Universitat Oberta de Catalunya

uoc.edu

Estudio de dispositivos móviles, vulnerabilidades y auditoría de seguridad de aplicaciones móviles

David Gonzalez Morte

Máster en Seguridad de las Tecnologías de Información

Seguridad en la Internet de las cosas

Nombre Consultor/a: Jorge Chinea

Nombre Profesor/a responsable de la asignatura: Helena Rifà

Fecha Entrega: 04/06/2019

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

A todas las personas importantes en mi vida y a ti, por tu gran apoyo, sabes que sin ti no soy nada.

So say we all.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Estudio de dispositivos móviles, vulnerabilidades y auditoría de seguridad de aplicaciones móviles
Nombre del autor:	David Gonzalez Morte
Nombre del consultor/a:	Jorge Chinea
Nombre del PRA:	Helena Rifà
Fecha de entrega :	06/2019
Titulación::	Máster en Seguridad de las Tecnologías de Información
Área del Trabajo Final:	Seguridad en la Internet de las cosas
Idioma del trabajo:	Castellano
Palabras clave	Seguridad, Android, Auditoría, Santoku, Móvil

Resumen del Trabajo

En este trabajo se estudiarán las tecnologías móviles poniendo su foco de atención en la seguridad de las mismas. Se realizará un estudio del estado histórico y actual de los dispositivos móviles y en concreto se profundizará más detalladamente en aquellos con sistema operativo *Android*.

Se analizarán las vulnerabilidades, problemas de privacidad y los programas maliciosos que existen en la actualidad.

Estos conceptos se enfocarán teniendo en cuenta como el usuario interactúa con la tecnología móvil y con las posibles infecciones de malware. En relación a esto, se analizará como se realiza la divulgación informativa de la seguridad móvil y se realizará un estudio estadístico con las afirmaciones realizadas por una muestra de usuarios.

Finalmente, se realizará una auditoría de seguridad a una aplicación *Android* generando su correspondiente informe final. Esta gestión ayudará a comprender las entrañas de las aplicaciones móviles y la sensibilidad en seguridad móvil que puede tener una aplicación

Abstract

The current society lives within a large number of mobile devices. The information on the use and possible vulnerabilities that can have is an important issue. The knowledge of this concepts is too important and it's explained on this work.

The purpose of this document is to inform of the current situation of mobile technologies and the surrounding security. That is why a study has been carried out on a theoretical way and also on a practical way of new technologies and mobile applications. In addition, through a brief survey, statistics have been extracted to corroborate the use that users do of mobile technologies and the type of problems they observed.

It has been found and has been concluded that mobile applications can have malicious code but also applications with ethical purposes can also take advantage of vulnerabilities. An insufficient divulgation of this information approach on mobile security has also been observed, and it's vital to have make an adaptation to the users of this information.

Índice

1. Introducción

1.1 Contexto y justificación del Trabajo

Alzamos la vista desde nuestro asiento de un medio de transporte público habitual, y observamos las interacciones de la mayoría de pasajeros con su teléfono móvil. Andamos por la ciudad, la mayoría de los transeúntes se encuentran trasteando su celular, unos hablando, otros usando la geo-localización, enviando un mensaje mediante mensajería instantánea e incluso jugando a *Pokemon-GO*.

Día a día nos encontramos con ejemplos como los indicados, y es que, es innegable la fuerza de acogida que han tenido las tecnologías móviles en nuestra sociedad, y más aún en la telefonía móvil. Según datos estimativos de *gsmaintelligence*, ya son casi 9.000 millones de dispositivos móviles en activo, superando así, con creces, el volumen de la población mundial.

El uso de aplicaciones móviles ha sido determinante en éste crecimiento, ya que es mediante éstas, con las que se ha establecido éste vínculo de dependencia entre usuario y dispositivo. Y es que, hablando en cifras, según datos de *xatakamoviles*, el usuario medio tiene alrededor de 80 aplicaciones instaladas.

Es fácil observar el gran volumen de aplicaciones que hay en circulación alrededor del mundo. Pero hasta aquí, tan sólo se han facilitado datos de uso de ésta tecnología, ¿qué visión tenemos si seguimos incluyendo datos a los ya mencionados? Según datos de *RiskIQ* y *F-Secure*, anualmente aparece una media de 300 vulnerabilidades nuevas. Podemos decir que casi un 100% de los usuarios de dispositivos móviles, usan aplicaciones de mensajería instantánea, convirtiéndose así en objetivos potenciales de distribución de malware o *phishing*. *TrendMicro* informó que actualmente existen más de 2,1 millones de amenazas para dispositivos *Android*. Según *Kaspersky Lab*, en el primer semestre de 2018, se detectaron 1.300.578 paquetes de instalación maliciosos para dispositivos móviles, *18.000* de los cuales eran destinados a troyanos bancarios móviles. *Kapersky Lab*, neutralizó en ése período, intentos de lanzar uno o más programas maliciosos para robar dinero de cuentas bancarias en los equipos de 204.448 usuarios. La misma compañía, y en el mismo período, también neutralizó *8.787* paquetes de instalación de troyanos móviles extorsionistas.

Con éstos datos, y sabiendo que tipo de información suelen tener los usuarios de dispositivos móviles en los mismos, es muy preocupante el alto volumen de programas maliciosos existentes preparados para colarse en nuestra tecnología. Asimismo, es preocupante la poca información y falta de concienciación que tienen los usuarios sobre el correcto uso de los dispositivos móviles.

Recientemente, tuve una conversación con un amigo sobre la seguridad en dispositivos móviles. En ése momento, según mi opinión, gran parte de la responsabilidad recaía en el usuario, en el uso que hacia éste de las nuevas tecnologías, ya que, en mayor parte, los usuarios se preocupan de que algo funcione sin indagar más en cómo se usa correctamente y en los riesgos que existen. Evidentemente, en la afirmación anterior, cabe destacar que el culpable real de las infecciones de malware, virus etc. son los creadores de los mismos, pero, partiendo de la base que los programas maliciosos existen y no se puede evitar su existencia, el usuario tiene la responsabilidad del buen uso de aplicaciones y de la tecnología. Mi amigo afirmaba que el usuario no tiene ninguna culpa y es el sistema en sí el que desprotege al usuario. Es decir, el usuario adquiere un dispositivo móvil y ya sólo al adquirirlo, está desprotegido, no dispone de un manual claro de buenas prácticas de uso del dispositivo, descarga de aplicaciones, autorización de credenciales, configuración de privacidad y seguridad del dispositivo, navegación de internet, entre otros. Me indicaba que bajo mi punto de vista puede resultar más sencillo al entender mejor el mundo tecnológico, pero que el usuario en sí, se encuentra en que debe buscar por si mismo ésta información y en la mayoría de casos la información es muy técnica. Que el problema radica en que el usuario no puede perder mucho tiempo en adquirir ésta información ya que seguramente no es su

target ni a nivel académico ni a nivel laboral, muy distinto de mi punto de vista que si es mi target tanto a nivel académico como a nivel laboral.

Tras ésta conversación llegué a la conclusión, que es cierto, el usuario no dispone de facilidades que le lleven a entender completamente los riesgos que existen, de lo que puede realizar una aplicación móvil sin que ello le conlleve leer tecnicismos especializados. En 2019, se puede observar que si se están llevando campañas de divulgación y herramientas que hacen que el usuario ponga password robustos y sea consciente de su importancia, aún así, los password más usados siguen siendo 123456 o Password. También existen muchas campañas que informan sobre como analizar si un correo es un intento de phishing o un intento de inyectar malware. Pero aún así, es insuficiente.

Éste trabajo, basándonos en primer lugar del planteamiento indicado propio del TFM y mis puntualizaciones, se basará en explicar:

- Estudio acerca de los diferentes problemas a los que se encuentran los Smartphones y tablets actuales.
- Análisis de las vulnerabilidades que más impacto han tenido sobre los sistemas basados en Android y las implicaciones que tiene la alta fragmentación de este sistema operativo
- Extrapolación de los puntos anteriores a nivel de usuario.
- Análisis forense a una APK y/o a una imagen de un dispositivo Android.

1.2 Objetivos

Basándonos en primer lugar del planteamiento indicado propio del TFM y mis puntualizaciones, se seguirán los siguientes objetivos:

- Estudio acerca de los problemas a los que se encuentran los smartphones y tablets actuales, generalizando en los tres sistemas operativos más usados, *Android*, *IOs* y *Windows Phone*.

    - Se realizará un informe detallado acerca de la problemática a la que se someten los smartphones/tablets hoy en día.

- Estudio sobre las fuentes de divulgación y tipo de información que reciben los usuarios sobre los problemas indicados anteriormente.

- Análisis de vulnerabilidades en sistemas *Android*.

    - Se elaborará un documento de análisis general sobre el que se recogerán las vulnerabilidades más problemáticas y con más impacto sobre dispositivos *iOS* y *Android* así como las referencias a las mismas y la posible mitigación.

    - Se ampliará la información sobre los sistemas *Android*.

- Estudio sobre las fuentes de información para el usuario sobre las vulnerabilidades. ¿Cómo se puede mejorar ésta divulgación?

- Análisis forense de una APK.

    - Se implementará una metodología para realizar una auditoría de seguridad sobre una aplicación Android y se elaborará un informe de reporte.

En global los objetivos del TFM se basan en el estudio de las vulnerabilidades de los dispositivos, los problemas que pueden tener y como afectan éstos a los usuarios, además de ver como reciben ésta información y como se puede mejorar ésta comunicación, para que, éstos sean consecuentes con las acciones que realizan. Se realizará a efectos prácticos un análisis forense de un *apk* para ejemplificar lo analizado a nivel teórico.

