los cuales el antimalware McAfee Security a utilizado 5,5% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 76% la app a consumido 6,3% de un total de 61,4% del consumo total del dispositivo, esto puede indicar que la app no está realizando ningún proceso que incida en el consumo de la batería.

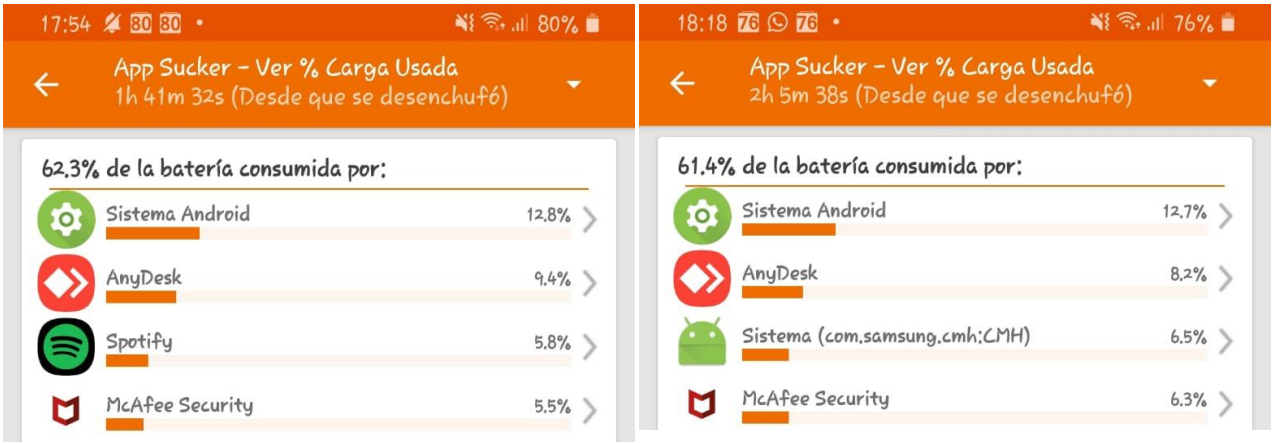



Figura 5615. Consumo de batería de la app McAfee Security

**Naver Cloud Line Antivirus**

En la figura 57 se observa que el dispositivo móvil a utilizado un promedio de batería de 53,4% de los cuales el antimalware Naver Cloud Line Antivirus a utilizado 0,3% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 89% la app a consumido 1,7% de un total de 56,5% del consumo total del dispositivo, este consumo bajo puede ser porque la app no está realizando ningún proceso que incida en el consumo de la batería.

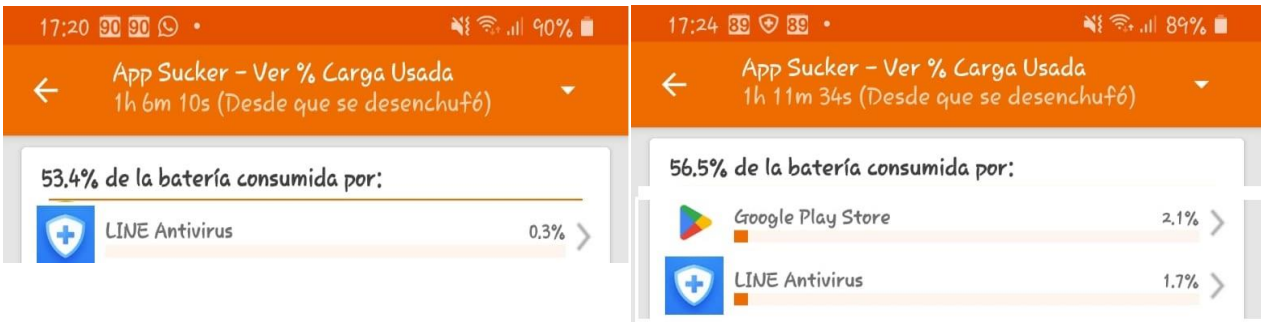



Figura 57. Consumo de batería de la app Naver Cloud Line Antivirus

**Kaspersky Security**

En la figura 58 se observa que el dispositivo móvil a utilizado un promedio de batería de uso de 67,1% de los cuales al antimalware Kaspersky Security utilizado es 1,3% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 83% la app a consumido 0,7% de un total de 68,1% del consumo total del dispositivo, esto podría ser causa de que la app no está realizando ningún proceso que incida en el consumo de la batería ya que su consuno en segundo plano disminuyo.

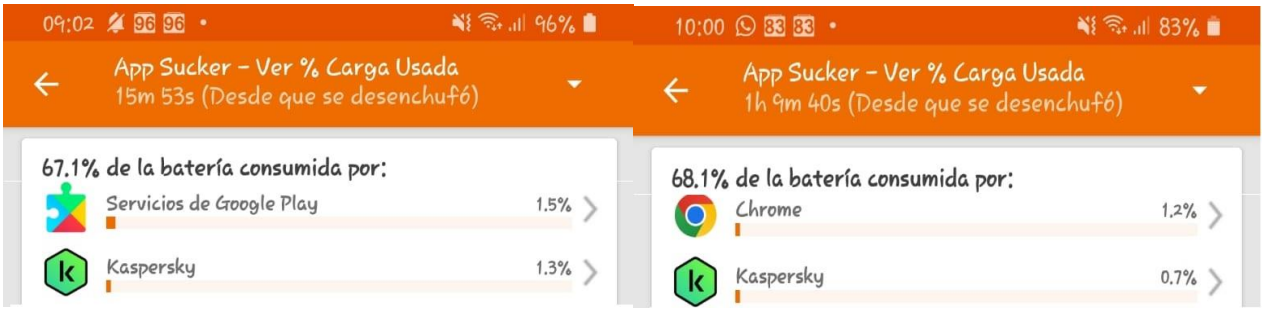



Figura 58. Consumo de batería de la app Kaspersky Security

**AhnLab V3 Mobile Security**

En la Figura 59 se observa que el dispositivo móvil a utilizado un promedio de batería de 58,8% de los cuales la app AhnLab V3 Mobile Security a utilizado 10,7% desde que fue instalado, al llegar el dispositivo a un nivel de batería del 89% la app a consumido 2,6% de un total de 61% del consumo total del dispositivo, de tal manera que existió una frecuencia a baja de consumo con el transcurso de los minutos.

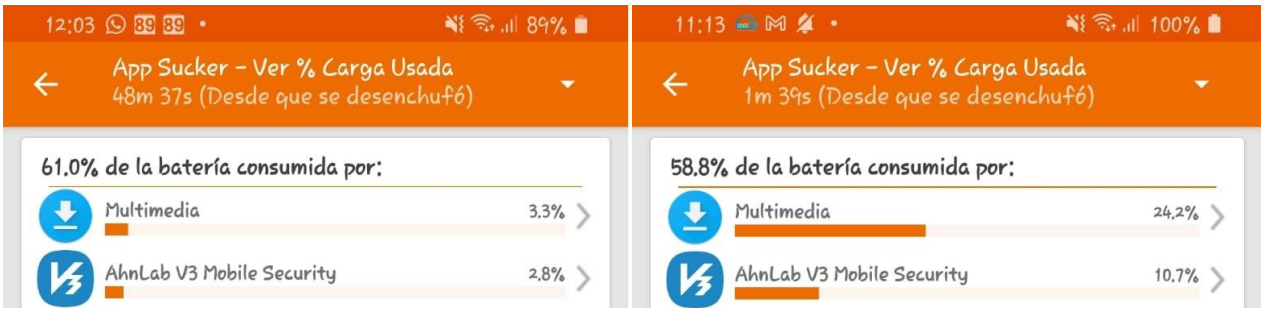



Figura 59. Consumo de batería de la app AhnLab V3 Mobile Security

**Resumen de Evaluación Rendimiento y Consumo de Batería**

En conclusión, se presenta en la tabla la información que reúne todo lo obtenido de las pruebas realizadas a las herramientas de prevención seleccionadas, las cuales se enfocaron en dos aspectos, uno de ellos el rendimiento y el otro el consumo de la batería.

**Consumo máximo de CPU**

Lo obtenido del test realizado a las herramientas de prevención se puedo evidenciar que Avira Security con una tasa de 11,92 % de consumo de la CPU, seguido de Avast Mobile Security con 9,03, seguido Sophos Intercept for Mobile con 7,93% sin dejar de lado a F-Secure Mobile Security consumió 4,64% y G Data Security con 2,33 que al no identificar las muestra en tiempo real su análisis manual gestionó la detección con un consumo bajo de recursos de la CPU. Kaspersky Security, AhnLab V3 y Bitdefender están en un rango de consumo de 1,77% a 1,40%, además se observa en la imagen 40 entre 0,92% y 0,81% están dos apps que el consumo fue bajo en comparación a otras soluciones como lo es Ikarus mobile security y McAfee, pero la que se lleva la fase de óptimo consumo considerando uno de los bajo es Line Antivirus con 0,66%, acompañado de 0,62% de AVG Mobile security como la app con más ahorro de recursos de CPU desde la instalación durante el proceso de detección de las muestras de malware.

