UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Tema:

DETECCIÓN DE VULNERABILIDADES DE SEGURIDAD EN BLOQUEADORES DE ANUNCIOS EN DISPOSITIVOS MÓVILES ANDROID.

Trabajo de Integración Curricular Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Tecnologías de la Información.

ÁREA: Hardware y Redes

LÍNEA DE INVESIGACIÓN: Sistemas administradores de recursos.

AUTOR: Byron Alexis Tunja Altamirano

TUTOR: PHD. Félix Oscar Fernández Peña

Ambato – Ecuador

marzo – 2023

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Integración Curricular con el tema: DETECCIÓN DE VULNERABILIDADES DE SEGURIDAD EN BLOQUEADORES DE ANUNCIOS EN DISPOSITIVOS MÓVILES ANDROID, desarrollado bajo la modalidad Proyecto de Investigación por el señor Byron Alexis Tunja Altamirano, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y el numeral 7.4 del respectivo instructivo del reglamento.

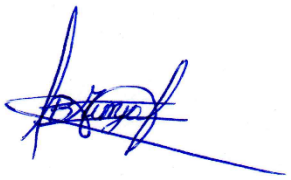
Ambato, marzo 2023

PHD. Félix Oscar Fernández Peña
TUTOR

AUTORÍA

El presente trabajo de Integración Curricular titulado: DETECCIÓN DE VULNERABILIDADES DE SEGURIDAD EN BLOQUEADORES DE ANUNCIOS EN DISPOSITIVOS MÓVILES ANDROID, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2023



Byron Alexis Tunja Altamirano

C.C. 1805326327

AUTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Integración Curricular como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Integración Curricular en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la Institución.

Ambato, marzo 2023

Byron Alexis Tunja Altamirano

C.C. 1805326327

AUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Integración Curricular presentado por el señor Byron Alexis Tunja Altamirano, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado DETECCIÓN DE VULNERABILIDADES DE SEGURIDAD EN BLOQUEADORES DE ANUNCIOS EN DISPOSITIVOS MÓVILES ANDROID, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 de las segundas reformas al Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y al numeral 7.6 del respectivo instructivo del reglamento. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, marzo 2023.

Firmado electrónicamente por:
ELSA PILAR URRUTIA URRUTIA

Ing. Elsa Pilar Urrutia Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
RUBEN EDUARDO NOGALES PORTERO

Ing. Mg. Rubén Eduardo Nogales Portero
PROFESOR CALIFICADOR

Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. Mg. David Omar Guevara Aulestia
PROFESOR CALIFICADOR

DEDICATORIA

El presente proyecto está dedicado a mi madre, padrastro y abuelos maternos, que me guiaron con ética y principios. Principios que forjaron mi carácter y me permitieron llegar hasta este punto de mi vida.

A mi profesor Oswaldo Quintana, quien me mostró el valor del esfuerzo.

Al colegio Atahualpa, lugar donde adquirí fuerza, orgullo y nuevos conocimientos.

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Ambato por ser el espacio donde se me presento una basta cantidad de conocimiento. Además de permitirme encontrar a docentes que me mostraron una nueva visión del mundo.

A mi familia, que me impulso a trabajar duro y no rendirme ante las dificultades de la vida.

A mi tutor, el Ingeniero Félix Fernández, por todo el apoyo brindado durante el desarrollo de este proyecto. Así como también su firme guía, mostrándome sin dudar como ser mejor.

A los amigos con los que compartí mi tiempo en la universidad. Quienes fueron tanto una inspiración como rivales y me llevaron a dar más de mí mismo.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

La proliferación de publicidad en las aplicaciones de los dispositivos móviles y el creciente número de *adware* llevó al desarrollo de aplicaciones bloqueadoras de anuncios. Su uso produjo un mejor rendimiento del dispositivo, experiencia de usuario y privacidad. Sin embargo, debido a los beneficios se dejó de lado aspectos relevantes, como qué información se recoge y comparte, qué acciones se toman para proteger la información y qué permisos son solicitados por la aplicación. De acuerdo con ello, el presente proyecto tiene como objetivo demostrar que las aplicaciones bloqueadoras de anuncios Android presentan vulnerabilidades informáticas y que, ante una posible explotación de una vulnerabilidad, toda la información que maneja la aplicación puede quedar comprometida. Para ello, se tomó una muestra aleatoria de cien aplicaciones bloqueadoras de anuncios, a las que se les realizó un análisis con la herramienta VirusTotal y una revisión manual del código fuente disponible con el IDE Android Studio. Como resultado se identificó ocho tipos de vulnerabilidades, fundamentadas a través de registros CVE. Finalmente, se planteó un total de trece recomendaciones, para dificultar la explotación de las vulnerabilidades encontradas. Que se estima dar lugar a una disminución en la posibilidad de explotar las vulnerabilidades que afectan a los *ad blockers*.

Palabras clave: Adware, dispositivos móviles, Android, bloqueador de anuncios, VirusTotal, Android Studio, CVE.

ABSTRACT

The proliferation of advertising in mobile device applications and the increasing number of adware led to the development of ad blocker applications. Its use produced better device performance, user experience and privacy. However, due to the benefits, relevant aspects were left aside, such as what information is collected and shared, what actions are taken to protect the information and what permissions are requested by the application. Agree with it, this project have as objective demonstrate that Android ad blocker applications present computer vulnerabilities and that, in the event of a possible exploitation of a vulnerability, all the information handled by the application may be compromised. To do this, a random sample of one hundred ad blocker applications was taken, which were analyzed with the VirusTotal tool and a manual review of the source code available with the Android Studio IDE. As a result, eight types of vulnerabilities were identified, substantiated by CVE records. Finally, a total of thirteen recommendations were raised, to make it difficult to exploit the vulnerabilities found. That is estimated to lead to a decrease in the possibility of exploiting vulnerabilities that affect ad blockers.

Keywords: Adware, Mobile devices, Android, Ad blocker, VirusTotal, Android Studio, CVE.

B. CONTENIDOS
CAPÍTULO I.- MARCO TEÓRICO

1.1 Tema de investigación

DETECCIÓN DE VULNERABILIDADES DE SEGURIDAD EN BLOQUEADORES DE ANUNCIOS EN DISPOSITIVOS MÓVILES ANDROID.

1.1.1 Planteamiento del problema

El auge de los dispositivos móviles Android también significó un desarrollo creciente de malware que afecte a su sistema operativo [1]. En la fecha presente, el internet se convirtió en el principal medio de propagación del malware [2]. El malware centrado en dispositivos móviles presta mayor atención a rastrear la trayectoria del usuario, realizar fraude, cobrar tarifas de servicios móviles adicionales y divulgar credenciales de usuario [3].

El malware que comete fraude publicitario es conocido como adware, esto afecta también a los anuncios incrustados en las aplicaciones de Android [4]. En consecuencia, se desarrollaron los bloqueadores de anuncios (ad blockers), los cuales cumplen con la necesidad del bloqueo de contenido publicitario, como consecuencia mejora el rendimiento del dispositivo, incrementa la privacidad y seguridad, además de proporcionar una experiencia agradable al usuario [5]. Debido a estas ventajas, en el año 2021 la cifra de usuarios que utilizan ad blockers en sus dispositivos móviles alcanzo los 586 millones [6].

En respuesta a la propagación del malware, se volvió necesario implementar normas de seguridad que fomenten un mejor manejo de los dispositivos móviles. Con el fin de impulsar el desarrollo empresarial y el manejo seguro de la información. Principalmente en Ecuador debido a que personal de las pequeñas y medianas empresas no cuentan con una cultura móvil en su organización [7].

Con respecto a las empresas que no cuentan con normas de seguridad móvil en su organización, como es el caso de Ecuador. El malware que afecte a los dispositivos móviles ejecutara acciones de recolección y envió de datos, comparte información personal a terceros y solicita privilegios root [8]. Puesto que secciones de código que toma ventaja de las vulnerabilidades de una aplicación para esparcir malware, mejor conocido como Exploit. Hace necesario el análisis de las posibles vulnerabilidades de dispositivos móviles [9].

La ciudad de Ambato no es la excepción, un ejemplo de esto es la empresa Ambacar. Ambacar, a pesar de haber realizado un sistema de gestión de seguridad en 2020, posteriormente tuvo que dar de baja a su módulo de facturación debido a sus vulnerabilidades. Las vulnerabilidades provocaban pérdida de la información, altos costos correctivos, frustración por parte de los usuarios y facilidad de secuestro de información, lo que genera un alto riesgo para la empresa [10].

1.2 Antecedentes investigativos

Espinosa Iván, Sanabria Marco, en el artículo científico titulado: "Estado del arte utilizando mapeo sistemático para las técnicas de análisis de Malware en Android", trabajo realizado como tesis de Universidad Politécnica Salesiana Sede Quito en el año 2021, explicaron que: Aplicando las metodologías de mapeo y revisión sistemáticos de la literatura según las siguientes fases: Fase 1 se definen los objetivos y el alcance de los criterios de selección. En la fase 2 se ejecuta la revisión, se definen los principales contenidos de la investigación y se dividen en dos pasos. En la fase 3 se reporta la revisión, los estudios seleccionados se clasifican en diferentes categorías. Determinaron que los factores que inciden en las técnicas de análisis de Malware en Android son: el poco conocimiento de métodos y herramientas utilizadas para su detección, además que la evolución del malware es capaz de usar técnicas de encriptación y ofuscación, haciendo que su detección sea más compleja [1].

Herrera Domingo, en su tesis: "Estudio de Vulnerabilidades en transacciones bancarias para dispositivos móviles con Sistema Operativo Android", trabajo realizado como tesis de Universidad Nacional de Loja en el año 2017, explico que: Realizó una

investigación sobre vulnerabilidades en la plataforma Android aplicando una metodología de revisión Sistemática de Bárbara Kitchenham que incluye las etapas: Planificación de la Revisión; Desarrollo de la Revisión; Publicación de los Resultados. Como resultado determino que la plataforma Android es la más atacada por piratas informáticas en comparación con iOS o Windows Phone, además los atacantes se centran específicamente en el hurto de información de usuarios, debido a que es vulnerable a ataques que emplean diferentes técnicas para violentar la seguridad [2].

Moncayo Viviana, en su tesis: "Aplicación de herramientas de hacking ético para ejecutar un test de intrusión en dispositivos móviles Android mediante un laboratorio virtual controlado enfocado en redes de área extensa e inalámbrica para pequeñas y medianas empresas de la ciudad de Guayaquil", trabajo realizado como tesis de Universidad De Guayaquil en el año 2021, menciona que: Aplicó la metodología cascada, con base en las fases de intrusión: descubrimiento, exploración, evaluación sobre un dispositivo Samsung A32, utilizando herramientas para el hacking y análisis de vulnerabilidades en dispositivos Android. Determinó que se debe fortalecer la confidencialidad de la información almacenada, además que los sistemas operativos Android son vulnerables a diferentes códigos maliciosos y a su vez poseen Exploit para que atacantes puedan explotar fallos de seguridad y tomar el control de un dispositivo móvil [3].

Kiran Garimella, Orestis Kostakis, Michael Mathioudakis[4], en el artículo científico titulado:" Ad-blocking: A Study on Performance, Privacy and Counter-measures" publicado en la Conferencia ACM sobre investigación internacional en educación informática 2017, explicaron que: Aplicando un análisis de rendimiento en configuraciones de escritorio y móviles para una gran cantidad de páginas web, así como una serie de medidas que describen la carga de trabajo del navegador con y sin el uso de un bloqueador de anuncios. Determinaron que los bloqueadores de anuncios reducen significativamente el consumo de datos, sin embargo, los beneficios en términos de tiempos de carga son limitados, además que los sitios web intentan contrarréstalos, pero también solicitan que sean desactivados, por último, los mismos evitan la transferencia de información de seguimiento de usuarios, lo que genera beneficios de privacidad para sus usuarios [4].

Muhammad Ikram, Mohamed Ali Kaafa, en el artículo científico titulado:" A First Look at Mobile Ad-Blocking Apps" publicado en 16to Simposio internacional sobre computación en red y aplicaciones IEEE 2017, explicaron que: Aplicando análisis estático del código sobre 97 aplicaciones bloqueadoras de anuncios de la Google Play Store, para investigar la presencia de malware y bibliotecas de seguimiento de terceros, además de analizar a la solicitud de los mismos para acceder a los permisos de Android. Como resultado se obtuvo una taxonomía de bloqueadores de anuncios móviles, de los cuales un 68% de ellos incorpora bibliotecas de anuncios y seguimiento de terceros en su código, un 89% pide acceso a permisos confidenciales, un 13% tiene presencia de malware en su código y un 24% muestra anuncios [5].

1.3 Fundamentación teórica

Seguridad informática

Seguridad informática es el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos. Para prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización. Además, que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos [6].

Seguridad informática consiste en asegurar la ausencia de riesgos en cualquiera de los componentes de un sistema (hardware, software, personal informático, redes, usuarios, datos y procedimientos). Lo que impediría a cualquier persona sin autorización pueda tener acceso a la información contenida en el sistema. Y, por lo tanto, no pueda modificarla, dañarla, alterarla, eliminarla o darle cualquier tratamiento que no esté autorizado [7].

La seguridad informática tiene relación con el enfoque de preservación digital. Y se establece como la unión de seis características esenciales: permanencia, accesibilidad, disponibilidad, confidencialidad (privacidad), autenticidad (integridad), aceptabilidad (no repudio) [6].

Amenazas informáticas

Amenazas informáticas son la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma [6].

La amenaza informática se la puede considerar como las acciones que pueden producir un fallo en la seguridad informática. Las amenazas aparecen con base en a la existencia de vulnerabilidades, es decir cuando una de ellas puede ser aprovechada para producir riesgo en el entorno informático [8].

Se dividen en dos grupos [8]:

- Intencionales: Código malicioso, Ingeniería social, Trashing.
- No intencionales: Acciones no ejecutadas a propósito.

Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades. Lo que afectaría directamente la información o los sistemas que la procesan. Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías: factores humanos (accidentales, errores), fallas en los sistemas de procesamiento de información, desastres naturales, actos maliciosos o malintencionados [7].

Vulnerabilidades informáticas

La vulnerabilidad informática se define como una debilidad en la lógica computacional que se encuentra en el software y en algunos componentes de hardware. Que, cuando se explota, tiene un impacto negativo en la confidencialidad, integridad o disponibilidad de activos de información [9].

Las vulnerabilidades son debilidades que ponen en riesgo el entorno informático. Al permitir que se pierda las condiciones primordiales de la seguridad de la información, como lo son la confidencialidad, integridad y disponibilidad [8].

Las vulnerabilidades son la consecuencia de bugs o fallos en los diseños de los sistemas. Así como también son el resultado de las limitaciones tecnológicas pendientes por ser resueltas por los especialistas en seguridad informática. Que hasta el momento impiden contar con un sistema de manejo de la información ciento por ciento seguro [10].

Hardware

Hardware se refiere a todo el conjunto de dispositivos electrónicos utilizados para configurar un Sistema de Información, una Tecnología de la Información (TI) o una Tecnología Operacional (TO) indistintamente. Independientemente de su complejidad, su campo de aplicación y la funcionalidad/ papel de los dispositivos dentro de él [11].

Hardware comprende todos aquellos dispositivos físicos y materiales usados en el proceso de información. Abarca el uso de la computadora y los aparatos conectados a ella. Y que proporciona el soporte físico que ayuda tanto al tratamiento como procesamiento de la información [12].

Hardware es un artefacto cuyas funciones se realizan en procesos que directa o indirectamente provocan el resultado de algún cálculo [13].

Sistemas administradores de recursos

Los sistemas administradores de recursos son los que gestionan, coordinan y organizan los recursos del hardware, archivos y directorios del dispositivo. Con el objetivo de coordinar tareas, usar la memoria, unidades de disco, etc. [14].

Los sistemas administradores de recursos es el software que busca satisfacer los requisitos de escalabilidad, procesamiento, volumen de información, seguridad y

almacenamiento. E incluyen procesos automatizados facilitan la administración y gestión de recursos del hardware [15].

Los sistemas administradores de recursos consisten en el control, asignación y uso de los recursos de hardware conectados a la computadora. Tales como: disco, pendrive, CD (disco compacto), impresora, escáner, mouse, teclado, etc. Y garantizan que todos los procesos en ejecución, incluidos los que corren en background, tengan su tiempo de procesador [16].

Bloqueadores de anuncios

Los bloqueadores de anuncios se refieren a diversas herramientas de software (por lo general, complementos de navegador), que supervisan las solicitudes de contenido editorial y publicitario de los navegadores. Además, evitan la visualización de cualquier contenido publicitario, que coincida con una entrada en las listas negras mantenidas por empresas de bloqueo de anuncios/comunidades de usuarios [17].

Los bloqueadores de anuncios son una categoría de programa de software informático. Normalmente, se ejecutan como extensiones de navegador web, que permiten a los usuarios eliminar selectivamente los anuncios de las páginas web que visitar. Este tipo de programas apuntan a una variedad de formatos de anuncios: banner imágenes, ventanas emergentes, enlaces patrocinados y videos. Son diseñados para mejorar las experiencias de los usuarios web al acortar el sitio, tiempos de carga, eliminar el desorden de la página web. Además de reducir la cantidad de información recopilada sobre el usuario y sus actividades [18].

Software de código abierto

Open Source Software (OSS) es un modelo de desarrollo de software. Que pone a disposición de una comunidad el código fuente con el fin de obtener ideas y crear soluciones de software más innovadoras [19].

Software de código cerrado

Closed Source Software (CSS) es un modelo de desarrollo. En el que solo los autores del software tienen derechos exclusivos para copiarlo, modificarlo o actualizarlo legalmente y restringen lo que los usuarios pueden hacer [19].

Developers Android

Sitio oficial para desarrolladores de aplicaciones Android. Contiene una amplia a documentos, guías y referencias API (Interfaces de programación de aplicaciones) y herramientas SDK (Software Development Kit) [20].

Google Play

Plataforma de distribución oficial de aplicaciones de Android y otros medios digitales, como música, películas y libros. Está disponible en dispositivos móviles y tabletas que ejecutan el sistema operativo Android (SO), dispositivos Chrome OS compatibles y en la web [21].

F-Droid

Catálogo instalable de aplicaciones de Software Libre y de Código Abierto (FOSS, Free and Open Source Software) para Android. Incluye un cliente Android para realizar instalaciones y actualizaciones, noticias, reseñas y otras características que cubren todo lo relacionado con Android y la libertad del software [22].

AppBrain

Plataforma de recopilación de información detallada sobre todas las aplicaciones en Google Play. Permite clasificar el historial y los datos técnicos de aplicaciones de terceros o propias, o explorar y filtrar aplicaciones. Y tiene como objetivo descubrir cuáles son las aplicaciones nuevas y favoritas para los usuarios [23].

ApkCombo

Plataforma de distribución digital de aplicaciones. Con tecnología de búsqueda y descarga de paquetes de aplicación Android (APK) sin restricciones de país o región. Cada archivo APK es el mismo que se encuentra disponible en Google Play y no se permiten archivos modificados [24].

Sistema de puntuación de vulnerabilidad común (CVSS)

Sistema de puntuación abierto y estandarizado para clasificar las vulnerabilidades de TI. Proporciona una forma de capturar las características principales de una vulnerabilidad. Además de producir una puntuación numérica que refleje su gravedad de manera cualitativa (como baja, media, alta y crítica) [25].

CVSS se basa en las siguientes métricas [25].

- Impacto de la confidencialidad.
- Impacto de integridad.
- Impacto en la disponibilidad.
- Condiciones de acceso (complejidad del ataque).
- Autenticación (credenciales necesarias para el ataque).
- Vector de acceso (acceso obtenido).

CVE details

Repositorio gratuito que recopila información sobre vulnerabilidades CVE (Common Vulnerabilities and Exposures) y su puntuación CVSS. Que se incluyen en la base de datos nacional de Estados Unidos [26].

Mobile Security Framework (MobSF)

Herramienta portable de código abierto. Que permite realizar pruebas de penetración, análisis de malware y marco de evaluación de seguridad. Así como también, análisis estáticos y dinámicos en aplicaciones (Android/iOS/Windows) [27].

SandDroid

Sistema de análisis automático de aplicaciones Android. Que combinas técnicas de análisis estático y dinámico. Y en función de los resultados del análisis, enumera los comportamientos de riesgo y calcula el puntaje de riesgo [28].

VirSCAN

Plataforma de detección de archivos en línea. Que hasta la fecha ha integrado 47 motores de escaneo de renombre internacional. Con el fin de reducir el riesgo de que los usuarios de Internet sean atacados por archivos maliciosos [29].

VirusTotal

Herramienta de seguridad informática online. Incluye un gran número de motores antivirus, escáneres de sitios web, herramientas de análisis de archivos y localizador uniforme de recursos (URL), además de contribuciones de los usuarios. El resultado produce un informe de dominios y direcciones IP contactadas, direcciones URL, archivos contenidos con su extensión, análisis dinámico y ejecución de complementos de análisis estático, motores heurísticos, firmas conocidas como malas, extracción de metadatos, identificación de señales maliciosas, etc. [30].

Android Studio

Entorno de desarrollo integrado (IDE) oficial para el desarrollo de aplicaciones para todo tipo dispositivo que cuente con un sistema operativo Android. Basado en potente editor de códigos y las herramientas para desarrolladores de IntelliJ IDEA [31].

Kanban

Palabra de origen japonés que significa “tarjetas visuales”. Es una metodología que consigue mostrar permanentemente y de forma muy visual el estado del proyecto a todos los implicados. También es útil en los casos en los que sea muy complicado planificar el trabajo. Así como también, cuando no se pueda comprometer un equipo

a trabajar con iteraciones de duración fija y predeterminada por el motivo que sea (interrupciones, cambios, dependencias, etc.) [32].

Los pasos para trabajar con Kanban son los siguientes [32]:

- Visualizar el flujo de todo el trabajo.
- Dividir el trabajo en ítems pequeños.
- Limitar el trabajo en curso (WIP).
- Medir el tiempo empleado en completar un ciclo completo.

Lean

Metodología de gestión de proyectos con la finalidad de reducir drásticamente el tiempo de entrega de un producto, reducir su precio y reducir también el número de defectos [32].
Los principios Lean son los siguientes [32]:

- Eliminar desperdicio.
- Crear conocimiento.
- Aplazar las decisiones.
- Entregar tan pronto como sea posible.
- Optimizar el todo.
- Respetar a las personas.

Scrum

Metodología de marco de trabajo que puede dar soporte a la innovación. Se basa en equipos autogestionados e iteraciones cortas (entre una y cuatro semanas) llamadas Sprints [32].

Los roles en el equipo Scrum son los siguientes [32]:

- Dueño del producto (Product Owner).

- Responsable de que el equipo (Scrum master).
- Equipo.
- Cliente.
- Coach.

Las reuniones Scrum son las siguientes [32]:

- Planificación del Sprint (Sprint Planning):
- Reunión diaria (Daily Meeting):
- Revisión del Sprint (Sprint Review):
- Retrospectiva del equipo (Sprint Retrospective):

Los artefactos de Scrum son los siguientes [32]:

- Pila de producto (Product Backlog).
- Pila de Sprint (Sprint Backlog).
- Pila de impedimentos (Burndown Chart).

End-User License Agreement (EULA)

Acuerdo de licencia de usuario final es un conjunto de cláusulas en las que el proveedor de la aplicación explica las restricciones a las que el usuario está sujeto al momento de aceptar la licencia de usuario e instalar la aplicación. Su uso es opcional, se incluye en los Términos y Condiciones de la aplicación. Se caracteriza por estar centrado en proteger únicamente al propietario de los derechos de autor. Además de permitir legalmente al proveedor acceder o compartir a la información privada de sus usuarios de la forma que deseen [33].

Las cláusulas que generalmente se incluyen son las siguientes [33]:

- Concesión de licencia.
- Restricciones de uso.
- Acuerdos relacionados.
- Infracción de copyright.

- Terminación de la licencia.
- Renuncia a la garantía.
- Limitaciones de responsabilidad.

ContentProvider

Un proveedor de contenido es una instancia que administra el acceso al conjunto de datos de la aplicación, que se comparten cuando otras aplicaciones realizan una solicitud. Un proveedor de contenido se exporta de manera predeterminada y cualquier aplicación en el sistema puede usarlos para leer y escribir datos. Por esta razón debe protegerse especificando la propiedad *exported* con el valor *"false"* en el manifiesto o protegiéndolo con un filtro de acción para que solo permitir el acceso a una determinada aplicación [34].

1.4 Objetivos

1.4.1 Objetivo general

Determinar las vulnerabilidades de seguridad que comúnmente se encuentran en la programación de distintas aplicaciones bloqueadoras de anuncios disponibles en plataformas de distribución digital en el año 2022.

1.4.2 Objetivos específicos

- Investigar políticas de seguridad de datos del usuario, permisos del dispositivo y modelos de desarrollo que presentan las aplicaciones bloqueadoras de anuncios.
- Detectar las vulnerabilidades de seguridad en la programación que presenta cada elemento de la muestra representativa de aplicaciones bloqueadoras de anuncios.
- Proponer soluciones para mejorar la seguridad informática de este tipo de aplicaciones.

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

Debido a la naturaleza del proyecto de investigación para la recolección de la información, se utilizó fichas electrónicas correspondientes al resumen de las políticas de seguridad de datos, que han hecho públicas los desarrolladores de aplicaciones bloqueadoras de anuncios. Así como también los permisos del dispositivo requeridos para su funcionamiento.

2.2 Métodos

El presente trabajo de investigación será desarrollado bajo enfoque mixto, porque es "un proceso sistemático, empírico y crítico, que combina la visión objetiva de la investigación cuantitativa y la visión subjetiva de la investigación cualitativa" [35]. Es cuantitativa debido a que se utiliza parámetros de medición en los datos recogidos sobre las aplicaciones, además es cualitativa porque se emiten juicios respecto al riesgo que presenta las vulnerabilidades de seguridad en dispositivos móviles Android.

2.2.1 Modalidad de la investigación

Investigación bibliográfica-documental

Porque es un estudio sistemático encaminado a compilar información de distintas fuentes documentales con los temas concretos: vulnerabilidades de seguridad y bloqueadores de anuncios [36].

Modalidades especiales

Porque es un estudio sistematizado orientado a la profundización y contribución en la solución de un problema de contexto muy específico, como es el caso en el problema de exceso de confianza en bloqueadores de anuncios [37].

2.2.2 Población y muestra

Para la presente investigación se tomó como población infinita debido a que no se puede contabilizar el número de aplicaciones bloqueadoras de anuncios disponibles en la internet.

Tabla 2.1 Población de aplicaciones bloqueadoras de anuncios.

Elaborado por: Investigador.

Población	**Número**	**Porcentaje**
Aplicaciones bloqueadoras de anuncios	Indefinido	100%
Total:	Indefinido	100%

2.2.2.1 Muestra

Para el cálculo del tamaño de la muestra representativa de una población infinita se utilizará un nivel de confianza deseado de 95% y un margen de error de 9.8% aplicando la siguiente fórmula:

$$\boldsymbol{Tamaño\ de\ la\ muestra}\ (\boldsymbol{n}) = \frac{z^2 * p * (1-p)}{e^2}$$

Tabla 2.2 Cálculo de muestra representativa.

Elaborado por: Investigador.

Variable	**Definición**	**Datos**
N	Población.	Indefinida.
NC	Nivel de confianza deseado.	95%
Z	Puntuación de valor z según NC.	1.96
P	Probabilidad de éxito.	0.5
E	Margen de error	9.8%

$$\boldsymbol{n} = \frac{1.96^2 * 0.5 * 0.5}{0.098^2} \quad \boldsymbol{n} = 100$$

De la población infinita de aplicaciones bloqueadoras de anuncios con un nivel de confianza de 95% y un margen de error 9.8% la fórmula estadística arrojo un tamaño de muestra de 100 aplicaciones bloqueadoras de anuncios.

2.2.3 Recolección de la información

La Tabla 2.3 presenta como se analizará las características obtenidas a través de la recolección de la información.

Tabla 2.3 Características a analizar de los *ad blocker*.

Elaborado por: Investigador.

<table>
<tr><td colspan="6">Ad blocker</td></tr>
<tr><td colspan="6">Criterios de elección: Aleatoriamente, mientras se encuentre disponible públicamente en plataformas de distribución digital e internet.</td></tr>
<tr><td rowspan="6">Características de extraídas de las cien aplicaciones</td><td rowspan="5">Presenta política de seguridad de datos.</td><td>No</td><td colspan="3">No se realiza otra clasificación.</td></tr>
<tr><td rowspan="4">Si</td><td rowspan="2">Tipo de datos</td><td>Recogidos</td><td rowspan="2">Con que objetivo</td></tr>
<tr><td>Compartidos</td></tr>
<tr><td colspan="2" rowspan="2">Incluye Prácticas de seguridad</td><td>No</td><td>No se realiza otra clasificación.</td></tr>
<tr><td>Si</td><td>Tipos de practica de seguridad.</td></tr>
<tr><td colspan="2">Permisos del dispositivo que solicita la aplicación</td><td colspan="3">Peligrosos</td></tr>
<tr><td colspan="2"></td><td colspan="3">Obsoletos</td></tr>
<tr><td colspan="2">Modelo de desarrollo de la aplicación</td><td colspan="3">Código abierto</td></tr>
<tr><td colspan="2"></td><td colspan="3">Código cerrado</td></tr>
</table>

Para la recolección de la información, a las cien aplicaciones se aplicó una revisión sistemática de fuentes electrónicas. Fuentes en las que desarrolladores hacen públicos los datos técnicos y las características de sus aplicaciones, tales como: Google Play, F-Droid, ApkCombo, AppBrain y sitios web de la aplicación. Información con la que se elaboró cien fichas electrónicas. Cada ficha, que se encuentra dentro del Anexo A, presenta el modelo de desarrollo de la aplicación, una síntesis de las políticas de seguridad de datos y los permisos solicitados por la aplicación.

2.2.3.1 Políticas de seguridad de datos.

Políticas de seguridad de datos del usuario públicas.

Las cien aplicaciones fueron investigadas en función de sus políticas públicas. En el Gráfico 2.1 se muestra, de manera gráfica, el resultado obtenido.

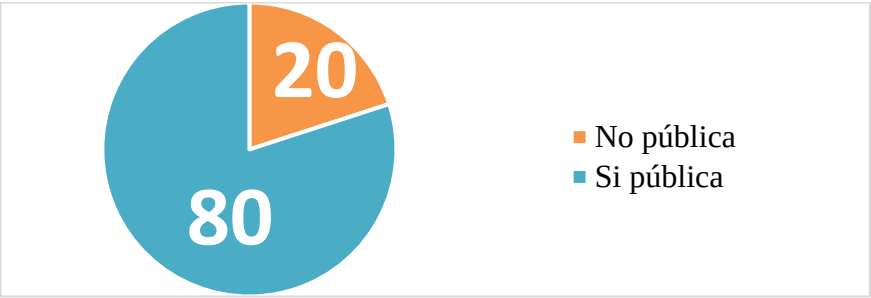


Gráfico 2.1 Políticas públicas de privacidad de datos.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.1 ilustra que, un total de ochenta aplicaciones, informan a sus usuarios que datos comparten, recogen y sus prácticas de seguridad. En el caso de las veinte aplicaciones restantes, por razones como: falta de actualización de la aplicación, desinterés por parte del desarrollador o evitar complicaciones legales al crear o modificar sus políticas, no presentan políticas de seguridad. Por esta razón, serán ochenta el total de aplicaciones catalogadas en función de los datos comparten, recogen y sus prácticas de seguridad.