1.3 Descripción de la metodología

Podemos observar que el TFM se divide en dos partes muy diferenciadas, una parte teórica y otra parte práctica. Teniendo en cuenta ésta premisa, se realizarán dos metodologías.

Parte Teórica

Por un lado se realizará una búsqueda de información vía internet, biblioteca, recursos universitarios y fuentes públicas de información.

Como se quiere realizar una extrapolación de los conceptos con los conocimientos de los usuarios, la intención inicial es formalizar una encuesta de conocimientos con la herramienta de encuestas que facilita *Google*.

A partir de los datos recogidos, se realizaran los respectivos análisis, informes y redactados para plasmar la información que se ha localizado.

Parte Práctica

Se preparará un entorno de análisis forense a través de una imagen con un entorno virtual tipo *VirtualBox*, y se analizará un *apk*. A priori, el *.apk* a analizar, es una aplicación realizada en el trabajo de fin de carrera, una aplicación de geolocalización.

Finalizados los análisis se prepararan los respectivos informes, conclusiones y mejoras.

Estos dos puntos se dividirán en un listado de tareas que se menciona en los siguientes puntos, al igual que, una planificación temporal de los mismos puntos. Para llevar a cabo con éxito la planificación, se gestionará a través de un gestor de tareas online, Trello.

1.4 Planificación

Se seguirá el siguiente listado de tareas. Se ampliará la información en la planificación temporal:

id	Nombre de Actividad
3	Búsqueda de información sobre problemas de dispositivos móviles, vulnerabilidades, herramientas y protocolos forenses.
4	Unión de información y esquema sobre el orden argumental
5	Redactado sobre los temas indicados, opiniones personales y breves conclusiones

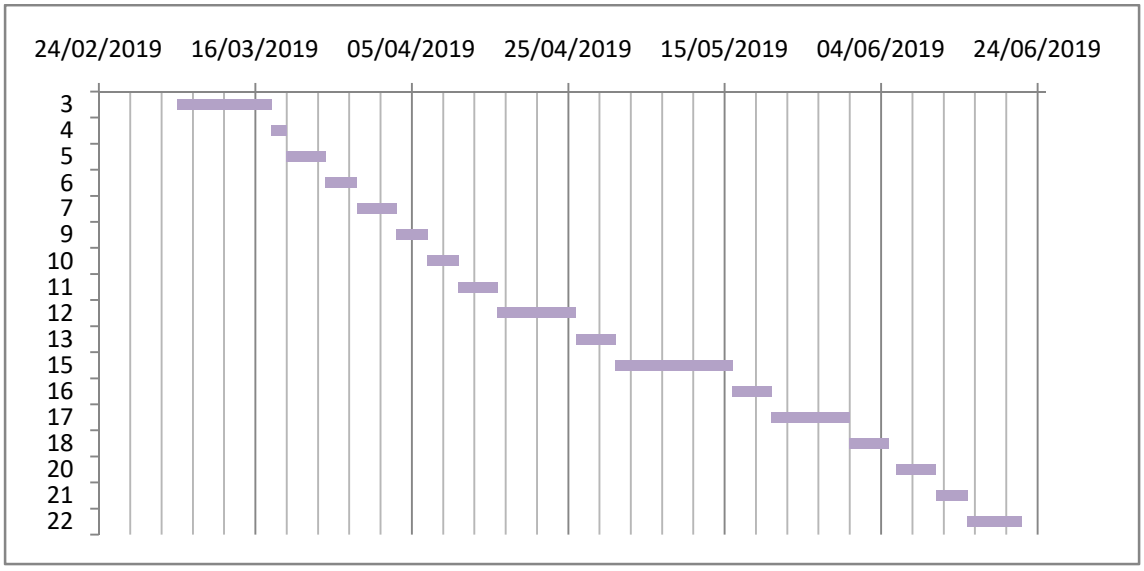
6	Preparación de informes detallados de problemas con dispositivos móviles y vulnerabilidades
7	1ª Fase de Corrección de errores
9	Búsqueda de información sobre como reciben la información los usuarios sobre los temas indicados anteriormente.
10	Redactado sobre los temas recogidos en punto 9, opiniones personales y breves conclusiones
11	Preparación entorno forense
12	Análisis forense apk
13	2ª Fase de Corrección de errores
15	Finalización de atrasos, finalización pruebas forenses. Ampliación pruebas forenses
16	Conclusiones del TFM y mejoras sobre la información que reciben los usuarios
17	Redactado entrega final
18	3ª Fase de Corrección de errores
20	Preparación guión
21	Grabación
22	Editar vídeo

Planificaciones de tareas

Se seguirá la siguiente planificación de tareas:

id	Nombre de Entrega	Nombre de Actividad	Fecha Inicio	Fecha Fin	Días	Comentarios
1	Entrega 1		25/02/2019	05/03/2019	9	
2	Entrega 2		06/03/2019	02/04/2019	28	
3		Búsqueda de información sobre problemas de dispositivos móviles, vulnerabilidades, herramientas y protocolos forenses.	06/03/2019	17/03/2019	12	
4		Unión de información y esquema sobre el orden argumental	18/03/2019	19/03/2019	2	
5		Redactado sobre los temas a indicados, opiniones personales y breves conclusiones	20/03/2019	24/03/2019	5	
6		Preparación de informes detallados de problemas con dispositivos móviles y vulnerabilidades	25/03/2019	28/03/2019	4	
7		1ª Fase de Corrección de errores	29/03/2019	02/04/2019	5	En caso que, no se llegue a las metas indicadas, ésta fase quedará reducida y se realizaría con más profundidad en la fase de la entrega final
8	Entrega 3		03/04/2019	30/04/2019	28	

9		Búsqueda de información sobre como reciben la información los usuarios sobre los temas indicados en la Entrega 2	03/04/2019	06/04/2019	4	Se estiman pocos días, ya que gran parte de ésta gestión se habrá realizado también durante la recogida de información del punto 3
10		Redactado sobre los temas recogidos en punto 9, opiniones personales y breves conclusiones	07/04/2019	10/04/2019	4	
11		Preparación entorno forense	11/04/2019	15/04/2019	5	A medida que se prepara el entorno con la información recogida en punto 3, se redactará un protocolo de preparación de entorno de laboratorio.
12		Análisis forense apk	16/04/2019	25/04/2019	10	Durante el análisis y recogida de pruebas o muestras, se irá redactando el informe forense.
13		2ª Fase de Corrección de errores	26/04/2019	30/04/2019	5	En caso que, no se llegue a las metas indicadas, ésta fase quedará reducida y se realizaría con más profundidad en la fase de la entrega final
14	Entrega final		01/05/2019	04/06/2019	35	
15		Finalización atrasos, finalización pruebas forenses. Ampliación pruebas forenses	01/05/2019	15/05/2019	15	En caso que queden pendientes tareas de fases anteriores, se dedicará éste espacio a la finalización de las mismas. En caso que no haya tareas pendientes, se mirará de mejorar las tareas realizadas y ampliar los periodos de las siguientes fases
16		Conclusiones del TFM y mejoras sobre la información que reciben los usuarios	16/05/2019	20/05/2019	5	
17		Redactado entrega final	21/05/2019	30/05/2019	10	
18		3ª Fase de Corrección de errores	31/05/2019	04/06/2019	5	
19	Entrega video		05/06/2019	21/06/2019	17	
20		Preparación guión	06/06/2019	10/06/2019	5	
21		Grabación	11/06/2019	14/06/2019	4	
22		Editar vídeo	15/06/2019	21/06/2019	7	



1.5 Sumario de productos obtenidos

Se obtendrá un análisis en profundidad sobre las tecnologías móviles así como de sus sistemas operativos, en concreto sobre *Android*.

Se obtendrá un análisis de la situación actual con la seguridad de las tecnologías móviles.

Se obtendrán estadísticas y análisis sobre la divulgación de la seguridad en las TIC.

Se obtendrá un informe de auditoría de seguridad sobre una aplicación *Android*, tras su correspondiente análisis.

1.6 Descripción de los otros capítulos de la memoria

1. Introducción tecnologías móviles

En este punto se introducirá el estado actual de las tecnologías móviles, adentrándonos al uso que se realiza de las mismas, su historia y evolución entre otros conceptos.

2. Sistemas Operativos

Se introducirán en el vertiente de los sistemas operativos para tecnologías móviles, en concreto smartphones y profundizando en *Android*.

3. Smartphones, problemas generales y seguridad

Se trataran temas sobre problemas con smartphones, seguridad, vulnerabilidades y privacidad.

4. Fuentes de divulgación

Se analizarán las fuentes de divulgación y se realizará una breve encuesta sobre el esta temática.

5. Análisis forense de una APK. (Aplicación Android)

Se realizará un análisis de una aplicación Android, redactando el correspondiente informe.

2. Las tecnologías móviles

Los dispositivos móviles son unos aparatos electrónicos que permiten realizar interacciones más allá de las llamadas; permiten, por ejemplo, hacer fotografías, comunicarse por mensajes, jugar, leer o incluso diseñar. La potencia de estos dispositivos es equivalente a la de un ordenador de sobremesa o portátil, teniendo su propio sistema operativo integrado, el cual ha evolucionado de forma notable en los últimos treinta años.

2.1 Breve repaso histórico

El primer teléfono inteligente conocido, fue el *IBM Simon*, que se empezó a comercializar en el año 1994 a un precio de 900 dólares. Éste combinaba los usos de una *PDA*, (la cual fue bastante popular en la década de los ochenta) dentro de un teléfono móvil. Así pues, se añadieron características propias de los asistentes de agenda personal, como un calendario, una calculadora, correo electrónico y conexión a internet, entre otros. Éste incluía también una pantalla táctil y un teclado *QWERTY* que permitía que el usuario pudiera escribir y usar un texto predictivo.