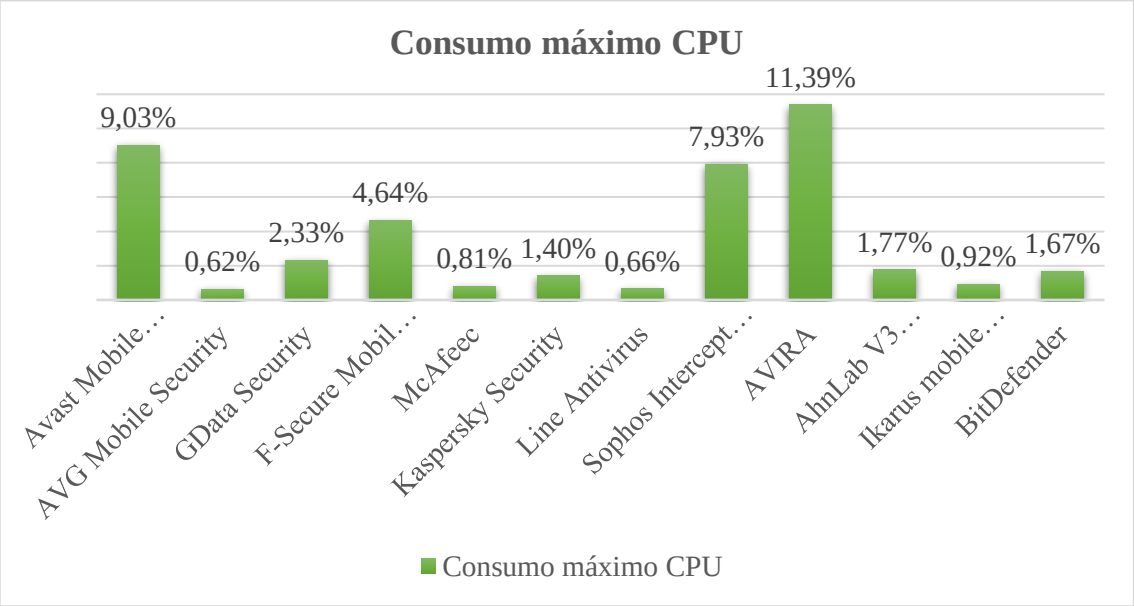



Figura 6016. Consumo máximo CPU

**Consumo máximo de memoria**

A diferencia de los resultados presentados con anterioridad sobre el consumo de CPU según la figura 39 la herramienta de prevención Kaspersky Security tiene un consumo de memoria RAM del 381MB siendo el más alto desde su instalación hasta el proceso de detección de malware, sin embargo, hay que recalcar que esta app realizó un análisis

automático de detección de malware en el smartphone. Seguido de F-Secure Mobile Security con un 31,11 % de consumo de Memoria RAM esto es debido a que esta app realizó un análisis de detección de malware en el entorno virtual controlado por esa razón puede ser que tenga ese excesivo consumo de memoria RAM. Además, se puede observar en la tabla que Avast Mobile Security, Mobile Security, McAfee Mobile Security y Kaspersky Security oscilan entre el 5 y el 3.92% de consumo de batería del dispositivo móvil. La app de prevención contra los malware que consume poca memoria RAM en su proceso de ejecución de Android en G Data Mobile Security quien en momento de la ejecución solo ocupo el 0,61% del consumo total de batería.

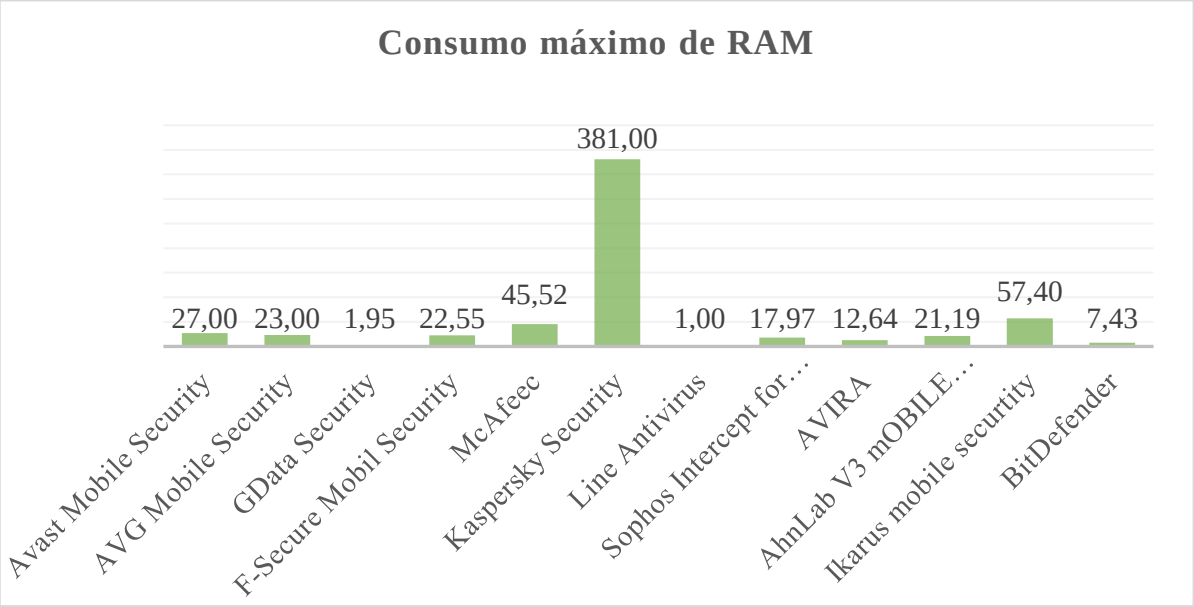



Figura 6117. Consumo máximo RAM

**Consumo máximo de batería**

El consumo de la batería por parte de las herramientas de prevención en general ha sido baja, en comparación a estudios anteriores. Los resultados presentados indican que las herramientas de prevención evaluadas pueden ser usadas en dispositivos móviles de gama baja, media y alta. La solución que más batería utilizo es F-Secure Mobile Security con un porcentaje de 3,8% seguido de Mobile Security con un porcentaje de 2,0% y GData

Mobile Security quien ocupó el tercer lugar de la lista con un consumo de batería de 1,9%. La solución que obtuvo un consumo bajo es McAfee con 0,8% del consumo de la batería.

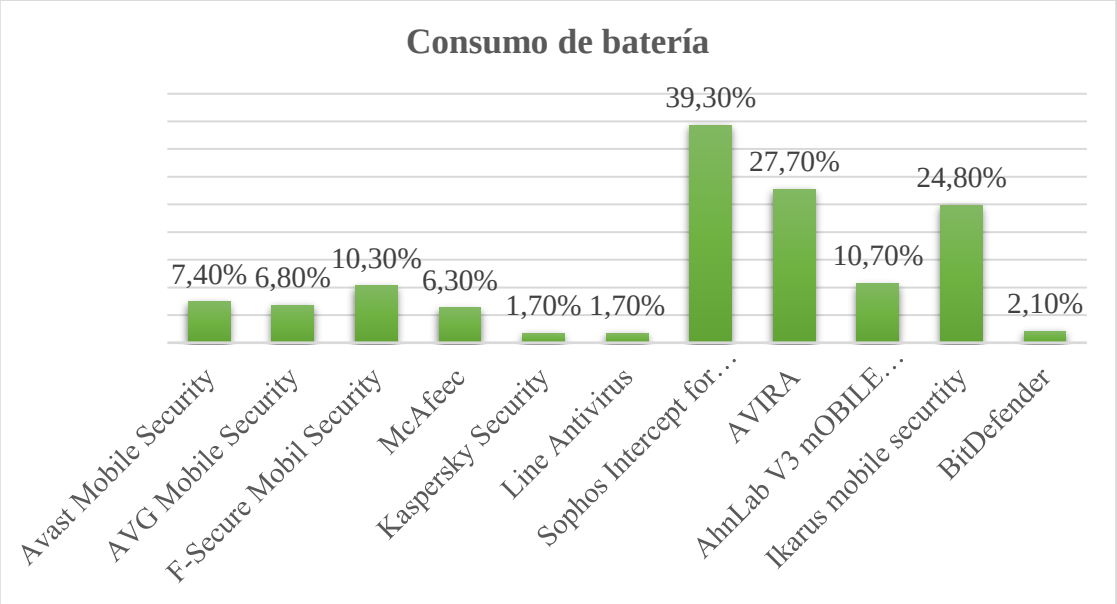



Figura 62. Consumo de batería

**Resumen del test a las herramientas de prevención. metodología de Efectividad y Rendimiento.**

| Resultados test de Efectividad y Rendimiento | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Herramientas de Prevención** | **Avast** | **AVG** | **AVIRA** | **Bitdefender** | **F-Secure** | **G Data** | **Kaspersky Lab** | **McAfee Mobile Security** | **AhnLab V3 MOBILE Security** | **Line Antivirus** | **Sophos Intercept X for Mobile** | **Ikarus Mobile Security 2.0** |
| **Detección tiempo real** | si | si | no | no | no | no | no | no | no | no | si | no |
| **Detección manual** | si | si | si | no | si | si | si | si | si | si | si | si |
| **Cantidad malware** | 31 | 31 | 31 | 0 | 29 | 33 | 33 | 40 | 29 | 38 | 32 | 40 |
| **Porcentaje de detección** | 78,0% | 78,0% | 77,5% | 0,0% | 73,0% | 82,5% | 80,0% | 100,0% | 72,5% | 95,0% | 80,0% | 100,0% |
| **Consumo máximo CPU** | 9,03% | 0,62% | 11,39% | 1,67% | 4,64% | 2,33% | 1,40% | 0,81% | 1,77% | 0,66% | 7,93% | 0,92% |
| **Consumo mínimo CPU** | 4,87% | 0,11% | 0,43% | 0,54% | 0,35% | 1,53% | 0,31% | 0,16% | 0,27% | 0,24% | 7,85% | 0,21% |
| **Consumo máximo RAM** | 27,46 | 23,26 | 12,83 | 7,43 | 22,55% | 1,95 | 381,13 | 45,52 | 21,19 | 1,5 | 17,97 | 57,4 |
| **Consumo mínimo RAM** | 25,38 | 20,53 | 12,39 | 6,87 | 21,97% | 0,77 | | 44,41 | 20,01 | 1,41 | 17,95 | 57,36 |
| **Consumo máximo Batería** | 7,60% | 6,80% | 19,10% | 0,60% | 10,30% | | 1,30% | 6,30% | 10,70% | 1,70% | 39,30% | 24,80% |
| **Consumo mínimo Batería** | 5,30% | 2,60% | 6,50% | 2,10% | 5,50% | | 0,70% | 5,50% | 2,80% | 0,30% | 0,20% | 3,20% |

## 2.6. DISCUSIÓN

En los resultados del estudio de caso se puede apreciar que los antimalware tienen un consumo de CPU, RAM y batería bajos en comparación a la investigación de Villanova [2], donde sus herramientas de prevención seleccionadas tienen gran impacto sobre los recursos físicos del dispositivo móvil esto podría darse por las características y versión de Android que utilizó, por otro lado se evidencia que los malware seleccionados coinciden y aún están entre los primeros por su tasa de efectividad y funcionalidad.