Aplicaciones que recogen datos.

Las ochenta aplicaciones que hacen públicas sus políticas fueron catalogadas en función de su postura de recolección de datos. En el Gráfico 2.2 se muestra, el resultado obtenido.

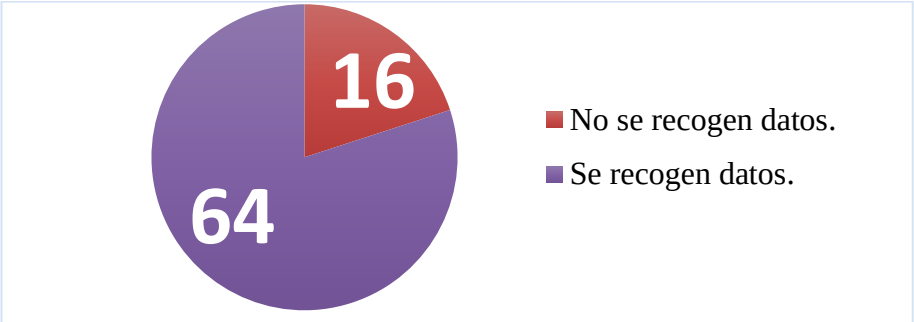


Gráfico 2.2 Aplicaciones que requieren recoger datos.
Elaborado por: Investigador.
Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.2 ilustra que, de las ochenta aplicaciones que hacen públicas sus políticas, sesenta y cuatro indican estar a favor de la recolección de datos. En el caso de las dieciséis aplicaciones restantes, públicamente indican que no recogen datos. Por ende, serán sesenta y cuatro el total de aplicaciones catalogadas en función de los tipos de datos recogidos y los motivos de recolección de datos.

Aplicaciones que comparten datos a terceros.

Las ochenta aplicaciones que hacen públicas sus políticas fueron catalogadas en función de su postura de compartición de datos. En el Gráfico 2.3 se muestra, el resultado obtenido.

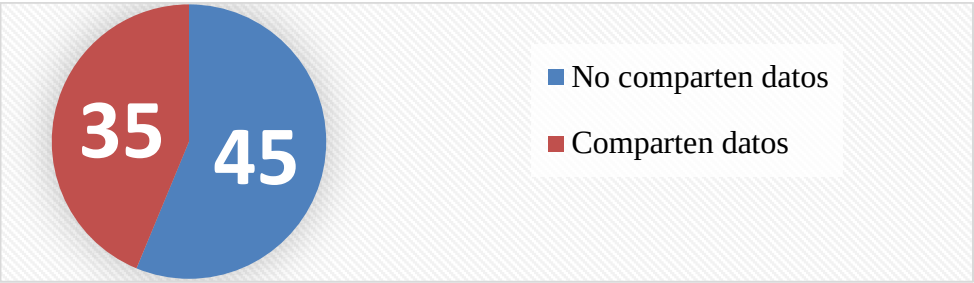


Gráfico 2.3 Aplicaciones que comparten datos con terceros.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.3 ilustra que, de las ochenta aplicaciones, cuarenta y cinco indican que no necesita compartir los datos que recogen con terceros para ofrecer sus servicios. Por otro lado, las treinta y cinco aplicaciones restantes públicamente expresan que están a favor de compartir los datos recogidos con terceros. Por tal motivo, serán treinta y cinco el total de aplicaciones catalogadas en función de los tipos de datos comparten.

Aplicaciones con prácticas de seguridad.

Las ochenta aplicaciones que hacen públicas sus políticas fueron catalogadas en función de sus prácticas de seguridad. En el Gráfico 2.4 se muestra, el resultado obtenido.

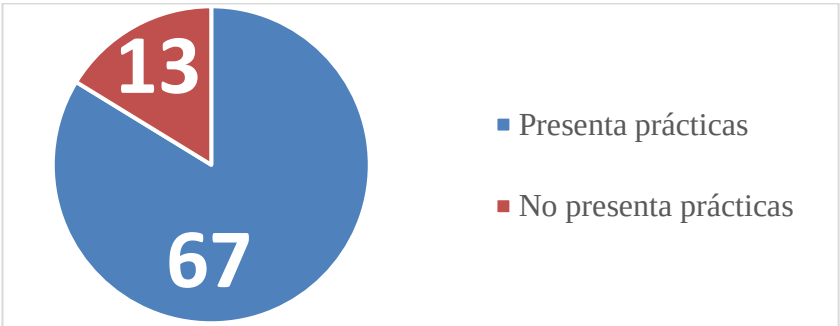


Gráfico 2.4 Aplicaciones que presentan prácticas de seguridad de datos.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

El Gráfico 2.4 ilustra que, de las ochenta aplicaciones que hacen públicas sus políticas de seguridad, sesenta y siete indican que acciones toman para proteger los datos de sus usuarios. Por otro lado, las trece aplicaciones restantes públicamente expresan que no realizan ninguna acción que proteja los datos de sus usuarios. En consecuencia, serán sesenta y siete el total de aplicaciones catalogadas en función de los tipos prácticas de seguridad que emplean.

Objetivos de la recolección de datos y transferencia de datos a terceros.

Las sesenta y cuatro aplicaciones que recogen datos fueron catalogadas en función de sus objetivos. En el Gráfico 2.5 se muestra, el resultado obtenido.

Gráfico 2.5 Finalidad de recolección y compartición de datos.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.5 ilustra que, se maneja información sensible como: procesar pagos con tarjeta de crédito, transferencia bancaria u otros medios y gestionar contactos del

usuario. Así como también existe un uso a los datos manejados que afecta directamente al usuario como el caso de enviar correo propaganda.

Información recogida por aplicaciones bloqueadoras de anuncios.

Las sesenta y cuatro aplicaciones que recogen datos fueron catalogadas en función del tipo de información recogida. En el Gráfico 2.6 se muestra, el resultado obtenido.

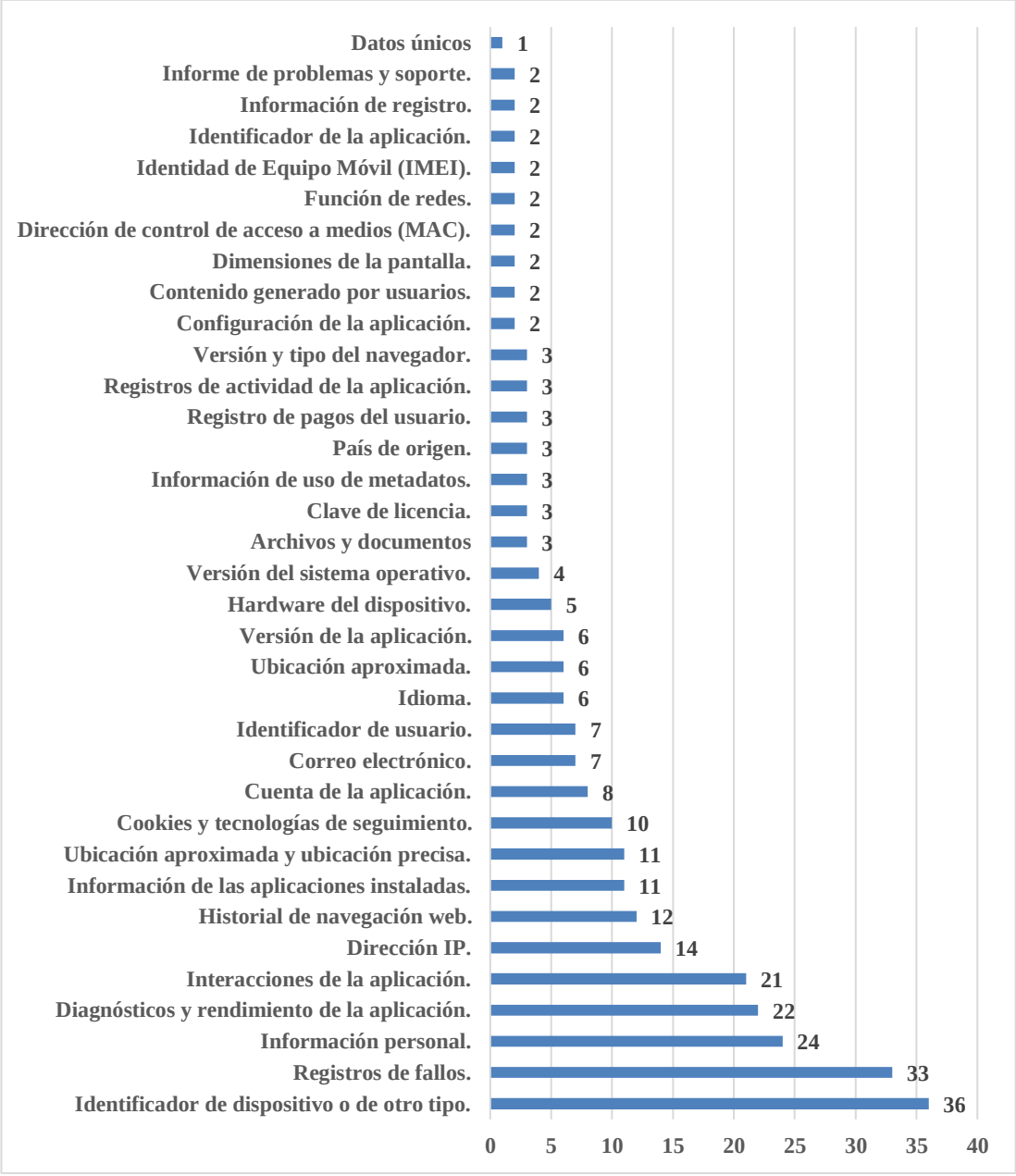


Gráfico 2.6 Estadísticas de datos recogidos.

Elaborado por: Investigador Anexo A.

Fuente: Fichas electrónicas.

Análisis e interpretación de resultados:

El Gráfico 2.6 ilustra que, entre los elementos de información que se consideran más sensibles, que los *ad blockers* recogen, se encuentran: información personal, correo electrónico, dirección IP, dirección MAC, identificador IMEI, perfil del usuario, ubicación, historial de navegación, archivos generados por el usuario, tipo de tarjeta, últimos 4 dígitos de la tarjeta.

Datos únicos se refiere a elementos de información para los que se encontró una sola aplicación ad blocker que los recoge. Estos son: anuncio solicitado, contenido del anuncio, datos biométricos, dirección URL, DNS de los servidores, duración de visita al sitio web, enrutadores cercanos, fecha de caducidad, fecha y hora del acceso, ID de cargo de Stripe, identificación genérica, identificador de compilación, identificador de sesión, idioma de la aplicación, información de conexión VPN, información de dispositivos vinculados, información de salud, información de voz, información del pedido, información posventa, historial de compras, lista de filtros habilitados, nombre de la aplicación que solicita el servicio, nombre de usuario, nombre del operador de la red móvil, número de serie del dispositivo, perfil de usuario, preferencias de navegación web, registro de comunicación, registro de transacciones, resolución de pantalla, soporte por correo electrónico, SSID de la red Wifi, tipo de tarjeta, últimos 4 dígitos de la tarjeta y uso de memoria. En el gráfico, todos estos datos quedan aglutinados en una única categoría para disminuir la complejidad de este.

Datos compartidos con terceros por aplicaciones bloqueadoras de anuncios.

Las treinta y cinco aplicaciones que comparten datos fueron catalogadas en función del tipo de información compartida. En el Gráfico 2.7 se muestra el resultado obtenido.

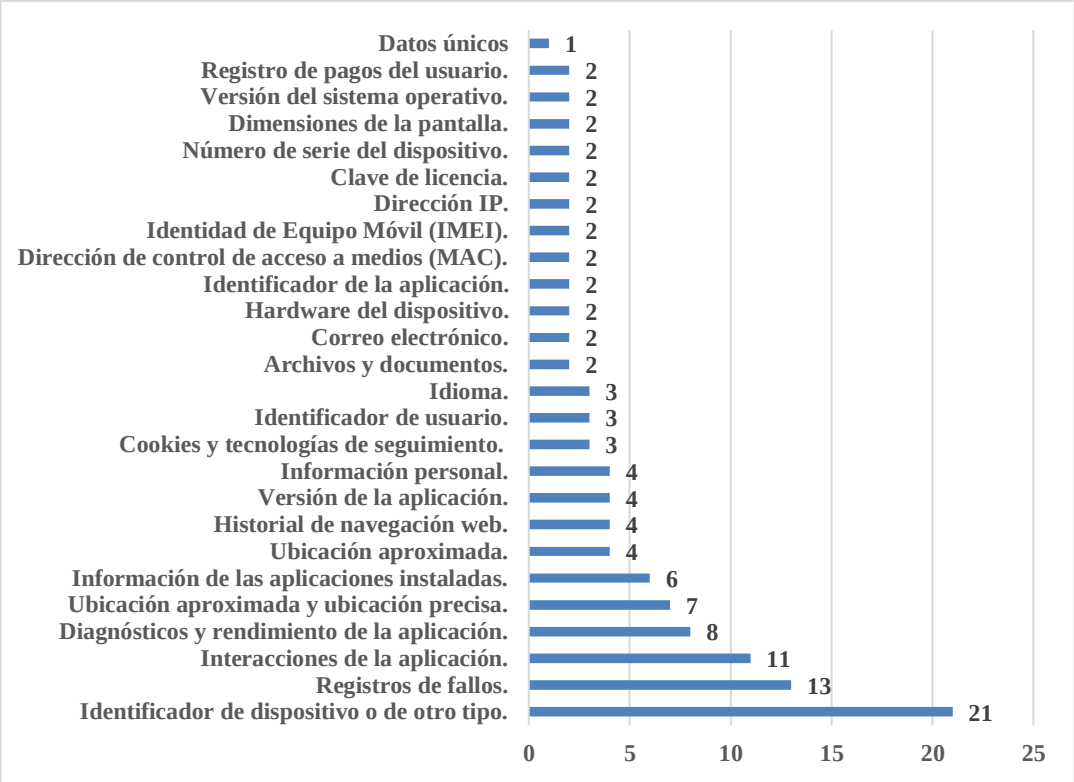


Gráfico 2.7 Estadísticas de datos compartidos por terceros.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.7 ilustra que, entre los elementos de información que se consideran más sensibles, cuando una aplicación los comparte con terceros, se encuentran: información personal, correo electrónico, dirección IP, dirección MAC, identificador IMEI, perfil del usuario, ubicación e historial de navegación.

Datos únicos se refiere a elementos de información para los que se encontró una sola aplicación *ad blocker* que los compartiese con terceros. Estos son: contenido de redes sociales generado por usuarios, datos biométricos, identificación genérica, información de dispositivos vinculados, información de uso de metadatos, información necesaria para actividades del controlador de datos, perfil de usuario y registro de transacciones. En el gráfico, todos estos datos quedan aglutinados en una única categoría para disminuir la complejidad de este.

Prácticas de seguridad de los desarrolladores con políticas públicas.

Las sesenta y siete aplicaciones que hacen públicas sus políticas fueron catalogadas en función del tipo de prácticas de seguridad de datos. En el Gráfico 2.8 se muestra, el resultado obtenido.

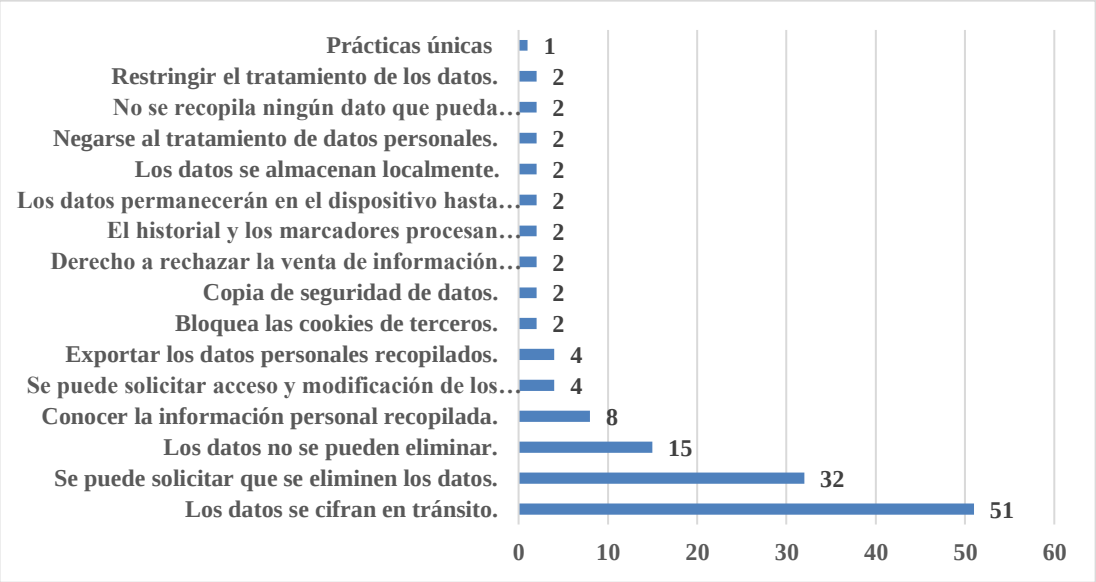


Gráfico 2.8 Estadísticas de prácticas de seguridad de datos.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.8 ilustra que, de las sesenta y siete aplicaciones que hacen públicas sus políticas de seguridad, cincuenta y uno presentan de manera formal que *cifran sus datos en tránsito*. Por otro lado, las veinte y nueve aplicaciones restantes no estarían cifrando sus datos en tránsito, lo que podría llevar a filtración de los datos que recoge la aplicación.

Cabe destacar las aplicaciones *"Adblock Fast" y "Adblock Less Ads"* que entre sus prácticas indican *el derecho a rechazar la venta de información personal*, sugiere que se realiza venta de información personal recopilada a menos que se solicite no hacerlo.

En el caso de las prácticas que corresponden a solicitudes como: restringir el tratamiento de los datos, exportar los datos, eliminar los datos o conservarlos de forma anónima, acceder a los datos recolectados, modificar los datos recolectados, entre otros. *P*roducirían el mismo efecto que las aplicaciones que no presentas prácticas de seguridad de datos, a menos que el usuario conozca correctamente las políticas de seguridad de la aplicación.

Las *prácticas únicas* se refieren a las prácticas de seguridad de datos para las que se encontró que una sola aplicación *ad blocker* las incluye. Estás son: negarse al uso de la información recolectada, administrar cookies y scripts, agregar un código de afiliado a algunos sitios de comercio electrónico, al desinstalar la aplicación todos los datos se vuelven anónimos permanentemente, almacenar información solo necesaria para el funcionamiento de los servicios, almacenar datos personales durante el tiempo que sea necesario para cumplir con requisitos y obligaciones legales, para su posterior eliminación, anonimizar la dirección IP, la conexión VPN no almacena ninguna información, control de acceso a los datos, control de acceso al sistema, control de transmisión, copia de seguridad de datos se almacenan hasta por un mes, elimina la cuenta y la información proporcionada si no ha utilizado los servicios durante un período prolongado, en el área de inicio de sesión se utiliza lhCaptcha, evitar la fuga de búsqueda de forma predeterminada, información personal es anónima con base a la identificación genérica, dirección IP se elimina dentro de las horas posteriores a la recepción, la información así recopilada se conservará solo durante el tiempo limitado, la información personal se conservará en el dispositivo y no será recopilada, los datos no se correlacionan con ninguna información personal y se usa de forma anónima, los datos personales del usuario se conservarán durante un plazo no superior a dos años a partir de la cancelación de la cuenta de la aplicación, los datos que no se requieran para obligaciones legales se eliminarán inmediatamente cuando el cliente, se dé de baja del producto, los datos recopilados se desasocian permanentemente al momento de la desinstalación, los datos recopilados sé pseudo anonimizan y se almacenan utilizando la identificación genérica, los datos se eliminen al cerrar la aplicación, navegación privada, ninguno de los datos se almacenará o enviará a los servidores, no recopila ningún dato, no se recopila datos de navegación, no se recopilaron direcciones IP, no se requiere identificación, no trabaja con ningún sitio que comparta información de

identificación personal, no utiliza a terceros para realizar la inserción del código, solo se recopila datos anónimos y puramente estadísticos, restringir el tratamiento de la información recolectada, revisión de seguridad independiente, se puede solicitar el tiempo de almacenamiento y fuente de los datos, se puede solicitar exportación de los datos, se puede solicitar que se eliminen los datos o se conserven de forma anónima, separación lógica, servidor VPN local incorporado, solicitar leer o modificar la información recolectada, solicitar una copia de la información recolectada, soporte de lista de filtros ad block, todos los datos se pueden eliminar fácilmente y se utiliza un identificador único generado aleatoriamente ("Identificación genérica"). En el gráfico, todas estas prácticas quedan aglutinadas en una única categoría para disminuir la complejidad de este.

2.2.3.2 Modelos de desarrollo de aplicaciones bloqueadoras de anuncios.

Las cien aplicaciones fueron catalogadas en función de su modelo de desarrollo. En el Gráfico 2.9 se muestra, el resultado obtenido.

Gráfico 2.9 Modelos de desarrollo de aplicaciones bloqueadoras de anuncios.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Análisis e interpretación de resultados:

El Gráfico 2.9 ilustra que, de la muestra de cien aplicaciones bloqueadoras de anuncios, ochenta y cinco son de código cerrado y prefieren mantener la confidencialidad de su código fuente. Por otra parte, las quince restantes expone su código fuente para los usuarios de su comunidad.

En las Tabla 2.4 y Tabla 2.5 se enlistan los *ad blockers* escogidos aleatoriamente según su modelo de desarrollo. E incluye los nombres con los que se encuentran en el mercado.

Tabla 2.4 Aplicaciones bloqueadoras de anuncios de código cerrado.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Aplicaciones bloqueadoras de anuncios de código cerrado	
1. ADB AdBlocker	44. eShild:Adblocker, Secure & Private, no more ads
2. Adblock Browser: veloz, seguro	45. FAB Adblocker Browser: Adblock
3. Ad Blocker Block All Ads	46. Ghostery Privacy Browser
4. dBlocker for Android	47. Goclean: Detector de anuncios
5. Ad Blocker for apps - Ad Clear	48. Godzilla Browser: AdBlocker
6. Ad Blocker - Stop the Ads	49. Guard My Web Adblock VPN
7. AdBlocker Ultimate Browser	50. Hi Browser- privado&rápido
8. AdBlock for Samsung Internet	51. IgeBlock - YouTube ad blocker
9. Adblock Less Ads	52. Incognito VPN - Fast VPN & Ad Blocker for Android
10. Adblock Mobile	53. Microsoft Edge
11. Adblock para navegadores	54. Mobile Adblock - remove all ad
12. Adblock - Private Adblocker Browser App	55. Moon Browser - Adblock
13. Ad Block REMOVER - NEED ROOT	56. Opera GX: navegador gaming
14. AdBlock VPN	57. Orions - Privacy Browser
15. AdBlock VPN for Android	58. Pando - Rewards Web Browser
16. AdClear: bloqueador de contenido	59. Private Browser - Privado&Safe
17. AdFree	60. Puffer: Privacy Protection & Ad-Blocking
18. AdGuard VPN – proxy privado	61. Pure Browser Pro-Ad Blocker

19. AdLock for Android	62. Pure Web Browser-Ad Blocker
20. AdLocker - Adblock & Firewall	63. Purple DNS | Fast Ads Blocker
21. AdProtect - Adblock & Firewall	64. Purple Ad Blocker - Family Protection
22. Ad Remover	65. Soul Browser
23. Ads Blocker for Android	66. Spark
24. AdShield - Ad blocker	67. Stampy Browser: AdBlocker, Incognito and Secure
25. Adware Hunter - Popup Ad Fixer	68. StopAd
26. Aloha Navegador + VPN privado	69. Super Browser Mini - Only 8MB
27. AppBrain Ad Detector	70. Tincat Browser m3u8 mpd live
28. Avast Secure Browser	71. Turbo Navegador: Privado & Bloqueador de anuncios
29. Awax Bloqueador de anuncios	72. UC Browser Turbo - Descarga rápida, Seguro
30. Banana Browser: Adblock, Secure DNS, Fast & Secure	73. Umbrella - Adblock & Firewall
31. Blocker by +Now: Ad Blocker	74. Unicorn Blocker:Adblocker, Fast & Private
32. Bloqueador de anuncios Direct CPV Technologies	75. Via-Rápido y liviano Navegador
33. Bloqueador de anuncios Maxsortube	76. Vider Adblock - Video Browser
34. BLU: AdBlock, Fast & Clean, Protege la Privacidad	77. Vivaldi Navegador
35. Bravo Navegador Rápido, AdBlock	78. Vivo Browser
36. Browser Popup Detector - Block Ads In Browser	79. VPN Dash: Fast VPN Proxy
37. Clario: Security & Privacy	80. VPN Galaxy - VPN Proxy & AdBlock
38. Clean Ads Skip Ads Universal Tool	81. VPN Owl: Fast and Secure VPN
39. CM Browser - Fast Download, Private, Ad Blocker	82. VPN + TOR Browser and Ad Block

40. Crystal para Samsung Internet	83. VPN Venus
41. Dolphin Browser Navegador Web	84. WebGuard - Adblock & Firewall
42. DuckDuckGo Privacy Browser	85. 고차단 브라우저 : 블로켓 - 인터넷 애드블록
43. Epic Privacy Browser Ad Block, Almacén, VPN	

Tabla 2.5 Aplicaciones bloqueadoras de anuncios de código abierto.

Elaborado por: Investigador.

Fuente: Fichas electrónicas Anexo A.

Aplicaciones bloqueadoras de anuncios de código abierto	
1. Ad Blocker Turbo - Adblocker Browser	9. DNS66
2. Adblock Fast	10. Firefox Focus: el navegador
3. ABP para Samsung Internet	11. FOSS Browser
4. AdGuard Content Blocker	12. Lightning Browser - Web Browser
5. Block This!	13. Midori Lite Navegador Web
6. Blokada 6: The Privacy App+VPN	14. personalDNSfilter
7. Brave navegador web privado	15. Proton VPN: VPN veloz y segura
8. Bromite - Take back your browser	

2.2.3.3 Permisos solicitados por aplicaciones bloqueadoras de anuncios.

Un permiso con nivel de protección peligroso es un permiso que puede afectar negativamente al usuario, debido al potencial riesgo de que el sistema otorgue a una aplicación solicitante el acceso a datos privados del usuario o control sobre el dispositivo [38].

La Tabla 2.6 presenta los permisos del dispositivo que las aplicaciones bloqueadoras de anuncios solicitan y han sido catalogados como peligrosos por la fuente Developers Android [39]. Incluyendo una ponderación promedio de gravedad del permiso. Basado en el sistema de puntaje de clasificación de estándar CVSS, a partir de los registros extraídos del repositorio CVE details relacionados con cada permiso.

Tabla 2.6 Matriz de permisos peligrosos.

Elaborado por: Investigador.

Permiso que se solicita	**Descripción**	**Identificador: gravedad***	$\bar{X}$
ACCESS_COARSE_LOCATION Ubicación aproximada (basada en red).	Permite que una aplicación acceda a la ubicación aproximada.	CVE-2019-9464: CVSS=4.3 CVE-2018-9526: CVSS=5.0 CVE-2014-0806: CVSS=4.3 CVE-2012-6335: CVSS=3.3 CVE-2012-6334: CVSS=2.9	4.0
ACCESS_FINE_LOCATION Ubicación precisa (basada en red y GPS).	Permite que una aplicación acceda a una ubicación precisa.	CVE-2022-30757: CVSS=2.1 CVE-2021-33057: CVSS=0.0 CVE-2019-15304: CVSS=6.4 CVE-2014-1887: CVSS=4.3	3.2

CAMERA Cámara.	Necesario para poder acceder al dispositivo de la cámara.	CVE-2022-23998: CVSS=4.3 CVE-2020-11990: CVSS=2.1 CVE-2019-11014: CVSS=10.0 CVE-2018-5832: CVSS=10.0 CVE-2017-0822: CVSS=7.5 CVE-2017-0544: CVSS=9.3 CVE-2016-8444: CVSS=7.6 CVE-2016-8412: CVSS=7.6 CVE-2016-3916: CVSS=9.3 CVE-2016-3915: CVSS=9.3 CVE-2016-3834: CVSS=4.3 CVE-2016-2449: CVSS=9.3 CVE-2009-2348: CVSS=6.9	7.5
GET_ACCOUNTS Buscar cuentas en el dispositivo.	Permite el acceso a la lista de cuentas en el Servicio de Cuentas.	CVE-2022-20303: CVSS=0.0 CVE-2019-11063: CVSS=8.3 CVE-2020-0448: CVSS=2.1	3.5
POST_NOTIFICATIONS Permitir publicar notificaciones.	Permite que una aplicación publique notificaciones.	CVE-2022-24886: CVSS=2.1	2.1

READ_CALENDAR Leer eventos de calendario.	Permite que una aplicación lea los datos del calendario del usuario.	CVE-2022-33705: CVSS=2.1 CVE-2021-0487: CVSS=7.2	4.7
READ_CONTACTS Consultar contactos.	Permite que una aplicación lea los datos de los contactos del usuario.	CVE-2021-25403: CVSS=2.1 CVE-2021-0953: CVSS=7.2 CVE-2021-0952: CVSS=4.7 CVE-2021-0603: CVSS=4.4 CVE-2021-0569: CVSS=1.9 CVE-2021-0304: CVSS=4.9 CVE-2020-27098: CVSS=2.1 CVE-2019-20468: CVSS=7.5 CVE-2018-14986: CVSS=5.0 CVE-2015-1541: CVSS=4.3 CVE-2011-1717: CVSS=2.1	4.2
READ_EXTERNAL_STORAGE Leer contenido del almacenamiento compartido.	Permite que una aplicación lea desde un almacenamiento externo.	CVE-2019-20468: CVSS=7.5 CVE-2019-12370: CVSS=4.3 CVE-2019-12369: CVSS=4.3 CVE-2019-12368: CVSS=4.3 CVE-2019-12367: CVSS=4.3 CVE-2019-12366: CVSS=4.3	3.7

		CVE-2019-12365: CVSS=4.3 CVE-2018-6599: CVSS=2.1 CVE-2018-15004: CVSS=4.3 CVE-2018-15002: CVSS=1.9 CVE-2018-15001: CVSS=2.1 CVE-2018-14995: CVSS=1.9 CVE-2018-14979: CVSS=1.9 CVE-2016-10135: CVSS=4.3	
READ_PHONE_STATE Consultar la identidad y el estado del teléfono.	Permite el acceso de solo lectura al estado del teléfono, información actual de la red celular, el estado de las llamadas en curso y una lista de los correos registrados en el dispositivo.	CVE-2016-0831: CVSS=4.3 CVE-2012-2640: CVSS=5.0	4.7
READ_SMS Enviar mensajes a los invitados sin el consentimiento de los propietarios.	Permite que una aplicación lea mensajes SMS.	CVE-2022-23835: CVSS=4.3 CVE-2018-15661: CVSS=2.6 CVE-2011-0680: CVSS=5.0 CVE-2011-4769: CVSS=5.8 CVE-2011-4772: CVSS=5.8 CVE-2011-4773: CVSS=5.8 CVE-2011-4863: CVSS=5.8	5.0

		CVE-2011-4698: CVSS=6.4	
RECEIVE_SMS Enviar mensajes a los invitados sin el consentimiento de los propietarios.	Permite que una aplicación reciba mensajes SMS.	CVE-2017-17175: CVSS=3.3 CVE-2016-3883: CVSS=4.3 CVE-2012-2562: CVSS=7.6 CVE-2009-2656: CVSS=5.0	5.1
RECORD_AUDIO Grabar sonido.	Permite que una aplicación grabe audio.	CVE-2020-0061: CVSS=4.9 CVE-2019-15743 CVSS=2.1 CVE-2019-15475: CVSS=2.1 CVE-2019-15474: CVSS=2.1 CVE-2019-15473: CVSS=2.1 CVE-2019-15472: CVSS=2.1 CVE-2019-15471: CVSS=2.1 CVE-2019-15470: CVSS=2.1 CVE-2019-15469: CVSS=2.1 CVE-2019-2219: CVSS=4.7 CVE-2018-14996: CVSS=7.2 CVE-2016-6715: CVSS=4.3 CVE-2009-2348: CVSS=6.9	3.4

SEND_SMS Añadir o modificar eventos de calendario y enviar mensajes a los invitados sin el consentimiento de los propietarios.	Permite que una aplicación envíe mensajes SMS.	CVE-2021-39781: CVSS=4.6 CVE-2020-0052: CVSS=1.9 CVE-2020-13626: CVSS=2.1 CVE-2017-18666: CVSS=5.0 CVE-2016-3888: CVSS=2.1 CVE-2016-11046: CVSS=5.0 CVE-2014-8610: CVSS=3.3 CVE-2013-4764: CVSS=2.1 CVE-2012-2217: CVSS=6.4	3.6
WRITE_CALENDAR Añadir eventos de calendario.	Permite que una aplicación escriba los datos del calendario del usuario.	CVE-2014-3084: CVSS=4.9	4.9
WRITE_CONTACTS Leer y escribir datos de contacto.	Permite que una aplicación escriba los datos de los contactos del usuario.	CVE-2021-25414: CVSS=4.6	4.6
WRITE_EXTERNAL_STORAGE Editar/eliminar contenido del almacenamiento compartido.	Permite que una aplicación escriba en el almacenamiento externo.	CVE-2021-0550: CVSS=4.6 CVE-2019-20468: CVSS=7.5 CVE-2014-1885: CVSS=6.4	6.2
*Identificador y puntaje CVSS de vulnerabilidades que hacen referencia al permiso peligroso, extraídos del repositorio *CVE details*. $\bar{X}$: Promedio.			