Pero el primer dispositivo que empezó a comercializarse como *smartphone* fue el *Ericsson R380* que se puso a la venta en el año 2000. En su momento fue descrito como el más pequeño y ligero de la historia y éste permitía el uso de una interfaz de usuario bastante innovadora. Usó el mismo sistema operativo que las *PDA*, el cual, finalmente, evolucionó hasta convertirse en *Symbian OS*, que fue muy popular y usado por la mayoría de marcas de teléfonos móviles que surgieron entonces, tales como *Nokia*, *Siemens* o *Motorola*, entre otras. El sistema operativo *Symbian OS* fue el más utilizado hasta el año 2007, con la entrada de *Apple* en el mercado, con los *iphone* y su propio sistema operativo *IOS*.

2.2 Evolución del uso y de la tecnología móvil

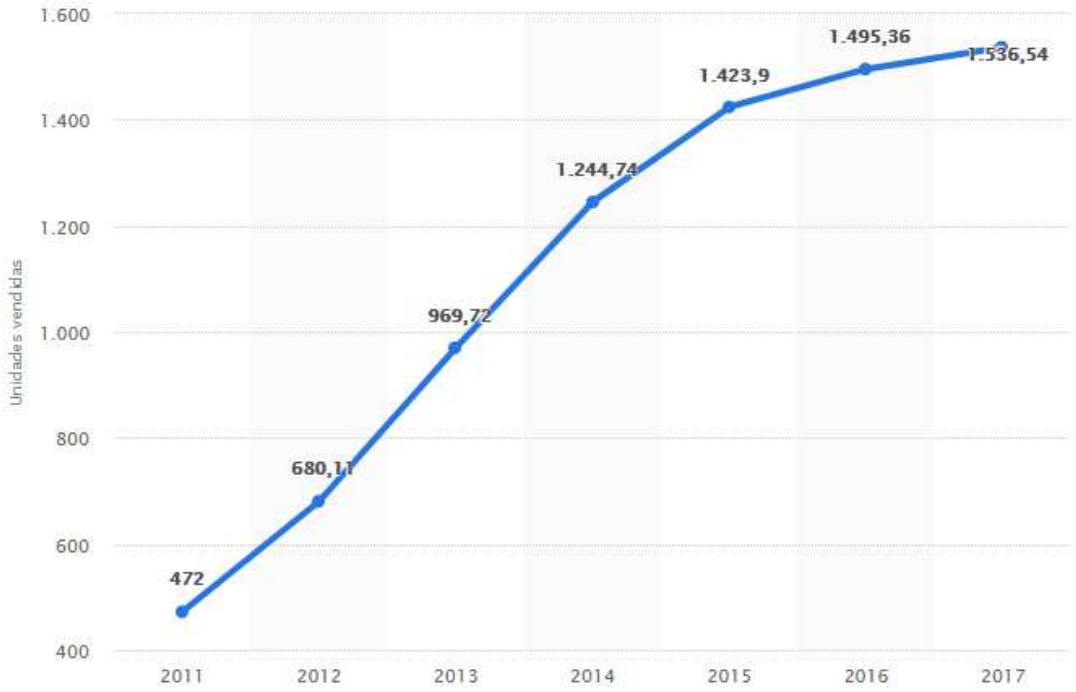
Si hay algo que está claro, es que el uso de la tecnología móvil ha cambiado el paradigma del mundo y ha evolucionado en todos los aspectos. El salto ha sido abismal. El usuario tiene en sus manos un dispositivo con la misma potencia que un ordenador, capaz de hacer lo mismo que una cámara y una videoconsola, relegando y menguando las ventas de algunos dispositivos que se encontraban en auge. Los dispositivos han cambiado costumbres, formas de comportamiento, la forma de interactuar unos con otros. El hecho de que los teléfonos hayan mejorado notablemente en los aspectos más prácticos, hace que, intrínsecamente, haya cambiado el comportamiento del usuario. En este punto, se analizarán ambos aspectos, por una parte, desde el punto de vista sociocultural, de cómo el usuario ha cambiado su forma de ver el mundo, creando nuevas necesidades, y la forma de comportarse. Por otro lado, se hablará del aspecto más tecnológico, de como los smartphones mejoran cada día, en algunos aspectos destacables, como por ejemplo, la durabilidad de la batería o la memoria interna. Ambos temas están unidos, siendo retroalimentados por el otro.

2.3 Desde el punto de vista sociocultural

Se utiliza el término sociocultural para hacer referencia a cualquier proceso o fenómeno, o cambio en el comportamiento de una sociedad o grupo social. Aquí se hablará sobre aspectos como el comportamiento o la forma de ver el mundo del usuario. Es un aspecto importante a tener en cuenta, cuanto más acceso se tenga, más puertas se abren para peligros y vulnerabilidades.

Entre el año 2011 y 2017, y según la fuente Statista, se vendieron en todo el mundo 7822,37 millones de teléfonos inteligentes. El auge fue tal, que en el 2014 se superó por primera vez la friolera cifra de mil

millones de smartphones vendidos. Estas cifras han estado creciendo desde entonces, haciendo que en el 2017 se vendieran 1500 millones de unidades.



Estos datos son muy significativos y muestran que forman parte de la sociedad, que millones de personas no conciben una vida sin este aparato. Se ha vuelto algo de primera necesidad. El día al día del individuo comienza y termina con un smartphone. Y aunque en un principio, el uso principal al que estaba destinado el teléfono móvil eran las llamadas, parece que lo último que se haga sea eso. Los smartphones se han convertido en las agendas de los usuarios, sus cámaras, incluso una herramienta más de trabajo; esto hace que las aplicaciones hayan tenido un auge abismal. «Hay una aplicación para todo» dicen los expertos. «Y si no la hay, acabará existiendo».

Millones de datos privados recorren las líneas de la red, sin descanso, a todas horas y en todo el mundo. Sabiendo esto, no es difícil deducir que, cuanto mayor sean las cifras, el número de ataques crecerá al unísono. Y lejos de la realidad, aquellos usuarios que creen que no hay peligro en las aplicaciones, estas son las más dañinas, no sólo aquellas que son descargadas en el exterior, sino las que podemos encontrar dentro las tiendas de apps oficiales.

¿Hasta qué punto el usuario es consciente de ello? ¿Se trata de ignorancia y falta de información o simplemente es porque se niega a ver la realidad?

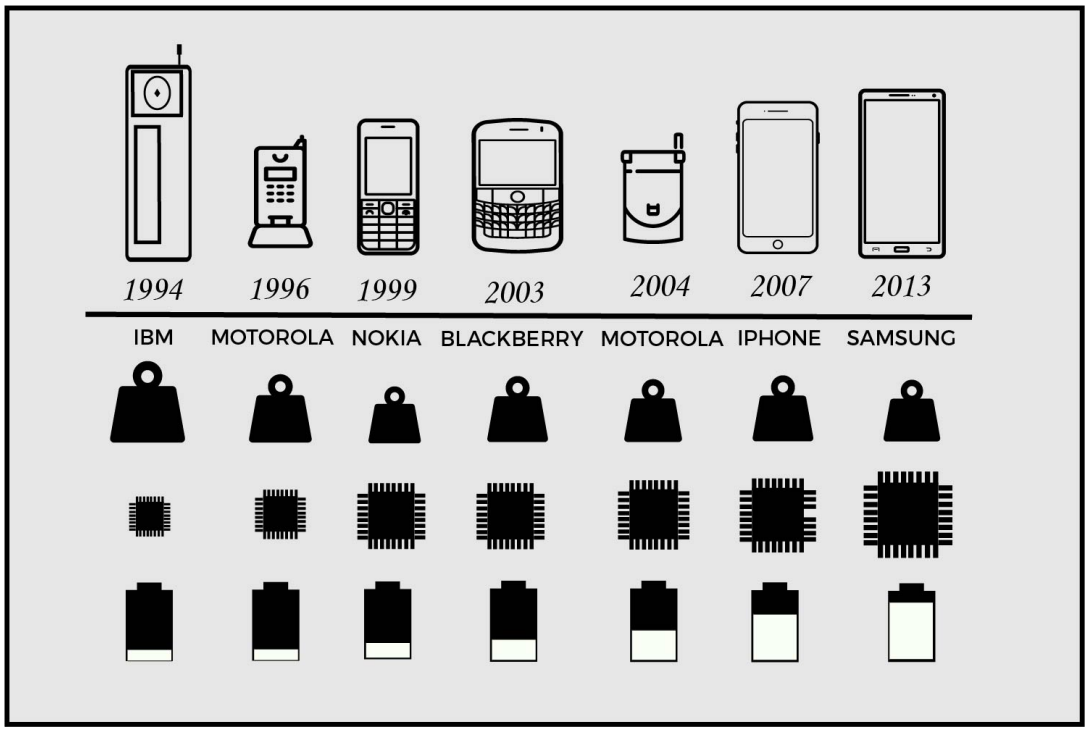
2.4 ¿Qué más ha cambiado?

De la misma manera que el ordenador simplificó la vida del usuario, mediante la digitalización del día a día, los smartphones también se han convertido en el sustituto de muchos *gadgets*. Podemos hablar de las cámaras digitales que obtuvieron su auge entre 2003 y 2008, que perdieron fuelle a raíz de la incorporación y mejora de las cámaras en los dispositivos. También de los reproductores de música o de las agendas electrónicas. No es necesario disponer de nada de esto, ya que el usuario puede disfrutar de

ellos en un sólo aparato. En cierta manera, incluso se ha relegado a segundo plano el ordenador, no siendo tan indispensable como lo fue en el pasado, en especial fuera del ámbito profesional.