El desarrollo del sistema operativo Android a lo largo del tiempo ha sacado a la luz muchas vulnerabilidades a los cuales los usuarios están expuesto y es que sin duda el alto nivel de contagio de malware en gran parte se debe al uso de aplicaciones gratuitas y sitios no seguros, como lo muestra el estudio realizado en Bangladés por Hossain y otros [1]. Ante esta situación, Pianchiche [5], en su investigación muestra cómo hallar información sobre este tipo de afectaciones delimitando la búsqueda o enfocándose en el análisis de la versión de Android 12, también muestra la utilización de una máquina virtual donde realizar las pruebas, cabe recalcar que este modelo es un medio accesible y práctico y muy real que puede ser usado en presentes y futuras investigaciones.

Por último, es inevitable en algún momento ser víctima de los cibercriminales o de un malware para ello se debe tomar algunas acciones de prevención, en la investigación de Zambrano [37], sobre *"Técnicas de Análisis de Malware en dispositivos móviles basados en Android"* menciona sobre la implementación de un método para la detección y la búsqueda de los malware el cual fue de gran ayuda para confirmar la validez del software maliciosos utilizando app sitios web que detentan las muestras de los malware antes de ser instaladas. Sumado a estas acciones se considera indispensable el uso de material informativo, por esta razón se aprueba y replica la iniciativa de Sánchez [38], de brindar recomendaciones tecnológicas preventivas sobre ciberseguridad ya que la educación es una de herramienta útil en esta problemática y es evidente el desconocimiento que existe del tema.

## 2.7. CONCLUSIONES

Queda claro que Android es una plataforma para teléfonos inteligentes que ha revolucionado el mercado tecnológico en cuanto a software se refiere, no solo por sus aplicaciones sino también por sus niveles de seguridad y adaptabilidad, sin dejar de lado el concepto de ser un software libre para que desarrolladores e investigadores realicen cambios al código fuente con el fin de petrolizarlos o con fines educativos. Android 12 sin duda ha sido un sistema operativo que desde su aparición en el 2021 no ha tenido tantas incidencias de vulnerabilidades como las otras versiones, según el sitio web CVE details en el 2021 tuvo un total de 84 incidencias de vulnerabilidades y en lo que va del 2022 solo 187 lo que demuestra que a medida que va pasando el tiempo de operatividad del sistema operativo su seguridad va decayendo, lo que obliga a los clientes finales a actualizar la versión y en muchos casos adquirir dispositivos de mejores características con el objetivo de estar protegidos.

Se menciona que la selección de antimalware fue en base a información recolectada del Instituto Independiente de seguridad AV-Test, dicho laboratorio indica que de un total de 21 antimalware analizados se encontró que solo 4 de ellos detectaron el malware con una taza de acierto de 93%, frente al 86% de detección del restante de antimalware, a diferencia de esta investigación donde los resultados demostraron una taza de detección de 100% y un 73% en base al antimalware que menos incidencias detectó, lo que evidencia que cada una de estas herramientas de prevención tiene sus pro y sus contra frente a la detección de malware en su entorno virtual. Además, se llegó a la conclusión que no todos los antimalware tienen licencia gratuita lo que podría limitar su compra ya que algunos solicitan la suscripción donde se tiene que ingresar los números de la tarjeta de débito y crédito.

La selección de malwares utilizados en el estudio de caso fue gracias al sitio web virusshare.com donde se tiene un repositorio de malware para ser descargados y poder realizar pruebas, las cuales son efectivas por la veracidad en los resultados, además se puede culminar indicando que no existe otro sitio web que gestione archivos con malware para su uso investigativo. Los malware utilizados fueron en su gran mayoría detectados por herramientas de prevención corroborando la efectividad de contenido

malicioso en dichas muestras, siendo este sitio web una referencia para futuras investigaciones sobre código malicioso en la plataforma Android.

La utilización de un entorno virtual controlado es la mejor forma de realizar pruebas con malware por el hecho que se puede simular el comportamiento real de estas amenazas sin afectar al dispositivo. Se puede indicar además que existen ciertos métodos para realizar pruebas con malware donde utilizan el emulador de Android, pero en esta investigación no fue de gran ayuda por el pésimo funcionamiento que tiene sobre el pc quien tiene recursos solicitados para el correcto funcionamiento del emulador. Se considera que el mejor método para la detección de malware en montar una máquina virtual con la versión de Android.

Es necesario plantear algunas recomendaciones en base a los resultados obtenidos de las pruebas realizadas a los antimalware, la cual es un aporte para los clientes de la plataforma Android 12. La información que se obtuvo del test mostró la efectividad frente a la detección del malware como también la información sobre sus ventajas y desventajas.

# 3. PROPUESTA DE INTERVENCIÓN

## 3.1. Titulo

Recomendaciones de buenas prácticas en seguridad móvil para prevenir la propagación del malware en lo dispositivos móviles con plataformas Android.

## 3.2. Descripción

Desarrollar recomendaciones sobre buenas prácticas tecnológicas que permitan a los usuarios prevenir la propagación de malware en los smartphones, también conocidos como dispositivos inteligentes, con el objetivo que personas naturales con los conceptos básicos sobre Android puedan hacer frente a esta problemática que afecta al mundo.

**Recomendaciones tecnológicas de prevención**

- Antes de realizar una instalación de alguna app es importante identificar el sitio web donde se va a descargar. Es recomendable utilizar tiendas de aplicaciones conocidas como Google Play Store, Amazon Appstore y ApkMirror. Además, de estos sitios o tiendas online también pueden descargarse aplicaciones de páginas web oficiales, como por ejemplo Sony Mobile o Samsung las cuales son marcas reconocidas a nivel mundial por la variedad de productos tecnológicos que oferta.
- Es importante identificar el origen de la app, verificando siempre los comentarios cibernautas, la calificación que dan a la aplicación después descarga en Google Play store.
- Es recomendable realizar un scanner por el sitio web www.virustotal.com que permiten evidenciar si el sitio web es seguro y la app también. Este sitio web permite realizar un análisis de la URL en aproximadamente 55 antivirus diferentes generando así reportes que ayudan al usuario a decidir si bien sigue con la idea de descarga e instalación de la app. Una vez analizado la app se podrá instalar en caso de no poseer código malicioso. Además, existe una app virus total Mobile en caso de querer descargar desde la play store.
- Para evitar el pago por una app es recomendable observar el tamaño del archivo referente a la tienda de aplicaciones de la play store de Google con el objetivo de comparar con el sitio web donde se vaya a descargar la app, porque esto puede determinar si este archivo podría contener código malicioso o no.
- Es importante identificar a la hora de instalar o actualizar una aplicación en el sistema Android los permisos que las aplicaciones en muchos de los casos solicitan a usuario para su ejecución. Existen aplicaciones que solicitan muchos permisos, aquellas apps son las que más conflictos provocan en los dispositivos móviles, causando un inadecuado funcionamiento en el rendimiento físico. Es importante que el usuario de plantee esta pregunta, ¿Qué puede a ser esta app por mí? En caso de no dar respuesta a esa pregunta es mejor dejarla pasar y no instalarla.
- Es recomendable utilizar una herramienta de prevención como las evaluadas en apartados anteriores como Avast Mobile Security, AVG Mobile Security,

GData Mobile Security, F-Secure Mobile, Mobile Secure de la compañía Bitdefender, McAfee Mobile Security y Kaspersky quienes son antimalware que pasaron las pruebas realizadas en el entorno virtual con una tasa de detección entre 88% y 100% de acierto de detección de malware.

- Es necesario que las aplicaciones y el sistema operativo de Android estén debidamente actualizados.
- Realiza copias de seguridad del smartphone de esta manera cuidaremos de la información personal en caso de robo o pérdida del equipo.
- No desactivar la opción de orígenes desconocidos en nuestro smartphone.

Hay que puntualizar que se recomienda actualizar la última versión de Android (cosa que no siempre es posible, porque existen mucha fragmentación) e instalarse las apps siempre desde el Play Store, algo que no todo el mundo hace. Además, de no rootear el dispositivo ya que entonces el modelo de seguridad implementado queda seriamente comprometido.