Permisos obsoletos y permisos removidos.

Un permiso catalogado como obsoleto es un elemento que puede quedar inservible por varias razones, por ejemplo: su uso probablemente generara errores, puede actualizarse de manera incompatible, ha sido reemplazado por una alternativa actual. También pueden eliminarse en una versión futura [40].

La Tabla 2.7 detalla los permisos removidos y obsoletos extraídos de la fuente Developers Android.

Tabla 2.7 Matriz de permisos obsoletos y permisos removidos.

Elaborado por: Investigador.

Código y permiso referido por la aplicación bloqueadora de anuncios.	Agregado en API	Funcional hasta API	Obsoleto en API	Removido en API
GET_TASKS: Recuperar aplicaciones en ejecución. **Generado:** 15/10/2014 **URL:**https://developer.android.com/sdk/api_diff/21/changes/android.Manifest.permission	1	20	21	
AUTHENTICATE_ACCOUNTS: Crear cuentas y establecer contraseñas.	5	22		23
MANAGE_ACCOUNTS: Añadir o eliminar cuentas.	5	22		23
READ_HISTORY_BOOKMARKS: Consultar historial y marcadores web.	4	22		23

READ_PROFILE: Leer datos de registro personales. **USE_CREDENTIALS:** Usar cuentas del dispositivo. **WRITE_HISTORY_BOOKMARKS:** Escribir en el historial y en los marcadores web. **Fuente:** Developers Android **URL:**https://developer.android.com/sdk/api_diff/23/changes/android.Manifest.permission **Generado:** 14/08/2015	14 5 4	22 22 22		23 23 23
Código y permiso referido por la aplicación bloqueadora de anuncios.	**Agregado en API**	**Funcional hasta API**	**Obsoleto en API**	**Removido en API**
FLASHLIGHT: Controlar linterna. **Fuente:** Developers Android **URL:**https://developer.android.com/sdk/api_diff/24/changes/android.Manifest.permission **Generado:** 13/06/2016	1	23		24
USE_FINGERPRINT: Permite usar hardware de huellas dactilares. **Vigente:** USE_BIOMETRIC (Permite usar modalidades biométricas compatibles con el dispositivo). **Fuente:** Developers Android **URL:**https://developer.android.com/sdk/api_diff/28/changes/android.Manifest.permission **Generado:** 01/06/2018	23	27	28	

2.2.4 Procesamiento y análisis de datos

De acuerdo con la información recolectada sobre las políticas de seguridad de datos, permisos del dispositivo y modelos del desarrollo han hecho públicas los desarrolladores de aplicaciones bloqueadoras de anuncios, se puede decir que:

- Es necesario conocer qué tipo de información quedaría expuesta ante la explotación de una vulnerabilidad en la programación de aplicaciones bloqueadoras de anuncios.
- Existen aplicaciones bloqueadoras de anuncios que no hacen públicas sus políticas de seguridad de datos del usuario.
- Existen aplicaciones que indican entre sus razones para recoger y compartir datos situaciones que afectarían directamente a sus usuarios como el enviar correo propaganda y gestionar los contactos del usuario.
- Existen aplicaciones bloqueadoras de anuncios que no hacen públicas sus prácticas de seguridad de datos.
- Existen aplicaciones bloqueadoras de anuncios que indican recoger y compartir información personal, historial de navegación, ubicación, entre otra información considerada sensible.
- Existen aplicaciones bloqueadoras de anuncios que indican no realizar el proceso de cifrado de los datos que transmiten.
- Existen aplicaciones bloqueadoras de anuncios que entre sus prácticas de seguridad de datos hacen alusión a la venta de información personal.
- Existen aplicaciones que solicitan permisos que pueden dar acceso a datos privados del usuario o control sobre el dispositivo.
- Existen aplicaciones que solicitan permisos que han sido catalogados como obsoletos o han sido removidos de la API de Android y que podrían generar fallos en el dispositivo.

CAPÍTULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

Posterior a la recolección de información sobre las políticas de seguridad de datos, permisos del dispositivo y modelos de desarrollo de aplicaciones bloqueadoras de anuncios, se procedió a elegir la metodología y las herramientas, que se utilizaran análisis de cada elemento de la muestra representativa para detectar vulnerabilidades informáticas que comprometerían la información de los usuarios.

3.1.1 Análisis comparativo de metodologías Ágiles

La elección de la metodología se realizó con el objetivo de definir como se gestionará el desarrollo del proyecto. Debido al reducido equipo de trabajo, los lapsos cortos para presentar los entregables, posibles eventos imprevistos y tareas secuenciales.

La Tabla 3.1 presenta las metodologías agiles que cumplen con el criterio de estar orientadas a el desarrollo de tareas.

Tabla 3.1 Comparación entre metodologías ágiles.

Elaborado por: Investigador.

Descripción	**Kanban**	**Lean**	**Scrum**
Plazos de trabajo	Ajustados.	Largos.	Largos.
Equipos de trabajo	Pequeños. Medianos.	Medianos. Grandes.	Pequeños. Grandes.
Roles	Roles adaptables.	Roles adaptables.	Cliente. Product Owner. Scrum master. Equipo. Coach.

Artefactos	Tablero Kanban. Tarjetas Kanban.	Desperdicio. Discrepancia. Sobrecarga.	Pila de producto. Pila de Sprint. Pila de impedimentos.
Orientación	Gestión de proyectos.	Organización y gestión de proyectos.	Organización y gestión de proyectos.
Método	Visualización de tareas.	Eliminación de desperdicio.	Ciclo de trabajo por sprints.
Tareas	No simultaneas.	En simultaneo.	En simultaneo.

Con base en el análisis comparativo realizado en la Tabla 3.1, se concluyó que la metodología Kanban es la mejor opción para el desarrollo de la propuesta, debido a que está orientada a grupos de trabajos pequeños, con plazos de trabajo ajustados. Además, está centrada en completar tareas antes de seguir con la siguiente y otorga flexibilidad en caso de eventos imprevistos.

3.1.2 Determinación de herramienta para el análisis de aplicaciones bloqueadoras de anuncios.

La elección se centró en las cláusulas EULA que se incluyen en los términos y condiciones de las aplicaciones. Las cuales prohíben acciones como ingeniería inversa y el acceso al código fuente de la aplicación. Por esta razón, se escogió herramientas online que realicen un análisis interno y no muestren el código fuente de la aplicación. Además de que generen el informe resultante con periodos de espera cortos.

La Tabla 3.2 presenta el resultado de la investigación de herramientas para análisis estático y dinámico de aplicaciones Android.

Tabla 3.2 Comparación entre herramientas de análisis de aplicaciones.

Elaborado por: Investigador.

Requerimientos	**Herramienta**			
	MobSF	**SanDroid**	**VirSCAN**	**VirusTotal**
Tipo de análisis	Malware	Malware	Malware	Malware

	Dinámico Estático	Dinámico Estático	Dinámico	Dinámico Estático
Formato de archivos	APK, XAPK, IPA, APPX	APK, ZIP	Cualquier formato	Cualquier formato
Tamaño máximo (MB)	No especifica	50	50	550
Código fuente	Obtenible	No obtenible	No obtenible	No obtenible
Reporte	Posterior al análisis	No especifica	Posterior al análisis	Posterior al análisis
Motores de escaneo	No especifica	70	47	70
Disponibilidad	Online Offline	Online	Online	Online APK

A partir el análisis realizado en la Tabla 3.2, se concluyó, que la herramienta VirusTotal es la que mejor se adapta para el desarrollo de la investigación, debido a que aplica análisis estático y dinámico de instaladores Android, el tiempo de espera para obtener el informe es corto, se encuentra disponible en línea, el tamaño máximo de subida de los archivos es suficiente y no implica problemas legales al no mostrar el código fuente de la aplicación.

3.1.3 Determinación de herramienta para la revisión de código fuente.

Para la revisión de código fuente disponible de las aplicaciones de código abierto se decidió utilizar el entorno de desarrollo Android Studio. Debido a que se centra únicamente en la plataforma Android y cuenta con gran cantidad de documentación para el desarrollo y revisión de aplicaciones Android.

3.1.4 Procesos para el análisis de aplicaciones bloqueadoras de anuncios

Análisis de aplicaciones bloqueadoras de anuncios de código cerrado.

- Aplicar herramienta VirusTotal.

- Registrar vulnerabilidades de seguridad detectadas.
- Interpretar los resultados obtenidos.

Análisis de aplicaciones bloqueadoras de anuncios de código abierto.

- Revisar el código fuente.
- Registrar vulnerabilidades detectadas.
- Aplicar herramienta VirusTotal.
- Registrar vulnerabilidades detectadas
- Comparar los resultados de la revisión y la aplicación de la herramienta.
- Interpretar los resultados obtenidos.

3.2 Desarrollo de la propuesta

3.2.1 Metodología Kanban

Para aplicar la metodología se realizó los siguientes pasos:

- **Definir el flujo de todo el trabajo.**

La Tabla 3.3 presenta como se definió el flujo de trabajo para el desarrollo de la propuesta.

Tabla 3.3 Flujo de trabajo Kanban.

Elaborado por: Investigador.

Etapas	**Tareas**	**Criterio para finalización**
Etapa 1 Análisis de bloqueadores de anuncios de código cerrado.	3	Matriz resultante del análisis. Interpretación de resultados.
Etapa 2 Análisis de bloqueadores de anuncios de código abierto.	6	Matriz resultante del análisis. Interpretación de resultados.

Etapa 3 Descripción de características de las vulnerabilidades detectadas.	4	Matriz de vulnerabilidades.
Etapa 4 Elaboración de propuesta de solución para las vulnerabilidades.	4	Matriz de propuestas de solución.

- **Crear el panel Kanban**

Se creó un panel Kanban organizado en columnas que representen los estados del proyecto. En este caso la primera columna representa las tareas por hacer, la segunda representa las tareas en progreso y la tercera representa las tareas completadas. El Gráfico 3.1 muestra de manera gráfica las columnas del panel Kanban.

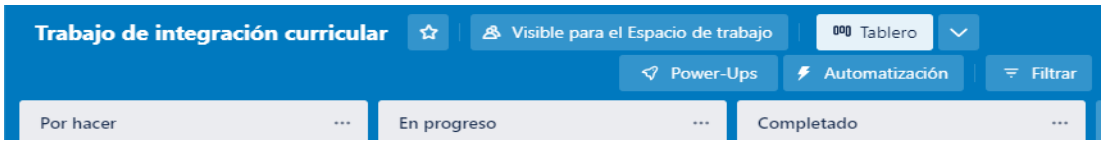


Gráfico 3.1 Panel Kanban del software Trello.

- **Dividir el trabajo en ítems pequeños.**

Se organizó los trabajos de manera descendente y la prioridad del trabajo se determina por el color de la tarjeta, siendo: color rojo los trabajos urgentes, color amarillo los trabajos regulares, color verde los trabajos ligeros.

- **Limitar el trabajo en curso (WIP).**

El valor del WIP se asignó con base en la etapa del flujo del trabajo con el menor número de tareas, debido a que para finalizar dicha etapa primero se debe completar todas sus tareas. Por lo cual se definió, que se puede tener en proceso un máximo de tres tareas.

- **Medir el tiempo empleado en completar un ciclo completo.**

Se estimó en relación con las tareas terminadas, que el tiempo para realizar los trabajos regulares puede disminuirse, pero a trabajos urgentes no se les puede reducir el tiempo sin afectar la calidad.

En el Gráfico 3.2, se muestra de manera gráfica el panel organizado Kanban con sus respectivas tareas organizadas y priorizadas.

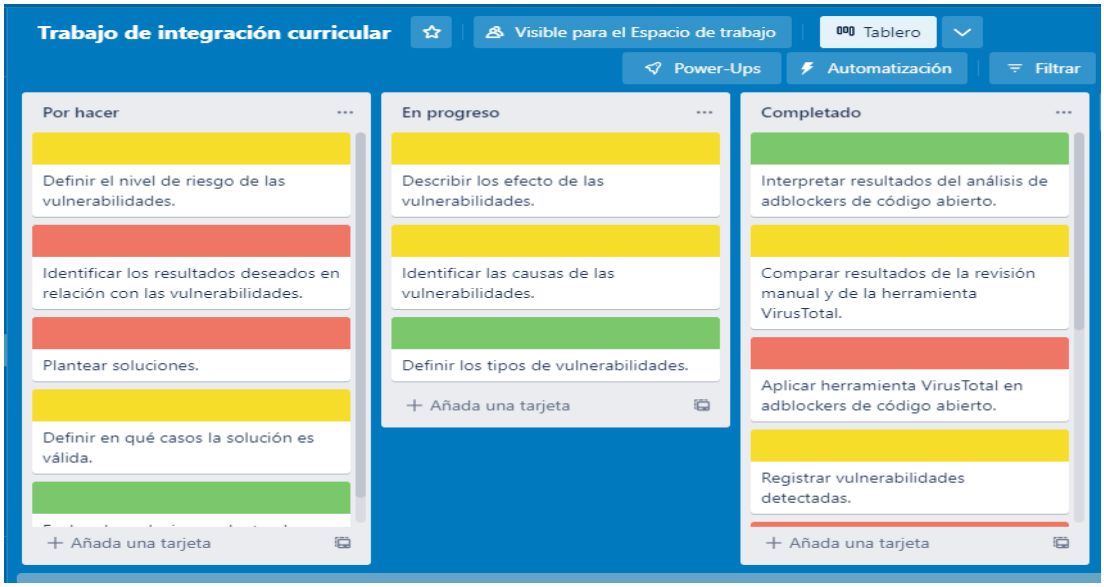


Gráfico 3.2 Panel Kanban resultante.

Elaborado por: Investigador.

3.2.2 Desarrollo de las tareas

3.2.2.1 Análisis de bloqueadores de anuncios de código cerrado

Cada aplicación fue cargada por el investigador a la base de datos de VirusTotal como se muestra en el Anexo B, por esta razón no hay necesidad de que otra persona cargue la aplicación y espere el análisis nuevamente.

La Tabla 3.4 corresponde al resumen de los reportes, del análisis de las aplicaciones de código cerrado utilizando la herramienta VirusTotal. Y está conformada por el nombre con el que se encuentra la aplicación en el mercado, el tipo de malware que contiene de ser el caso, los permisos peligros u obsoletos que incluyen y los sitios web maliciosos que la aplicación contacta.

Tabla 3.4 Matriz de amenazas informáticas en aplicaciones bloqueadoras de anuncios de código cerrado.

Elaborado por: Investigador.

Aplicación	**Malware**	**Permisos solicitados****	**Dominios, direcciones IP, URL maliciosas*****
ADB AdBlocker	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE FLASHLIGHT	216.58.212.238
Adblock Browser: veloz, seguro	Ninguno.	USE_CREDENTIALS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE GET_ACCOUNTS POST_NOTIFICATIONS	Ninguno.
Ad Blocker Block All Ads	Ninguno.	READ_PHONE_STATE	Ninguno.
AdBlocker for Android	Ninguno.	WRITE_EXTERNAL_STORAGE	Ninguno.

Ad Blocker for apps - Ad Clear	Ninguno.	WRITE_EXTERNAL_STORAGE	34.120.195.249
Ad Blocker - Stop the Ads	Virus.Generic-Script.Save.ba4	READ_EXTERNAL_STORAGE POST_NOTIFICATIONS	Ninguno.
AdBlocker Ultimate Browser	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
AdBlock for Samsung Internet	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE	Ninguno.
Adblock Less Ads	Android.adware.suad.a	WRITE_EXTERNAL_STORAGE	216.239.34.21 216.239.36.21
Adblock Mobile	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE	172.217.164.163
Adblock para navegadores	A.gray.andrsca.f	Ninguno.	185.199.108.133 185.199.109.133 185.199.110.133 185.199.111.133 raw.githubusercontent.com

Adblock - Private Adblocker Browser App	Ninguno.	WRITE_EXTERNAL_STORAGE GET_TASKS	216.239.32.21 216.239.34.21 216.239.36.21
Ad Block REMOVER - NEED ROOT	Ninguno.	WRITE_EXTERNAL_STORAGE	Ninguno.
AdBlock VPN	Ninguno.	WRITE_EXTERNAL_STORAGE READ_PHONE_STATE GET_TASKS	Ninguno.
AdBlock VPN for Android	Ninguno.	READ_EXTERNAL_STORAGE READ_PHONE_STATE	Ninguno.
AdClear: bloqueador de contenido	Ninguno.	Ninguno.	Ninguno.
Adfree	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
AdGuard VPN – proxy privado	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
AdLock for Android	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE USE_FINGERPRINT	Ninguno.

AdLocker - Adblock & Firewall	Ninguno.	GET_TASKS	8.8.8.8
AdProtect - Adblock & Firewall	Ninguno.	GET_TASKS	8.8.8.8
Ad Remover Privacy Browser	Trojan/Generic.ASCommon.25C	WRITE_EXTERNAL_STORAGE POST_NOTIFICATIONS	Ninguno.
Ads Blocker for Android	Ninguno.	Ninguno.	Ninguno.
AdShield - Ad blocker	Ninguno.	READ_EXTERNAL_STORAGE	Ninguno.
Adware Hunter - Popup Ad Fixer	Ninguno.	Ninguno.	216.58.212.227
Aloha Navegador + VPN privado	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE USE_FINGERPRINT POST_NOTIFICATIONS	Ninguno.
AppBrain Ad Detector	Ninguno.	Ninguno.	188.114.96.2 188.114.97.2
Avast Secure Browser	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.

		USE_FINGERPRINT POST_NOTIFICATIONS	
Awax Bloqueador de anuncios	Trojan/Generic.ASCommon.25C	Ninguno.	Ninguno.
Banana Browser: Adblock, Secure DNS, Fast & Secure	Trojan/Generic.ASCommon.25C	USE_CREDENTIALS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE GET_ACCOUNTS MANAGE_ACCOUNTS POST_NOTIFICATIONS USE_FINGERPRINT	Ninguno.
Blocker by +Now: Ad Blocker	Ninguno.	READ_PHONE_STATE	Ninguno.
Bloqueador de anuncios Direct CPV Technologies	Ninguno.	POST_NOTIFICATIONS	Ninguno.
Bloqueador de anuncios Maxsortube	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	Ninguno.
BLU: AdBlock, Fast & Clean	Ninguno.	ACCESS_FINE_LOCATION WRITE_EXTERNAL_STORAGE	Ninguno.

Bravo, Navegador Rápido, AdBlock	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE GET_TASKS READ_PHONE_STATE	Ninguno.
Browser Popup Detector - Block Ads In Browser	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
Clario: Security & Privacy	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE	Ninguno.
Clean Ads Skip Ads Universal Tool	Ninguno.	Ninguno.	Ninguno.
CM Browser - Fast Download, Private, Ad Blocker	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE CAMERA	104.18.225.52 104.18.226.52 104.244.42.67 52.94.232.32
Crystal para Samsung Internet	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE	Ninguno.

Dolphin Browser Navegador Web	Ninguno.	USE_CREDENTIALS WRITE_EXTERNAL_STORAGE GET_ACCOUNTS	216.58.198.195 31.13.71.1
DuckDuckGo Privacy Browser	Ninguno.	WRITE_EXTERNAL_STORAGE USE_FINGERPRINT	93.184.220.29
Epic Privacy Browser Ad Block, Almacén, VPN	Ninguno.	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	216.58.212.238
eShild:Adblocker, Secure & Private, no more ads	Ninguno.	WRITE_EXTERNAL_STORAGE	Ninguno.
FAB Adblocker Browser: Adblock	Ninguno.	USE_CREDENTIALS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE MANAGE_ACCOUNTS GET_ACCOUNTS READ_PHONE_STATE	208.95.112.1
Ghostery Privacy Browser	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.

		USE_FINGERPRINT	
Goclean: Detector de anuncios	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE GET_TASKS READ_PHONE_STATE FLASHLIGHT	Ninguno.
Godzilla Browser: AdBlocker	Trojan/Generic.ASCommon.25C Trojan.AndroidOS.Agent.qw	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE FLASHLIGHT	185.199.108.133
Guard My Web Adblock VPN	Trojan.Trojan.Dropper.AndroidOS.Hqwar.bb	GET_TASKS	8.8.8.8
Hi Browser-privado&rápido	Ninguno.	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.

IgeBlock - YouTube ad blocker	Ninguno.	Ninguno.	Ninguno.
Incognito VPN - Fast VPN & Ad Blocker for Android	Ninguno.	Ninguno.	Ninguno.
Microsoft Edge	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE USE_CREDENTIALS GET_ACCOUNTS MANAGE_ACCOUNTS AUTHENTICATE_ACCOUNTS POST_NOTIFICATIONS FLASHLIGHT	Ninguno.
Mobile Adblock - remove all ad	Ninguno.	WRITE_EXTERNAL_STORAGE	172.217.15.78
Moon Browser - Adblock	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	Ninguno.
Opera GX: navegador gaming	Ninguno.	WRITE_EXTERNAL_STORAGE	raw.githubusercontent.com 185.199.108.133

			185.199.109.133 185.199.110.133 185.199.111.133 8.8.4.4 8.8.8.8
Orions - Privacy Browser	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	157.240.241.35
Pando - Rewards Web Browser	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	Ninguno.
Private Browser - Privado&Safe	Ninguno.	USE_CREDENTIALS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE MANAGE_ACCOUNTS GET_ACCOUNTS	Ninguno.
Puffer: Privacy Protection & Ad-Blocking	Ninguno.	Ninguno.	Ninguno.
Pure Browser Pro-Ad Blocker	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	https://www.duckduckgo.com/?q=3yjGZB8uiU 31.13.92.36

Pure Web Browser - Adblocker	Trojan/Generic.ASCommon.25C	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	216.58.208.99 216.58.214.10
Purple DNS | Fast Ads Blocker	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	Ninguno.
Purple Ad Blocker - Family Protection	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	104.18.225.52 104.18.226.52
Soul Browser	Ninguno.	READ_EXTERNAL_STORAGE USE_FINGERPRINT	104.18.20.226 104.18.21.226 185.199.108.133 185.199.109.133 185.199.110.133 185.199.111.133
Spark	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE ACCESS_FINE_LOCATION ACCESS_COARSE_LOCATION	Ninguno.
Stampy Browser: AdBlocker, Incognito and Secure	Ninguno.	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	Ninguno.

StopAd	Ninguno.	WRITE_EXTERNAL_STORAGE	Ninguno.
Super Browser - Mini & Fast	Trojan.Generic-JS.Save.Redirector	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE WRITE_CONTACTS READ_CONTACTS GET_ACCOUNTS READ_PHONE_STATE	Ninguno.
Tincat Browser m3u8 mpd live	Ninguno.	GET_TASKS POST_NOTIFICATIONS	Ninguno.
Turbo Navegador: Privado & Bloqueador de anuncios	Ninguno.	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS WRITE_EXTERNAL_STORAGE GET_ACCOUNTS READ_PROFILE READ_PHONE_STATE	Ninguno.
UC Browser Turbo - Descarga rápida, Seguro	Ninguno.	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS	https://gjapplog.ucweb.com/collect?chk=76b9c345&vno=1451531020202&uuid=db43ffc5-f561-

		READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE GET_TASKS	43f1-bff9- f6d015748f35&app=4ea4e41a3993&enc=aes https://gjapplog.ucweb.com/collect?chk=594f57 94&vno=1451531019029&uuid=cacb0855- 71e6-455c-9ed3- d9433e095ce3&app=4ea4e41a3993&enc=aes
Umbrella - Adblock & Firewall	Ninguno.	GET_TASKS	104.18.225.52 104.18.226.52 130.211.34.183 35.186.241.51 35.190.25.25
Unicorn Blocker:Adblocker, Fast & Private	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
Via Navegador Rápido y liviano	Ninguno.	WRITE_EXTERNAL_STORAGE POST_NOTIFICATIONS	https://accounts.google.com/signin/v2/usernamer ecovery?continue=https://policies.google.com/pr ivacy?gl=US&hl=en&dsh=S- 1996213116:1664141549332153&flowEntry=Se rviceLogin&flowName=GlifWebSignIn&follow

			up=https://policies.google.com/privacy?gl=US&hl=en&hl=en&ifkv=AQDHYWoVnwhWnUQnE1J3iR2wPw43Qz5UxejltqdRZGWPfsFfEP864E620dvplS8Ng-rBIc52bQG4WQ https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=https://www.google.com/search?q=S5928Jtqh4yPo&ec=GAZAAQ https://accounts.google.com/TOS?loc=US&hl=en&privacy=true
Vider Adblock - Video Browser	Ninguno.	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE USE_CREDENTIALS GET_ACCOUNTS MANAGE_ACCOUNTS	216.58.212.238
Vivaldi Navegador	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE USE_CREDENTIALS	216.58.212.238

		POST_NOTIFICATIONS	
Vivo Browser	VEX.Webshell Android.WIN32. Dnotua.axbt	READ_CALENDAR READ_CONTACTS READ_PROFILE READ_HISTORY_BOOKMARKS RECEIVE_SMS WRITE_CALENDAR MANAGE_ACCOUNTS SEND_SMS USE_CREDENTIALS READ_PHONE_STATE WRITE_HISTORY_BOOKMARKS GET_ACCOUNTS WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE AUTHENTICATE_ACCOUNTS READ_SMS GET_TASKS FLASHLIGHT	Ninguno.

		USE_FINGERPRINT	
VPN Dash: Fast VPN Proxy	Ninguno.	Ninguno.	Ninguno.
VPN Galaxy - VPN Proxy & AdBlock	Ninguno.	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
VPN Owl: Fast and Secure VPN	Ninguno.	WRITE_EXTERNAL_STORAGE POST_NOTIFICATIONS	Ninguno.
VPN + TOR Browser and Ad Block	Ninguno.	Ninguno.	Ninguno.
VPN Venus	Ninguno.	Ninguno.	104.18.225.52 104.18.226.52
WebGuard - Adblock & Firewall	Ninguno.	GET_TASKS	216.58.212.238 8.8.8.8
고차단 브라우저 : 블로켓 - 인터넷 애드블록	Android.W32.Bray.h	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Ninguno.
* Permisos que el análisis de la aplicación presenta, escogidos según la Tabla 2.6 y Tabla 2.7. ** Malware detectado en la aplicación. *** Sitios web maliciosos contactados por la aplicación.			

Resultados del análisis

Aplicaciones código cerrado que contienen malware.

Las ochenta y cinco aplicaciones de código cerrado fueron analizadas en función del malware. En el Gráfico 3.3 presenta, el resultado obtenido.

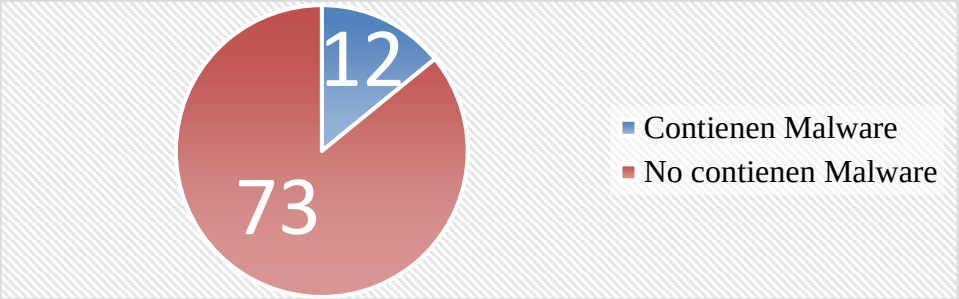


Gráfico 3.3 Aplicaciones de código cerrado que contienen malware.

Elaborado por: Investigador.

Fuente: Matriz de amenazas informáticas Tabla 3.4.

El Gráfico 3.3 ilustra que, de las ochenta y cinco aplicaciones con modelo de desarrollo cerrado, doce afectarían directamente a sus usuarios debido a que contienen malware.

Aplicaciones de código cerrado que contienen permisos de riesgo.

Las ochenta y cinco aplicaciones de código cerrado fueron analizadas también en función de permisos que solicitan y que constituyen un riesgo. En el Gráfico 3.4 se muestra, el resultado obtenido.