2.5 Evolución de la tecnología móvil

¿Qué es lo que más valora el usuario en un dispositivo móvil? Teniendo en cuenta lo dicho anteriormente, que se trata de algo indispensable para el usuario de a pie, sin ninguna duda hablaríamos del uso de la batería, siendo un reclamo publicitario de las principales marcas de smartphone, la mejora de la memoria y nuevos gadgets que tratan de mejorar la seguridad del usuario, como apps de reconocimiento facial o las huellas dactilares, algo que no es realmente novedoso si tenemos en cuenta que esto ya se aplica para ordenadores. Pero, ¿hasta qué punto las empresas se preocupan por el bienestar del usuario más allá de que adquieran estos dispositivos? Otros elementos con los que juegan las empresas tecnológicas son el peso y el tamaño de los smartphones. En la siguiente infografía se puede ver se forma más clara, cómo las necesidades de los usuarios han modificado los diseños y han hecho que las prioridades en la creación y su mejora hayan cambiado de tercio.



2.6 Futuro Predictivo uso tecnología móvil.

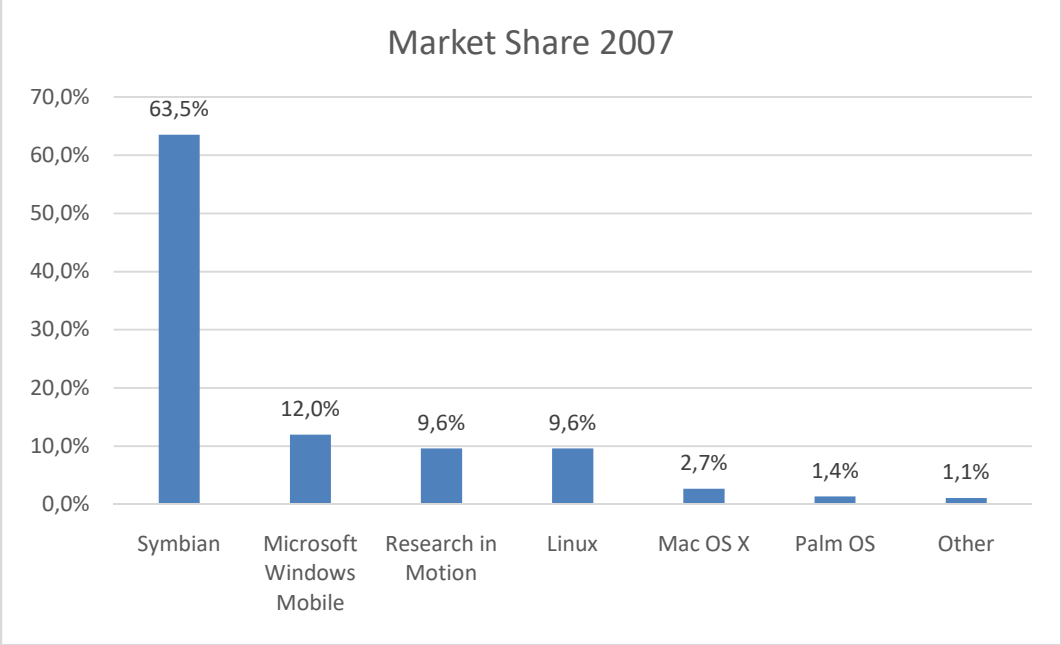
Si hay algo que está claro, es que los smartphones han venido para quedarse. Los usuarios no conciben una vida sin ellos, y su frecuencia de uso es cada vez mayor. Sabiendo esto, es importante que tanto las empresas, como los usuarios sean conscientes del peligro constante al que están expuestos. El teléfono se usa para todo, incluso para pagar las compras, tanto físicas como online; y estos datos tan sensibles, cuya exposición puede vulnerar los derechos básicos de los usuarios, deben protegerse al mismo compás que su crecimiento.

3. Sistemas Operativos.

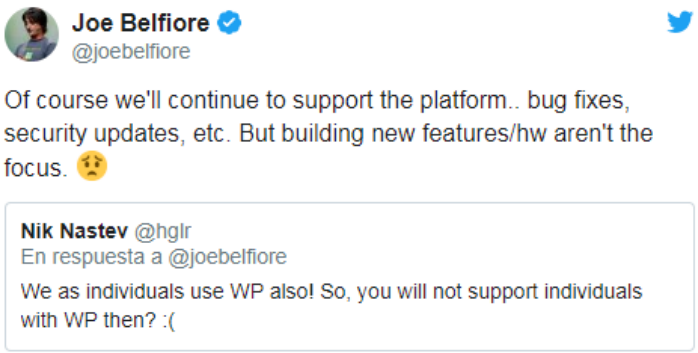
Hablando a nivel de consumo de usuario, desde que los dispositivos móviles se hicieron eco en el mercado, varios sistemas operativos lo han dominado en diversas épocas del *time-line Mobile*.

Y es que en el mercado *Mobile*, desde sus inicios hasta la actualidad, han aparecido varios sistemas operativos tales como *Symbian*, el primer sistema operativo puntero, *Android*, *iOs*, *Firefox OS*, *Ubuntu touch* o *BlackBerry*.

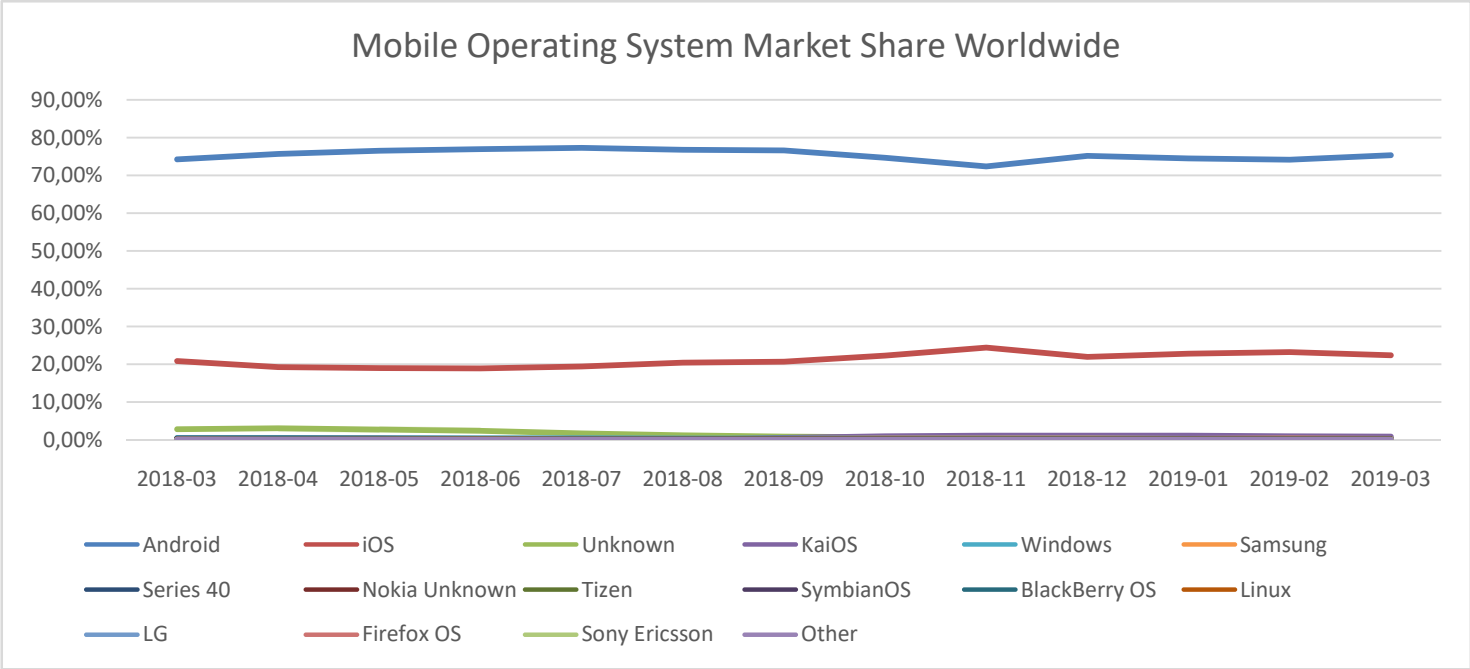
2007 fue el año de presentación del primer *iPhone*, que ejecutaba una versión reducida del conocido MAC OS X, y que evolucionaría a *iOS*. El mismo año, se anunció la primera versión de *Android*, el *Android 1.0 Apple Pie*. Ésta fecha es importante ya que marcaría un antes y un después en el mercado *Mobile*. Hasta el 2007, el mercado era dominado por dispositivos *Android*, según la fuente de datos estadística *Stadista*, el 63,5% del mercado era *Symbian*.



A partir del 2007, y con la aparición de *iOS* y *Android*, el mercado se ha balanceado entre ambos, siempre decantándose el mercado hacia *Android*. Y es que en los últimos años, tres sistemas operativos han sido los protagonistas, los dos mencionados y *Windows*. Éste último, por eso, ha sucumbido a la omnipresencia de *Android* e *iOS*, y según las últimas informaciones, *Windows* dejará el mercado *Mobile* entre 2018 y 2019, una información que confirmó Joe Belfiore, uno de los máximos responsables del desarrollo de *Windows 10*, dónde indicaba a través de *Twitter* que seguirían dando soporte a actualizaciones de *Windows 10* pero que no desarrollarían nuevas funcionalidades.