## 5. REFERENCIAS BILIOGRÁFICAS


[1] FH Shezan, SF Afroze y A. Iqbal, "Detección de vulnerabilidades en aplicaciones recientes de Android: un estudio empírico", Conferencia internacional sobre redes, sistemas y seguridad (NSysS) de 2017 , Dhaka, Bangladesh, 2017, págs. 55 a 63, doi: 10.1109/NSysS.2017.7885802..

[2] P. O. Villanova, «"Malware en Android y medidas de prevención",» 27 enero 2016. [En línea]. Available: https://reunir.unir.net/bitstream/handle/123456789/3622/VILLANOVA%20PASCUAL%2c%20OSCAR.pdf?sequence=1&isAllowed=y. [Último acceso: 27 enero 2022].

[3] A. Sanchéz Magraner, «Vulnerabilidades y malware en dispositivos móviles,» 8 enero 2017. [En línea]. Available: http://hdl.handle.net/10609/60607. [Último acceso: 4 Agosto 2022].

[4] R. J. Zambrano Baron, «Técnicas de análisis de Malware en dispositivos móviles basados en Android,» 2012. [En línea]. Available: http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0697_ZambranoBaronRJ.pdf. [Último acceso: 4 Agosto 2022].

[5] J. . N. Pianchiche Largo, «Análisis de las vulnerabilidades en dispositivos móviles con sistema operativo Android,» *Repositorio Digital PUCESE*, p. 178, 14 Mayo 2019.

[6] L. C. Daza, Artist, *Aplicación móvil para androide del sistema virtual de gestión académica de la Corporación Universitaria Acdventista*. [Art]. Corporación Universitaria Adventista, 2015.

[7] T. J. Gironés, El Gran libro de Androide, 7.ª ed., Bogotá: Alfaomega, 2019, p. 551.

[8] F. Laricchia, «Statista,» 16 noviembre 2022. [En línea]. Available: https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/. [Último acceso: 26 diciembre 2022].

[9] Statcounter, «Cuota de mercado de sistemas operativos móviles en todo el mundo,» Marzo 2022. [En línea]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide. [Último acceso: 5 Agosto 2022].

[10] Statcounter, «Mobile Operating System Market Share Ecuador,» Marzo 2022. [En línea]. Available: https://gs.statcounter.com/os-market-share/mobile/ecuador. [Último acceso: 26 diciembre 2022].

[11] ESET Segurity Report, «Segurity Report Latinoamerica 2021 "INTRODUCCIÓN CONCLUSIONES HALLAZGOS CIBERSEGURIDAD EN TIEMPOS DE PANDEMIA PREOCUPACIONES INCIDENTES CONTROLES"4rtg,» 2021.

[12] J. D. Luján Castillo, Desarrollo de aplicaciones android con android studio, Ciudad de México, 2019, p. 280.

[13] M. López Michelone, «La historia de android,» 23 Septiembre 2013. [En línea]. Available: https://www.unocero.com/noticias/gadgets/smartphones/android/la-historia-de-android/. [Último acceso: 10 Agosto 2022].

[14] C. Collado, «Versiones de Android: de la primera a la última versión de Android,» 16 enero 2023. [En línea]. Available: https://andro4all.com/android/versiones-android-historia. [Último acceso: 14 junio 2022].

[15] Statcounter global Stats, «Mobile & Tablet Android Versión Market Share Worldwide,» Marzo 2022. [En línea]. Available: https://gs.statcounter.com/os-market-share/mobile/worldwide. [Último acceso: 14 Junio 2022].

[16] A. Chavez, «Introducing the Privacy Sandbox on Android,» 16 febrero 2022. [En línea]. Available: https://blog.google/products/android/introducing-privacy-sandbox-android/. [Último acceso: 2022 Agosto 2022].

[17] Developers, «Permisos en Android,» 10 enero 2017. [En línea]. Available: https://developer.android.com/guide/topics/permissions/overview?hl=es-419. [Último acceso: 11 septiembre 2022].

[18] R. Virlouvet, «La hausse des appareils Android non pris en charge menace la sécurité en ligne,» 10 junio 2022. [En línea]. Available:

https://www.bitdefender.fr/blog/hotforsecurity/la-hausse-des-appareils-android-non-pris-en-charge-compromet-la-securite-en-ligne/. [Último acceso: 14 junio 2022].

[19] Redaccion KeepCoding, «¿Qué es CVE Details?,» 22 diciembre 2022. [En línea]. Available: https://keepcoding.io/blog/que-es-cve-details-ciberseguridad/. [Último acceso: 12 septiembre 2022].

[20] CVE Details, «Vulnerability Trends Over Time,» 2022. [En línea]. Available: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224. [Último acceso: 2022 junio 2022].

[21] O. Murillo, «¿Qué es una ataque de denegación de servicio (DoS)?,» 5 noviembre 2020. [En línea]. Available: https://blog.sarenet.es/ataque-de-denegacion-de-servicio/. [Último acceso: 27 junio 2022].

[22] O. E. Mena Asprilla, «Anáslisis de riesgo de seguridad en los dispositivos móviles,» 2021. [En línea]. Available: https://repository.unad.edu.co/bitstream/handle/10596/48690/oemenaa-.pdf?sequence=3&isAllowed=y. [Último acceso: 21 junio 2022].

[23] C. Sánchez y D. Méndez Acuña, «Un estudio al modelo de seguridad de Android y de lo que se ha echo para mejorarlo,» 2018. [En línea]. Available: http://paradigma.uniandes.edu.co/images/sampledata/PARADIGMA/ediciones/Edicion7/Numero1/Articulo1/mendez-sanchez_ed7-1.pdf. [Último acceso: 13 Agosto 2022].

[24] R. O. Ramirez Gutiérrez y O. A. Reyes Fuentes, «Implementación de un laboratorio de,» 20 Octubre 2012. [En línea]. Available: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/1150/Tesis.pdf?sequence=1&isAllowed=y. [Último acceso: 27 diciembre 2022].

[25] R. Kovac, «Aumentó un 20% la detección de amenazas informáticas en 2022,» 2 junio 2022. [En línea]. Available: https://www.welivesecurity.com/la-es/2022/06/02/aumento-deteccion-amenazas-informaticas-2022/. [Último acceso: 14 Septiembre 2022].

[26] Fortinet, «Colombia sufrió más de 11.200 millones de intentos de ciberataques en 2021,» 8 Febrero 2022. [En línea]. Available: https://acis.org.co/portal/content/colombia-sufri%C3%B3-m%C3%A1s-de-11200-millones-de-intentos-de-ciberataques-en-2021. [Último acceso: 10 agosto 2022].

[27] R. Aguilar, «BRATA un peligroso troyano,» 13 abril 2021. [En línea]. Available: https://www.xatakandroid.com/seguridad/brata-peligroso-troyano-que-se-descarga-google-play-puede-controlar-tu-android. [Último acceso: 28 junio 2022].

[28] J. M. Ferro, «Iniciación a la forencia informática y ciberdelicuencia,» 2020. [En línea]. Available: https://books.google.com.ec/books?id=dr_MDwAAQBAJ&pg=PA222&dq=virus+en+inform%C3%A1tica&hl=es-419&sa=X&ved=2ahUKEwj8zeTNtpr8AhWrSzABHbMCDno4ChDoAXoECAcQAg#v=onepage&q=virus%20en%20inform%C3%A1tica&f=false. [Último acceso: 27 diciembre 2022].

[29] J. Lemonnier y N. Latto, «¿Qué es el spyware?,» 2 Enero 2020. [En línea]. Available: https://www.avg.com/es/signal/what-is-spyware. [Último acceso: 14 Noviembre 2022].

[30] R. A. Garcia Monje, «Seguridad informática y el malware,» *Repository Uni Piloto,* p. 11, 2017.

[31] Google Play Protect, «Categorías de software malicioso,» 03 Abrirl 2023. [En línea]. Available: developers.google.com/android/play-protect/phacategories#backdoor. [Último acceso: 26 junio 2022].

[32] M. G. Sánchez, «Ciberespacio y el crimen organizado. Los nuevos desafios del siglo XXI,» *Revista Enfoques: Ciencia Política y Administración Pública,* vol. 10, nº 16, pp. 71-78, 22 Junio 2012.

[33] E. R. Soto Ramírez y E. Escribano Hervis, «El método estudio de caso y su significado en la investigación educativa,» *Dialnet,* p. 20, 2019.

[34] L. Castellanos, «Metodologia de la investigación,» 2 marzo 2017. [En línea]. Available: https://lcmetodologiainvestigacion.wordpress.com/2017/03/02/tecnica-de-observacion/. [Último acceso: 4 Noviembre 2022].

[35] AV-Test, «AVTEST The Independent It Security Institute,» 2022. [En línea]. Available: https://www.av-test.org/es/antivirus/moviles/. [Último acceso: 23 Julio 2022].

[36] Virus Total, «Virus Total,» 08 Enero 2017. [En línea]. Available: https://www.virustotal.com/#/home/upload.

[37] R. J. Zambrano, «Técnicas de Análisis de Malware en dispositivos móviles basados en Android,» *Biblioteca Digital FCE,* p. 113, 2012.

[38] A. Sánchez Magraner, «Análisis de vulnerabilidades y malware,» 2017. [En línea]. Available: https://openaccess.uoc.edu/bitstream/10609/60607/6/asanchezmag0117TFMmem%C3%B2ria.pdf. [Último acceso: 12 Diciembre 2022].