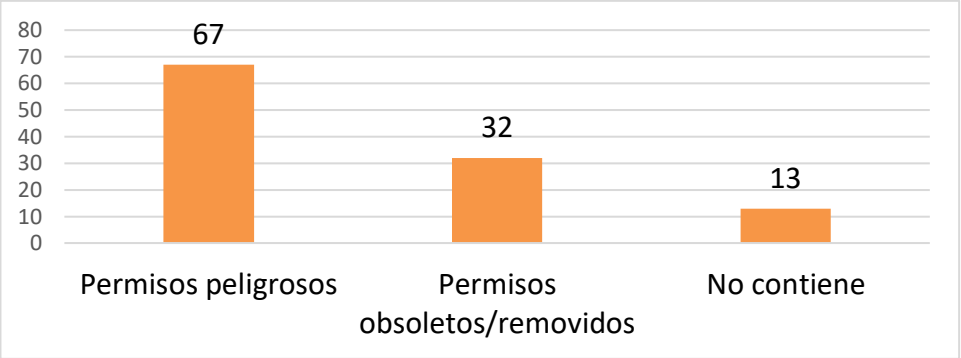


Gráfico 3.4: Estadísticas de aplicaciones con permisos de riesgo.

Elaborado por: Investigador.

Fuente: Matriz de amenazas informáticas Tabla 3.4.

El Gráfico 3.4 ilustra que, de las ochenta y cinco aplicaciones de código cerrado, sesenta y siete solicitan permisos para acceder a datos privados del usuario u otorgar control del dispositivo y que puede afectar negativamente al usuario. Treinta y dos solicitan permisos que pueden producir errores y son catalogados como obsoletos o han sido removidos por la fuente Developers Android. Las trece restantes no afectaría ni al usuario, ni al dispositivo debido a que no contiene permisos peligrosos, obsoletos o removidos.

Dominios, direcciones IP, URL maliciosas contactadas por las aplicaciones.

Las ochenta y cinco aplicaciones de código cerrado fueron analizadas en función de dominios, direcciones IP, URL maliciosas que contactan. En el Gráfico 3.4 se muestra, el resultado obtenido.

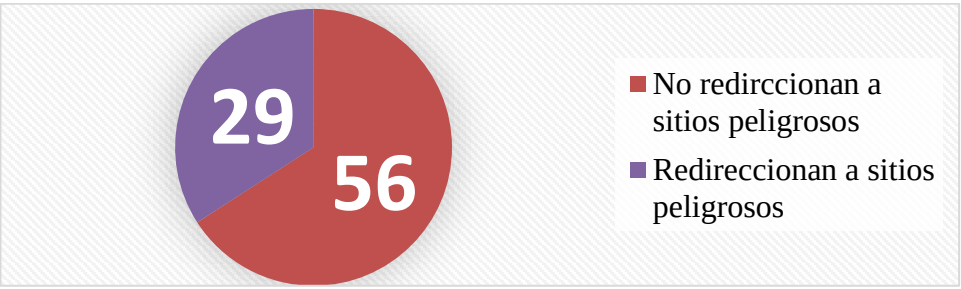


Gráfico 3.5: Aplicaciones con dominios, direcciones IP, URL maliciosas.

Elaborado por: Investigador.

Fuente: Matriz de amenazas informáticas Tabla 3.4.

El Gráfico 3.5 ilustra que, de las ochenta y cinco aplicaciones de código cerrado, cincuenta y seis contactan con dominios o sitios web que no representan una amenaza informática para sus usuarios. Las veinte y nueve restantes de las aplicaciones, mientras brindan sus servicios, redireccionan a sus usuarios a dominios y sitios web con presencia de malware. Las razones de esta acción son por publicidad, marketing, gestión de cuentas, comunicaciones con el desarrollador, facturación, interacciones con plataformas de soporte.

3.2.2.2 Análisis de bloqueadores de anuncios de código abierto

Resultados del análisis

La información a continuación se refiere a los resultados de la revisión manual del código fuente disponible públicamente por los desarrolladores de la aplicación, con el entorno de desarrollo Android Studio, y a lo encontrado en la documentación disponible en Developers Android hasta la fecha.

Tabla 3.5 Resultado del análisis de Adblock Fast

Elaborado por: Investigador.

Adblock Fast
El Anexo C presenta la configuración del *ContentProvider* de *Adblock Fast*. De la ausencia de filtros de acción se entiende que la información solo está destinada para el uso interno del *ad blocker*. Sin embargo, el valor de la propiedad *exported* es *true*, lo que indica que los datos se comparten con otra aplicación. En este caso, se supone que se trate del navegador con el cual se integra el *ad blocker*, pero no aparece el filtro que limitaría a que otras aplicaciones accedan a dichos datos. Es decir, que todas las aplicaciones tienen acceso a dichos datos, lo que constituye una vulnerabilidad importante de esta herramienta.

El análisis del *ad blocker* con la herramienta *VirusTotal* tuvo como resultado que no existen permisos peligrosos u obsoletos, ninguna dirección IP o dominio con presencia de malware contactado y no contiene malware. El permiso peligroso GET_ACCOUNTS se encuentra comentado en el manifiesto. Sin embargo, dentro de la *MainActivity.java* existen métodos relacionados al permiso, tal y como se evidencia en el Anexo D. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.

Clases	
Obsoleto	**Vigente**
android.preference.PreferenceManager	androidx.preference.PreferenceManager

Tabla 3.6 Resultado del análisis de ABP para Internet de Samsung.

Elaborado por: Investigador.

ABP para Internet de Samsung	
De la revisión manual del código, *ABP para Internet de Samsung* utiliza un permiso peligroso. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación contiene el malware *Android.W32.Bray.h* y tres permisos peligrosos. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Permisos	
Manual	**Herramienta**
WRITE_EXTERNAL_STORAGE	WRITE_EXTERNAL_STORAGE READ_PHONE_STATE READ_EXTERNAL_STORAGE
Obsoleto	**Vigente**
Clases	
android.preference.PreferenceManager android.os.AsyncTask	androidx.preference.PreferenceManager java.util.concurrent

Métodos	
org.apache.commons.lang.StringUtils. chompLast(String str, String sep)	org.apache.commons.lang.StringUtils. chomp(String str, String sep)

Tabla 3.7 Resultado del análisis de Ad Blocker Turbo.

Elaborado por: Investigador.

Ad Blocker Turbo - Adblocker Browser	
De la revisión manual del código, *Ad Blocker Turbo* utiliza tres permisos peligrosos y dos obsoletos. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación contacta con direcciones IP maliciosas y utiliza la misma cantidad peligrosos y obsoletos, pero un permiso es diferente al de la revisión. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	
ACCESS_FINE_LOCATION WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	RECORD_AUDIO WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE
Permisos Obsoletos	
WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS	WRITE_HISTORY_BOOKMARKS READ_HISTORY_BOOKMARKS
Dirección IP o dominio con malware	
Ninguno.	216.58.198.195
Obsoleto	**Vigente**
Clases	
android.webkit.CookieSyncManager android.os.AsyncTask	android.webkit.CookieManager java.util.concurrent

Tabla 3.8 Resultado del análisis de AdGuard Content Blocker.

Elaborado por: Investigador.

<table>
<tr><th colspan="2">AdGuard Content Blocker</th></tr>
<tr><td colspan="2">El Anexo E presenta la configuración del ContentProvider de AdGuard Content Blocker. De la ausencia de filtros de acción se entiende que la información solo está destinada para el uso interno del ad blocker. Sin embargo, el valor de la propiedad exported es true, lo que indica que los datos se comparten con otra aplicación. En este caso, se supone que se trate del navegador con el cual se integra el ad blocker, pero no aparece el filtro que limitaría a que otras aplicaciones accedan a dichos datos. Es decir, que todas las aplicaciones tienen acceso a dichos datos, lo que constituye una vulnerabilidad importante de esta herramienta.

El Anexo F corresponde a la configuración de seguridad que permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que significaría que los datos que envié el ad blocker hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios.

El análisis del ad blocker con la herramienta VirusTotal la aplicación contiene el malware Virus.Trojan.Faceliker.Gen y no existen permisos peligrosos u obsoletos, ninguna dirección IP o dominio malicioso contactado.</td></tr>
<tr><th>Obsoleto</th><th>Vigente</th></tr>
<tr><td colspan="2">Clases</td></tr>
<tr><td>androidx.fragment.app.
FragmentPagerAdapter</td><td>androidx.viewpager2.adapter.
FragmentStateAdapter</td></tr>
<tr><td colspan="2">Métodos</td></tr>
<tr><td>org.apache.commons.io.IOUtils.
write(String, OutputStream)</td><td>org.apache.commons.io.IOUtils.
write(String, OutputStream, Charset).</td></tr>
</table>

Tabla 3.9 Resultado del análisis de Block This!.

Elaborado por: Investigador.

Block This!	
De la revisión manual del código, *Block This!* no contacta con ninguna dirección IP o dominio malicioso. Sin embargo, el análisis con la herramienta *VirusTotal* presento, que la aplicación contacta con una Dirección IP maliciosa. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	
READ_PHONE_STATE	READ_PHONE_STATE
Dirección IP o dominio con malware	
Ninguno.	216.58.198.195
Obsoleto	**Vigente**
Clases	
android.os.AsyncTask	java.util.concurrent

Tabla 3.10 Resultado del análisis de Blokada 6.

Elaborado por: Investigador.

Blokada 6: The Privacy App+VPN	
De la revisión manual del código, *Blokada 6* utiliza cinco permisos peligrosos y uno obsoleto. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación tiene dos permisos peligrosos y dos obsoletos. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	

READ_PHONE_STATE WRITE_EXTERNAL_STORAGE ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION READ_EXTERNAL_STORAGE	READ_PHONE_STATE WRITE_EXTERNAL_STORAGE
Permisos Obsoletos	
GET_TASKS	GET_TASKS USE_FINGERPRINT

Tabla 3.11 Resultado del análisis de navegador Brave.

Elaborado por: Investigador.

Brave navegador web privado	
De la revisión manual del código, *Brave* contacta con direcciones URL por motivos de marketing o para presentar información de la aplicación. Entre las que se encontró tres direcciones maliciosas. Además, utiliza cinco permisos peligrosos y uno obsoleto. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación no contacta con direcciones URL maliciosas y cuenta con tres permisos peligrosos. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	
WRITE_EXTERNAL_STORAGE ACCESS_FINE_LOCATION POST_NOTIFICATIONS RECORD_AUDIO CAMERA	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE POST_NOTIFICATIONS
Permisos Obsoletos	
USE_FINGERPRINT	Ninguno
Dirección IP o dominio con malware	

151.101.2.110: https://laptop-updates.brave.com/1/feedback 151.101.130.110: https://brave.com/faq-rewards/#unclaimed-funds 108.156.107.78: https://brave.com/privacy-features	Ninguno.
Obsoleto	**Vigente**
Clases	
android.hardware.Camera	android.hardware.camera2
Métodos	
android.os.Build.CPU_ABI android.view.View. setBackgroundDrawable android.content.Intent.FLAG_ ACTIVITY_CLEAR_WHEN_ TASK_RESET	android.os.SUPPORTED_ABIS android.view.View.setBackground. android.content.Intent.FLAG_ ACTIVITY_NEW_DOCUMENT

Tabla 3.12 Resultado del análisis de Bromite browser.

Elaborado por: Investigador.

Bromite - Take back your browser
El Anexo G corresponde al método que verifica que se permita el tráfico sin cifrar hacia el host de *Bromite*, lo que significaría que los datos sensibles que envié el *ad blocker* hacia su host, pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios. De la revisión manual del código, *Bromite* utiliza cinco permisos peligrosos y uno obsoleto. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación tiene tres permisos peligrosos. Esto demuestra que el

código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.

Manual	**Herramienta**
Permisos	
READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE POST_NOTIFICATIONS RECORD_AUDIO CAMERA	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE POST_NOTIFICATIONS
Permisos Obsoletos	
USE_FINGERPRINT	Ninguno.

Tabla 3.13 Resultado del análisis de DNS66.

Elaborado por: Investigador.

DNS66
De la revisión manual del código, *DNS66* contacta con direcciones URL para acceder a una lista de servidores acreditados y permitir o denegar su uso. Entre las que se encontró dos direcciones maliciosas. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación no contacta con direcciones URL maliciosas, lo que sugiere que al no utilizarlas por defecto la herramienta no los analizo.

Manual	**Herramienta**
Permisos	
WRITE_EXTERNAL_STORAGE.	WRITE_EXTERNAL_STORAGE.
Dirección IP o dominio con malware	
185.199.111.133: https://raw.githubusercontent.com/ StevenBlack/hosts/master/hosts	Ninguno.

185.199.109.153: https://adaway.org/hosts.txt	
Clases	
android.os.AsyncTask androidx.localbroadcastmanager. content.LocalBroadcastManager androidx.fragment.app. FragmentPagerAdapter	java.util.concurrent androidx.lifecycle.LiveData androidx.viewpager2.adapter. FragmentStateAdapter

Tabla 3.14 Resultado del análisis de Firefox Focus.

Elaborado por: Investigador.

Firefox Focus: el navegador	
El Anexo H corresponde a la declaración de aplicación *Firefox Focus*, resaltando la propiedad *usesCleartextTraffic* con valor *"true"* la cual permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que significaría que los datos que envié el *ad blocker* hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios. De la revisión manual del código, *Firefox Focus* utiliza siete permisos peligrosos y uno obsoleto. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación tiene dos permisos peligrosos y uno obsoleto. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	
READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE READ_PHONE_STATE RECORD_AUDIO	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE

ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION CAMERA	
Permisos Obsoletos	
USE_FINGERPRINT	USE_FINGERPRINT
Obsoleto	**Vigente**
Clases	
android.os.AsyncTask android.preference.PreferenceManager androidx.test.runner.AndroidJUnit4	java.util.concurrent androidx.preference.PreferenceManager androidx.test.ext.junit.runners. AndroidJUnit4
Métodos	
JavaExecSpec.getMain	JavaExecSpec.getMainClass

Tabla 3.15 Resultado del análisis de FOSS Browser.

Elaborado por: Investigador.

FOSS Browser
El Anexo I corresponde a la declaración de aplicación *FOSS Browser*, resaltando la propiedad *usesCleartextTraffic* con valor *"true"* la cual permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que significaría que los datos que envié el *ad blocker* hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios. De la revisión manual del código, *FOSS Browser* contacta con direcciones URL para obtener listas de servidores acreditados o servir como motor de búsqueda. Entre las que se encontró dos direcciones maliciosas. Además, utiliza cinco permisos peligrosos. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación cuenta con dos permisos peligrosos, contacta con seis direcciones IP maliciosas y una de las direcciones URL es distinta. Esto demuestra

que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.	
Manual	**Herramienta**
Permisos	
READ_EXTERNAL_STORAGE CAMERA WRITE_EXTERNAL_STORAGE ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE
Dirección IP o dominio con malware	
185.199.111.133: https://raw.githubusercontent.com/ StevenBlack/hosts/master/hosts 158.101.202.236: https://searx.be/?q=	github.githubassets.com raw.githubusercontent.com 185.199.108.133 185.199.108.154 185.199.109.133 185.199.109.154 185.199.110.133 185.199.111.133
Obsoleto	**Vigente**
Clases	
android.preference.PreferenceManager	androidx.preference.PreferenceManager

Tabla 3.16 Resultado del análisis de Lightning Browser.

Elaborado por: Investigador.

Lightning Browser - Web Browser
El Anexo J corresponde a la declaración de aplicación *Lightning Browser*, resaltando la propiedad *usesCleartextTraffic* con valor *"true"* la cual permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que

significaría que los datos que envié el *ad blocker* hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios.

De la revisión manual del código, *Lightning Browser* utiliza cinco permisos peligrosos. Sin embargo, el análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación tiene dos permisos peligrosos. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la *Google Play*.

Manual	**Herramienta**
Permisos	
WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE ACCESS_FINE_LOCATION RECORD_AUDIO CAMERA	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE
Obsoleto	**Vigente**
Clases	
android.preference.Preference android.preference.SwitchPreference android.preference. CheckBoxPreference android.preference.PreferenceFragment	androidx.preference.Preference androidx.preference.SwitchPreference androidx.preference. CheckBoxPreference androidx.preference. PreferenceFragmentCompat
Métodos	
androidx.core.view.ViewCompat. setAlpha setTranslationY setTranslationX getTranslationY getTranslationX info.guardianproject.netcipher. proxy.OrbotHelper.isOrbotRunning	android.view.View. setAlpha setTranslationY setTranslationX getTranslationY getTranslationX org.torproject.android.intent. action.STATUS

Tabla 3.17 Resultado del análisis de Midori Lite.

Elaborado por: Investigador.

<table>
<tr><th colspan="2">Midori Lite Navegador Web</th></tr>
<tr><td colspan="2">El Anexo K corresponde a la declaración de aplicación Midori Lite, resaltando la propiedad usesCleartextTraffic con valor “true" la cual permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que significaría que los datos que envié el ad blocker hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios.

De la revisión manual del código, Midori Lite utiliza seis permisos peligrosos. Sin embargo, el análisis de con la herramienta VirusTotal tuvo como resultado que la aplicación tiene dos permisos peligrosos. Esto demuestra que el código fuente publicado no coincide con el de la aplicación disponible en la Google Play.</td></tr>
<tr><th>Manual</th><th>Herramienta</th></tr>
<tr><td colspan="2">Permisos</td></tr>
<tr><td>WRITE_EXTERNAL_STORAGE
READ_EXTERNAL_STORAGE
ACCESS_FINE_LOCATION
RECORD_AUDIO
READ_PHONE_STATE
CAMERA</td><td>WRITE_EXTERNAL_STORAGE
READ_EXTERNAL_STORAGE</td></tr>
<tr><th>Obsoleto</th><th>Vigente</th></tr>
<tr><td colspan="2">Clases</td></tr>
<tr><td>android.preference.Preference
android.preference.SwitchPreference
android.webkit.CookieSyncManager
android.preference.
CheckBoxPreference
android.preference.PreferenceFragment</td><td>androidx.preference.Preference
androidx.preference.SwitchPreference
android.webkit.CookieManager
androidx.preference.
CheckBoxPreference
androidx.preference.
PreferenceFragmentCompat</td></tr>
</table>

Métodos	
androidx.core.view.ViewCompat.	android.view.View.
setAlpha	setAlpha
setTranslationY	setTranslationY
setTranslationX	setTranslationX
getTranslationY	getTranslationY
getTranslationX	getTranslationX
info.guardianproject.netcipher.	org.torproject.android.intent.
proxy.OrbotHelper.isOrbotRunning	action.STATUS
android.os.Environment.	android.os.Environment.
getExternalStoragePublicDirectory	getExternalStorageState
RecyclerView.viewHolder.	RecyclerView.viewHolder.
getAdapterPosition	getBindingAdapterPosition

Tabla 3.18 Resultado del análisis de personalDNSfilter.

Elaborado por: Investigador.

personalDNSfilter
El Anexo L corresponde a la declaración de aplicación *personalDNSfilter*, resaltando la propiedad *usesCleartextTraffic* con valor *"true"* la cual permite conectarse a destinos que no garantizan la protección del tráfico sensible, lo que significaría que los datos que envié el *ad blocker* hacia sus hosts pueden ser interceptados por redes hostiles, afectando la privacidad de sus usuarios. De la revisión manual del código, *personalDNSfilter* contacta con direcciones URL para acceder a una lista de servidores acreditados y permitir o denegar su uso. Entre las que se encontró una dirección maliciosa. Sin embargo, análisis de con la herramienta *VirusTotal* tuvo como resultado que la aplicación la aplicación contiene el malware *Android.WIN32.Agent.eq y* no contacta con direcciones URL maliciosas, lo que sugiere que, al no utilizar la dirección maliciosa por defecto, la herramienta no lo analizo.

Manual	Herramienta
Permisos	
WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE	WRITE_EXTERNAL_STORAGE READ_EXTERNAL_STORAGE
Dirección IP o dominio con malware	
185.199.109.153: https://adaway.org/hosts.txt	Ninguno.
Obsoleto	**Vigente**
Clases	
android.net.NetworkInfo	android.net.ConnectivityManager. NetworkCallback
Métodos	
android.net.ConnectivityManager. TYPE_WIFI	android.net.NetworkCapabilities. hasTransport

Tabla 3.19 Análisis de vulnerabilidades de Proton VPN.

Elaborado por: Investigador.

Proton VPN: VPN veloz y segura	
El análisis de *Proton VPN* con la herramienta *VirusTotal* tuvo el mismo resultado que la revisión manual, no existen permisos peligrosos u obsoletos, ninguna dirección IP o dominio malicioso contactado y no contiene malware.	
Obsoleto	**Vigente**
Clases	
androidx.security.crypto. MasterKeys	androidx.security.crypto. MasterKey.Builder

A partir de los resultados del análisis revisión de código fuente y la aplicación de la herramienta VirusTotal se realizó, la Tabla 3.20. Que incluyen las acciones inseguras, el tipo de malware y el número de permisos peligrosos, elementos obsoletos y direcciones IP inseguras.

Tabla 3.20 Matriz de amenazas informáticas en aplicaciones bloqueadoras de anuncios de código abierto.

Elaborado por: Investigador.

Aplicación	**Revisión manual***						**Análisis de la herramienta****			
	Inseguridad	**PP**	**PO**	**CO**	**MO**	**IP**	**PP**	**PO**	**IP**	**Malware**
Adblock Fast	Proveedor de contenido sin configuración de filtro.	1	0	1	0	0	0	0	0	Ninguno.
ABP para Internet de Samsung	Ninguna.	1	0	2	1	0	3	0	0	Android.W32.Bray.h
Ad Blocker Turbo - Adblocker Browser	Ninguna.	3	2	2	0	0	3	2	1	Ninguno.
AdGuard Content Blocker	Proveedor de contenido sin configuración de filtro. Tráfico sin cifrar.	1	1	0	0	0	0	0	0	Virus.Trojan.Facelik er.Gen
Block This!	Ninguna.	1	0	1	0	0	1	0	1	Ninguno.
Blokada 6: The Privacy App+VPN	Ninguna.	5	1	0	0	0	2	2	0	Ninguno.
Brave navegador web privado	Ninguna.	5	1	1	3	3	3	0	0	Ninguno.

Bromite - Take back your browser	Tráfico sin cifrar.	5	1	0	0	0	3	0	0	Ninguno.
DNS66	Ninguna.	1	0	3	0	2	1	0	0	Ninguno.
Firefox Focus: el navegador	Tráfico sin cifrar.	7	1	3	1	0	2	1	0	Ninguno.
FOSS Browser	Tráfico sin cifrar.	5	0	1	0	2	2	0	6	Ninguno.
Lightning Browser - Web Browser	Tráfico sin cifrar.	5	0	4	6	0	2	0	0	Ninguno.
Midori Lite Navegador Web	Tráfico sin cifrar.	6	0	5	8	0	2	0	0	Ninguno.
personalDNSfilter	Tráfico sin cifrar.	2	0	1	1	1	2	0	0	Android.WIN32.Agent.eq
Proton VPN: VPN veloz y segura	Ninguna.	0	0	1	0	0	0	0	0	Ninguno.

* Revisión manual del código fuente realizada por el investigador.

** Resultados del análisis con la herramienta VirusTotal.

PP: Permisos peligrosos.

PO: Permisos obsoletos.

CO: Clases obsoletas.

MO: Métodos obsoletos.

IP: Direcciones IP, URL y dominios maliciosos contactados.

Interpretación de resultados

La Tabla 3.20 presenta que, de las quince aplicaciones de código abierto, catorce solicitan permisos para acceder a datos privados del usuario u otorgar control del dispositivo y que puede afectar negativamente al usuario. Doce incluyen clases o métodos que pueden producir errores y son catalogados como obsoletos. Seis solicitan permisos que son obsoletos o han sido removidos por la fuente Developers Android y redireccionan a sus usuarios a dominios o sitios web con presencia de malware. Tres afectarían directamente a sus usuarios debido a que contienen malware.

3.2.2.3 Descripción de características de las vulnerabilidades detectadas.

La Tabla 3.21 presenta las especificaciones de gravedad cualitativas para las distintas puntuaciones, según el estándar CVSS.

Tabla 3.21 Calificación CVSS.

Fuente: CVE details [26].

Puntaje CVSS	**Calificación**	
0 - 2.9	Baja	
3 - 6.9	Media	
7 - 8.9	Alta	
9 – 10	Crítica	

La Tabla 3.22 presenta características de la vulnerabilidad tales como: causa de la vulnerabilidad, registros relacionados de la vulnerabilidad extraídos del repositorio CVE details, calificación de gravedad de la vulnerabilidad según la Tabla 3.21 y los efectos producidos al explotar la vulnerabilidad.

Tabla 3.22 Matriz de descripción vulnerabilidades.

Elaborado por: Investigador.

Vulnerabilidad	**Causa**	**Registros relacionados**		**Calificación**		**Efectos de explotar la vulnerabilidad***
		CVE	**CVSS**	$\bar{X}$	**Gravedad**	
Acceso a datos privados del usuario o control sobre el dispositivo, a través de permisos de la aplicación.	Solicitar acceso de: **Almacenamiento** READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	CVE-2021-0550 CVE-2019-20468 CVE-2019-12370 CVE-2019-12369 CVE-2019-12368 CVE-2019-12367 CVE-2019-12366 CVE-2019-12365 CVE-2018-6599 CVE-2018-15004 CVE-2018-15002 CVE-2018-15001 CVE-2018-14995 CVE-2018-14979 CVE-2016-10135	4.6 7.5 4.3 4.3 4.3 4.3 4.3 4.3 2.1 4.3 1.9 2.1 1.9 1.9 4.3	4.0	Media	Obtiene los datos contenidos en el registro de Android de todo el sistema. Provoca denegación de servicio a través de subida excesiva de archivos. Modifica de manera remota los archivos de la memoria externa.

		CVE-2014-1885	6.4			
	Calendario READ_CALENDAR WRITE_CALENDAR	CVE-2022-33705 CVE-2021-0487 CVE-2014-3084	2.1 7.2 4.9	4.7	Media	Acceso remoto la programación del calendario. Exporta los datos del calendario. Modifica de manera remota los eventos del calendario.
	Cámara. CAMERA	CVE-2022-23998 CVE-2020-11990 CVE-2019-11014 CVE-2018-5832 CVE-2017-0822 CVE-2017-0544 CVE-2016-8444 CVE-2016-8412 CVE-2016-3916 CVE-2016-3915 CVE-2016-3834 CVE-2016-2449	4.3 2.1 10.0 10.0 7.5 9.3 7.6 7.6 9.3 9.3 4.3 9.3	7.5	Alta	Realiza fotografías en estado de bloqueo de pantalla. Accedo remoto a las imágenes tomadas con la aplicación. Suplanta el servicio de la cámara original. Produce una condición Use-After-Free que bloquea la aplicación. Ejecuta código malicioso a través de un archivo reconocido como

		CVE-2009-2348	6.9			una imagen, pero con una extensión incorrecta.
	Contactos GET_ACCOUNTS READ_CONTACTS WRITE_CONTACTS	CVE-2022-20303 CVE-2021-25414 CVE-2021-25403 CVE-2021-0953 CVE-2021-0952 CVE-2021-0603 CVE-2021-0569 CVE-2021-0304 CVE-2020-27098 CVE-2020-0448 CVE-2019-11063 CVE-2019-20468 CVE-2018-14986 CVE-2015-1541 CVE-2011-1717	0.0 4.6 2.1 7.2 4.7 4.4 1.9 4.9 2.1 2.1 8.3 7.5 5.0 4.3 2.1	4.1	Media	Acceso remoto la información de las cuentas del dispositivo. Acceso remoto la información de contactos del usuario. Modificación remota la información de contactos del usuario.

	 **Micrófono** RECORD_AUDIO	CVE-2020-0061 CVE-2019-15743 CVE-2019-15475 CVE-2019-15474 CVE-2019-15473 CVE-2019-15472 CVE-2019-15471 CVE-2019-15470 CVE-2019-15469 CVE-2019-2219 CVE-2018-14996 CVE-2016-6715 CVE-2009-2348	4.9 2.1 2.1 2.1 2.1 2.1 2.1 2.1 2.1 4.7 7.2 4.3 6.9	3.4	Media	Almacena grabaciones audios no autorizados en un almacenamiento externo. Almacena grabaciones de llamadas telefónicos en un almacenamiento externo.
	 **Notificaciones** POST_NOTIFICATIONS	CVE-2022-24886	2.1	2.1	Baja	Acceso remoto a los contactos de cuentas ligadas a la aplicación, sin solicitar el permiso necesario.
	 **SMS** READ_SMS	CVE-2022-23835 CVE-2021-39781 CVE-2020-0052	4.3 4.6 1.9	4.5	Media	Acceso remoto del contenido de los mensajes SMS.

	RECEIVE_SMS SEND_SMS	CVE-2020-13626 CVE-2018-15661 CVE-2017-17175 CVE-2017-18666 CVE-2016-11046 CVE-2016-3888 CVE-2016-3883 CVE-2014-8610 CVE-2013-4764 CVE-2012-2562 CVE-2012-2217 CVE-2011-0680 CVE-2011-4769 CVE-2011-4772 CVE-2011-4773 CVE-2011-4863 CVE-2011-4698 CVE-2009-2656	2.1 2.6 3.3 5.0 5.0 2.1 4.3 3.3 2.1 7.6 6.4 5.0 5.8 5.8 5.8 5.8 6.4 5.0			Produce denegación de servicios a través de un mensaje alterado. Envió de mensajes SMS premium arbitrarios. Envió de mensajes SMS almacenados, lo que generaría cargos adicionales por mensaje.

	Teléfono READ_PHONE_STATE	CVE-2016-0831 CVE-2012-2640	4.3 5.0	4.7	Media	Acceso remoto del estado del teléfono, red celular, estado de las llamadas en curso y lista de las cuentas telefónicas.
	Ubicación ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION	CVE-2022-30757 CVE-2021-33057 CVE-2019-15304 CVE-2019-9464 CVE-2018-9526 CVE-2014-1887 CVE-2014-0806 CVE-2012-6335 CVE-2012-6334	2.1 0.0 6.4 4.3 5.0 4.3 4.3 3.3 2.9	3.6	Media	Acceso remoto de la ubicación estimada del dispositivo. Remplaza los datos de ubicación. Acceso remoto del Carrier ID_1. Acceso remoto de la ubicación precisa del dispositivo.
Acceso libre a la información que genera la aplicación.	Proveedor de contenido sin configuración de filtro.	CVE-2019-14339 CVE-2018-14902 CVE-2014-1986	4.3 5.0 5.8	5.0	Media	Acceso a información confidencial.