Viendo los datos de mercado del último año (entre marzo del 2018 y marzo del 2019), según la fuente de datos Statcounter, podemos ver ésta abrumadora dominación de mercado dónde prevalece por encima del resto el Sistema Operativo *Android*.



Tanto en éste punto, como en el resto del presente documento, se centrará en el estudio de las diversas casuísticas de los dos sistemas operativos más presentes: *Android* y *iOS*.

3.1 Android

Inicios

Para viajar a los orígenes del sistema operativo objeto de éste punto, debemos remontarnos a la fecha de fundación de *Android Inc.* en 2003 con el objeto de desarrollar un nuevo sistema operativo que, en primera instancia, estaba enfocado a las cámaras digitales, pero que por conclusiones de poca viabilidad en el mercado de ese año, su objetivo de desarrollo se decantó hacia la telefonía móvil.

En el año 2005, *Google* realizó la compra de *Android Inc*. catapultando así el desarrollo del sistema operativo con base *Linux*.

En el año 2007, coincidiendo con la fundación de *Open Handset Alliance* (alianza donde formaban parte empresas de los sectores de fabricación de terminales móviles, operadores de telecomunicaciones, fabricantes de chips y desarrolladores de software), se anunció la primera versión de *Android*, el llamado *Android Apple Pie* o *Android 1.0*. Pero no fue hasta el 2008 que apareció el primer terminal móvil con *Android,* el *HTC Dream*.

*Imagen con licencia de wikipedia

Versiones Destacadas

· Android 1.0

Se trata de la primera versión pública de *Android*, la 1.0, lanzada el 23 de septiembre del 2008, sin tener una gran interfaz gráfica cumplió positivamente con las características propias de un smartphone.

Características Destacables

- *Android Market*: Fue la primera aplicación de tienda de aplicaciones para *Android*, que disponía en ese momento de muy pocas aplicaciones.

- Aplicaciones básicas: El sistema operativo disponía de aplicaciones básicas tales como navegador web, calculadora, Ajustes, Galería de Imágenes, Reproductor Multimedia, Alarma o Reloj.

- Integración entorno *Google*: Se realizó la integración de los servicios de *Google* como *Gmail, Google Calendar, Google Contacts, Google Search, Google Talk y Google Maps.*

- Notificaciones y *Widgets*: En la misma barra de estado aparecían las notificaciones pudiendo configurar las mismas con diversas casuísticas. Los *widgets* se mostraban en la pantalla de inicio y se disponía de gran variedad.

- *Youtube*: Inclusión del aplicativo reproductor de vídeo de la plataforma *Youtube*.

· Android CupCake

Versión 1.5 con lanzamiento el 27 de abril del 2009. Ésta versión inició la tradición de nombrar los distintos sistemas operativos *Android* como nombres de dulces ordenados alfabéticamente. Con *CupCake* se empezó a pulir el detalle de la interfaz gráfica haciéndola más atractiva.

Características Destacables

- Teclado Virtual: Hasta la fecha no se disponía de teclado virtual *QWERTY* y con la aparición de éste sistema operativo se mostró por primera vez dicho teclado, coincidiendo además, con la salida del *HTC Magic*, el primer *Android* con pantalla táctil y sin teclado físico.

- *Widgets*: Se mejoró la experiencia de los *widgets* ofreciendo vistas de miniaturas de aplicaciones y la inclusión de *widgets* desarrollados por terceros con la inclusión del *SDK*.

- Otros: Se realizaron otros cambios menores que ofrecieron una mejor experiencia al usuario como permisos para subir vídeos a las plataformas de *Youtube* y *Picassa* o la inclusión de pegado del portapapeles al navegador web.

·Android Donut

Versión 1.6 con lanzamiento 15 de septiembre del 2009. Éste lanzamiento coincidió con la aparición de múltiples tipos de dispositivos con distintas resoluciones de pantalla y diversos tamaños, como consecuencia, el sistema operativo se adaptó para poder disfrutar de las múltiples resoluciones tales como *QVGA, HVGA, WVGA, FWVGA, QHD o 720p*.

Características Destacables

-Conectividad: Se incluye soporte para *CDMA* y *VPN*.

-Sintetizador de voz.

-Se incluye nueva herramienta de desarrollo *GestureBuilder*.

· Android Eclair

Versión 2.0 con lanzamiento el 26 de octubre del 2009 donde gran parte de las actualizaciones fueron de mejoras y la novedad más destacada fue la inclusión de multicuentas.

· Android Froyo

Versión 2.2 con lanzamiento 20 de mayo del 2010 que destacó por las grandes mejoras en velocidad y rendimiento.

Características Destacables

- Mejora de navegador web con la inclusión del motor V8 de *JavaScript*.

- Creación de puntos de acceso *WIFI*.

- Soporte comandos de voz.

- Soporte para el servicio *Android Cloud to Device Messaging* habilitando las notificaciones *push*.

- Se agrega la opción de mover aplicaciones a tarjeta SD.

· Android Gingerbread

Versión 2.3 con lanzamiento 06 de diciembre del 2010 que tuvo la curiosidad de la inclusión de huevos de Pascua.

Características Destacables

- Se introduce *API* para juegos.

- *Soporte Near Field Communication (NFC).*

- Soporte nativo para sensores.

- Soporte nativo para *SIP* y *VoIP*.

·Android HoneyComb

Versión 3.0 con lanzamiento 22 de febrero del 2011 que destacó por ser una versión exclusiva para tablets y TV, que se basó en actualizaciones de mejoras enfocadas a su exclusividad.

·A**ndroid Ice Cream Sandwich**

Versión 4.0 con lanzamiento 12 de octubre del 2011 donde se incluyeron muchas novedades.

Características Destacables

- *WI-FI Direct*.

- Grabación 1080.

- Se incluye *Face Unlock* o desbloqueo facial, aumentando así la seguridad del dispositivo.

- Aparición *Android Beam*.

·**Android Jelly Bean**

Versión 4.1 con lanzamiento 30 de junio del 2012 que se centró en mejoras de la interfaz y de la experiencia del usuario.

· **Android KitKat**

Versión 4.4 con lanzamiento 31 de octubre del 2013 que destacó ser una de las versiones más usadas.

Características Destacables:

-Se incluye la maquina virtual *ART, Android RunTime* reemplazando así a *Dalvik*.

- En su versión 4.4.4, eliminaron la vulnerabilidad de *OpenSSl, man-in-the-middle*. (CVE-2014-0224)

·**Android Lollipop**

Versión 5.0 con lanzamiento 03 de noviembre del 2014 que destacó por la aparición del *Material Design* dando un renovación al aspecto general del SO. A destacar que en su versión 5.1 se incluyó la protección antirrobo.

· **Android Marshmallow**

Versión 6.0 con lanzamiento 05 de octubre del 2015

Características Destacables

- Soporte para huellas dactilares.

- Se incluye *Android Pay*.

- Llegada de *Direct Share* y *Now On Tap*.

- Soporte a *USB-C, 4K* y multiventana.

· **Android Nougat**

Versión 7.0 con lanzamiento 22 de agosto del 2016, donde la mayoría de novedades son de mejoras. A destacar la inclusión de *Java 8*.

· **Android Oreo**

Versión 8.0 con lanzamiento 21 de agosto del 2017 donde se intenta mejorar la seguridad con la creación de proyecto *Treble*, con la intención de frenar la fragmentación y la inclusión de *Google Play Protect*.

·**Android Pie**

Versión 9.0 con lanzamiento 6 de agosto del 2018 que es el sistema más actual y se encuentra en fase de distribución. Incluye mejoras de rendimiento y de experiencia de usuario.

4. Smartphones, problemas generales y seguridad

Como cualquier aparato electrónico, los smartphones pueden presentar incidencias que impidan el correcto funcionamiento del dispositivo. Éstos problemas pueden presentarse desde multitud de vertientes, desde las ya conocidas incidencias tales como defecto de fábrica, paso del tiempo, deterioro de componentes o bien mal uso del dispositivo, hasta problemas a nivel informático o digitales tales cómo vulnerabilidades o *malware*.

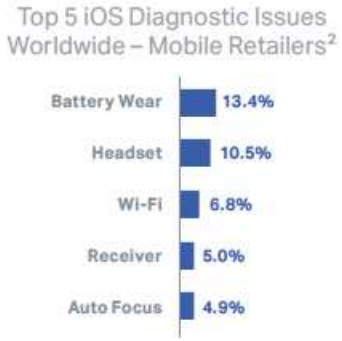
Cabe destacar que, los smartphones, no sólo pueden tener malfuncionamiento en sí del dispositivo, sino también pueden derivar a problemas para el usuario, a nivel de salud y psicológico, tales como, síndrome del túnel Carpiano, daños auditivos, problemas en el sistema nervioso, enfermedades oculares o bien adicción.

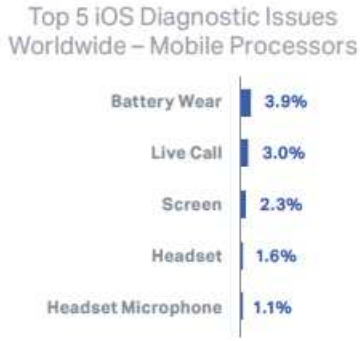
En éste punto, nos centraremos en los problemas en sí de la tecnología móvil.