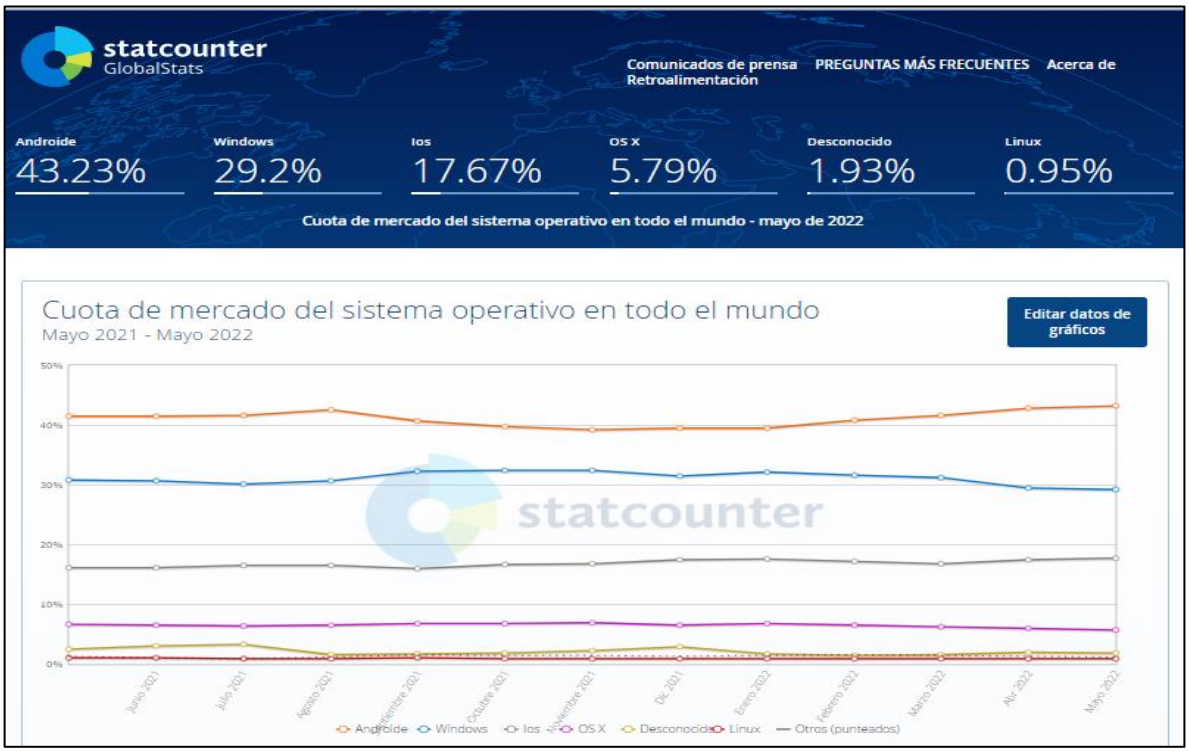
[39] N. Xie, X. Wang, W. Wei y J. Liu, «Identificación de familias de malware de android,» *Link Springer,* vol. 13, pp. 637-646, 30 Junio 2019.

[40] Vsantivirus, «W32/Trojan.Swizzor. Descripción genérica,» 14 Noviembre 2004. [En línea]. Available: https://vsantivirus.com/swizzor.htm. [Último acceso: 11 agosto 2022].

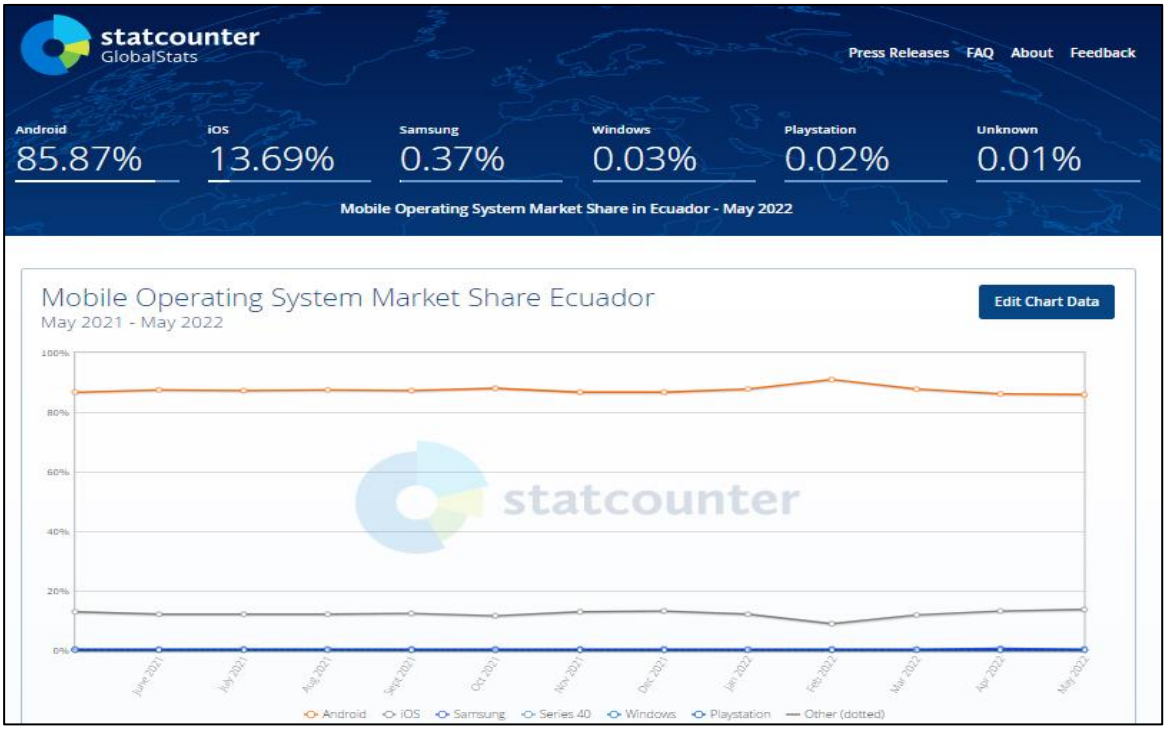
[41] ESET Segurity Report, «Segurity Report Latinoamerica 2021 "Introducción Conclusiones Hallazgos Ciberseguridad en tiempos de pandemia preocupaciones incidentes controles"4rtg,» 2021.

# 6. ANEXOS

Anexo 1. Aceptación de sistemas operativos móviles en el mundo.



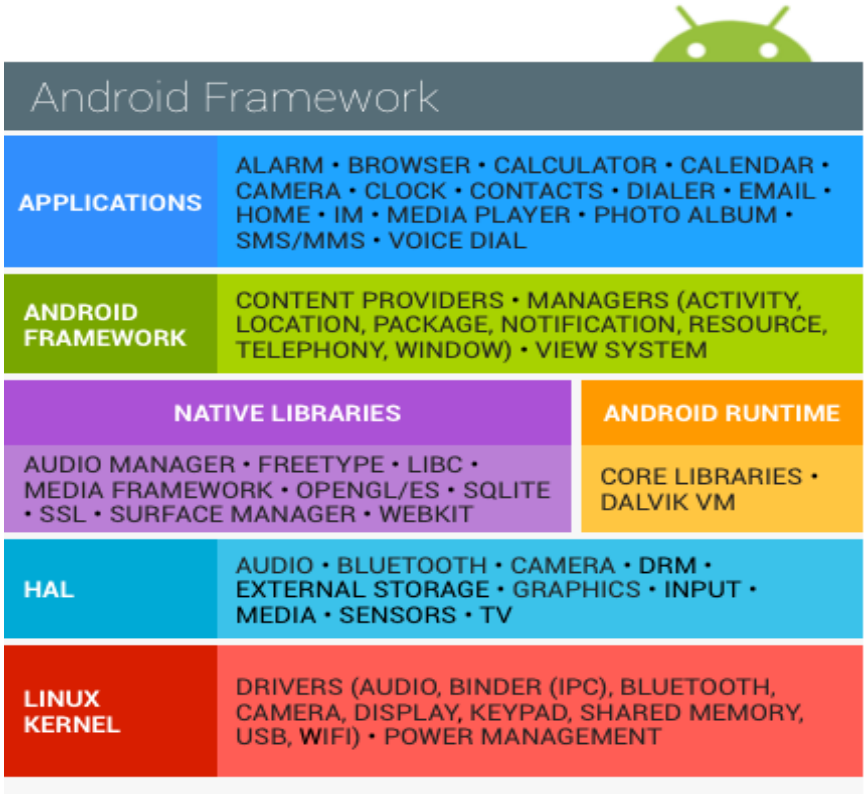

Anexo 2. Aceptación de sistemas operativos móviles en Ecuador.