Comunicación con sitios web maliciosos.	Contactar con dominios, direcciones IP, URL maliciosas	CVE-2022-28868 CVE-2021-29953 CVE-2018-5138 CVE-2017-7770 CVE-2017-12358	4.3 4.3 5.0 4.3 3.5	4.3	Media	Acceso de la información confidencial basada en el navegador. Falsificación el sitio web que está realmente cargado y en uso. Ejecución de código JavaScript.
Producción de errores, a través de clases y métodos de la aplicación.	Instanciar una clase o llamar a un método que la API ha marcado como obsoletos.	CVE-2020-8908	2.1	2.1	Baja	Acceso remoto de la información de directorios temporales.
Producción de errores, a través de permisos de la aplicación.	Solicitar permisos que la API ha removido o marcado como obsoletos.	CVE-2015-3858	9.3	9.3	Crítica	Evasión de requisitos de confirmación del usuario.
Tráfico de red sin utilizar protocolos de protección de	Propiedad de tráfico de texto sin cifrar permitida.	CVE-2022-20219 CVE-2021-32612 CVE-2020-4092 CVE-2020-26230	2.1 4.3 5.0 2.6	4.6	Media	Acceso remoto de la información confidencial.

transferencia de datos.		CVE-2020-8507 CVE-2020-8506 CVE-2020-15509 CVE-2019-19464 CVE-2019-14319 CVE-2019-12820 CVE-2018-6017 CVE-2018-5402 CVE-2018-5401 CVE-2018-16225 CVE-2018-15752 CVE-2018-11477 CVE-2017-16905	5.0 5.0 3.3 5.0 3.3 4.3 6.4 6.5 4.3 6.1 4.3 3.3 6.8			

*Efectos registrados del resultado de aprovechar la vulnerabilidad, según *vulnerabilidad CVE*.

CVE: Identificadores de registros relacionados de la vulnerabilidad, extraídos del repositorio *CVE details*.

CVSS: Puntuación de la vulnerabilidad.

$\bar{X}$: Promedio.

1: Identificador que contiene información, como dirección MAC y un número de serie del proveedor, así como datos opcionales, incluyendo las coordenadas GPS, el nombre del operador y las coordenadas de contacto del usuario [41].

3.2.2.4 Elaboración de propuesta de solución para las vulnerabilidades.

La Tabla 3.23 presenta las soluciones que se plantearon para las vulnerabilidades informáticas detalladas en la Tabla 3.22. Partiendo de resultados del análisis y bajo la premisa de evitar que un atacante obtenga credenciales y aumentar la dificultad de explotación de la vulnerabilidad.

Tabla 3.23 Matriz de propuestas de solución.

Elaborado por: Investigador.

Vulnerabilidad	Soluciones propuestas	Válido para	Justificación
Acceso a datos o control del dispositivo a través de permisos de: **Almacenamiento**	Retirar los permisos.	C,S	No se requiere permisos para guardar los archivos exclusivos del propio *ad blocker* en el almacenamiento interno del dispositivo.
	Incluir nuevas opciones en el cuadro de diálogo de solicitud de permiso.	N	Limitar el uso del almacenamiento .
Calendario	Retirar los permisos.	C,N,S	No es necesaria ninguna interacción con el calendario.
Cámara	Incluir nuevas opciones en el cuadro de diálogo de solicitud de permiso.	N	Limitar el uso de la cámara.
	Retirar el permiso.	C,S	No es necesaria ninguna interacción con la cámara.

Contactos	Retirar los permisos.	C,N,S	No es necesario el acceso a la lista de cuentas, si utiliza la autenticación compartida por otra aplicación como Google o Facebook. No es necesaria ninguna interacción con los contactos del usuario.
Micrófono	Incluir nuevas opciones en el cuadro de diálogo de solicitud de permiso.	N	Limitar el uso del micrófono.
	Retirar el permiso.	C,S	No es necesaria ninguna interacción con el micrófono.
Notificaciones	Permitir por defecto solo las notificaciones generales como descargas, incógnito, uso de cámara o micrófono.	N	Reducir el número de notificaciones mostradas al usuario. Evitar que el usuario acepte notificaciones potencialmente maliciosas.
	Permitir por defecto solo las notificaciones de status.	C,S	
SMS	Retirar los permisos.	C,N,S	No es necesaria ninguna interacción con el sistema de mensajería.
Teléfono	Retirar los permisos.	C,N,S	No es necesario acceder al estado del teléfono, red celular, estado de las llamadas en curso y lista de las cuentas telefónicas registradas en el dispositivo.

Ubicación	Incluir nuevas opciones en el cuadro de diálogo de solicitud de permiso. Redirigir a la aplicación Mapas de ser necesario.	N	No se necesitan actualizaciones constantes de los datos de ubicación del usuario.
	Retirar los permisos.	C,S	No es necesario a acceder a los datos de ubicación del usuario.
Acceso libre a la información que genera la aplicación.	Agregar un control de acceso de datos, a través de un filtro de solicitudes. Listar los navegadores aprobados.	C	Permitir solo solicitudes de los navegadores con las que el *ad blocker* se integra. Advertir en caso de que se intente integrar el *ad blocker* con un navegador que no se encuentre dentro de la lista.
	Asignar *"false"* a la propiedad *exported* de los proveedores de contenido.	N,S	La información generada solo está destinada para el uso interno de la aplicación.
Comunicación con sitios web maliciosos.	Utilizar un comprobador de seguridad de direcciones IP y URL.	C,N,S	Verificar que el sitio web es legítimo y seguro.
Producción de errores, a través de clases y métodos de la aplicación.	Remplazar por las clases y métodos vigentes.	C,N,S	Mejorar la compatibilidad con versiones más actuales de la API Android.

Producción de errores, a través de permisos de la aplicación.	Remplazar por los permisos vigentes. Agregar excepciones o sentencias condicionales.	C,N,S	Mejorar la compatibilidad con versiones más actuales de la API Android actual. Controlar las versiones de la API Android en la que los permisos todavía eran válidos.
Tráfico de red sin utilizar protocolos de protección de transferencia de datos.	Integrar servicios que se encarguen del cifrado de la información.	C,N,S	Evitar interferencia con sitios web que contengan elementos HTTP, de la misma manera que lo han hecho ad blockers que también brindan servicios de VPN.
C: *Ad blocker* complemento de navegador. **N:** *Ad blocker* y navegador. **S:** *Ad blocker* que brinda servicio VPN o proxy DNS.			

CAPÍTULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Con el desarrollo del trabajo se cumplieron los objetivos propuestos. A partir de la información analizada de los cien *ad blockers* correspondientes al total de la muestra representativa. Se obtuvo que 80 aplicaciones hacen públicas sus políticas de seguridad de datos, 67 hacen uso de prácticas para proteger los datos de sus usuarios, 64 recogen los datos que proporciona el usuario o produce la aplicación y 35 comparten dichos datos con terceros.

Como resultado de la investigación sobre los modelos de desarrollo de los *ad blockers*, se obtuvo que 85 aplicaciones son de código cerrado, una cantidad muy superior a las 15 aplicaciones de código abierto.

Con respecto a los permisos que los *ad blockers* solicitan, se obtuvo que 16 son permisos catalogados como peligrosos y 9 son catalogados como obsoletos por la fuente Android Developers.

Referente al análisis de la muestra de 100 *ad blockers* con la herramienta VirusTotal, se obtuvo que 15 aplicaciones son una amenaza para sus usuarios, debido a que contienen malware. Se detectaron 8 vulnerabilidades de seguridad en la programación de *ad blockers*, que incluyen aspectos como: solicitud de permisos peligrosos u obsoletos, acceso sin restricciones a la información recolectada o generada, uso de métodos obsoletos, uso de clases obsoletas, transferencia de datos sin cifrar y comunicación con sitios maliciosos.

Las soluciones que se propuso con la finalidad de mejorar la seguridad informática de los ad blockers, involucran: agregar un control de acceso de datos a los proveedores de contenido, retirar permisos peligrosos innecesarios, modificar las opciones de los cuadros de diálogo de solicitud de permiso, permitir solo notificaciones necesarias, integrar servicios de cifrado, remplazar o condicionar los permisos obsoletos,

comprobar que los sitios web contactados sean seguros y conducir al usuario a la aplicación que se especialice en la tarea deseada. Todo esto con el fin de dificultar la explotación de las vulnerabilidades y evitar que los atacantes obtengan credenciales que faciliten realizar estas acciones. En consecuencia, se estima que tendrá lugar una disminución en la posibilidad de explotar las vulnerabilidades que afectan a los *ad blockers*.

4.2 Recomendaciones

Durante el desarrollo del presente trabajo de investigación, se encontró que es recomendable continuar la investigación sobre los siguientes temas:

- Estudio de vulnerabilidades que afectan a los *ad blockers* para sistemas IOS, detallando sus causas y efectos, con el fin de dificultar la posibilidad de su explotación.
- Definir una clasificación para los tipos de *ad blockers*, con el objetivo de distinguirlos según sus características funcionales y facilitar el desarrollo de futuras aplicaciones.
- Analizar en profundidad los aspectos éticos relacionados con la disputa entre *ad blockers* y los anuncios como fuente de ingresos.
- Estudio de como las cláusulas EULA que se incluyen en los Términos y Condiciones de la aplicación, afectan a sus usuarios y desarrolladores.

C. MATERIALES DE REFERENCIA

Referencias bibliográficas

[1] I. E. Espinosa Miranda and M. S. Sanabria Altamirano, "Salesiana Sede - Quito," p. 18, 2021, [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/21310.

[2] D. D. Herrera Loaiza, "Estudio de Vulnerabilidades en transacciones bancarias para dispositivos móviles con Sistema Operativo ANDROID," p. 84, 2017, [Online].Available:http://dspace.unl.edu.ec/jspui/bitstream/123456789/18940/1/Herrera Loaiza%2C Domingo Daniel.pdf.

[3] G. V. Martínez Moncayo, "Aplicación de herramientas de hacking ético para ejecutar un test de intrusión en dispositivos móviles Android mediante un laboratorio virtual controlado enfocado en redes de área extensa e inalámbrica para pequeñas y medianas empresas de la ciudad de Gua," p. 124, 2021, [Online]. Available: http://repositorio.ug.edu.ec/handle/redug/56448.

[4] K. Garimella, O. Kostakis, and M. Mathioudakis, "Ad-blocking: A study on performance, privacy and counter-measures," WebSci 2017 - Proc. 2017 ACM Web Sci. Conf., pp. 259–262, 2017, doi: 10.1145/3091478.3091514.

[5] M. Ikram and M. A. Kaafar, "*A First Look at Ad Blocking Apps on Google Play*," 2017, [Online]. Available: http://arxiv.org/abs/1709.02901.

[6] S. Quiroz Zambrano and D. Macías Valencia, "Computer security: considerations," Dominio las Ciencias, vol. 3, no. 3, pp. 676–688, 2017.

[7] E. Téllez Carvajal, "Tecnologías, Seguridad Informática y Derechos Humanos," *IUS Sci.*, vol. 1, no. 4, pp. 19–39, 2018, doi: 10.12795/IETSCIENTIA.2018.i01.03.

[8] L. J. M. Iza Sanhueza, “Propuesta Metodológica para evaluar la seguridad del entorno informático de la Caja Central de cooperativas mediante procesos de Hardening.,” Pap. Knowl. . Towar. a Media Hist. Doc., pp. 1–82, 2020, [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/24845.

[9] R. Syed, “Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system,” Inf. Manag., vol. 57, no. 6, p. 103334, 2020, doi: 10.1016/j.im.2020.103334.

[10] L. Holguín, “Seguridad Informática: herramientas de mantenimiento y vulnerabilidades,” Univ. St. Tomás Sede Medellín, p. 18, 2019, [Online]. Available: http://hdl.handle.net/11634/17877.

[11] P. Prinetto and G. Roascio, “Hardware security, vulnerabilities, and attacks: A comprehensive taxonomy,” CEUR Workshop Proc., vol. 2597, pp. 177–189, 2020.

[12] B. Rincón and M. Eduardo, “Tecnología de información: ¿Herramienta potenciadora para gestionar el capital intelectual?,” Rev. Ciencias Soc., vol. XXVI, no. 1, 2021, doi: 10.31876/rcs.v27i1.35305.

[13] W. D. Duncan, “Ontological distinctions between hardware and software,” *Appl. Ontol.*, vol. 12, no. 1, pp. 5–32, 2017, doi: 10.3233/AO-170175.

[14] F. M. Quispe Delgado, “Concepto y definición de Software libre, historia y evolución, características de los Software libre, Software libre y la educación, aplicaciones.,” pp. 16–18, 2019, [Online]. Available: http://repositorio.une.edu.pe/handle/UNE/4616.

[15] J. F. C. Altamirano, C. E. Terán, S. Silva, and R. Córdova, “Análisis y estudio de las infraestructuras hiperconvergentes para centros de datos definidos por software,” *Recimundo*, vol. 1, no. 5, pp. 524–546, 2017, doi: 10.26820/recimundo/1.5.2017.524-546.

[16] S. Allende, F. Gibellini, C. Sánchez, and M. Serna, Sistema operativo linux: teoría y práctica 2º edición. 2019.

[17] I. Redondo and G. Aznar, To use or not to use ad blockers? The roles of knowledge of ad blockers and attitude toward online advertising, vol. 35, no. 6. 2018.

[18] A. Zambrano and C. Pickard, "A defense of ad blocking and consumer inattention," Ethics Inf. Technol., vol. 20, no. 3, pp. 143–155, 2018, doi: 10.1007/s10676-018-9454-8.

[19] IBM, "¿Qué es el software de código abierto? | IBM," IBM Topics. https://www.ibm.com/es-es/topics/open-source (accessed Oct. 25, 2022).

[20] G. Developers, "Desarrolladores de Android | Android Developers," Android Developers. https://developer.android.com/guide/topics/manifest/permission-element.html (accessed Oct. 11, 2022).

[21] Google, "How Google Play Works," Google Play. https://play.google.com/about/howplayworks/ (accessed Sep. 23, 2022).

[22] F-Droid Limited, "F-Droid - Free and Open Source Android App Repository," F-Droid. https://f-droid.org/ (accessed Sep. 23, 2022).

[23] AppTornado GmbH, "Monetize, advertise and analyze Android apps," AppBrain. https://www.appbrain.com/ (accessed Sep. 23, 2022).

[24] H. Phi and J. Nguyen, "About us - APKCombo.com," APKCombo, 2018. https://apkcombo.com/es/about (accessed Nov. 28, 2022).

[25] FIRST, "Common Vulnerability Scoring System version 3.1 Specification Document Revision 1," pp. 1–24, 2019, [Online]. Available: https://www.first.org/cvss/.

[26] CVE, “Number Of Security Vulnerabilities By CVSS Scores,” CVE Details. https://www.cvedetails.com/cvss-score-distribution.php (accessed Oct. 17, 2022).

[27] A. Abraham, “MobSF Documentation,” *GitHub*. https://mobsf.github.io/docs/#/ (accessed Nov. 01, 2022).

[28] Sanddroid, “SandDroid User ’ s Manual,” pp. 1–18, 2018.

[29] B. P. N. Security, “VirScan - Plataforma de inspección en línea de archivos multimotor,” VirSCAN. http://www.virscan.org./intruduce (accessed Nov. 01, 2022).

[30] VirusTotal, “How it works – VirusTotal,” Support VirusTotal. https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works (accessed Oct. 20, 2022).

[31] G. Developers, “Introducción a Android Studio | Desarrolladores de Android | Android Developers,” Android Developers. https://developer.android.com/studio/intro (accessed Nov. 02, 2022).

[32] C. Lasa, A. Álvarez, and R. Heras, “Manual Imprescindible Métodos Ágiles Scrum, Kanban, Lean,” pp. 1–366, 2018.

[33] ContractsCounsel, “End User License Agreement: Everything You Need to Know,” ContractsCounsel, Inc. https://www.contractscounsel.com/t/us/end-user-license-agreement (accessed Dec. 07, 2022).

[34] G. Developers, “Conceptos básicos sobre proveedores de contenido | Desarrolladores de Android | Android Developers,” Android Developers. https://developer.android.com/guide/topics/providers/content-provider-basics (accessed Nov. 03, 2022).

[35] A. Otero Ortega, “Enfoques De Investigación,” Univ. del Atl., no. August, pp. 3–5, 2018, [Online]. Available: https://www.researchgate.net/publication/326905435%0Ahttps://www.researchgate.net/profile/Alfredo-Otero-Ortega/publication/326905435_ENFOQUES_DE_INVESTIGACION/links/5b6b7f9992851ca650526dfd/ENFOQUES-DE-INVESTIGACION.pdf.

[36] N. L. Posada-González, “Algunas nociones y aplicaciones de la investigación documental denominada estado del arte,” Investig. Bibl., vol. 31, no. 73, pp. 237–263, 2017, doi: 10.22201/iibi.24488321xe.2017.73.57855.

[37] “Cu.059/2010,” pp. 2–18, 2010.

[38] G. Developers, “Android Developers | Permission element,” Android Developers. https://developer.android.com/guide/topics/manifest/permission-element (accessed Dec. 02, 2022).

[39] G. Developers, “Manifest.permission | Android Developers,” Android Developers.https://developer.android.com/reference/android/Manifest.permission (accessed Dec. 02, 2022).

[40] G. Developers, “Deprecated | Android Developers,” Android Developers. https://developer.android.com/reference/java/lang/Deprecated#forRemoval() (accessed Oct. 16, 2022).

[41] ST Engineering iDirect, “ID de operador (DVB-CID) - ST Engineering iDirect,” ST Engineering iDirect. https://www-idirect-net.translate.goog/products/carrier-id-dvb-cid/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sc (accessed Nov. 15, 2022).

Anexos

Anexo A Fichas electrónicas.

Elaborado por: Investigador.

<table>
<tr><td colspan="2">No: 1 ADB AdBlocker
Ofrecido por: hrynkoigor
Versión: 1.0
Fecha de publicación: 02/06/2022
Última actualización: 02/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.quickadbblockeradvertapplications.adbadblocker
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Ubicación aproximada.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Ubicación aproximada.
Finalidad:
Análisis.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos</td></tr>
<tr><td>Ubicación precisa (basada en red y GPS).
Leer contenido del almacenamiento compartido.
Editar/eliminar contenido del almacenamiento compartido.
Cámara.</td><td>Ver conexiones de red.
Controlar linterna.
Acceso completo a red.
Impedir modo de suspensión del dispositivo.
Ver conexiones Wifi.</td></tr>
</table>

No: 2 **Adblock Browser: veloz, seguro**

Ofrecido por: eyeo GmbH
Versión: 3.2.1
Fecha de publicación: 07/09/2015
Última actualización: 20/09/2022
Fuente: https://adblockbrowser.org/
URL: https://adblockplus.org/en/privacy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Contenido generado por usuarios.
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Registros de fallos.
Versión de la aplicación.
Datos que se recogen:
Contenido generado por usuarios.
Cuenta de aplicación.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Información personal.
Interacciones de la aplicación.
Historial de navegación web.
Registros de fallos.
Versión de la aplicación.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Conocer la información personal recopilada.
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones Wifi.	Conectarse a redes Wifi y desconectarse.
Recuperar aplicaciones en ejecución.	Controlar Comunicación de campo cercano (NFC).
Cámara.	Emparejar con dispositivos Bluetooth.
Grabar sonido.	Impedir modo de suspensión del dispositivo.
Consultar contactos.	Controlar la vibración.
Buscar cuentas en el dispositivo.	Cambiar la conectividad de red.
Añadir o eliminar cuentas.	Usar cuentas del dispositivo.
Leer contenido del almacenamiento compartido.	Instalar accesos directos.
Editar/eliminar contenido del almacenamiento compartido.	Acceso completo a red.
Descargar archivos sin notificación.	Consultar aplicaciones instaladas.
Recibir datos de Internet.	Crear cuentas y establecer contraseñas.
Leer estadísticas de sincronización.	Activar y desactivar la sincronización.
Leer la configuración de sincronización.	Reorganizar aplicaciones en ejecución.
Acceder a los ajustes de Bluetooth.	Ver conexiones de red.
Modificar los ajustes del sistema.	Desinstalar accesos directos.
Ejecutarse al inicio.	Cambiar la configuración de audio.

No: 3 **Ad Blocker Block All Ads**

Ofrecido por: Ashwath Hegde
Versión: 3.0

Fecha de publicación: 25/09/2021
Última actualización: 04/10/2022
Fuente: https://play.google.com
URL: https://pages.flycricket.io/ad-blocker-0/privacy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Interacciones de la aplicación.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Información de las aplicaciones instaladas.
Registros de fallos.
Finalidad:
Análisis, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Ver conexiones Wifi. Consultar la identidad y el estado del teléfono. Expandir/contraer la barra de estado. Ver conexiones de red. Consultar aplicaciones instaladas.	Impedir modo de suspensión del dispositivo. Controlar la vibración. Ejecutarse al inicio. Acceso completo a red.

No: 4 **AdBlocker for Android**
Ofrecido por: jTreasure
Versión: 1.0.0
Fecha de publicación: 29/06/2022
Última actualización: 29/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.adblocker.adblock_android
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Recibir datos de Internet.	Ver conexiones de red. Acceso completo a red. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Ubicación aproximada (basada en red).

No: 5 **Ad Blocker for apps - Ad Clear**
Ofrecido por: Joettaraub Offline & Online Featured Mobile Apps
Versión: 1.60
Fecha de publicación: 21/02/2019
Última actualización: 15/08/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.joettaapps.adblocker
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:

Identificador de dispositivo o de otro tipo.
Datos que se recogen:
Identificador de dispositivo o de otro tipo.
Finalidad:
Publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones de red.	Acceso completo a red. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.

No: 6 **Ad Blocker - Stop the Ads**
Ofrecido por: AMBITIOUS GAIN LP
Versión: 1.0.7
Fecha de publicación: 30/05/2022
Última actualización: 28/09/2022
Fuente: https://play.google.com
URL: https://sites.google.com/view/adblockforbrowser/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de usuario.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Datos que se recogen:
Identificador de usuario.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Finalidad:
Funcionalidad de la aplicación, análisis, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Ver conexiones Wifi. Recibir datos de Internet. Ver conexiones de red. Emparejar con dispositivos Bluetooth. Acceder a los ajustes de Bluetooth.	Acceso completo a red. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo. Ubicación aproximada (basada en red).

No: 7 **Ad Blocker Turbo - Adblocker Browser**
Ofrecido por: Big Data Technologies ltd.
Versión: 1.0.5
Fecha de publicación: 04/01/2018
Última actualización: 29/01/2018
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.adblocker.turbo.browser
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido.	Acceder a los ajustes de Bluetooth. Acceso completo a red. Cambiar la configuración de audio.

Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ver conexiones Wifi. Descargar archivos sin notificación. Recibir datos de Internet. Ver conexiones de red. Emparejar con dispositivos Bluetooth.	Controlar Comunicación de campo cercano (NFC). Ejecutarse al inicio. Reorganizar aplicaciones en ejecución. Controlar la vibración. Impedir modo de suspensión del dispositivo. Escribir en el historial y en los marcadores web. Instalar accesos directos. Consultar historial y marcadores web.

No: 8 **AdBlocker Ultimate Browser**

Ofrecido por: AdAvoid
Versión: 1.1084
Fecha de publicación: 18/10/2018
Última actualización: 19/05/2022
Fuente: https://adblockultimate.net
URL: https://adblockultimate.net/privacy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Cookies y tecnologías de seguimiento.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Ubicación aproximada y ubicación precisa.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Correo electrónico.
Identificador de dispositivo o de otro tipo.
Información personal.
Interacciones de la aplicación.
Ubicación aproximada y ubicación precisa.
Finalidad:
Análisis, comunicaciones del desarrollador, funcionalidad de la aplicación.
Prácticas de seguridad:
Conocer la información personal recopilada.
Exportar los datos personales recopilados.
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones Wifi. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Cámara. Grabar sonido.	Recibir datos de Internet. Cambiar la configuración de audio. Controlar la vibración. Impedir modo de suspensión del dispositivo. Ver conexiones de red. Acceso completo a red. Instalar accesos directos.

No: 9 **Adblock Fast**

Ofrecido por: Rocketship Apps
Versión: 2.0.0
Fecha de publicación: 11/01/2016
Última actualización: 04/09/2018
Fuente: https://adblockfast.com
URL: https://www.iubenda.com/privacy-policy/216992
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:

Identificador de dispositivo o de otro tipo.
Información personal.
Ubicación aproximada y ubicación precisa.

Datos que se recogen:

Cookies y tecnologías de seguimiento.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Idioma.
Información personal.
Interacciones de la aplicación.
Registros de fallos.
Ubicación aproximada y ubicación precisa.

Finalidad:

Funcionalidad de la aplicación, publicidad, marketing.

Prácticas de seguridad:

Derecho a rechazar la venta de información personal.
Los datos se cifran en tránsito.
Restringir el tratamiento de los datos.
Se puede solicitar que se eliminen los datos.

Permisos

Ver conexiones de red. Acceso completo a red. Recibir datos de internet. Emparejar con dispositivos Bluetooth. Acceder a los ajustes de Bluetooth. Leer y escribir datos de contacto.	Impedir modo de suspensión del dispositivo. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación precisa (basada en red y GPS).

No: 10 **AdBlock for Samsung Internet**

Ofrecido por: BetaFish
Versión: 3.2.0
Fecha de publicación: 25/01/2016
Última actualización: 28/02/2022
Fuente: https://getadblock.com/es/
URL: https://getadblock.com/es/privacy/
Modelo de desarrollo: Cerrado.

Política de seguridad de los datos, que los desarrolladores presentan públicamente

No se comparten datos con terceros.

Datos que se recogen:

Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.

Finalidad:

Análisis.

Prácticas de seguridad:

Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.

Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Acceso completo a red.	Ejecutarse al inicio. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Consultar la identidad y el estado del teléfono.

No: 11 **Adblock Less Ads**

Ofrecido por: Rucksack Mobile App Development
Versión: 2.0.5.0-adblock

Fecha de publicación: 02/09/2019
Última actualización: 12/09/2022
Fuente: https://rucksack.dev
URL: https://rucksack.dev/legal/privacy-policy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Información personal.
Datos que se recogen:
Información personal.
Cookies y tecnologías de seguimiento.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Registros de fallos.
Finalidad:
Análisis.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Conocer la información personal recopilada.
Se puede solicitar acceso y modificación de los datos.
Derecho a rechazar la venta de información personal.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Ubicación aproximada (basada en red). Leer datos de registro personales. Interactuar con los usuarios.	Ejecutarse al inicio. Acceso completo a red. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Controlar la vibración. Establecer una alarma.

No: 12 **Adblock Mobile**
Ofrecido por: ST Advanced
Versión: 7.10.3.1567
Fecha de publicación: 22/07/2015
Última actualización: 04/10/2020
Fuente: https://nomobileads.com
URL: https://sensortower.com/vpn-privacy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificación genérica.
Registros de fallos.
Datos que se recogen:
Anuncio solicitado.
Contenido del anuncio.
Dirección IP.
Identificación genérica.
Identificador de dispositivo o de otro tipo.
Información personal.
Nombre de la aplicación solicitante.
País de origen.
Registros de fallos.
Versión y tipo del navegador.
Finalidad:
Análisis, funcionalidad de la aplicación, comunicaciones del desarrollador.
Prácticas de seguridad:
Utiliza un identificador único generado aleatoriamente ("Identificación genérica").

Información personal es anónima con base a la identificación genérica.
Al desinstalar la aplicación todos los datos se vuelven anónimos permanentemente.
La dirección IP se elimina dentro de las horas posteriores a la recepción.
Los datos recopilados se pseudo anonimizan y se almacenan utilizando la ID genérica.
Los datos recopilados se desasocian permanentemente al momento de la desinstalación.

Permisos

Consultar la identidad y el estado del teléfono. Editar/eliminar contenido del almacenamiento compartido.	Acceso completo a red. Ejecutarse al inicio. Leer contenido del almacenamiento compartido.

No: 13 **Adblock para navegadores**

Ofrecido por: AdBlock Block All Ads
Versión: 3.0.117
Fecha de publicación: 01/04/2019
Última actualización: 07/09/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.spaceship.netprotect&hl=es_EC&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.

Permisos

Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.	Acceso completo a red. Ver conexiones de red.

No: 14 **ABP para Internet de Samsung**

Ofrecido por: eyeo GmbH
Versión: 2.3.0
Fecha de publicación: 08/01/2016
Última actualización: 08/04/2022
Fuente: https://adblockplus.org/es/
URL: https://adblockplus.org/en/privacy
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de dispositivo o de otro tipo.
Idioma.
Historial de navegación web.
Registros de fallos.
Versión de la aplicación.
Datos que se recogen:
Cuenta de aplicación.
Identificador de dispositivo o de otro tipo.
Idioma.
Información personal.
Historial de navegación web
Registros de fallos.
Versión de la aplicación..
Finalidad:
Funcionalidad de la aplicación, análisis, publicidad, marketing.
Prácticas de seguridad:
Conocer la información personal recopilada.
Los datos se cifran en tránsito.

Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ejecutarse al inicio.	Impedir modo de suspensión del dispositivo. Ver conexiones de red. Acceso completo a red. Consultar la identidad y el estado del teléfono.

No: 15 **Adblock - Private Adblocker Browser App**
Ofrecido por: marketing66
Versión: 1.0.8
Fecha de publicación: 06/05/2021
Última actualización: 22/03/2021
Fuente: https://play.google.com
URL: https://docs.google.com/document/d/1H-AjMmX_UVT31oR1ZpyPe8PUo5yxCiKVuVDi6pBrSRs/edit
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de dispositivo o de otro tipo.
Registros de fallos.
Ubicación aproximada.
Datos que se recogen:
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Registros de fallos.
Ubicación aproximada.
Finalidad:
Funcionalidad de la aplicación, análisis.
Prácticas de seguridad:
Se puede solicitar que se eliminen los datos.
Permisos

Recuperar aplicaciones en ejecución. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Recibir datos de Internet.	Ver conexiones de red. Acceso completo a red. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo. Establecer una alarma.

No: 16 **Ad Block REMOVER - NEED ROOT**
Ofrecido por: Marty McFly
Versión: 3.2
Fecha de publicación: 11/07/2013
Última actualización: 16/12/2013
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.av1rus.adblockremover&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos
Leer contenido del almacenamiento compartido.
Modificar los ajustes del sistema.
Editar/eliminar contenido del almacenamiento compartido.

No: 17 **AdBlock VPN**
Ofrecido por: Browser by Fulldive Co.

Versión: 1.5.5
Fecha de publicación: 04/09/2021
Última actualización: 21/09/2022
Fuente: https://www.fulldive.com
URL: https://www.fulldive.com/privacy-policy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Información personal.
Identificador de usuario.
Finalidad:
Análisis, comunicaciones del desarrollador, funcionalidad de la aplicación, seguridad.
No presenta prácticas de seguridad.
Permisos

Recuperar aplicaciones en ejecución.	Interactuar con los usuarios.
Leer datos de registro personales.	Ver conexiones de red.
Leer contenido del almacenamiento compartido.	Acceso completo a red.
Editar/eliminar contenido del almacenamiento compartido.	Ejecutarse al inicio.
	Controlar la vibración.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
ID de dispositivo e información de llamada	Establecer una alarma.

No: 18 **AdBlock VPN for Android**
Ofrecido por: BetaFish
Versión: 3.9.1
Fecha de publicación: 07/07/2021
Última actualización: 20/04/2022
Fuente: https://vpn.getadblock.com
URL: https://vpn.getadblock.com/es/privacy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Información personal.
Datos que se recogen:
Información personal.
Dirección IP.
Finalidad:
Seguridad.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Consultar la identidad y el estado del teléfono.	Conectarse a redes Wifi y desconectarse.
Leer contenido del almacenamiento compartido.	Ejecutarse al inicio.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
Ver conexiones de red.	Acceso completo a red.
Recibir datos de Internet.	Ubicación precisa (basada en red y GPS).