4.1 Problemas generales

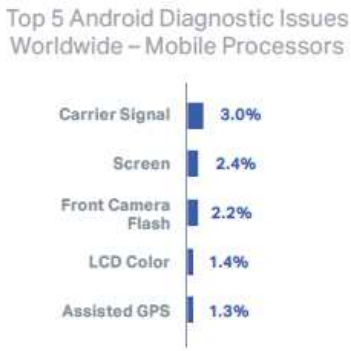
Basándonos en los estudios realizados por la empresa Blancco, empresa especializada en borrado de datos y reutilización de dispositivos, se muestran los principales problemas localizados en dispositivos móviles. Cabe destacar que, las estadísticas mostradas a continuación son realizadas en base a los dispositivos trasladados a ésta compañía y durante el último tercio del 2018.

En cuanto a dispositivo con sistema operativo *iOS*, nos encontramos que los problemas destacados son la duración de la batería y los auriculares.





Si centramos la visión en dispositivos *Android*, observamos que destacan los problemas de la cámara y lo problemas con la tarjeta *SIM* dual, éste último problema destaca por su reciente salida en mercado.



Con los datos facilitados podemos observar que uno de los principales problemas que tienen los usuarios con los dispositivos móviles es la batería. Y es que la duración de la batería ha sido un rompecabezas para todos los fabricantes aparte de dar continuos problemas a los usuarios.

Éste problema se encuentra tan presente, que ha aumentado la venta y fabricación de baterías portátiles, cuyo principal objetivo es alimentar de energía en cualquier momento o lugar un dispositivo móvil y así paliar las deficiencias de las mismas.

La duración media, de vida útil, de una batería suele estar en torno a los tres años, varias variables como su uso o su mantenimiento pueden afectar a la vida de la misma. El calor, las cargas rápidas o las cargas continuas son casuísticas de dicho deterioro.

Cabe destacar, que no sólo las incidencias con las baterías afectan en la experiencia del usuario con la tecnología móvil sino que, ya desde un inicio, la duración de la misma es insuficiente, contando que, según datos de la página web mundial de estadísticas, Statista, en 2017 el promedio de uso del teléfono móvil era de 2 horas y 11 minutos, teniendo en cuenta una tendencia ascendente en el uso del mismo, y comparando con datos de duración de baterías de la misma fuente estadística, podemos observar que según mercado de febrero del 2019, el *Motorola Moto g7 Power*, tiene una duración de 20h, y la mayoría de los dispositivos suelen tener una duración de entre las 12-15h de duración (hablando siempre de pleno uso del mismo).

Otros de los problemas destacados son la pantalla y los auriculares. En el primer caso, la fragilidad de los teléfonos móviles provoca múltiples incidencias con roturas o grietas en la pantalla, situación que se agrava cuando el dispositivo también tiene cristal en la parte trasera. El segundo caso trata más sobre la conexión entre auriculares y smartphone, una pieza que suele fallar con asiduidad.

4.1.1 Fragmentación Android

La fragmentación en los dispositivos móviles se basa en el hecho que, hay muchos dispositivos en funcionamiento que disponen de dispares versiones de un mismo sistema operativo, es decir, diferentes versiones de un sistema operativo.

En el caso de *iOS*, el problema no es del todo relevante ya que no tienen tantos dispositivos distintos en el mercado, no tienen varias marcas que ofrezcan el mismo sistema operativo y esto provoca que *Apple* tenga un buen control sobre sus dispositivos.

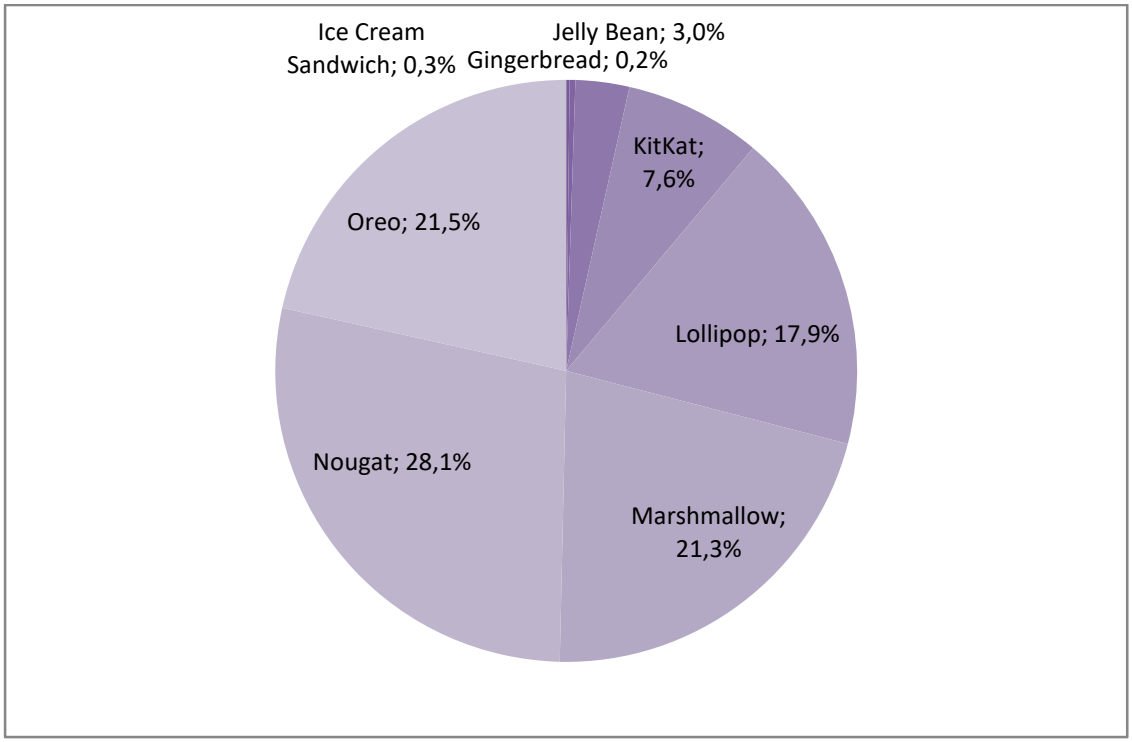
En Android, el problema es grave dado el elevado número de marcas que ofrecen dispositivos con éste sistema operativo. Hasta la fecha han salido 16 versiones distintas de éste sistema operativo desde 2008 con la salida de la versión *Android 1.0* o *Apple Pie*.

Y es que las grandes marcas fabricantes de dispositivos móviles se comprometen a actualizar las versiones de los sistemas operativos durante dos años desde la salida al mercado del dispositivo, el mínimo exigible por parte de *Google* hasta la fecha. Ejemplificando en una marca en concreta, en el caso de *Samsung*, ésta publica en su página web que dispositivos se actualizan a la última versión, aquellos que no aparecen en el listado no dispondrán de actualización. Así que, para la última versión, la llamada *Android Pie*, que tuvo como fecha de lanzamiento el 6 de agosto de 2018, empezó a actualizarse en sus dispositivos en Enero del 2019, empezando por sus recientes modelos, *Samsung S9*. Observamos que la actualización empieza cinco meses más tarde de la fecha de lanzamiento y finalizará en agosto del 2019, un año más tarde, para los últimos dispositivos actualizables, aparatos del 2017.

Se pueden observar las distintas versiones de *Android*, su fecha de lanzamiento y su distribución en el mercado. Los datos de distribución de versiones en el mercado son aportados por *Google*, aunque

desde octubre de 2018, se encuentran éstos datos paralizados a causa de la activa distribución *Android Pie* y la preparación de otra nueva versión *Android Q*, prevista para agosto del 2019.

Nombre código	Número de versión	Fecha de lanzamiento	Nivel de API	Distribución
Apple Pie	1.0	23 de septiembre de 2008	1	
Banana Bread	1.1	9 de febrero de 2009	2	
Cupcake	1.5	25 de abril de 2009	3	
Donut	1.6	15 de septiembre de 2009	4	
Eclair	2.0 – 2.1	26 de octubre de 2009	5 – 7	
Froyo	2.2 – 2.2.3	20 de mayo de 2010	8	
Gingerbread	2.3 – 2.3.7	6 de diciembre de 2010	9 – 10	0,2%
Honeycomb	3.0 – 3.2.6	22 de febrero de 2011	11 – 13	
Ice Cream Sandwich	4.0 – 4.0.5	18 de octubre de 2011	14 – 15	0,3%
Jelly Bean	4.1 – 4.3.1	9 de julio de 2012	16 – 18	3,0%
KitKat	4.4 – 4.4.4	31 de octubre de 2013	19 – 20	7,6%
Lollipop	5.0 – 5.1.1	12 de noviembre de 2014	21 – 22	17,9%
Marshmallow	6.0 – 6.0.1	5 de octubre de 2015	23	21,3%
Nougat	7.0 – 7.1.2	15 de junio de 2016	24 – 25	28,1%
Oreo	8.0 – 8.1	21 de agosto de 2017	26 – 27	21,5%
Pie	9.0	6 de agosto de 2018	28	
Q	10.0	Agosto del 2019	29	



Podemos observar que las estadísticas de usuarios según la versión *Android* se encuentra muy repartida centrándose en un 80% en las versiones de *Lollipop, Marshmallow, Nougat* y *Oreo*.

Ésta evidente fragmentación provoca consecuencias negativas entre los usuarios, tales como, problemas en actualizaciones de aplicaciones móviles, imposibilidad de descarga de aplicaciones en función de la versión mínima exigible, problemas de seguridad en aplicaciones móviles, problemas de seguridad en dispositivos móviles, experiencias dispares con un mismo sistema operativo, posibles vulnerabilidades no resueltas y desamparo de usuarios con versiones antiguas.