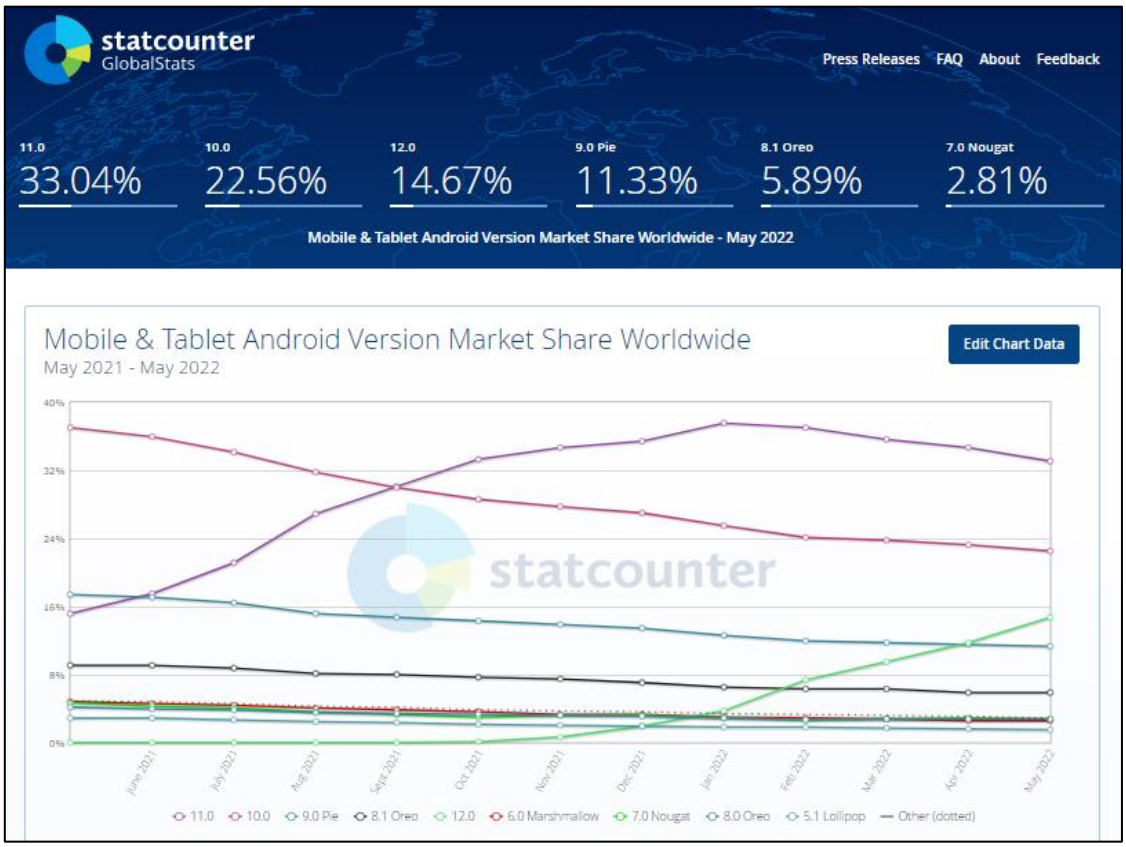

Anexo 3. Versiones de Android.

| Versión Android | Fecha de Lanzamiento |
|---|---|
| Android Apple Pie 1.0 (Tarta de manzana) | 23 septiembre 2008 |
| Android Banana Bread 1.1 (Pan de plátano) | 9 febrero 2009 |
| Android 1.5 Cupcake (Panque) | 30 abril del 2009 |
| Android 1.6 Donut (Rosquilla) | 15 septiembre 2009 |
| Android 2.0/2.1 Eclair (Pepito) | 26 octubre 2009 |
| Android 2.2 Froyo (Yogur helado) | 20 mayo 2010 |
| Android 2.3 Gingerbread (Pan de jengibre) | 6 diciembre 2010 |
| Android 3.0 Honeycomb (Panal de miel) | 22 febrero 2011 |
| Android 4.0 Ice Cream Sandwich (Sándwich de helado) | 12 octubre 2011 |
| Android 4.1 Jelly Bean (Gominola) | 30 junio 2012 |
| Android 4.4 KitKat (Kit Kat) | 31 octubre 2013 |
| Android 5.0 Lollipop (Piruleta) | 3 noviembre 2014 |
| Android 6.0 Marshmallow (Malvavisco) | 5 octubre 2015 |
| Android 7.0 Nougat | 22 agosto 2016 |
| Android 8.0 Oreo | 21 agosto 2017 |
| Android 9.0 Pie | 6 de agosto 2018 |
| Android 10.0 | 3 de septiembre 2019 |
| Android 11 | 8 de septiembre 2020 |
| Android 12 | 7 de octubre 2021 - 8 de marzo 2022 |
| Android 13 | agosto – septiembre 2022 |

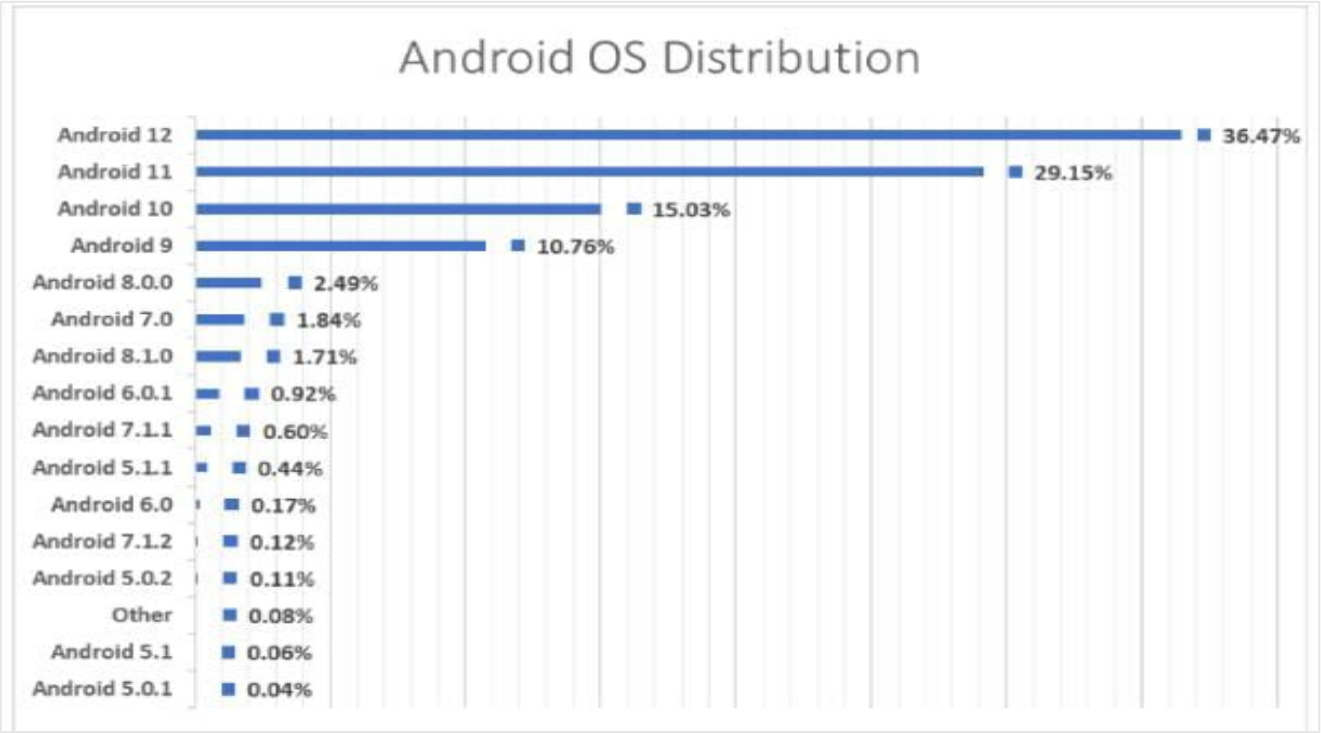
Anexo 4. Arquitectura de Android.




Anexo 5. Versión de Android con mayor aceptación en el mundo.



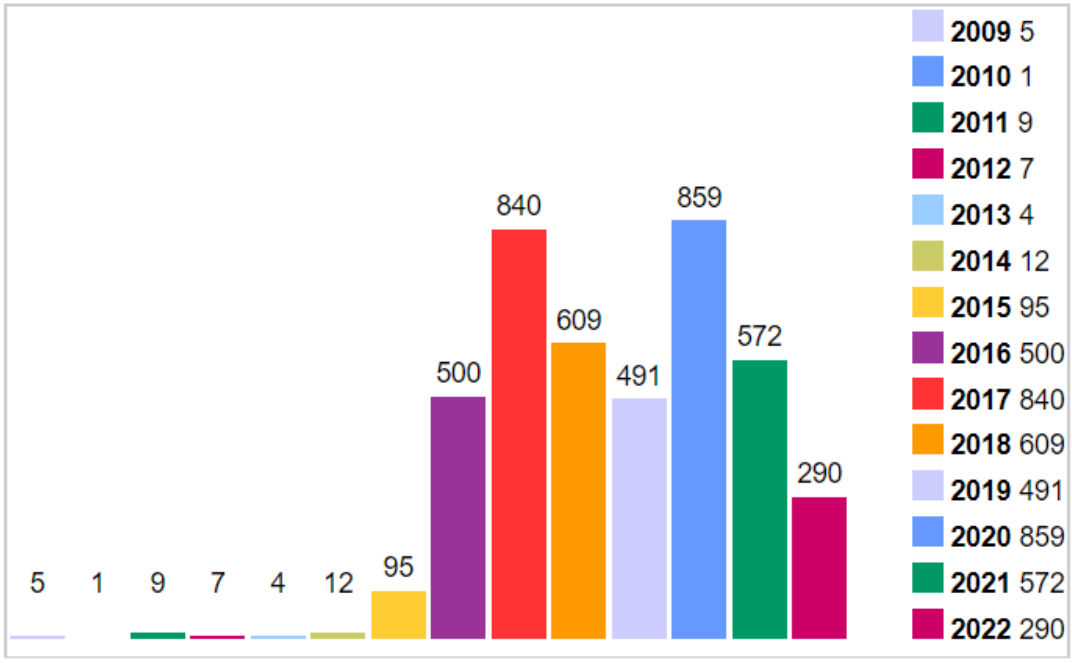
Anexo 6. Aceptación de sistemas operativos android en el mundo.