No: 19 **AdClear: bloqueador de contenido**
Ofrecido por: SEVEN Networks
Versión: 3.4.2.330-play

Fecha de publicación: 20/05/2016
Última actualización: 29/04/2022
Fuente: https://adclear.com
URL: https://adclear.com/app-privacy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de dispositivo o de otro tipo.
Información de uso de metadatos.
Datos que se recogen:
Cuenta de aplicación.
Dirección IP.
Identificador de dispositivo o de otro tipo.
Información de uso de metadatos.
Registro de comunicación.
Ubicación aproximada y ubicación precisa.
Finalidad:
Funcionalidad de la aplicación, análisis.
Prácticas de seguridad:
Se puede solicitar acceso y modificación de los datos.
Se puede solicitar que se eliminen los datos.
Permisos

Grabar sonido. Ver conexiones Wifi. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones de red.	Recibir datos de Internet. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Acceso completo a red. Cambiar la configuración de audio.

No: 20 **Adfree**
Ofrecido por: BigTinCan Pty Ltd.
Versión: 0.9.18
Fecha de publicación: 03/11/2013
Última actualización: 28/02/2022
Fuente: https://adfree.odiousapps.com
URL: https://adfree.odiousapps.com/about.php
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos
Recibir notificación cuando el sistema termine de iniciarse.
Acceso de super usuario.
Leer contenido del almacenamiento compartido.
Recibir datos de Internet.
Acceso completo a red.
Editar/eliminar contenido del almacenamiento compartido.

No: 21 **AdGuard Content Blocker**
Ofrecido por: AdGuard Software Limited
Versión: 2.7.0
Fecha de publicación: 23/06/2016
Última actualización: 31/03/2022
Fuente: https://adguard.com
URL: https://adguard.com/es/privacy/android.html#license-status-check
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.

Datos que se recogen:
Clave de licencia.
Configuración de la aplicación.
Cuenta de aplicación.
Identificador de la aplicación.
Identificador del dispositivo.
Identificador de compilación.
Idioma de la aplicación.
Lista de filtros habilitados.
Registros de fallos.
Versión de la aplicación.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos no se correlacionan con ninguna información personal y se usa de forma anónima.
Permisos

Ver conexiones de red. Acceso completo a red.	Impedir modo de suspensión del dispositivo. Ejecutarse al inicio.

No: 22 **AdGuard VPN – proxy privado**
Ofrecido por: AdGuard Software Limited
Versión: 2.1.54
Fecha de publicación: 12/11/2020
Última actualización: 26/08/2022
Fuente: https://adguard-vpn.com
URL: https://adguard-vpn.com/en/privacy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Cuenta de aplicación.
Diagnósticos y otros datos de rendimiento de la aplicación.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación, gestión de cuentas.
Prácticas de seguridad:
Controles de acceso al sistema.
Controles de acceso a los datos.
Controles de transmisión.
Copia de seguridad de datos.
Los datos se cifran en tránsito.
Se puede solicitar acceso y modificación de los datos.
Se puede solicitar exportación de los datos.
Se puede solicitar el tiempo de almacenamiento y fuente de los datos.
Se puede solicitar que se eliminen los datos.
Separación lógica.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Interactuar con los usuarios.	Acceso completo a red. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Conectarse a redes Wifi y desconectarse. Ejecutarse al inicio.

No: 23 **AdLock for Android**
Ofrecido por: Hankuper, s. r. o.

Versión: 2.1.6.9
Fecha de publicación: 03/02/2020
Última actualización: 24/07/2022
Fuente: https://adlock.com
URL: https://adlock.com/privacy-policy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Clave de licencia.
Dirección de control de acceso a medios (MAC).
Dirección IP.
Dimensiones de la pantalla.
Identidad de Equipo Móvil (IMEI).
Identificador de dispositivo o de otro tipo.
Identificador de la aplicación.
Información de las aplicaciones instaladas.
Idioma.
Número de serie del dispositivo.
Versión de la aplicación.
Versión del sistema operativo.
Datos que se recogen:
Clave de licencia.
Dirección de control de acceso a medios (MAC).
Dirección IP.
Dimensiones de la pantalla.
Identidad de Equipo Móvil (IMEI).
Información personal.
Identificador de dispositivo o de otro tipo.
Identificador de la aplicación.
Información de las aplicaciones instaladas.
Idioma.
Número de serie del dispositivo.
Versión del sistema operativo.
Versión de la aplicación.
Finalidad:
Análisis, correo de propaganda , hosting e infraestructura backend, interacciones basadas en la ubicación, interacción con plataformas de soporte, manejo de pagos.
Prácticas de seguridad:
Conocer la información personal recopilada.
Exportar los datos personales recopilados.
Negarse al tratamiento de datos personales.
Se puede solicitar que se eliminen los datos.
Permisos

Recibir datos de Internet. Ver conexiones de red.	Acceso completo a la red. Impedir modo de suspensión del dispositivo.

No: 24 **AdLocker - Adblock & Firewall**
Ofrecido por: Juan Pablo Ibanez Ramos
Versión: 1.1.8
Fecha de publicación: 22/02/2021
Última actualización: 19/05/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=app.adlocker&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Recuperar aplicaciones en ejecución. Ver conexiones Wifi. Ver conexiones de red. Conectarse a redes Wifi y desconectarse. Eliminar todos los datos de caché de la aplicación.	Acceso completo a red. Cerrar otras aplicaciones. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo.

No: 25 **AdProtect - Adblock & Firewall**

Ofrecido por: AdProtect Solution
Versión: 1.1.0
Fecha de publicación: 04/11/2021
Última actualización: 13/03/2022
Fuente: https://en.adprotect.app
URL: https://adprotect.app/agreements/en/privacy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Dirección IP.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación, marketing, publicidad.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Recuperar aplicaciones en ejecución. Ver conexiones Wifi. Ver conexiones de red. Conectarse a redes Wifi y desconectarse. Eliminar todos los datos de caché de la aplicación.	Acceso completo a red. Cerrar otras aplicaciones. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo.

No: 26 **Ad Remover Privacy Browser**

Ofrecido por: BrowseTech LLC
Versión: 2.0.9
Fecha de publicación: 07/05/2019
Última actualización: 18/10/2022
Fuente: https://www.adremover.org
URL: https://www.adremover.org/privacy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de dispositivo o de otro tipo.
Datos que se recogen:
Dirección IP.
Identificador de dispositivo o de otro tipo.
Información personal.
Información de las aplicaciones instaladas.
Hardware del dispositivo.
Versión de la aplicación.
Versión y tipo del navegador.
Versión del sistema operativo.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:

Almacenar datos personales durante el tiempo que sea necesario para cumplir con requisitos y obligaciones legales, para su posterior eliminación.
Los datos que no se requieran para obligaciones legales se eliminarán inmediatamente cuando el cliente, se dé de baja del producto.

Permisos

Leer contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Recibir datos de Internet. Ver conexiones de red. Ejecutarse al inicio.	Editar/eliminar contenido del almacenamiento compartido. Acceso completo a red. Instalar accesos directos. Impedir modo de suspensión del dispositivo.

No: 27 **Ads Blocker for Android**

Ofrecido por: J.P.A. Soft.
Versión: 1.0
Fecha de publicación: 03/03/2021
Última actualización: 04/03/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.jpa.soft
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.

Permisos
Esta aplicación no requiere permisos especiales para ejecutarse**.**

No: 28 **AdShield - Ad blocker**

Ofrecido por: +Now Studio
Versión: 5.9.5.6
Fecha de publicación: 04/05/2019
Última actualización: 08/02/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=
me.plusnow.shield.stable
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar

Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones de red.	Acceso completo a red. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.

No: 29 **Adware Hunter - Popup Ad Fixer**

Ofrecido por: HMT Developer
Versión: adwarehunter.21-11-21.V1.6
Fecha de publicación: 25/12/2020
Última actualización: 20/11/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=
com.hamatim.adwarehunter
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:

No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones de red. Acceso completo a red. Ejecutarse al inicio.	Consultar aplicaciones instaladas. Impedir modo de suspensión del dispositivo.

No: 30 **Aloha Navegador + VPN privado**
Ofrecido por: Aloha Mobile
Versión: 4.4.3
Fecha de publicación: 25/09/2019
Última actualización: 17/10/2022
Fuente: https://alohabrowser.com
URL: https://alohabrowser.com/policy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Registros de fallos.
Datos que se recogen:
Correo electrónico.
Interacciones de la aplicación.
Finalidad:
Análisis, comunicaciones del desarrollador, gestión de cuentas.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos se almacenan localmente.
Se puede solicitar que se eliminen los datos.
Revisión de seguridad independiente.
Permisos

Ubicación. Consultar la identidad y el estado del teléfono. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Ver conexiones de red. Ver conexiones Wifi.	Recibir datos de Internet. Cambiar la conectividad de red. Acceso completo a red. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo. Instalar accesos directos. Desinstalar accesos directos.

No: 31 **AppBrain Ad Detector**
Ofrecido por: AppTornado
Versión: 2.6.3
Fecha de publicación: 28/02/2012
Última actualización: 11/08/2021
Fuente: https://www.appbrain.com
URL: https://www.appbrain.com/info/help/privacy/index.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Información personal.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Almacena información solo necesaria para el funcionamiento de los servicios.
Todos los datos se pueden eliminar fácilmente.
Permisos

Ver conexiones de red.	Consultar aplicaciones instaladas.

Acceso completo a red. Ejecutarse al inicio.	Impedir modo de suspensión del dispositivo.

No: 32 **Avast Secure Browser**

Ofrecido por: Avast Software
Versión: 7.0.0
Fecha de publicación: 23/03/2020
Última actualización: 29/09/2022
Fuente: https://www.avast.com
URL: https://www.avast.com/products-policy#pc
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Contenido generado por usuarios.
Correo electrónico.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Ejecutarse al inicio. Ver conexiones Wifi.	Recibir datos de Internet. Ver conexiones de red. Controlar la vibración. Instalar accesos directos. Impedir modo de suspensión del dispositivo. Acceso completo a red.

No: 33 **Awax Bloqueador de anuncios**

Ofrecido por: Virtual Education OU
Versión: 1.0.109
Fecha de publicación: 25/01/2021
Última actualización: 05/03/2022
Fuente: https://awaxtech.com
URL: https://awaxtech.com/privacy-policy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Clave de licencia.
Dimensiones de la pantalla.
Dirección de control de acceso a medios (MAC).
Dirección IP.
Identidad de Equipo Móvil (IMEI).
Identificador de la aplicación.
Identificador de dispositivo o de otro tipo.
Idioma.
Información de las aplicaciones instaladas.
Número de serie del dispositivo.
Versión de la aplicación.
Versión del sistema operativo.
Datos que se recogen:
Clave de licencia.
Dimensiones de la pantalla.
Dirección de control de acceso a medios (MAC).

Dirección IP.
Identidad de Equipo Móvil (IMEI).
Identificador de la aplicación.
Identificador de dispositivo o de otro tipo.
Idioma.
Información de las aplicaciones instaladas.
Número de serie del dispositivo.
Versión de la aplicación.
Versión del sistema operativo.

Finalidad:

Análisis, gestión de contactos, hosting e infraestructura backend, interacción con plataformas de soporte, interacciones basadas en la ubicación, manejo de pagos.

Prácticas de seguridad:

Conocer la información personal recopilada.
Exportar los datos personales recopilados.
Se puede solicitar que se eliminen los datos.
Negarse al tratamiento de datos personales.
Los datos se cifran en tránsito.

Permisos

Cámara.	Ejecutarse al inicio.
Recibir datos de Internet.	Impedir modo de suspensión del dispositivo.
Acceso completo a red.	Ver conexiones de red.

No: 34 **Banana Browser: Adblock, Secure DNS, Fast & Secure**

Ofrecido por: TripleBanana
Versión: 14.06
Fecha de publicación: 23/03/2020
Última actualización: 18/08/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=org.triple.banana
Modelo de desarrollo: Cerrado.

Política de seguridad de los datos, que los desarrolladores presentan públicamente

No se comparten datos con terceros.

Datos que se recogen:

No se recogen datos.

No presenta prácticas de seguridad.

Permisos

Leer contenido del almacenamiento compartido.	Acceso completo a red.
Editar/eliminar contenido del almacenamiento compartido.	Cambiar la configuración de audio.
Buscar cuentas en el dispositivo.	Ejecutarse al inicio.
Consultar contactos.	Controlar Comunicación de campo cercano (NFC).
Grabar sonido.	Ver conexiones de red.
Ubicación aproximada (basada en red).	Emparejar con dispositivos Bluetooth.
Ubicación precisa (basada en red y GPS).	Reorganizar aplicaciones en ejecución.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
Añadir o eliminar cuentas.	Controlar la vibración.
Cámara.	Usar cuentas del dispositivo.
Descargar archivos sin notificación.	Instalar accesos directos.
Recibir datos de Internet.	Acceder a los ajustes de Bluetooth.

No: 35 **Block This!**

Ofrecido por: Sava Georgiev
Versión: 3.1
Fecha de publicación: 09/08/2015

Última actualización: 05/05/2020
Fuente: https://block-this.com
URL: https://block-this.com/privacy_policy.html
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Registros de fallos.
Datos que se recogen:
Información personal.
Registros de fallos.
Finalidad:
Funcionalidad de aplicación.
No presenta prácticas de seguridad.
Permisos

Acceso completo a red. Consultar la identidad y el estado del teléfono.	Recibir datos de Internet.

No: 36 **Blocker by +Now: Ad Blocker**
Ofrecido por: +Now Studio
Versión: 0.819-rc05
Fecha de publicación: 27/10/2021
Última actualización: 11/02/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=me.plusnow.blocker
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Consultar la identidad y el estado del teléfono. Ver conexiones Wifi. Ver conexiones de red. Acceso completo a red.	Impedir modo de suspensión del dispositivo. Controlar la vibración. Ejecutarse al inicio.

No: 37 **Blokada 6: The Privacy App+VPN**
Ofrecido por: Blocka AB
Versión: 22Q3A
Fecha de publicación: 13/06/2022
Última actualización: 26/07/2022
Fuente: https://community.blokada.org
URL: https://community.blokada.org/t/privacy-policy/6
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Correo electrónico.
Datos que se recogen:
Correo electrónico.
Dirección IP.
ID de cargo de Stripe.
Informe de problemas y soporte.
Fecha de caducidad.
Función de redes.
Nombre del operador de la red móvil.
País de origen.

Registro de fallos.
Registros de actividad de la aplicación.
Soporte por correo electrónico.
SSID de la red Wifi.
Tipo de tarjeta.
Últimos 4 dígitos de la tarjeta.
Finalidad:
Facturación, cumplimiento legal, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos permanecerán en el dispositivo hasta borrar los datos de la aplicación o desinstalar la aplicación.
Los datos se cifran en tránsito.
Permisos

Leer la identidad y el estado del dispositivo. Leer datos de registro personales. Recuperar aplicaciones en ejecución. Leer el contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (según la red).	Impedir modo de suspensión del dispositivo. Establecer una alarma. Acceso completo a la red. Ejecutarse al inicio. Controlar la vibración. Ver conexiones de red. Interactuar con los usuarios.

No: 38 **Bloqueador de anuncios**
Ofrecido por: Direct CPV Technologies
Versión: 2.9
Fecha de publicación: 09/12/2021
Última actualización: 29/07/2022
Fuente: https://directcpv.org
URL: https://directcpv.org/privacy-policy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Interacciones de la aplicación.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Ver conexiones Wifi. Recibir datos de Internet. Cerrar otras aplicaciones. Ver conexiones de red.	Acceso completo a red. Impedir modo de suspensión del dispositivo. Ejecutarse al inicio. Controlar la vibración.

No: 39 **Bloqueador de anuncios**
Ofrecido por: Maxsortube
Versión: 0.0.9.0
Fecha de publicación: 04/08/2022
Última actualización: 12/10/2022
Fuente: https://play.google.com
URL: https://yougreentube.ru/index1.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Correo electrónico.

Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Identificador de usuario.
Interacciones de la aplicación.
Registros de fallos.
Ubicación aproximada.
Datos que se recogen:
Correo electrónico.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Identificador de usuario.
Información personal.
Interacciones de la aplicación.
Registros de fallos.
Ubicación aproximada
Finalidad:
Análisis, comunicaciones del desarrollador, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones de red.	Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Acceso completo a red. Consultar aplicaciones instaladas.

No: 40 **BLU: AdBlock, Fast & Clean, Protege la Privacidad**
Ofrecido por: BlueHack
Versión: 1.0.3
Fecha de publicación: 03/10/2018
Última actualización: 02/12/2019
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=net.bluehack.blu
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación precisa (basada en red y GPS). Consultar la identidad y el estado del teléfono. Cámara.	Recibir datos de Internet. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Ver conexiones de red. Acceso completo a red. Instalar accesos directos.

No: 42 **Bravo-Rápido, AdBlock Navegador**
Ofrecido por: BravoSoftware
Versión: 2.2.4
Fecha de publicación: 26/06/2019
Última actualización: 22/05/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.blink.browser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.

No presenta prácticas de seguridad.
Permisos

Recuperar aplicaciones en ejecución. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Consultar la identidad y el estado del teléfono. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi.	Ver conexiones de red. Acceso completo a red. Ejecutarse al inicio. Establecer fondo de pantalla. Consultar aplicaciones instaladas. Impedir modo de suspensión del dispositivo. Modificar los ajustes del sistema. Instalar accesos directos.

No: 41 **Brave Navegador web privado**
Ofrecido por: Brave Software
Versión: 1.44.114
Fecha de publicación: 12/10/2016
Última actualización: 14/10/2022
Fuente: https://brave.com/es/
URL: https://brave.com/privacy/browser/
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Dirección IP.
Informe de problemas y soporte.
Registro de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Solicitar leer o modificar la información recolectada.
Restringir el tratamiento de la información recolectada.
Negarse al uso de la información recolectada.
Solicitar una copia de la información recolectada.
Permisos

Editar/eliminar contenido del almacenamiento compartido. Leer el contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación precisa (según el GPS y la red) Ubicación aproximada (según la red). Ver conexiones Wifi. Descargar archivos sin notificación. Recibir datos de Internet.	Ver conexiones de red. Cambiar la configuración de audio. Ejecutarse al inicio. Emparejar con dispositivos Bluetooth. Acceder a la configuración de Bluetooth. Instalar accesos directos. Acceso completo a la red. Impedir modo de suspensión del dispositivo. Controlar la vibración. Leer la configuración de sincronización. Reorganizar aplicaciones en ejecución.

No: 43 **Bromite - Take back your browser**

Ofrecido por: Bromite
Versión: 104.0.5112.91
Fecha de publicación: 11/10/2017
Última actualización: 15/08/2022
Fuente: https://www.bromite.org
URL: https://www.bromite.org/privacy
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Cookies y tecnologías de seguimiento.
Información de dispositivos vinculados.
Interacciones de la aplicación.
Perfil de usuario.
Registro de pagos del usuario.
Registro de transacciones.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Información de dispositivos vinculados.
Información personal.
Interacciones de la aplicación.
Perfil de usuario.
Registro de pagos del usuario.
Registro de transacciones.
Finalidad:
Funcionalidad de la aplicación, análisis, seguridad, cumplimiento legal.
Prácticas de seguridad:
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones Wifi. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Emparejar con dispositivos Bluetooth Acceder a los ajustes de Bluetooth. Reorganizar aplicaciones en ejecución Permitir instalar paquetes. Descargar archivos sin notificación. Recibir datos de Internet. Recibir notificación cuando el sistema termine de iniciarse. Impedir modo de suspensión del dispositivo. Cámara.	Grabar sonido. Leer información de accesos directos y de configuración de la pantalla de inicio. Cambiar la configuración de audio. Controlar Comunicación de campo cercano (NFC). Permitir publicar notificaciones. Consultar aplicaciones instaladas. Leer contenido del almacenamiento compartido. Permite usar hardware de huellas dactilares. Controlar la vibración. Editar/eliminar contenido del almacenamiento compartido.

No: 44 **Browser Popup Detector - Block Ads In Browser**

Ofrecido por: TT Design: Ad & Airpush Detector, Adware Removal
Versión: 0.2.2
Fecha de publicación: 14/07/2019
Última actualización: 20/05/2020
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=adblock.browser.popup.detector
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Recibir datos de Internet.	Ver conexiones de red. Acceso completo a red. Cambiar la configuración de audio. Impedir modo de suspensión del dispositivo. Instalar accesos directos.

No: 46 **Clean Ads Skip Ads Universal Tool**
Ofrecido por: ZHN.APP
Versión: 1.1
Fecha de publicación: 09/08/2021
Última actualización: 16/08/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=youtube.skip.ads
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Información personal.
Registro de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
La información personal se conservará en el dispositivo y no será recopilada.
Permisos

Acceso completo a red.	Cerrar otras aplicaciones.

No: 45 **Clario: Security & Privacy**
Ofrecido por: Clario Tech DMCC
Versión: 1.9.20.400927
Fecha de publicación: 25/06/2020
Última actualización: 15/09/2022
Fuente: https://clario.co
URL: https://clario.co/privacy-policy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Archivos y documentos.
Hardware del dispositivo.
Interacciones de la aplicación.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Registros de fallos.
Datos que se recogen:
Archivos y documentos.
Correo electrónico.
Información personal.
Identificador de usuario.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.

Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Consultar la identidad y el estado del teléfono. Ver conexiones Wifi.	Recibir datos de Internet. Acceso completo a red. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Controlar la vibración. Ejecutarse al inicio.

No: 47 **CM Browser - Fast Download, Private, Ad Blocker**

Ofrecido por: Kadamakini
Versión: CM Browser
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=cm.browser.privatewindow.download
Modelo de desarrollo: Cerrado.
Fecha de publicación: 07/12/2020
Última actualización: 07/12/2020
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Recibir datos de Internet.	Ver conexiones Wifi. Ver conexiones de red. Acceso completo a red. Cambiar la configuración de audio. Ejecutarse al inicio. Controlar la vibración. Impedir modo de suspensión del dispositivo. Instalar accesos directos.

No: 48 **Crystal para Samsung Internet**

Ofrecido por: eyeo GmbH
Versión: 2.5.0
Fecha de publicación: 23/01/2016
Última actualización: 22/08/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=co.crystalapp.crystal
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Identificador de dispositivo o de otro tipo.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Consultar la identidad y el estado del teléfono. Leer contenido del almacenamiento compartido. Ver conexiones de red. Acceso completo a red.	Editar/eliminar contenido del almacenamiento compartido. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.

No: 49 **DNS66**

Ofrecido por: Julian Andres Klode
Versión: 0.6.8
Fuente: https://f-droid.org/es/packages/org.jak_linux.dns66/
URL: https://jak-linux.org/projects/dns66/
Modelo de desarrollo: Abierto.
Fecha de publicación: 19/10/2016
Última actualización: 23/03/2021
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Acceso completo a la red. Ver conexiones de red. Ejecutarse al inicio. Ejecutar servicio en primer plano.	Editar/eliminar contenido de almacenamiento compartido. Leer contenido del almacenamiento compartido.

No: 50 **Dolphin Browser Navegador Web**

Ofrecido por: Dolphin Browser
Versión: 12.2.9
Fecha de publicación: 08/10/2010
Última actualización: 12/08/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=mobi.mgeek.TunnyBrowser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Recuperar aplicaciones en ejecución. Leer datos de registro personales. Buscar cuentas en el dispositivo. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Grabar sonido. Ver conexiones Wifi. Leer información de accesos directos y de Configuración de la pantalla de inicio. Recibir datos de Internet.	Ver conexiones de red. Medir el espacio de almacenamiento de la aplicación. Acceso completo a red. Controlar Comunicación de campo cercano (NFC). Ejecutarse al inicio. Establecer fondo de pantalla. Usar cuentas del dispositivo. Controlar la vibración. Impedir modo de suspensión del dispositivo. Instalar accesos directos. Desinstalar accesos directos.

No: 51 **DuckDuckGo Privacy Browser**

Ofrecido por: Hidden Reflex
Versión: 5.138.1
Fecha de publicación: 23/01/2018
Última actualización: 01/10/2022
Fuente: https://duckduckgo.com
URL: https://duckduckgo.com/privacy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Correo electrónico.
Historial de navegación web.
Finalidad:
Análisis, funcionalidad de la aplicación.

Prácticas de seguridad:
Agrega un código de afiliado a algunos sitios de comercio electrónico.
Evita la fuga de búsqueda de forma predeterminada.
Los datos se cifran en tránsito.
No utiliza a terceros para realizar la inserción del código.
No trabaja con ningún sitio que comparta información de identificación personal.
Permisos

Editar/eliminar contenido de almacenamiento compartido.	Ver conexiones Wifi.
Leer cont. de almacenamiento compartido.	Acceso completo a red.
Ubicación aproximada (basada en red).	Cambiar la configuración de audio.
Ubicación precisa (basada en red y GPS).	Ver conexiones de red.
Cámara.	Instalar accesos directos.
Grabar sonido.	Impedir modo de suspensión del dispositivo.
	Ejecutarse al inicio.

No: 52 **Epic Privacy Browser Ad Block, Almacén, VPN**
Ofrecido por: Hidden Reflex
Versión: 102.0.5005.80
Fecha de publicación: 04/10/2019
Última actualización: 02/06/2022
Fuente: https://www.epicbrowser.com
URL: https://epicbrowser.com/privacypolicy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Bloquea las cookies de terceros.
Los datos se cifran en tránsito.
Los datos se eliminen al cerrar la aplicación.
No se recopila datos de navegación.
Permisos

Consultar historial y marcadores web.	Controlar la vibración.
Leer contenido del almacenamiento compartido.	Reorganizar aplicaciones en ejecución.
Editar/eliminar contenido del almacenamiento compartido.	Impedir modo de suspensión del dispositivo.
Ver conexiones Wifi.	Emparejar con dispositivos Bluetooth.
Ubicación aproximada (basada en red).	Acceder a los ajustes de Bluetooth.
Ubicación precisa (basada en red y GPS).	Cambiar la conectividad de red.
Descargar archivos sin notificación.	Acceso completo a red.
Recibir datos de Internet.	Cambiar la configuración de audio.
Escribir en el historial y en los marcadores web.	Instalar accesos directos.
Ver conexiones de red.	Ejecutarse al inicio.

No: 53 **eShild:Adblocker, Secure & Private, no more ads**
Ofrecido por: Avrora Sp. z o.o
Versión: 1.2.6
Fecha de publicación: 13/02/2019
Última actualización: 19/02/2019
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=org.mainsoft.eshield
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.

Permisos	
Leer contenido del almacenamiento compartido. Ver conexiones de red. Acceso completo a red.	Editar/eliminar contenido del almacenamiento compartido.

No: 54 **FAB Adblocker Browser: Adblock**

Ofrecido por: Adblock – Rocketshield Browser Technology Limited
Versión: 96.0.2016123579
Fecha de publicación: 03/05/2015
Última actualización: 04/10/2022
Fuente: https://www.freeadblockerbrowser.com
URL: https://www.freeadblockerbrowser.com/data-privacy-website/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Archivos y documentos.
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.

Permisos	
Buscar cuentas en el dispositivo. Consultar contactos. Añadir o eliminar cuentas. Grabar sonido. Cámara. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Ver conexiones Wifi. Descargar archivos sin notificación. Leer estadísticas de sincronización. Recibir datos de Internet. Instalar accesos directos.	Usar cuentas del dispositivo. Cambiar la conectividad de red Emparejar con dispositivos Bluetooth. Controlar Comunicación de campo cercano (NFC). Ejecutarse al inicio. Activar y desactivar la sincronización. Controlar la vibración. Leer la configuración de sincronización. Acceder a los ajustes de Bluetooth. Ver conexiones de red. Cambiar la configuración de audio. Reorganizar aplicaciones en ejecución. Impedir modo de suspensión del dispositivo. Acceso completo a red.

No: 55 **Firefox Focus: el navegador**

Ofrecido por: Mozilla
Versión: 105.2.0
Fecha de publicación: 19/06/2017
Última actualización: 04/10/2022
Fuente: https://www.mozilla.org
URL: https://www.mozilla.org/es-ES/privacy/firefox-focus/
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Cuenta de aplicación.
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Información de las aplicaciones instaladas.

Registros de fallos.
Ubicación aproximada.
Finalidad:
Análisis, gestión de cuentas, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Acceso completo a red. Permite usar hardware de huellas dactilares.	Recibir datos de Internet. Descargar archivos sin notificación. Impedir modo de suspensión del dispositivo. Cambiar la configuración de audio. Ejecutarse al inicio. Ver conexiones de red. Instalar accesos directos. Leer el estado del dispositivo. Consultar aplicaciones instaladas.

No: 57 **Ghostery Privacy Browser**
Ofrecido por: Ghostery, Inc.
Versión: 2015907849
Fecha de publicación: 03/12/2014
Última actualización: 06/10/2022
Fuente: https://www.ghostery.com
URL: https://www.ghostery.com/privacy/privacy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Registros de fallos.
Ubicación aproximada.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
El historial y los marcadores procesan localmente.
No se requiere identificación.
No se recopilaron direcciones IP.
Recopila datos anónimos y puramente estadísticos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Acceso completo a red. Controlar la vibración.	Descargar archivos sin notificación. Impedir modo de suspensión del dispositivo. Cambiar la configuración de audio. Ejecutarse al inicio. Ver conexiones de red. Instalar accesos directos. Recibir datos de Internet. Permite usar hardware de huellas dactilares.

No: 56 **FOSS Browser**
Ofrecido por: FOSS Android Development
Versión: 9.4
Fecha de publicación: 17/07/2021
Última actualización: 12/07/2022
Fuente: https://github.com/scoute-dich/browser/blob/master/PRIVACY.md
URL: https://github.com/scoute-dich/browser
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Bloquea las cookies de terceros.
Los datos se eliminen al cerrar la aplicación.
No recopila ningún dato.
Permisos

Editar/eliminar contenido de almacenamiento compartido. Leer cont. de almacenamiento compartido. Grabar sonido. Grabar video.	Cambiar la configuración de audio. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Acceso completo a red. Cámara.

No: 58 **Goclean: Detector de anuncios**
Ofrecido por: Irongate
Versión: 1.4.8
Fecha de publicación: 27/04/2016
Última actualización: 10/07/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.gobest.goclean&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Ubicación aproximada y ubicación precisa.
Identificador de dispositivo o de otro tipo.
Datos que se recogen:
Ubicación aproximada y ubicación precisa.
Identificador de dispositivo o de otro tipo.
Finalidad:
Funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Recuperar aplicaciones en ejecución. Ver conexiones Wifi. Ubicación precisa (basada en red y GPS). Leer el contenido de tu almacenamiento USB. Modificar o eliminar contenido del almacenamiento USB. Cámara. Consultar la identidad y el estado del teléfono. Actualizar estadísticas de uso de componentes. Instalar accesos directos. Controlar la vibración. Ejecutarse al inicio.	Impedir modo de suspensión del dispositivo. Conectarse a redes Wifi y desconectarse. Eliminar todos los datos de caché de la aplicación. Cerrar otras aplicaciones. Acceso completo a red. Ver conexiones de red. Leer estadísticas de la batería. Modificar los ajustes del sistema. Medir el espacio de almacenamiento de la aplicación. Controlar linterna.