Los problemas más graves son los relacionados con la seguridad del dispositivo móvil, algunas marcas se han comprometido a realizar actualizaciones de seguridad para versiones antiguas, como en el caso de *Samsung* que recientemente se compromete a actualizar versiones de hasta cuatro años de antigüedad, de hecho en los próximos meses se lanzará una actualización de seguridad para los dispositivos *S6*. A pesar de estos compromisos, no todas las marcas realizan ésta gestión y siguen siendo actos insuficientes para ofrecer garantías de seguridad actualizada en el 100% de los dispositivos activos.

Ésta situación tiene difícil solución, pues las grandes empresas ven en la fragmentación un modelo de negocio y suelen ajustarse al mínimo exigible. De hecho, si contrastamos la vida útil de cualquier otro aparato electrónico o electrodoméstico, ésta es mucho más amplia que en los dispositivos móviles, llegando a un punto que muchos usuarios cambian de dispositivo anualmente concordándose así con la agresiva política de marketing de las marcas de dispositivos móviles.

Podemos concluir que no se observa en un futuro próximo una solución definitiva con la fragmentación y que su solución pasaría por facilitar la distribución de versiones a los fabricantes, tal como se ha intentado, implantando *Google*, el *Project Treble*, y además, endureciendo las políticas de actualización protegiendo siempre al usuario, al consumidor.

4.2 Privacidad

Nuestra privacidad en Internet es uno de los temas más preocupantes que se enfrenta la comunidad de usuarios. La creciente preocupación, el desfase tecnológico, el atraso y lentitud legislativa, y la falta de conocimiento provocan un conjunto de parcheados sobre parcheados, en son de aferrarse a la navegación privada, libre y segura, que dista mucho de esta realidad. Y es que podemos afirmar, que hoy en día, no tenemos privacidad en Internet y estamos muy lejos de llegar a un desenlace óptimo.

Ya en 1999, en una publicación en la revista tecnológica *Smart Reseller*, David Gerrold, escritor y guionista muy conocido por sus trabajos en la serie *Star Trek*, predijo una sociedad que usaría smartphones, o bien tal como viene definido en su artículo, *PITA (Personal Information Telecommunications Agents)*, dónde indicaba que el uso de éste aparato tecnológico dejaría sin privacidad a sus usuarios, y cito textualmente:

«*Having all that connectivity is going to destroy what's left of everyone's privacity****».***

Tan solo realizando un pequeño vistazo a las noticias más populares sobre privacidad en los últimos años, ya podemos observar la vulnerabilidad de nuestra privacidad, tales como, las informaciones de las filtraciones publicadas en *WikiLeaks* a partir de 2006, el robo de datos en *Playstation Network* en 2011, el robo de datos personales a políticos alemanes en 2018 entre muchos otros, nos dan a entender la creciente importancia que tienen nuestros datos.

Pero, sin tener en cuenta hechos puntuales de hackeo de datos, ¿está protegida nuestra privacidad? La respuesta a esta pregunta es muy clara: no.

En el evento de los premios Cinco Días a la Innovación Empresarial en 2016, Chema Alonso, en representación de *Telefónica*, realizó una ponencia explicando la fragilidad de nuestra privacidad y la inexistencia de la misma.

En ésta ponencia, Chema Alonso, nos indicaba que todos somos usuarios que navegamos en redes gratuitas y usamos aplicaciones gratuitas, pero éstas, no son realmente gratuitas, el precio es la privacidad. Y es que, tan sólo por usar cualquier herramienta que implique una conexión a internet, ya dejamos un pequeño rastro de nuestra huella digital. Una mínima conexión ya implica facilitar nuestros datos, y es que a día de hoy tan sólo por conectarnos ya decimos quiénes somos, desde donde navegamos, a qué hora, qué sistema operativo tenemos, que IP tenemos, dónde nos conectamos o bien que vemos. A partir de aquí, dependiendo del uso y permisos que facilitemos, aportamos aún más información, tales cómo, nuestra localización geográfica, nuestro tiempo de conexión según nuestra posición geográfica, nuestro tiempo de inactividad, nuestros datos de contacto o bien nuestros datos de cuentas online tales como redes sociales.

Tan sólo con esta pequeña fuga de datos personales que aportamos ya podemos extrapolar muchísima información privada, si se realiza un estudio del tiempo de inactividad del dispositivo móvil podemos saber dónde dormimos, dónde vivimos. Si extrapolamos nuestros recorridos según nuestra geolocalización, podemos saber dónde trabajamos, dónde vamos de vacaciones, cuando vamos de vacaciones, dónde compramos. Si estudiamos nuestros contactos con nuestras redes sociales y lo juntamos con nuestra geolocalización podemos ver aún mucho más de un usuario, cómo quienes son nuestros amigos, nuestros familiares, cuando los vemos o bien dónde solemos reunirnos.

Hay tan sólo dos tipos de permisos de aplicaciones en los dispositivos móviles que ya permiten mostrar ésta información a éstas aplicaciones, son los permisos de acceso a cuentas y acceso a ubicación. En las tiendas oficiales de aplicaciones, hay más un millón de *apps* que los precisan para su completo funcionamiento.

Los dispositivos móviles dan una falsa percepción de seguridad con nuestra privacidad facilitando herramientas de control de éstos datos. Para ejemplificar esta falsa percepción de seguridad, se citará nuevamente a Chema Alonso, quién facilita el ejemplo del botón activar/desactivar el botón de la geolocalización en el dispositivo móvil. Y es que para saber el posicionamiento de un dispositivo móvil no es necesario tener activada esta opción. Existen mapeos de redes inalámbricas realizadas a través de la técnica *wardriving* que permiten cruzar la posición de un dispositivo mediante la conexión a una red inalámbrica y éste mapeo, de hecho se puede incluso apurar más la localización sabiendo qué redes inalámbricas puede ver el dispositivo y según el número de redes extrapolarlo a una ubicación. Otra técnica que permite localizar un dispositivo sin necesidad de tener activa la localización sería mediante *battery cookie*, técnica con la cual se cruza la ubicación con el esfuerzo que realiza la batería según lo lejos o cerca que estemos de una antena.

Podemos afirmar que a día de hoy no hay garantías de protección de nuestros datos personales y es inexistente la privacidad en internet. A pesar de ésta afirmación y que aún estamos alejados de una situación ideal para los internautas y usuarios de smartphone, se está avanzando con diferentes ramas para mejorar la privacidad.

Herramientas cómo los textos legales redactados bajo la tutela del nuevo reglamento europeo de protección de datos aprobado el pasado 25 de mayo de 2018, pretenden regular el tratamiento de los datos personales intentando proteger así la privacidad de los usuarios. A pesar de ser un buen avance legislativo, es evidente que aún necesita mejorarse y trasladarlo a los usuarios de una forma más

sencilla. Los usuarios se encuentran con largos textos legales, transcritos en vocabulario específico con tecnicismos legales y que son muchas de las veces de difícil compresión.

Además, tanto internautas como usuarios de smartphone, a día de hoy, relacionan y hacen uso de las nuevas tecnologías, gran parte de las veces, como herramientas de uso rápido. Según *Google Analytics*, el 53% de las personas abandonan una página web si tarda más de tres segundos en cargar. Es bien sabido en la comunidad de diseñadores web, que un usuario puede perder el interés en una página web en los primeros cinco segundos de su estancia. Es decir, bajo éstas premisas, es muy difícil que un usuario lea al completo un texto legal para poder acceder a una aplicación o bien hacer uso de una página web.

Podemos decir que, a pesar del nuevo reglamento RGPD, la forma de transmitir la gestión de privacidad a los usuarios, no es la más óptima ni la más eficiente.

4.3 Vulnerabilidades

El término vulnerabilidad en los sistemas informáticos viene definido por puntos débiles de un sistema informático que permiten a un atacante explotar la situación para comprometer la integridad, disponibilidad o confidencialidad del mismo.

Estos agujeros de seguridad o vulnerabilidades pueden ser conocidos o desconocidos, en caso que se conozca la vulnerabilidad, ésta deberá ser tratada y reportada lo antes posible para su solución e implementación de parche de seguridad o actualización.

Las vulnerabilidades conocidas se documentan en varios repositorios, tales como, la base de datos con ésta información puede localizarse en el *National Vulnerability Database (NVD),* repositorio del gobierno federal de Estados Unidos usado de forma global. Su versión en castellano puede encontrarse en la URL de INCIBE. Las vulnerabilidades vendrán marcadas por el estándar de nomenclatura *Common Vulnerabilities and Exposures (CVE).*

La tecnología móvil, como sistema informático, también tiene vulnerabilidades. Por muy evidente que sea ésta información, parece muy necesaria su indicación ya que a pesar de que los usuarios ya son conscientes de los peligros en entornos como PC o portátiles, no hay una extrapolación de éste conocimiento en los dispositivos móviles tan evidente. Campañas como las de *Apple* donde aseguran que sus dispositivos son 100% seguros o como las de *Android* asegurando una alta fiabilidad a su tienda online, desfavorecen al conocimiento dando una falsa sensación de seguridad al usuario.

Y es que hoy por hoy la seguridad en los dispositivos móviles es esencial por el crecimiento de dispositivos activos y de usuarios activos tal como se ha observado a lo largo de éste documento. Éste hecho se encuentra intrínsecamente relacionado con una creciente evolución de malware, llegando en 2018, según datos estadísticos de *Kaspersky Lab* a 5.321.142 paquetes de instalación maliciosos, 151.359 nuevos troyanos bancarios móviles y 60.176 nuevos troyanos extorsionadores móviles.

Existen varios tipos de amenazas que atacan vulnerabilidades y a continuación se mostrarán los diferentes tipos de malware que acechan a la tecnología móvil.