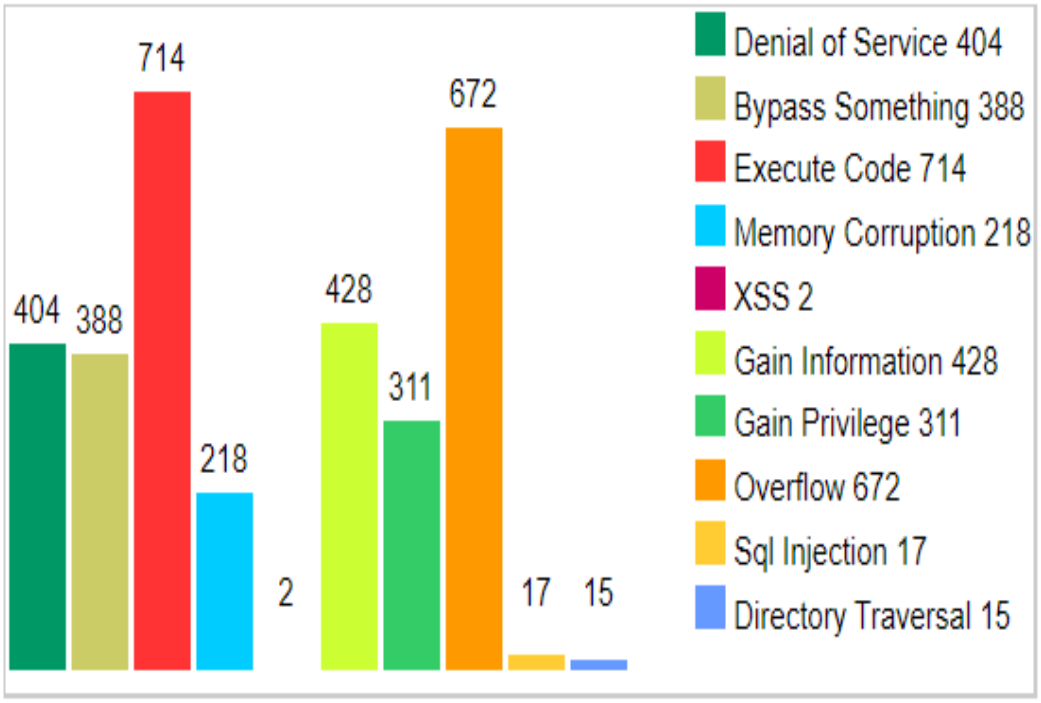

Anexo 7. Tendencias de vulnerabilidades a lo largo del tiempo.

| Año | # de Vulnerabilidades | DoS | Ejecución de código | Desbordamiento | Corrupción de memoria | Inyección SQL | XSS | Recorrido de directorios | Omitir algo | Obtener información | Obtenga privilegios | # de exploits |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2009 | 5 | 3 | | | | | | | 1 | | | |
| 2010 | 1 | 1 | 1 | | | | | | | | | |
| 2011 | 9 | 1 | 1 | | 1 | | 1 | | 4 | 1 | 3 | |
| 2012 | 7 | 5 | 3 | 2 | | | | | | 1 | | 1 |
| 2013 | 4 | | 1 | 1 | 1 | | | | 1 | 1 | 1 | |
| 2014 | 12 | 2 | 4 | 1 | | 1 | | | 1 | 2 | 1 | 1 |
| 2015 | 95 | 46 | 49 | 50 | 37 | | | | 13 | 14 | 17 | |
| 2016 | 500 | 104 | 72 | 91 | 38 | | | | 47 | 96 | 236 | |
| 2017 | 840 | 86 | 206 | 170 | 32 | | | 1 | 30 | 113 | 36 | |
| 2018 | 609 | 32 | 84 | 143 | 12 | 2 | 1 | 2 | 17 | 63 | 3 | |
| 2019 | 491 | 37 | 107 | 41 | 24 | 3 | | 1 | 39 | 21 | 1 | |
| 2020 | 859 | 46 | 97 | 104 | 27 | 9 | | 5 | 148 | 96 | 3 | |
| 2021 | 572 | 28 | 61 | 49 | 40 | 2 | | 4 | 54 | 15 | 7 | |
| 2022 | 290 | 13 | 28 | 20 | 6 | | | 2 | 33 | 5 | 3 | |
| Total | 4294 | 404 | 714 | 672 | 218 | 17 | 2 | 15 | 388 | 428 | 311 | 2 |
| % de todos | | 9.4 | 16.6 | 15.6 | 5.1 | 0.4 | 0.0 | 0.3 | 9.0 | 10.0 | 7.2 | |

Anexo 8. Tendencias de vulnerabilidades en Android desde el 2009 hasta 2022.




Anexo 9. Tendencias de vulnerabilidades según su tipo desde el 2009 hasta 2022.



Anexo 10. Tendencias de vulnerabilidades en Android 12 a lo largo del tiempo.

| Tendencias de vulnerabilidad a lo largo del tiempo | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Año | # de Vulnerabilidades | DoS | Ejecución de código | Desbordamiento | Corrupción de memoria | Recorrido de directorios | Omitir algo | Obtener información | Obtenga privilegios |
| 2021 | 84 | 5 | 12 | 4 | | | 6 | 5 | 1 |
| 2022 | 187 | 15 | 22 | 14 | 1 | 2 | 24 | 1 | 2 |
| Total | 271 | 20 | 34 | 18 | 1 | 2 | 30 | 6 | 3 |
| % de todos | | 7.4 | 12.5 | 6.6 | 0.4 | 0.7 | 11.1 | 2.2 | 1.1 |

Anexo 11. Listado de herramientas de prevención contra malware que existen en el mercado tecnológico.

| Aspecto para evaluar / Herramientas de Seguridad | | AhnLab V3 Mobile Security 3.1 | Bitdefender Mobile Security 3.3 | Avast Mobile Security 6.23 | AVG AntiVirus Free 6.23 |
|---|---|---|---|---|---|
| Protección | Detección de malware más recientes para Android en tiempo real. | 99,80% | 99% | 99,90% | 99,90% |
| | Detección de malware actual para Android descubierto en las últimas 4 semanas | 99,80% | 99,6% | 99,80% | 99,80% |
| Rendimiento | La aplicación no influye en la duración de la batería. | si | si | si | si |
| | La aplicación no ralentiza el uso normal del dispositivo. | si | si | si | si |
| | La aplicación apenas genera carga de red. | si | si | si | si |
| Usabilidad | Falsas alarmas durante la instalación y el uso de una aplicación desde Google Play Store | 1 | 0 | 1 | 1 |
| | Falsas alarmas durante la instalación y el uso de una aplicación desde store de terceros. | 0 | 0 | 0 | 0 |
| Funciones | Control de aplicaciones: función para la autorización, bloqueo o restricción del acceso de determinadas aplicaciones. | si | no | si | si |
| | Copia de seguridad: aseguramiento de datos personales en la tarjeta SD o mediante almacenamiento en la nube. | No | no | no | no |
| | Bloqueo de llamadas: Bloquear las llamadas de números desconocidos o de determinados números. | si | si | si | si |
| | Asesor de privacidad (Privacy Advisor): funciones para evaluar los datos recopilados por las aplicaciones basándose en autorizaciones, tráficos de datos y confianza merecida. | si | no | si | si |
| | Navegación segura: protección contra páginas web maliciosas u contra páginas web de phishing. | si | no | si | si |
| | VPN: Utilización de una red privada virtual (Virtual Private Network) para proteger el tráfico de datos y navegar de forma anónima. | no | no | si | si |
| | Asesor/control de wifi: Comprobación para detectar conexiones de wifi seguras o inseguras. | No | No | si | si |

| Aspecto para evaluar / Herramientas de Seguridad | | F-Secure SAFE 17.7 | G Data Internet Security 26.6 | Ikarus mobile. security 1.8 | Avira Antivirus Security 6.0 |
|---|---|---|---|---|---|
| Protección | Detección de malware más recientes para Android en tiempo real. | 99,70% | 100% | 99,60% | 100% |
| | Detección de malware actual para Android descubierto en las últimas 4 semanas | 100% | 100% | 100% | 100% |
| Rendimiento | La aplicación no influye en la duración de la batería. | si | si | si | si |
| | La aplicación no ralentiza el uso normal del dispositivo. | si | si | si | si |
| | La aplicación apenas genera carga de red. | si | si | si | si |
| Usabilidad | Falsas alarmas durante la instalación y el uso de una aplicación desde Google Play Store | 0 | 0 | 0 | 0 |
| | Falsas alarmas durante la instalación y el uso de una aplicación desde store de terceros. | 1 | 0 | 0 | 0 |
| Funciones | Control de aplicaciones: función para la autorización, bloqueo o restricción del acceso de determinadas aplicaciones. | no | si | si | si |
| | Copia de seguridad: aseguramiento de datos personales en la tarjeta SD o mediante almacenamiento en la nube. | no | no | no | no |
| | Bloqueo de llamadas: Bloquear las llamadas de números desconocidos o de determinados números. | no | si | no | no |
| | Asesor de privacidad (Privacy Advisor): funciones para evaluar los datos recopilados por las aplicaciones basándose en autorizaciones, tráficos de datos y confianza merecida. | si | si | si | no |
| | Navegación segura: protección contra páginas web maliciosas u contra páginas web de phishing. | si | si | si | si |
| | VPN: Utilización de una red privada virtual (Virtual Private Network) para proteger el tráfico de datos y navegar de forma anónima. | no | no | no | si |
| | Asesor/control de wifi: Comprobación para detectar conexiones de wifi seguras o inseguras. | no | si | no | si |