No: 59 **Godzilla Browser: AdBlocker**
Ofrecido por: Exacode
Versión: 4.1.3
Fecha de publicación: 11/11/2020
Última actualización: 19/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.mosoft.godzilla&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Ubicación aproximada (basada en red).	Ver conexiones de red.
Ubicación precisa (basada en red y GPS).	Controlar linterna.
Leer contenido del almacenamiento compartido.	Acceso completo a red.
Editar/eliminar contenido del almacenamiento compartido.	Cambiar la configuración de audio.
Cámara.	Ejecutarse al inicio.
Grabar sonido.	Controlar la vibración.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
	Modificar los ajustes del sistema.

No: 60 **Guard My Web Adblock VPN**
Ofrecido por: Guard My Web Solutions
Versión: 1.5.90
Fecha de publicación: 30/09/2018
Última actualización: 09/03/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.mobisoft.webguard
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Los datos se analizan sin el uso de un servidor VPN de terceros.
Datos que se recogen:
No presenta.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Servidor VPN local incorporado.
Permisos

Acceso total a la red.	Recuperar aplicaciones en ejecución.
Recibir datos de Internet.	Cerrar otras aplicaciones.
Controlar la vibración.	Evitar que el teléfono entre en modo de suspensión.
Conectarse y desconectarse de Wifi.	Ver conexiones de red.
Eliminar todos los datos de caché de aplicaciones.	Ver conexiones Wifi.
Ejecutar al inicio.	

No: 61 **Hi Browser- privado&rápido**

Ofrecido por: Dating Group
Versión: 2.6.3.1
Fecha de publicación: 06/04/2021
Última actualización: 25/08/2022
Fuente: https://play.google.com
URL: http://cdn.shalltry.com/transsionholdings/en/policy.html
Modelo de desarrollo: Cerrado.

Política de seguridad de los datos, que los desarrolladores presentan públicamente

No se comparten datos con terceros.

Datos que se recogen:

Cookies y tecnologías de seguimiento.
Cuenta de aplicación.
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Información del pedido.
Información posventa.
Información de registro.
Información de salud.
Información de voz.
Interacciones de la aplicación.
Ubicación aproximada y ubicación precisa.

Finalidad:

Análisis, gestión de cuentas, funcionalidad de la aplicación, publicidad, marketing, personalización.

Prácticas de seguridad:

Los datos se cifran en tránsito.
Los datos no se pueden eliminar.

Permisos

Leer contenido del almacenamiento compartido.	Modificar o eliminar el contenido del almacenamiento de medios interno.
Editar/eliminar contenido del almacenamiento compartido.	Leer información de accesos directos y de configuración de la pantalla de inicio.
Ver conexiones Wifi.	Inhabilitar el bloqueo de pantalla.
Buscar cuentas en el dispositivo.	Modificar los ajustes del sistema.
Ubicación aproximada (basada en red).	Leer la configuración de sincronización.
Ubicación precisa (basada en red y GPS).	Activar y desactivar la sincronización.
Cámara.	Acceso completo a red.
Consultar historial y marcadores web.	Desinstalar accesos directos.
Recuperar aplicaciones en ejecución.	Reorganizar aplicaciones en ejecución.
Iniciar cualquier actividad.	Consultar aplicaciones instaladas.
Recibir datos de Internet.	Escribir en el historial y en los marcadores web.
Interactuar con los usuarios.	Crear cuentas y establecer contraseñas.
Impedir modo de suspensión del dispositivo.	Expandir/contraer la barra de estado.
Cambiar la conectividad de red.	Establecer fondo de pantalla.
Conectarse a redes Wifi y desconectarse.	Emparejar con dispositivos Bluetooth.
Controlar la vibración.	Controlar Comunicación de campo cercano (NFC).
Ejecutarse al inicio.	
Instalar accesos directos.	
Ver conexiones de red.	

No: 62 **IgeBlock - YouTube ad blocker**

Ofrecido por: ljo
Versión: 1.0.29
Fecha de publicación: 23/08/2021

Última actualización: 04/10/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.ljo.blocktube
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Ver conexiones de red. Emparejar con dispositivos Bluetooth. Acceso completo a red.	Ejecutarse al inicio. Reorganizar aplicaciones en ejecución. Impedir modo de suspensión del dispositivo.

No: 63 **Incognito VPN - Fast VPN & Ad Blocker for Android**
Ofrecido por: Incognito Network
Versión: 2.2.1
Fecha de publicación: 28/10/2019
Última actualización: 16/09/2020
Fuente: https://www.incognitonetwork.com
URL: https://www.incognitonetwork.com/privacy-policy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Interacciones de la aplicación.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Interacciones de la aplicación.
Información de uso de metadatos.
Ubicación aproximada y ubicación precisa.
Finalidad:
Análisis, cumplimiento legal, funcionalidad de la aplicación, publicidad, marketing, facturación.
Prácticas de seguridad:
Conexión VPN no almacena ninguna información.
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Ver conexiones Wifi. Actualizar estadísticas de uso de componentes. Acceso completo a red.	Ver conexiones de red. Impedir modo de suspensión del dispositivo. Recibir datos de Internet.

No: 64 **Lightning Browser - Web Browser**
Ofrecido por: Anthony Restaino
Versión: 5.1.0
Fecha de publicación: 17/01/2013
Última actualización: 02/10/2019
Fuente: https://f-droid.org/es/packages/acr.browser.lightning/
URL: http://acrdevelopment.org
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación precisa (basada en red y GPS). Acceso completo a red.	Consultar historial y marcadores web. Escribir en el historial y en los marcadores web. Cambiar la configuración de audio. Ejecutarse al inicio. Ver conexiones de red. Instalar accesos directos.

No: 65 **Microsoft Edge**

Ofrecido por: Microsoft Corporation
Versión: 105.0.1343.50
Fecha de publicación: 18/02/2018
Última actualización: 26/09/2022
Fuente: https://www.microsoft.com
URL: https://privacy.microsoft.com/es-es/privacystatement
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Identificador de usuario.
Ubicación aproximada y ubicación precisa.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Historial de navegación web.
Identificador de usuario.
Identificador de dispositivo o de otro tipo.
Información personal.
Registro de pagos del usuario.
Registros de fallos.
Ubicación aproximada y ubicación precisa.
Finalidad:
Análisis, gestión de cuentas, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Cámara. Buscar cuentas en el dispositivo. Consultar contactos. Añadir o eliminar cuentas. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Grabar sonido. Descargar archivos sin notificación. Recibir datos de Internet. Leer estadísticas de sincronización. Activar y desactivar la sincronización. Ejecutarse al inicio.	Controlar linterna. Acceder a los ajustes de Bluetooth. Leer la configuración de sincronización. Emparejar con dispositivos Bluetooth. Cambiar la configuración de audio. Controlar Comunicación de campo cercano (NFC). Impedir modo de suspensión del dispositivo. Controlar la vibración. Acceso completo a red. Usar cuentas del dispositivo. Cambiar la conectividad de red. Crear cuentas y establecer contraseñas. Ver conexiones de red. Reorganizar aplicaciones en ejecución. Instalar accesos directos.

No: 66 **Midori Lite Navegador Web**

Ofrecido por: Astian, Inc.
Versión: 2.0.35
Fecha de publicación: 14/05/2020
Última actualización: 04/10/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=org.midorinext.android
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Administra cookies y scripts.
El historial y los marcadores procesan localmente.
Los datos permanecerán en el dispositivo hasta borrar los datos de la aplicación o desinstalar la aplicación.
Navegación privada.
Soporte de lista de filtros Adblock.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación precisa (basada en red y GPS).	Ubicación aproximada (basada en red). Consultar la identidad y el estado del teléfono. Instalar accesos directos. Cambiar la configuración de audio. Acceso completo a red. Ver conexiones de red.

No: 67 **Mobile Adblock - remove all ad**

Ofrecido por: Vtreasure Developer
Versión: 1.1.1
Fecha de publicación: 12/06/2022
Última actualización: 01/07/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.adblock.adblocker.mobile
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Acceso completo a red.	Ver conexiones de red. Impedir modo de suspensión del dispositivo. Ejecutarse al inicio.

No: 68 **Moon Browser – Adblock**

Ofrecido por: Moona Dev
Versión: 1
Fecha de publicación: 21/02/2022
Última actualización: 21/02/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.moona.superfastbrowser&hl=es_EC&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Leer el contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido.	Ver conexiones de red. Acceso completo a la red. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.

No: 69 **Opera GX: navegador gaming**

Ofrecido por: Opera
Versión: 1.6.7
Fecha de publicación: 14/07/2021
Última actualización: 05/07/2022
Fuente: https://www.opera.com/es-419/gx
URL: https://legal.opera.com/privacy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Registros de fallos.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Registros de fallos.
Finalidad:
Análisis, comunicaciones del desarrollador.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones Wifi. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Grabar sonido. Cámara. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Recibir datos de Internet.	Ver conexiones de red. Acceso completo a red. Cambiar la configuración de audio. Instalar accesos directos. Ejecutarse al inicio. Controlar Comunicación de campo cercano (NFC). Impedir modo de suspensión del dispositivo. Controlar la vibración.

No: 70 **Orions - Privacy Browser**
Ofrecido por: Apps by Marcelo de Souza
Versión: 1.0.339
Fecha de publicación: 24/05/2018
Última actualización: 07/10/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=br.marcelo.monumentbrowser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Acceder a comandos de proveedor de ubicación adicional. Editar/eliminar contenido del almacenamiento compartido.	Instalar accesos directos. Leer contenido del almacenamiento compartido. Ver conexiones Wifi. Ver conexiones de red. Acceso completo a red. Consultar aplicaciones instaladas.

No: 71 **Pando - Rewards Web Browser**
Ofrecido por: Pando Software Inc.
Versión: 2.0.23
Fecha de publicación: 01/09/2020
Última actualización: 19/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.pandora.browser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Cámara. Grabar sonido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Descargar archivos sin notificación. Leer estadísticas de sincronización. Recibir datos de Internet. Activar y desactivar la sincronización.	Leer la configuración de sincronización. Cambiar la conectividad de red. Emparejar con dispositivos Bluetooth. Impedir modo de suspensión del dispositivo. Ejecutarse al inicio. Controlar la vibración. Cambiar la configuración de audio. Acceder a los ajustes de Bluetooth. Reorganizar aplicaciones en ejecución. Ver conexiones de red. Instalar accesos directos. Acceso completo a red.

No: 72 **personalDNSfilter**
Ofrecido por: ryder203
Versión: 1.50.53.5
Fecha de publicación: 03/11/2020
Última actualización: 01/09/2022
Fuente: https://www.zenz-solutions.de
URL: https://www.zenz-solutions.de/privacy/
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
DNS de los servidores.
Dirección URL.
Duración de visita al sitio web.
Fecha y hora del acceso.
Idioma.
Resolución de pantalla.
Versión y tipo del navegador.
Versión del sistema operativo.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
En el área de inicio de sesión se utiliza lhCaptcha.
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen o modifiquen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones de red.	Acceso completo a red. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo.

No: 73 **Proton VPN: VPN veloz y segura**
Ofrecido por: Proton AG
Versión: 4.3.52.0
Fecha de publicación: 30/12/2019
Última actualización: 07/10/2022
Fuente: https://proton.me
URL: https://proton.me/legal/privacy
Modelo de desarrollo: Abierto.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Dirección IP.
Historial de compras.
Información personal.
Registros de fallos.
Finalidad:
Análisis, cumplimiento legal, gestión de cuentas, prevención de fraudes, seguridad.
Prácticas de seguridad:
Copia de seguridad de datos.
Copia de seguridad de datos se almacenan hasta un mes.
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ver conexiones de red. Conectarse a redes Wifi y desconectarse. Ejecutarse al inicio.	Impedir modo de suspensión del dispositivo. Acceso completo a red.

No: 74 **Private Browser - Privado&Safe**
Ofrecido por: Adblock – Rocketshield Browser Technology Limited
Versión: 80.0.2016123390
Fecha de publicación: 30/12/2017
Última actualización: 15/11/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.hsv.privatebrowser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Grabar sonido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Buscar cuentas en el dispositivo. Añadir o eliminar cuentas. Consultar contactos. Ver conexiones Wifi. Descargar archivos sin notificación. Leer estadísticas de sincronización. Ejecutarse al inicio. Recibir datos de Internet.	Impedir modo de suspensión del dispositivo. Acceso completo a red. Cambiar la configuración de audio. Emparejar con dispositivos Bluetooth. Instalar accesos directos. Acceder a los ajustes de Bluetooth. Leer la configuración de sincronización. Controlar Comunicación de campo cercano (NFC). Controlar la vibración. Reorganizar aplicaciones en ejecución. Ver conexiones de red. Usar cuentas del dispositivo. Activar y desactivar la sincronización.

No: 75 **Puffer: Privacy Protection & Ad-Blocking**
Ofrecido por: Parsed
Versión: 0.40Stable
Fecha de publicación: 15/02/2021
Última actualización: 11/06/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.parsed.securitywall
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Información de uso de metadatos.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Ninguno de los datos se almacenará o enviará a los servidores.
Permisos

Acceso completo a red.	Ejecutarse al inicio.

No: 76 **Pure Browser Pro-Ad Blocker**
Ofrecido por: PureBrowser
Versión: 2.5.7
Fecha de publicación: 19/06/2020
Última actualización: 15/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.pure.browser.plus
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
No se recopila ningún dato que pueda identificar personalmente.
Permisos

Acceder a sistema archivos de almacenamiento compartido. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Ubicación aproximada (basada en red).	Ubicación precisa (basada en red y GPS. Comprobación de licencia de Google Play. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Instalar accesos directos. Acceso completo a red. Cámara.

No: 77 **Pure Web Browser-Ad Blocker**
Ofrecido por: PureBrowser
Versión: 2.2.2
Fecha de publicación: 05/04/2019
Última actualización: 28/08/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=pure.lite.browser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
No se recopila ningún dato que pueda identificar personalmente.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Cámara.	Ver conexiones de red. Impedir modo de suspensión del dispositivo. Instalar accesos directos. Acceso completo a red. Ubicación aproximada (basada en red).

No: 78 **Purple Ad Blocker - Family Protection**
Ofrecido por: Big Boss Code
Versión: 1.28
Fecha de publicación: 16/06/2021
Última actualización: 13/01/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.purple.ads.blocker
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Ubicación aproximada y ubicación precisa.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Ubicación aproximada y ubicación precisa.
Finalidad:
Análisis, comunicaciones del desarrollador, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Leer contenido del almacenamiento compartido.	Descargar archivos sin notificación.
Editar/eliminar contenido del almacenamiento compartido.	Impedir modo de suspensión del dispositivo.
Ubicación precisa (basada en red y GPS).	Cambiar la configuración de audio.
Acceso completo a red.	Ejecutarse al inicio.
Ver conexiones Wifi.	Ver conexiones de red.
Conectarse a redes Wifi y desconectarse.	Modificar la configuración segura del sistema.
Controlar la vibración.	Recibir datos de Internet.
Consultar aplicaciones instaladas.	Modificar los ajustes del sistema.
	Cambiar la conectividad de red.

No: 79 **Purple DNS | Fast Ads Blocker**
Ofrecido por: Purple Smart TV
Versión: 1.20
Fecha de publicación: 30/03/2021
Última actualización: 07/10/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.purple.dns.safe
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.

Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación precisa (basada en red y GPS). Ver conexiones Wifi. Modificar la configuración segura del sistema. Acceso completo a red.	Modificar los ajustes del sistema. Conectarse a redes Wifi y desconectarse. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Ver conexiones de red. Cambiar la conectividad de red.

No: 80 **Soul Browser**
Ofrecido por: SoulSoft
Versión: 1.3.25
Fecha de publicación: 26/02/2019
Última actualización: 19/09/2022
Fuente: https://soulsofthome.blogspot.com
URL: https://soulsofthome.blogspot.com/2020/09/soul-browser-soulsoft.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Información personal.
Registros de actividad de la aplicación.
Finalidad:
Análisis, funcionalidad de la aplicación.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Cámara. Grabar sonido. Ver conexiones Wifi. Ver conexiones de red. Conectarse a redes Wifi y desconectarse.	Acceso completo a red. Cambiar la configuración de audio. Ejecutarse al inicio. Establecer fondo de pantalla. Consultar aplicaciones instaladas. Impedir modo de suspensión del dispositivo. Instalar accesos directos.

No: 81 **Spark**
Ofrecido por: WhiteHat.dev
Versión: 1.0
Fecha de publicación: 10/08/2020
Última actualización: 10/08/2020
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.browser.spark&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Acceso completo a red.	Ubicación aproximada (basada en red). Instalar accesos directos. Ubicación precisa (basada en red y GPS).

No: 82 **Stampy Browser: AdBlocker, Incognito and Secure**
Ofrecido por: Stampy Browser
Versión: 1.9
Fecha de publicación: 16/04/2019
Última actualización: 09/05/2019
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=app.stampy.browser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ver conexiones Wifi. Recibir datos de Internet. Impedir modo de suspensión del dispositivo. Inhabilitar el bloqueo de pantalla.	Ejecutarse al inicio. Modificar ajustes de visualización del sistema. Controlar la vibración. Acceso completo a red. Instalar accesos directos. Ver conexiones de red.

No: 83 **StopAd**
Ofrecido por: StopAd
Versión: 1.0.534
Fecha de publicación: 19/06/2017
Última actualización: 06/04/2020
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.stopad.stopadandroid
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Archivos y documentos.
Hardware del dispositivo.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Interacciones de la aplicación.
Registros de fallos.
Datos que se recogen:
Archivos y documentos.
Correo electrónico.
Hardware del dispositivo.
Identificador de usuario.
Identificador de dispositivo o de otro tipo.
Información de las aplicaciones instaladas.
Información personal.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis, funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Consultar la identidad y el estado del teléfono. Ejecutarse al inicio.	Ver conexiones Wifi. Recibir datos de Internet. Acceso completo a red. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Controlar la vibración.

No: 84 **Super Browser - Mini & Fast**

Ofrecido por: Super Unlimited
Versión: 3.2.5
Fecha de publicación: 18/06/2020
Última actualización: 03/10/2022
Fuente: https://superunlimited.com
URL: https://superunlimited.com/privacy/supermini_privacypolicy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Historial de navegación web.
Ubicación aproximada y ubicación precisa.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Dirección IP.
Enrutadores cercanos.
Identificador de dispositivo o de otro tipo.
Historial de navegación web.
Preferencias de navegación web.
Registros de fallos.
Ubicación aproximada y ubicación precisa.
Uso de memoria.
Finalidad:
Análisis, funcionalidad de la aplicación, seguridad, publicidad, marketing.
Prácticas de seguridad:
La información así recopilada se conservará solo durante el tiempo limitado.
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Buscar cuentas en el dispositivo. Consultar contactos. Modificar contactos. Editar/eliminar contenido del almacenamiento compartido. Leer contenido del almacenamiento compartido. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Consultar historial y marcadores web. Cámara. Grabar sonido.	Ver conexiones Wifi. Enviar notificaciones de descarga. Recibir datos de Internet. Impedir modo de suspensión del dispositivo. Instalar accesos directos. Acceso completo a red. Cambiar la configuración de audio. Ejecutarse al inicio. Escribir en el historial y en los marcadores web. Ver conexiones de red.

No: 85 **Tincat Browser m3u8 mpd live**

Ofrecido por: Netsky Tech
Versión: 4.7.0
Fecha de publicación: 28/08/2020
Última actualización: 04/10/2022
Fuente: https://www.netsky123.com
URL: https://www.netsky123.com/app/vidcat/policy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.

Datos que se recogen:
Información de la aplicación.
Finalidad:
Análisis, funcionalidad de la aplicación.
No presenta prácticas de seguridad.
Permisos

Recuperar aplicaciones en ejecución. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS). Cámara. Grabar sonido. Ver conexiones Wifi. Recibir datos de Internet. Ver conexiones de red.	Permitir recepción multidifusión Wifi. Conectarse a redes Wifi y desconectarse. Acceso completo a red. Cambiar la configuración de audio. Ejecutarse al inicio. Impedir modo de suspensión del dispositivo. Comprobación de licencia de Google Play.

No: 86 **Turbo Navegador: Privado & Bloqueador de anuncios**
Ofrecido por: mie-alcatel.support
Versión: v8.0.0.1.0301.2
Fecha de publicación: 09/03/2018
Última actualización: 23/04/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.hawk.android.browser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Cookies y tecnologías de seguimiento.
Datos biométricos.
Identificador de dispositivo o de otro tipo.
Información de registro.
Información personal.
Datos que se recogen:
Cookies y tecnologías de seguimiento.
Datos biométricos.
Identificador de dispositivo o de otro tipo.
Información de registro.
Información personal.
Finalidad:
Funcionalidad de la aplicación, publicidad, marketing.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
No presenta permisos.

No: 87 **UC Browser Turbo - Descarga rápida, Seguro**
Ofrecido por: UCWeb Singapore Pte. Ltd.
Versión: 1.10.6.900
Fecha de publicación: 29/03/2019
Última actualización: 27/10/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.ucturbo
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Configuración de la aplicación.
Función de redes.
Historial de navegación web.

Hardware del dispositivo.
Información personal.
Información de las aplicaciones instaladas.
Registros de fallos.
Ubicación aproximada y ubicación precisa.

Finalidad:

Análisis, comunicaciones del desarrollador, funcionalidad de la aplicación, publicidad, marketing.

Prácticas de seguridad:

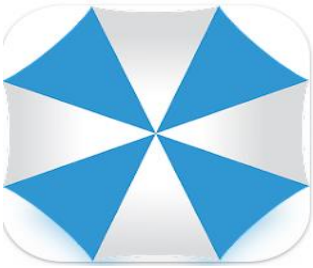
Elimina la cuenta y la información proporcionada si no ha utilizado los servicios durante un período prolongado.
Se puede solicitar que se eliminen los datos o se conserven de forma anónima.

Permisos

Ubicación aproximada (basada en red).	Modificar los ajustes del sistema.
Ubicación precisa (basada en red y GPS).	Establecer fondo de pantalla.
Consultar la identidad y el estado del teléfono.	Controlar la vibración.
Consultar historial y marcadores web.	Conectarse a redes Wifi y desconectarse.
Recuperar aplicaciones en ejecución.	Impedir modo de suspensión del dispositivo.
Leer el contenido del almacenamiento compartido.	Emparejar con dispositivos Bluetooth.
Editar/eliminar contenido del almacenamiento compartido.	Acceso completo a red.
Cámara.	Consultar aplicaciones instaladas.
Acceder a sistema archivos de almacenamiento compartido.	Permitir recepción multidifusión Wifi.
Ver conexiones Wifi.	Medir el espacio de almacenamiento de la aplicación.
Grabar sonido.	Ver conexiones de red.
Actualizar estadísticas de uso de componentes.	Expandir/contraer la barra de estado.
Recibir datos de Internet.	Escribir en el historial y en los marcadores web.
	Cambiar la conectividad de red.

No: 88 **Umbrella - Adblock & Firewall**

Ofrecido por: Buntai Apps
Versión: 1.6.1
Fecha de publicación: 29/05/2017
Última actualización: 30/03/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.consulenza.umbrellacare
Modelo de desarrollo: Cerrado.



Política de seguridad de los datos, que los desarrolladores presentan públicamente

No presenta.

Permisos

Recuperar aplicaciones en ejecución.	Acceso completo a red.
Ver conexiones Wifi.	Cerrar otras aplicaciones.
Recibir datos de Internet.	Ejecutarse al inicio.
Ver conexiones de red.	Controlar la vibración.
Conectarse a redes Wifi y desconectarse.	Impedir modo de suspensión del dispositivo.

No: 89 **Unicorn Blocker:Adblocker, Fast & Private**

Ofrecido por: Unicorn Soft, Inc.
Versión: 1.9.9.35
Fecha de publicación: 03/03/2016
Última actualización: 17/07/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=kr.co.lylstudio.unicorn
Modelo de desarrollo: Cerrado.

Política de seguridad de los datos, que los desarrolladores presentan públicamente

No presenta.

Permisos

Consultar la identidad y el estado del teléfono. Ver conexiones Wifi. Leer contenido del almacenamiento compartido. Recibir datos de Internet. Ejecutarse al inicio.	Impedir modo de suspensión del dispositivo. Acceso completo a red. Ver conexiones de red. Editar/eliminar contenido del almacenamiento compartido.

No: 90 **Via Navegador Rápido y liviano**

Ofrecido por: Tu Yafeng
Versión: 4.4.4
Fecha de publicación: 18/08/2016
Última actualización: 25/09/2022
Fuente: https://viayoo.com/en/
URL: https://viayoo.com/en/docs/privacy-policy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Interacciones de la aplicación.
Registros de fallos.
Datos que se recogen:
Diagnósticos y otros datos de rendimiento de la aplicación.
Identificador de dispositivo o de otro tipo.
Identificador de usuario.
Interacciones de la aplicación.
Registros de fallos.
Finalidad:
Análisis.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ubicación precisa (basada en red y GPS). Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara.	Ver conexiones Wifi. Ver conexiones de red. Acceso completo a red. Impedir modo de suspensión del dispositivo. Instalar accesos directos.

No: 91 **Vider Adblock - Video Browser**

Ofrecido por: Vider Applications
Versión: 88.0.4324.96
Fecha de publicación: 08/06/2021
Última actualización: 22/06/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.viderbrowser
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Grabar sonido. Cámara. Buscar cuentas en el dispositivo. Consultar contactos. Ver conexiones Wifi. Añadir o eliminar cuentas. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS. Consultar historial y marcadores web. Acceder a los ajustes de Bluetooth. Leer la configuración de sincronización. Impedir modo de suspensión del dispositivo. Controlar la vibración.	Descargar archivos sin notificación. Leer estadísticas de sincronización. Recibir datos de Internet. Ejecutarse al inicio. Activar y desactivar la sincronización. Instalar accesos directos. Cambiar la conectividad de red. Controlar Comunicación de campo cercano (NFC). Usar cuentas del dispositivo. Reorganizar aplicaciones en ejecución. Escribir en el historial y en los marcadores web Ver conexiones de red. Cambiar la configuración de audio. Acceso completo a red. Emparejar con dispositivos Bluetooth.

No: 92 **Vivaldi Navegador**

Ofrecido por: Vivaldi Technologies
Versión: 5.5.2807.32
Fecha de publicación: 06/09/2019
Última actualización: 13/10/2022
Fuente: https://vivaldi.com
URL: https://vivaldi.com/es/privacy/browser/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Los datos se almacenan localmente.
Permisos

Grabar sonido. Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Cámara. Consultar historial y marcadores web. Buscar cuentas en el dispositivo. Añadir o eliminar cuentas. Ver conexiones Wifi. Consultar contactos. Ubicación aproximada (basada en red). Ubicación precisa (basada en red y GPS. Recibir datos de Internet. Leer estadísticas de sincronización. Controlar Comunicación de campo cercano (NFC).	Descargar archivos sin notificación. Usar cuentas del dispositivo. Instalar accesos directos. Emparejar con dispositivos Bluetooth. Ejecutarse al inicio. Controlar la vibración. Activar y desactivar la sincronización. Escribir en el historial y en los marcadores web. Acceder a los ajustes de Bluetooth. Leer la configuración de sincronización. Reorganizar aplicaciones en ejecución. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Acceso completo a red. Cambiar la configuración de audio.

No: 93 **Vivo Browser**
Ofrecido por: PT. Vivo Mobile Indonesia
Versión: 4.0.0.0
Fecha de publicación: 05/25/2019
Última actualización: 17/01/2022
Fuente: https://www.vivo.com
URL: https://www.vivo.com/en/index/privacyPolicy
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Ubicación aproximada y ubicación precisa.
Datos que se recogen:
Cuenta de aplicación.
Historial de navegación web.
Identificador de dispositivo o de otro tipo.
Información personal.
Registros de fallos.
Ubicación aproximada y ubicación precisa.
Finalidad:
Funcionalidad de la aplicación.
Prácticas de seguridad:
Conocer la información personal recopilada.
Exportar los datos personales recopilados.
Los datos se cifran en tránsito.
Restringir el tratamiento de los datos.
Se puede solicitar que se eliminen los datos.
Permisos

Consultar contactos.	Reservar espacio en caché de descargas.
Añadir o eliminar cuentas.	Modificar cálculo de uso de red.
Buscar cuentas en el dispositivo.	Actualizar estadísticas de uso de componentes.
Consultar tarjeta de contacto.	Leer memoria de almacenamiento intermedio.
Ver conexiones Wifi.	Recuperar aplicaciones en ejecución.
Añadir o modificar eventos de calendario y enviar mensajes a los invitados sin el consentimiento de los propietarios.	Enviar notificaciones de descarga.
	Evitar cambios de aplicación.
	Modificar estadísticas de la batería.
Leer eventos de calendario e información confidencial.	Modificar o eliminar el contenido del almacenamiento de medios interno.
Leer contenido del almacenamiento compartido.	Etiqueta de SmartcardServicePermission.
Editar/eliminar contenido del almacenamiento compartido.	Descargar archivos sin notificación.
	Acceso completo a red.
Acceder a sistema archivos de almacenamiento compartido.	Consultar aplicaciones instaladas.
	Conectarse a redes Wifi y desconectarse.
Grabar sonido.	Cambiar la configuración de audio.
Consultar la identidad y el estado del teléfono.	Cerrar otras aplicaciones.
Ubicación aproximada (basada en red).	Crear cuentas y establecer contraseñas.
Ubicación precisa (basada en red y GPS).	Escribir en el historial y en los marcadores web.
Recuperar aplicaciones en ejecución.	Ver conexiones de red.
Leer datos de registro personales.	Reorganizar aplicaciones en ejecución.
Consultar historial y marcadores web.	Permitir recepción multidifusión Wifi.
Cámara.	Activar y desactivar la sincronización.
Acceder a todas las descargas del sistema.	Ejecutarse al inicio.
Acceder al sistema de archivos almacenado en Caché.	Cambiar la conectividad de red.
	Usar cuentas del dispositivo.
Acceder al administrador de descargas.	Instalar accesos directos.
Funciones avanzadas del administrador de descargas.	Modificar los ajustes del sistema.
	Impedir modo de suspensión del dispositivo.
Habilitar o inhabilitar componentes de la aplicación.	Inhabilitar el bloqueo de pantalla.
	Leer la configuración de sincronización.

Eliminar datos de otras aplicaciones. Apagar o encender el dispositivo. Cerrar otras aplicaciones. Interactuar con los usuarios. Controlar la vibración.	Controlar Comunicación de campo cercano (NFC). Establecer fondo de pantalla. Controlar linterna.

No: 94 **VPN Dash: Fast VPN Proxy**

Ofrecido por: Act Mobile Networks
Versión: 3.880
Fecha de publicación: 17/06/2014
Última actualización: 17/06/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/datasafety?id=com.actmobile.dashvpn
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Ver conexiones Wifi. Controlar la vibración. Impedir modo de suspensión del dispositivo.	Recibir datos de Internet. Ver conexiones de red. Acceso completo a red.

No: 95 **VPN Galaxy - VPN Proxy & AdBlock**

Ofrecido por: AppLine Ltd.
Versión: 1.1.16
Fecha de publicación: 29/09/2020
Última actualización: 13/07/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.vpngalaxy.app
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Ubicación aproximada.
Registros de fallos.
Registro de pagos del usuario.
Datos que se recogen:
Ubicación aproximada.
Registros de fallos.
Registro de pagos del usuario.
Finalidad:
Análisis, comunicaciones del desarrollador, funcionalidad de la aplicación, publicidad, marketing, personalización.
No presenta prácticas de seguridad.
Permisos

Leer contenido del almacenamiento compartido. Editar/eliminar contenido del almacenamiento compartido. Acceder a sistema archivos de almacenamiento compartido. Recibir datos de Internet.	Ejecutarse al inicio. Acceso completo a red. Ver conexiones de red. Impedir modo de suspensión del dispositivo. Controlar la vibración.

No: 96 **VPN Owl: Fast and Secure VPN**
Ofrecido por: VPN LLC (open-vpn.org)
Versión: 3.898
Fecha de publicación: 01/06/2019
Última actualización: 11/10/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=openvpn.vpn&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
No se recogen datos.
No presenta prácticas de seguridad.
Permisos

Ubicación aproximada (basada en red).	Ver conexiones de red.
Ubicación precisa (basada en red y GPS).	Acceso completo a red.
Leer contenido del almacenamiento compartido.	Ejecutarse al inicio.
Editar/eliminar contenido del almacenamiento compartido.	Controlar la vibración.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
	Recibir datos de Internet.

No: 97 **VPN + TOR Browser and Ad Block**
Ofrecido por: Falling Rain Software, Limitedh
Versión: 3.890
Fecha de publicación: 18/11/2021
Última actualización: 06/09/2022
Fuente: http://fallingrain.com/
URL: http://abv.fallingrain.com/privacy-policy/
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
Datos compartidos con terceros:
Información necesaria para actividades del controlador de datos.
Datos que se recogen:
Dirección IP.
Hardware del dispositivo.
Identificador de dispositivo o de otro tipo.
Idioma.
Información personal.
País de origen.
Finalidad:
Funcionalidad de la aplicación, análisis, marketing o publicidad, cumplimiento legal.
Prácticas de seguridad:
Los datos personales del usuario se conservarán durante un plazo no superior a dos años a partir de la cancelación de la cuenta de la aplicación.
Conocer la información personal recopilada.
Se puede solicitar acceso y modificación de los datos.
Permisos

Ver conexiones Wifi.	Acceso completo a red.
Recibir datos de Internet.	Ver conexiones de red.
Controlar la vibración.	Impedir modo de suspensión del dispositivo.

No: 98 **VPN Venus**

Ofrecido por: Meg Digital LTD
Versión: 1.0
Fecha de publicación: 04/03/2021
Última actualización: 21/05/2021
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=com.vpnvenus.android
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Identificador de sesión.
Información de conexión VPN.
Nombre de usuario.
Registros de actividad de la aplicación.
Finalidad:
Cumplimiento legal, funcionalidad de la aplicación, prevención de fraudes, seguridad.
Prácticas de seguridad:
Los datos se cifran en tránsito.
Se puede solicitar que se eliminen los datos.
Permisos

Ubicación precisa (basada en red y GPS).	Recibir datos de Internet.
Ver conexiones Wifi.	Controlar la vibración.
Ver conexiones de red.	Acceso completo a red.
Impedir modo de suspensión del dispositivo.	Ejecutarse al inicio.

No: 99 **WebGuard - Adblock & Firewall**

Ofrecido por: Primera Solución Móvil S.L.
Versión: 1.6.2
Fecha de publicación: 06/03/2021
Última actualización: 05/05/2021
Fuente: https://en.webguard.app
URL: https://webguard.app/agreements/en/privacy.html
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No se comparten datos con terceros.
Datos que se recogen:
Dirección IP.
Hardware del dispositivo.
Identificador de dispositivo o de otro tipo.
Registros de fallos.
Finalidad:
Análisis y funcionalidad de la aplicación.
Prácticas de seguridad:
Anonimizan la dirección IP.
Los datos se cifran en tránsito.
Los datos no se pueden eliminar.
Permisos

Recuperar aplicaciones en ejecución.	Acceso completo a red.
Ver conexiones Wifi.	Cerrar otras aplicaciones.
Ver conexiones de red.	Ejecutarse al inicio.
Conectarse a redes Wifi y desconectarse.	Controlar la vibración.
Eliminar todos los datos de caché de la aplicación.	Impedir modo de suspensión del dispositivo.

No: 100 **광고차단 브라우저 : 블로켓 - 인터넷 애드블록**

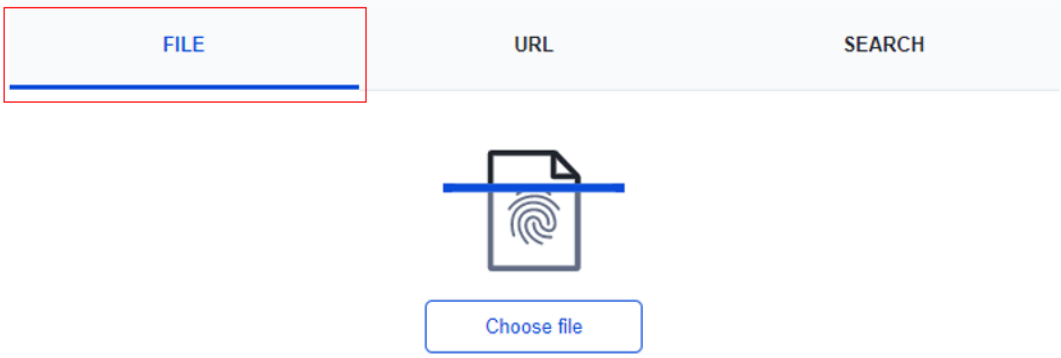
Ofrecido por: Common Computer Inc.
Versión: 2.8.0
Fecha de publicación: 13/12/2019
Última actualización: 14/04/2022
Fuente: https://play.google.com
URL: https://play.google.com/store/apps/details?id=ai.blokee.browser.android&hl=es&gl=US
Modelo de desarrollo: Cerrado.
Política de seguridad de los datos, que los desarrolladores presentan públicamente
No presenta.
Permisos

Ubicación aproximada (basada en red).	Recibir datos de Internet.
Ubicación precisa (basada en red y GPS).	Ver conexiones de red.
Leer contenido del almacenamiento compartido.	Acceso completo a red.
Editar/eliminar contenido del almacenamiento compartido.	Ejecutarse al inicio.
Ver conexiones Wifi.	Impedir modo de suspensión del dispositivo.
	Instalar accesos directos.

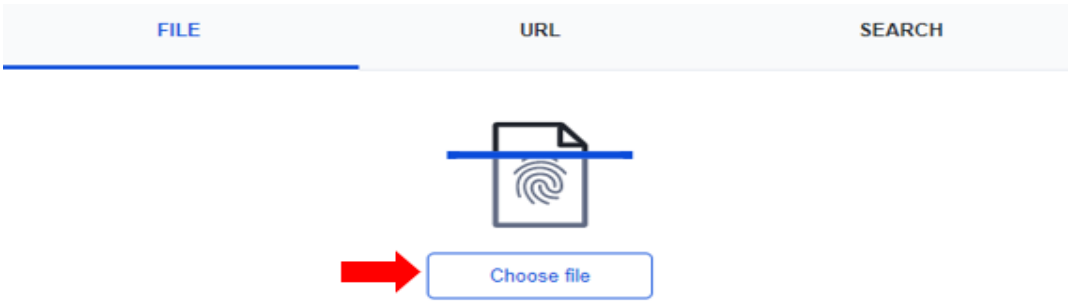
Anexo B Manual de uso de VirusTotal.

Acceda en el navegador a el sitio web de VirusTotal, utilizando el siguiente enlace: https://www.virustotal.com/gui/home/upload

Elija la opción de análisis de archivos, pulsando "*File"* .

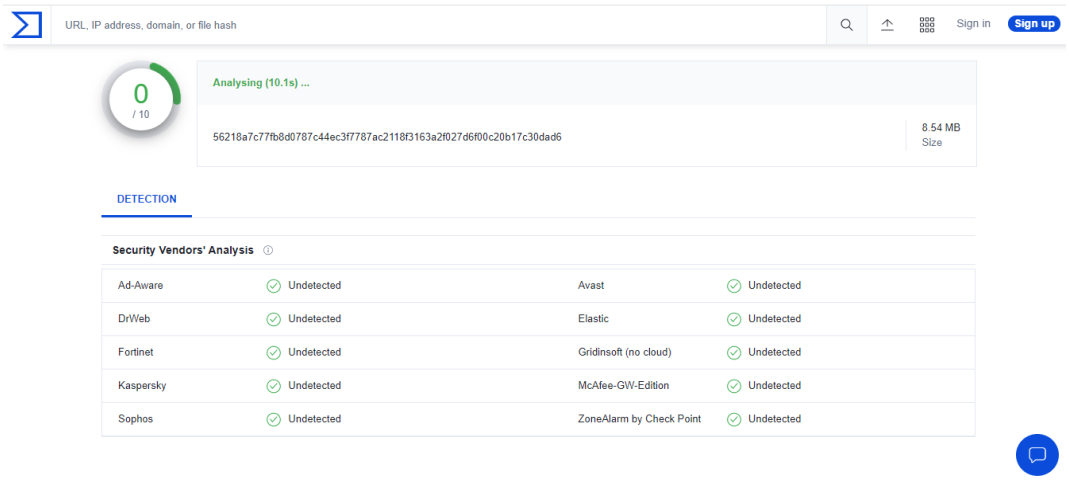


Pulse el botón "*Choose file"* y elija el archivo APK a analizar. El tamaño máximo del archivo no debe ser superior a 550mb.

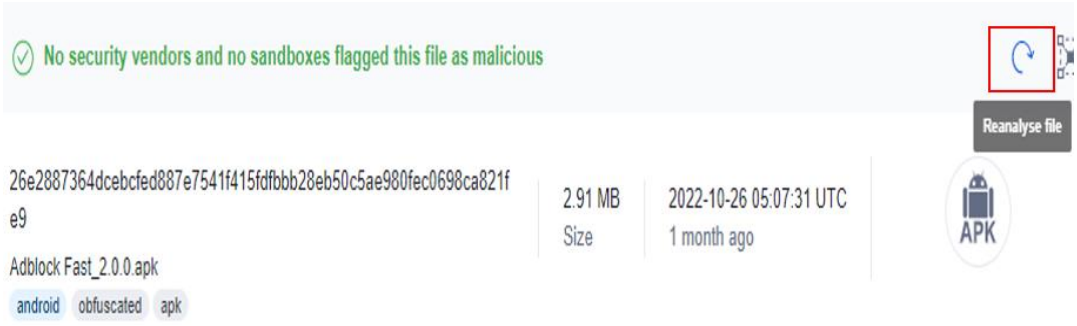


Confirme la subida del archivo APK a la base de datos de VirusTotal. Espere a que termine la subida del archivo, no cierre o actualice el sitio web. Una vez termine la subida el análisis comenzara.

Espere que termine el análisis del archivo APK. La duración depende del tamaño del archivo.

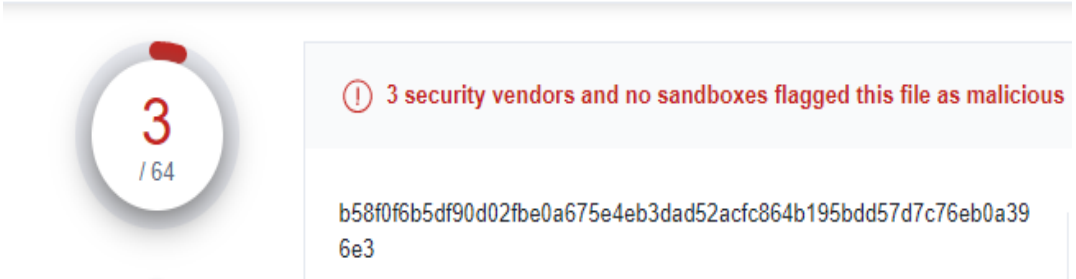


Si el archivo fue cargado anteriormente por otro usuario, el informe resultante del análisis aparecerá sin necesidad de espera. Sin embargo, es recomendable realizar nuevamente el análisis, para que el análisis se realice con los motores de escaneo más actuales. Para realizar nuevamente el análisis presione *"Reanalyze file"*.

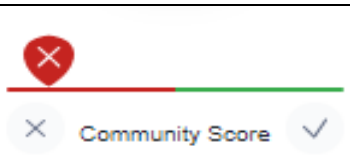


Posterior al análisis se mostrarán los siguientes elementos:

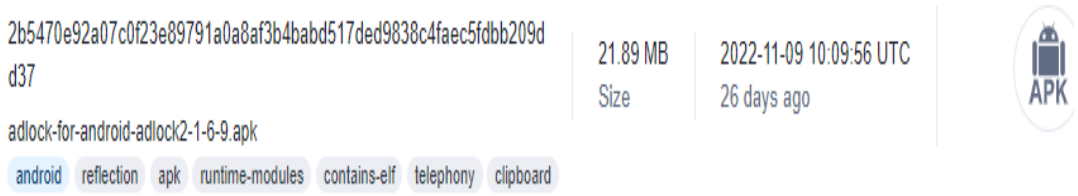
Número de proveedores de seguridad que han marcado a el archivo como malicioso.



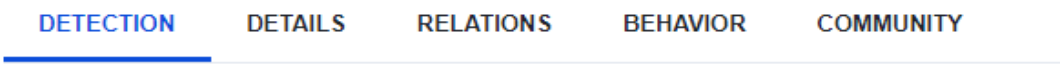
Puntaje de comunidad *"Community Score"*.



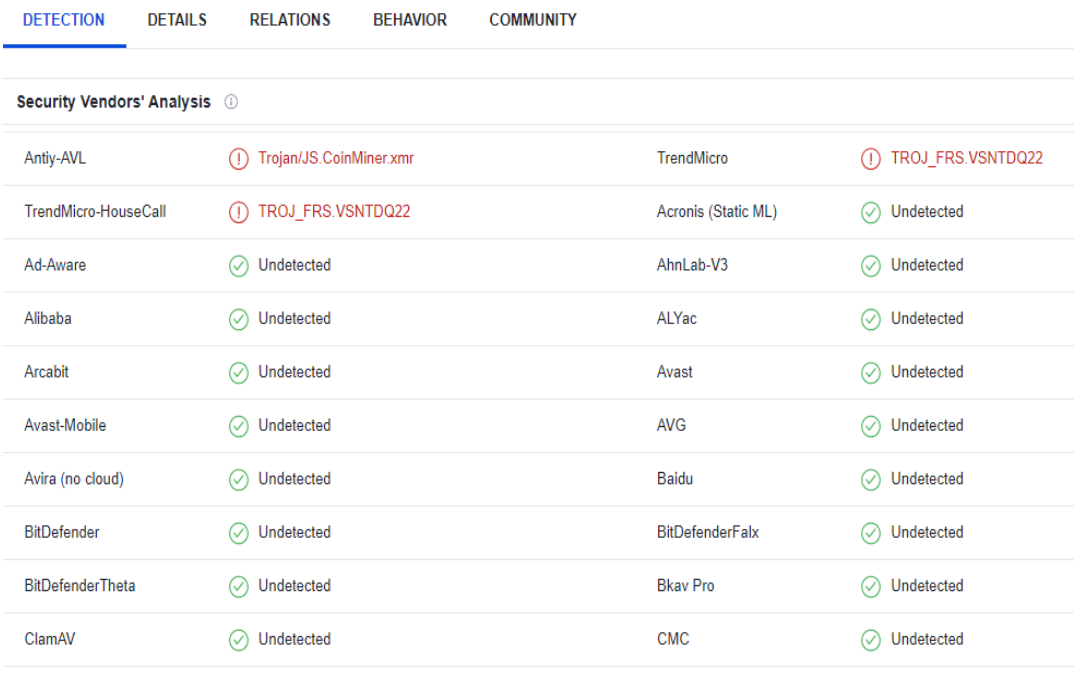
Información básica sobre el archivo y fecha del análisis.



Pestañas *Detections, Details, Relations, Behavior y Community*.



La pestaña *"Detections"* permite verificar cuales son los proveedores de seguridad que analizaron el archivo y su resultado. En el caso de que el proveedor detecte malware especificara su nombre.



La pestaña *"Details"* contiene información de certificados, permisos, tipos de archivos, los nombres de las actividades, proveedores, clientes y servicios de la aplicación.

Permissions

- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.QUERY_ALL_PACKAGES
- android.permission.CHANGE_WIFI_STATE

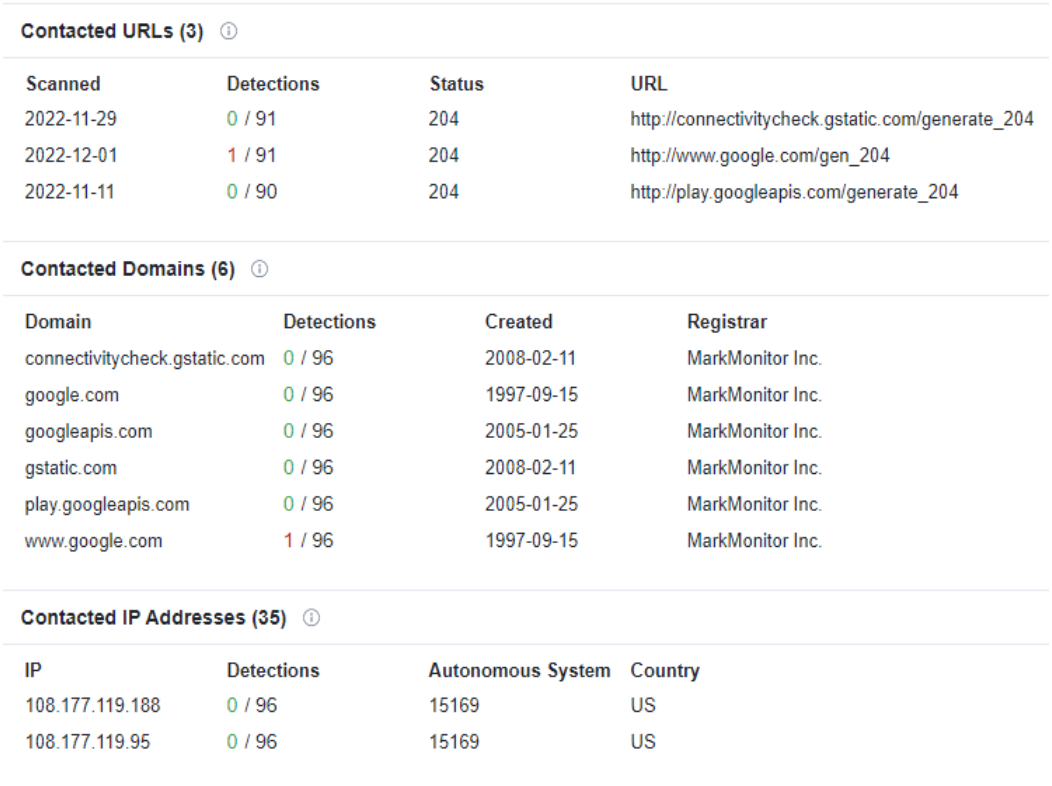
Activities

com.protonvpn.android.ui.onboarding.SplashActivity
com.protonvpn.android.ui.home.vpn.SwitchDialogActivity
com.protonvpn.android.tv.main.TvMainActivity
com.protonvpn.android.tv.TvUpgradeActivity
me.proton.core.auth.presentation.ui.AddAccountActivity
me.proton.core.auth.presentation.ui.signup.SignupActivity
me.proton.core.auth.presentation.ui.LoginActivity
me.proton.core.auth.presentation.ui.AuthHelpActivity
me.proton.core.presentation.ui.alert.ForceUpdateActivity
com.protonvpn.android.ui.main.MobileMainActivity

Services

org.strongswan.android.logic.VpnStateService
com.protonvpn.android.vpn.ikev2.ProtonCharonVpnService

La pestaña *"Relations"* contiene información sobre los dominios, direcciones URL y direcciones IP contactadas por la aplicación.



Contacted URLs (3)

Scanned	Detections	Status	URL
2022-11-29	0 / 91	204	http://connectivitycheck.gstatic.com/generate_204
2022-12-01	1 / 91	204	http://www.google.com/gen_204
2022-11-11	0 / 90	204	http://play.googleapis.com/generate_204

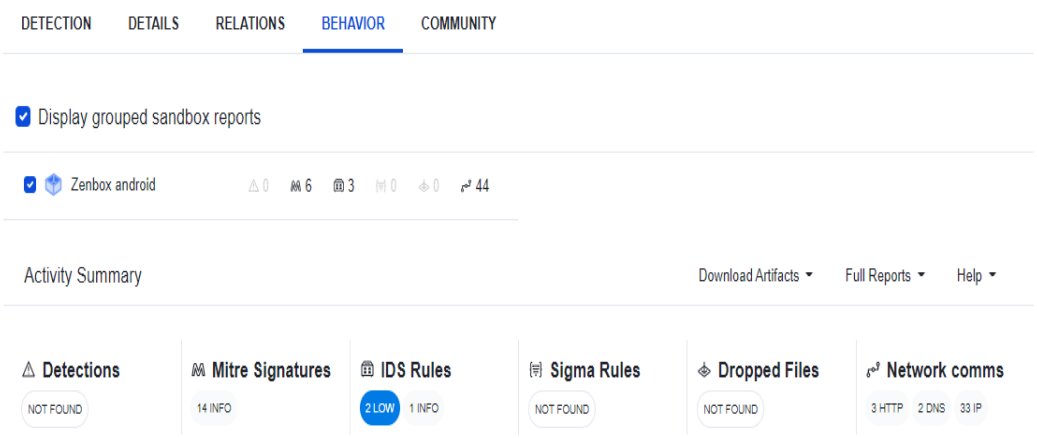
Contacted Domains (6)

Domain	Detections	Created	Registrar
connectivitycheck.gstatic.com	0 / 96	2008-02-11	MarkMonitor Inc.
google.com	0 / 96	1997-09-15	MarkMonitor Inc.
googleapis.com	0 / 96	2005-01-25	MarkMonitor Inc.
gstatic.com	0 / 96	2008-02-11	MarkMonitor Inc.
play.googleapis.com	0 / 96	2005-01-25	MarkMonitor Inc.
www.google.com	1 / 96	1997-09-15	MarkMonitor Inc.

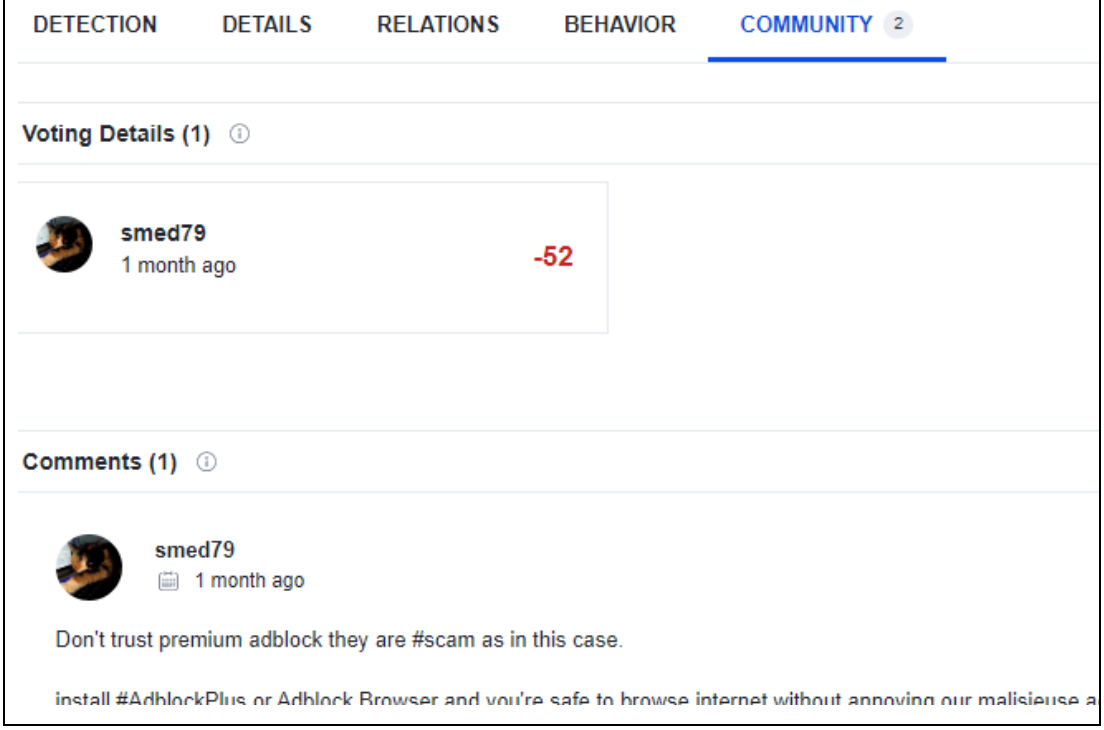
Contacted IP Addresses (35)

IP	Detections	Autonomous System	Country
108.177.119.188	0 / 96	15169	US
108.177.119.95	0 / 96	15169	US

La pestaña *"Behavior"* contiene información sobre el comportamiento del archivo APK como: detecciones, archivos eliminados, comunicaciones de red.



La pestaña "*Community*" contiene una sección para agregar un comentario o leer comentarios de otros usuarios sobre el archivo. Es necesario crear una cuenta para agregar comentarios.



Anexo C Proveedor de contenido de Adblock Fast.

Fuente:

https://github.com/rocketshipapps/adblockfast/blob/main/android/app/src/main/AndroidManifest.xml

```
<provider
    android:name=".FiltersContentProvider"
    android:authorities="com.adguard.android.contentblocker.contentBlocker.contentProvider"
    android:enabled="true"
    android:exported="true"
    android:grantUriPermissions="true" />
```

Anexo D Método para verificar permiso GET_ACCOUNTS.

Fuente:

https://github.com/rocketshipapps/adblockfast/blob/main/android/app/src/main/java/com/rocketshipapps/adblockfast/MainActivity.java

```
private void checkAccountPermission() {
    if (preferences.getBoolean(RETRIEVED_ACCOUNT_PREF, false))
return;

    if (ContextCompat.checkSelfPermission(this,
Manifest.permission.GET_ACCOUNTS) ==
PackageManager.PERMISSION_DENIED) {
        getAccounts();
    } else if (Build.VERSION.SDK_INT >= Build.VERSION_CODES.M) {
        if
(ActivityCompat.shouldShowRequestPermissionRationale(this,
Manifest.permission.GET_ACCOUNTS)) {
            showAccountPermissionAlert(
            );
        } else {
            requestPermissions(new
String[]{Manifest.permission.GET_ACCOUNTS},
REQUEST_PERMISSION_GET_ACCOUNTS);
        }
    }
}
```

Anexo E Proveedor de contenido de Adguard.

Fuente:

https://github.com/AdguardTeam/ContentBlocker/blob/master/adguard_cb/src/main/AndroidManifest.xml

```
<provider
    android:name=".FiltersContentProvider"
    android:authorities="com.adguard.android.contentblocker.contentBlocker.contentProvider"
    android:enabled="true"
    android:exported="true"
    android:grantUriPermissions="true" />
```

Anexo F Configuración de seguridad de la red Adguard.

Fuente:
https://github.com/AdguardTeam/ContentBlocker/blob/master/adguard_cb/src/main/es/xml/network_security_config.xml

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

Anexo G Método para verificar el tráfico no cifrado.

Fuente: https://github.com/bromite/bromite/blob/master/build/patches/Add-bookmark-import-export-actions.patch

```
#if BUILDFLAG(IS_ANDROID)
+    if
(base::FeatureList::IsEnabled(net::features::kIsCleartextPermitted)
== false) {
+      return std::make_unique<URLRequestErrorJob>(request,
+
ERR_CLEARTEXT_NOT_PERMITTED);
+    }
     // Check whether the app allows cleartext traffic to this host,
and return
     // ERR_CLEARTEXT_NOT_PERMITTED if not.
     if (request->context()->check_cleartext_permitted() &&
```

Anexo H Declaración de la aplicación Firefox Focus.

Fuente: https://github.com/mozilla-mobile/focus-android/blob/main/app/src/main/AndroidManifest.xml

```
<application
    android:allowBackup="false"
    android:extractNativeLibs="true"
    android:icon="@mipmap/ic_launcher"
    android:label="@string/app_name"
    android:supportsRtl="true"
    android:theme="@style/Theme.App.Starting"
    android:name=".FocusApplication"
    android:usesCleartextTraffic="true">
```

Anexo I Declaración de la aplicación FOSS Browser

Fuente: https://github.com/scoute-dich/browser/blob/master/app/src/main/AndroidManifest.xml

```
<application
    android:allowBackup="true"
    android:dataExtractionRules="@xml/data_extraction_rules"
    android:fullBackupContent="@xml/backup"
    android:hardwareAccelerated="true"
    android:icon="@mipmap/ic_launcher"
    android:label="@string/app_name"
    android:largeHeap="true"
    android:requestLegacyExternalStorage="true"
    android:resizeableActivity="true"
    android:roundIcon="@mipmap/ic_launcher_round"
    android:supportsRtl="true"
    android:usesCleartextTraffic="true"
    tools:ignore="GoogleAppIndexingWarning"
    tools:targetApi="s">
```

Anexo J Declaración de la aplicación Lightning Browser.

Fuente: https://github.com/anthonycr/Lightning-Browser/blob/browser2/app/src/main/AndroidManifest.xml

```
<application
    android:name=".BrowserApp"
    android:allowBackup="true"
    android:hardwareAccelerated="true"
    android:icon="@mipmap/ic_launcher"
    android:roundIcon="@mipmap/ic_launcher"
    android:usesCleartextTraffic="true"
    android:label="@string/app_name">
```

Anexo K Declaración de la aplicación Midori Lite.

Fuente: https://gitlab.com/midori-web/midori-android/-/blob/master/app/src/main/AndroidManifest.xml

```
<application
    android:name=".BrowserApp"
    android:allowBackup="true"
    android:debuggable="false"
    android:fullBackupContent="true"
    android:hardwareAccelerated="true"
    android:icon="@mipmap/ic_midori_round"
    android:label="@string/app_name"
    android:roundIcon="@mipmap/ic_midori"
    android:usesCleartextTraffic="true"
    android:supportsRtl="true"
    android:resizeableActivity="true"
    tools:ignore="HardcodedDebugMode">
```

Anexo L Declaración de la aplicación personalDNSfilter.

Fuente: https://github.com/IngoZenz/personaldnsfilter/blob/master/app/src/main/AndroidManifest.xml

```
<application
    android:usesCleartextTraffic="true"
    android:icon="@mipmap/ic_launcher"
    android:label="personalDNSfilter"
    android:theme="@style/Theme.phttpp.TitleBar" >
```