| Aspecto para evaluar / Herramientas de Seguridad | | McAfee Mobile Security 5.3 | Line Antivirus 2.1 | Sophos Intercept for Mobile | Kaspersky Security |
|---|---|---|---|---|---|
| Protección | Detección de malware más recientes para Android en tiempo real. | 99,90% | 99% | 99% | 99% |
| | Detección de malware actual para Android descubierto en las últimas 4 semanas | 100% | 99,6% | 99,66 | 99,6% |
| Rendimiento | La aplicación no influye en la duración de la batería. | si | Si | si | si |
| | La aplicación no ralentiza el uso normal del dispositivo. | si | Si | si | si |
| | La aplicación apenas genera carga de red. | si | Si | si | si |
| Usabilidad | Falsas alarmas durante la instalación y el uso de una aplicación desde Google Play Store | 0 | 0 | no | 0 |
| | Falsas alarmas durante la instalación y el uso de una aplicación desde store de terceros. | 0 | 0 | no | 0 |
| Funciones | Control de aplicaciones: función para la autorización, bloqueo o restricción del acceso de determinadas aplicaciones. | si | Si | si | si |
| | Copia de seguridad: aseguramiento de datos personales en la tarjeta SD o mediante almacenamiento en la nube. | si | No | no | no |
| | Bloqueo de llamadas: Bloquear las llamadas de números desconocidos o de determinados números. | no | No | no | si |
| | Asesor de privacidad (Privacy Advisor): funciones para evaluar los datos recopilados por las aplicaciones basándose en autorizaciones, tráficos de datos y confianza merecida. | si | Si | si | no |
| | Navegación segura: protección contra páginas web maliciosas u contra páginas web de phishing. | si | Si | si | si |
| | VPN: Utilización de una red privada virtual (Virtual Private Network) para proteger el tráfico de datos y navegar de forma anónima. | si | no | no | si |
| | Asesor/control de wifi: Comprobación para detectar conexiones de wifi seguras o inseguras. | si | si | si | si |

Anexo 12. Muestras de malware a evaluar.

| Malware | Muestra MD5 |
|---|---|
| Trojan/Android.FakeInst.547158 | 0b53d37afa0971e2295c537991b4b7d5 |
| FakeInst se camufla como una aplicación para mirar videos pornográficos, la cual pide que acepte enviar un mensaje de texto para comprar contenidos, además se disfraza de muy aplicaciones populares. Envía mensajes SMS a números de tarifa premium [39]. | |
| Trojan/Generic.ASMalwAD.33E | 0d194dcaa683c43699ca6d9d84f3a3cf |
| Cuando el programa se ejecuta, descarga e instala a su vez un plug-in capaz de actuar como spyware y adware (programa espía y publicidad) [40]. | |
| Android:SMSSend-AHS [Trj] | 1b4c6b2e39336a1aa3939ee3a9c5865e |
| Es considerado peligroso por muchos expertos en seguridad. Cuando esta infección está activa, puede notar procesos no deseados en la lista [39]. | |
| .ANDROID/SMSForw.FIFC.Gen | 1bfbf379b54460842e7aa9b7a85c6fc9 |
| Envía mensajes SMS a números de tarifa premium [39]. | |
| PUP/Android.Plankton.7168 | 95bcbe87750cc5dc2c2d2b02505effee |
| Plankton roba información e intenta abrir una puerta trasera en dispositivos Android. Se vuelve a empaquetar en aplicaciones legítimas que están disponibles para descargar en el mercado de Android. De este modo, recoge el dispositivo información y la envía a un servidor remoto [39]. | |
| Install | 4a8c3560f3393128b77aa4906df0e9fb |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |
| Talking-larry-the-bird-v1_1_5 | 04e22d05f6975a1be9d975221ee65d7e |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |
| CoPilot_Live_Premium | 3f8ce65548534da7e9f40e8853975281 |
| Launcher_0_9_0_rus | 3e2b98fe3d5d8079abd03d448ae19f41 |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |
| Taiwang Beutyleg Models | 0a2da16728537ccbd11c086a7b0c6695 |
| Esta aplicación maliciosa que roba mensajes SMS y entradas de contactos de un dispositivo infectado. | |
| Google Play | 0a1d3b51c66016e00cc24516ff3f7a74 |
| Envía copias de mensajes SMS a otros dispositivos. | |
| ChangElockScreen | 00aff44926031e0b337c1a2789725231 |
| Obtiene acceso de root y recopila datos en teléfonos inteligentes infectados. Estos datos se envían a un servidor remoto posteriormente. | |
| Angry_Birds_Rio | 00dc7d61c6646551915172c792d40c10 |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |
| Yin The Cat | 00cf703f8b9c4af28e6c8b45243d2642 |
| Este troyano envía mensajes SMS a números calificados premium. | |
| Skype | 0d14205db8e9bbabfdfc4b76a0e572c3 |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |
| Device Health Application | 0d8e05ef966b80cb156fd9b1b9804ee2 |
| El fraude más común. Estas aplicaciones envían mensajes SMS premium. | |

Anexo 13. Malware para Android en la actualidad

| Malware | Mobile Security | F- Secure |
|---|---|---|
| Yctahobka | Android.Trojan.FakeInst.BB | Trojan:Android/Fakeinst.CB |
| Com_fring_37_3.8.16 | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Talking-Tom_1_6 | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Iping Pong 3d_v1_0_0 | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Htcdesirehd | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Install | Android.Trojan.FakeInst.BX | Trojan:Android/Fakeinst.AA |
| Talking-larry-the-bird-v1_1_5 | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| CoPilot_Live_Premium | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.BA |
| Launcher_0_9_0_rus | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Taiwang Beutyleg Models | Android.Adware.Wapsx.A | Adware: Android/AirPush |
| Google Play | Android.Trojan.Badao.B | Trojan:Android/SmsSend.CA |
| ChangElockScreen | Android.Trojan.GingerMaster.gOJG | Adware:Android/Dowgin |
| Angry_Birds_Rio | Android.Trojan.FakeInst.DA | Trojan:Android/Fakeinst.GJ |
| Yin The Cat | Android.Trojan.FakeInst.FE | Trojan:Android/Fakeinst.CB |
| Skype | Android.Trojan.FakeInst.D | Trojan:Android/Fakeinst.DL |
| Device Health Application | Android.Trojan.FakeInst.AY | Trojan:Android/Fakeinst.DZ |
| Resultados | 100% | 100% |

| Malware | McAfee | Kaspersky |
|---|---|---|
| Yctahobka | Artemis!4A74DB8A6057 | HEUR:Trojan-SMS.AndroidOS.Opfake.bo |
| Com_fring_37_3.8.16 | Artemis!4B366C6A2729 | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Talking-Tom_1_6 | Artemis!4B366C6A2729 | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Iping Pong 3d_v1_0_0 | Artemis!4A8D378E1B73 | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Htcdesirehd | Artemis!4A75A32E5B60 | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Install | Artemis!4A8C3560F339 | HEUR:Trojan-SMS.AndroidOS.FakeInst.a |
| Talking-larry-the-bird-v1_1_5 | Artemis!04E22D05F697 | HEUR:Trojan-SMS.AndroidOS.FakeInst.a |
| CoPilot_Live_Premium | Artemis!3F8CE6554853 | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Launcher_0_9_0_rus | Artemis!3E2B98FE3D5D | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Taiwang Beutyleg Models | Artemis!0A2DA1672853 | not-a-virus:HEUR:AdWare.AndroidOS.Waps.a |
| Google Play | Artemis!0A1D3B51C660 | HEUR:Trojan.AndroidOS.Badao.a |
| ChangElockScreen | Artemis!00AFF4492603 | not-a-virus:HEUR:AdWare.AndroidOS.Jedan.a |
| Angry_Birds_Rio | Artemis!00DC7D61C664 | HEUR:Trojan-SMS.AndroidOS.FakeInst.a |
| Yin The Cat | Artemis!00CF703F8B9C | HEUR:Trojan-SMS.AndroidOS.Opfake.bo |
| Skype | Artemis!0D14205DB8E9 | HEUR:Trojan-SMS.AndroidOS.FakeInst.a |
| Device Health Application | Artemis!0D8E05EF966B | HEUR:Trojan-SMS.AndroidOS.Agent.aax |
| Resultados | 100% | 100% |

| Malware | Avast Mobile | AVG |
|---|---|---|
| Yctahobka | Android:Agent-EMD [Trj] | Android:Agent-EMD [Trj] |
| Com_fring_37_3.8.16 | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Talking-Tom_1_6 | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Iping Pong 3d_v1_0_0 | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Htcdesirehd | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Install | Android:FakeInst-DA [Trj] | Android:FakeInst-AQX [Trj] |
| Talking-larry-the-bird-v1_1_5 | Android:Agent-HKP [Trj] | Android/G2P.U.D77C9EBF7992 |
| CoPilot_Live_Premium | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Launcher_0_9_0_rus | Android:FakeInst-AKK [Trj] | Android:Agent-HKP [Trj] |
| Taiwang Beutyleg Models | | |
| Google Play | Android:Badao-F [Trj] | Android:Badao-F [Trj] |
| ChangElockScreen | | |
| Angry_Birds_Rio | Android:TrojanSMS-CB [Trj] | Android:Agent-ELI [Trj] |
| Yin The Cat | Android:Boxer-AZ [Trj] | Android:Boxer-AZ [Trj] |
| Skype | Android:SMSSend-AHS [Trj] | Android:FakeInst-AJJ [Trj] |
| Device Health Application | Android:FakeInst-AKK [Trj] | Android:FakeInst-AKK [Trj] |
| Resultados | 88% | 88% |