4.3.1 Tipos de amenazas

- *RiskTool*: Según datos de *Kaspersky Labs*, éste tipo de malware es el más usado durante el último bienio (entre 2017 y 2018), ésta amenaza daña tanto a nivel de software como de hardware de la propia terminal, atacando a través de aplicaciones móviles. Es un tipo de malware muy parecido a un troyano.

- *Trojan-Dropper*: Se trata de herramientas que eluden detecciones y medidas de seguridad con tal de instalar un troyano. En 2017 la compañía de seguridad informática eslovaca, ESET, detectaron como *Android/TrojanDropper.Agent.BKY* varias aplicaciones móviles en la *Android Store* con éste malware y que habían conseguido evitar los algoritmos de protección de la tienda online.

- *Adware*: Éste tipo de malware es uno de los más conocidos y que afectan en gran medida a equipos informáticos, aunque también tiene como objetivo los dispositivos móviles. Básicamente se trata de herramientas o aplicaciones que introducen grandes cantidades de anuncios publicitarios.

- Troyanos bancarios (*Trojan-Banker*): Éste tipo de malware tiene como objetivo el robo de datos bancarios.

- Troyano SMS (*Trojan -SMS):* Éste tipo de malware realiza envíos a de SMS a servicios Premium o de tarificación especial sin que el usuario se dé cuenta. De esta forma, el ataque en sí lo que realiza es un robo de dinero del usuario. A pesar de que, su gran auge fue sobre el 2012, sobre todo con la aparición del troyano *SMS Boxer* que afectó a una gran cantidad de usuarios, a día de hoy sigue estando situado en el top 5 de malware móvil.

- *Trojan-Ransom*: Éste tipo de malware bloquean archivos del dispositivo o el dispositivo en sí, generalmente mediante cifrado, para que el usuario no pueda acceder a los mismos. En general funcionan como un secuestro, el malware secuestra archivos o el dispositivo en sí, solicita un rescate y tras el pago del mismo, en teoría facilitan la clave de desencriptado.
  Éste tipo de malware se hizo mundialmente famoso a nivel equipos informáticos, en 2017 tras el gran ataque mundial con *WannaCry* donde miles de empresas en todo el mundo fueron afectadas.

- *Trojan-Spy*: Tal como se deduce del mismo nombre, se trata de un malware que tiene como finalidad espiar al usuario.

- *Backdoor*: Se trata de una malware que sirve como puerta trasera en una aplicación y así tomar el control del dispositivo. Éste tipo de malware destaca por su sencillez en su realización, de hecho, realizando una simple búsqueda por internet, encontramos numerosos tutoriales de cómo introducir una puerta trasera en cualquier aplicación en cuestión de pocos minutos.
  Existe incluso software gratuito que permite incorporar este malware en cualquier aplicación, como por ejemplo *Spade*.

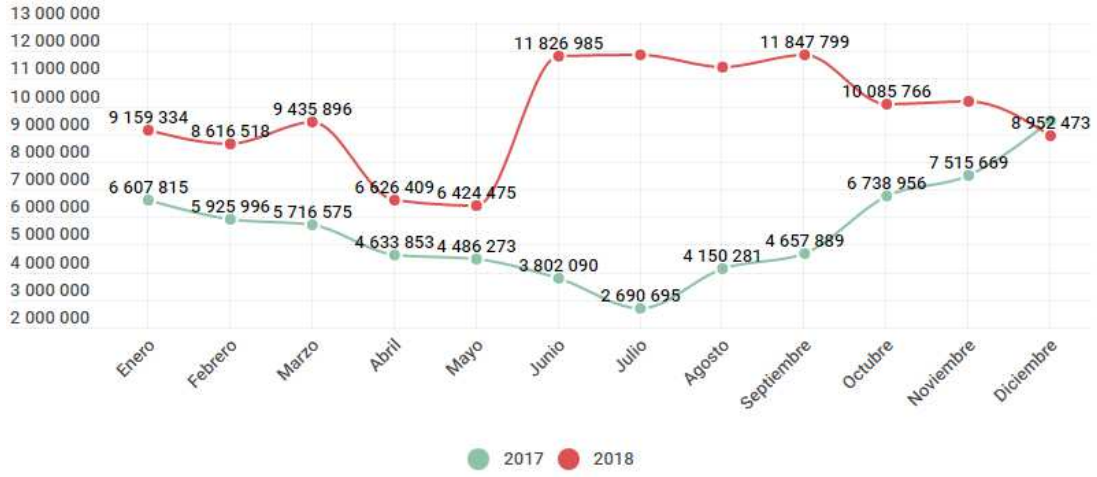
- *Monitor*: Malware con el que se puede monitorizar un dispositivo móvil.

- *Downloader*: Malware que realiza descargas de aplicaciones maliciosas en el dispositivo móvil.

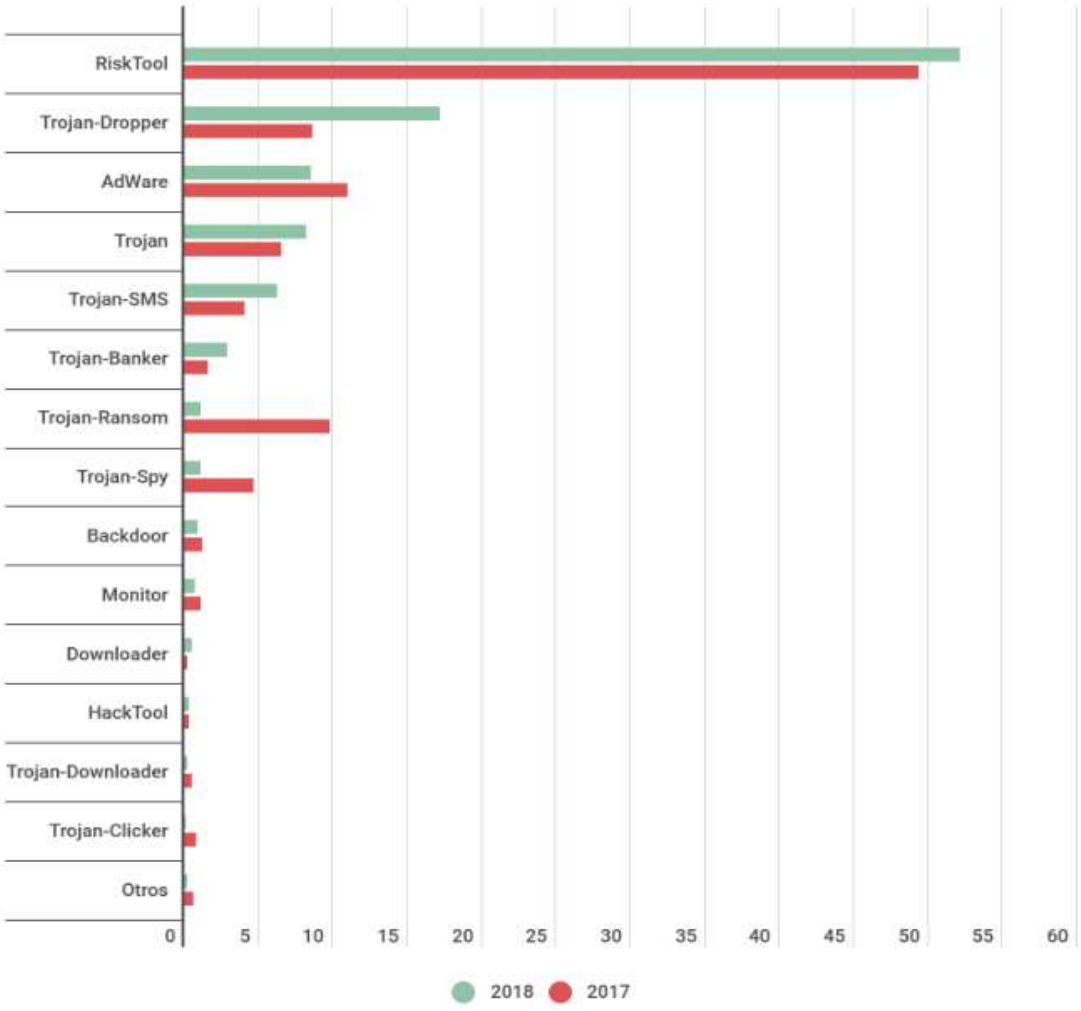
4.3.2 Estadísticas de malware

Kaspersky Labs nos ofrece una serie de datos estadísticos que nos aportan información relevante a la evolución del malware y nos da una buena visión global de la situación.

Así que, según sus datos, los ataques informáticos a dispositivos móviles han ido en aumento a lo largo de los años, alcanzando en 2018 la cifra de 116,5 millones de ataques.



Si analizamos las estadísticas en función del tipo de malware observamos lo siguiente:



Si se analizan estos datos se observa que, a pesar del auge en el robo de datos bancarios, la lista de malware la encabezan los *RiskTool* con 52,06%.

Se observa que *RiskTool, Trojan-Dropper, Trojan-Banker, Trojan y Trojan-SMS* son los malware que han evolucionado de forma ascendente desde el 2017 al 2018. Sorprende ver que *Trojan-SMS* aumente a 6,20% ya que la previsión es que descendiera después del auge en 2012.

Se destaca de éstos datos, el descenso de los *Trojan-Ransom* de un 9,7% en 2017 a un 1,12% en 2018. No es sorprendente, ya que, tras *WannaCry* se ha puesto foco de atención en éste tipo de malware y los usuarios son conocedores del mismo, debido a su frecuente aparición en el sector periodístico. Así pues, es lógico que la tendencia sea a la baja y su infección se potencie a través de ingeniería social con ataques de *phishing*.

Si ponemos el foco estadístico a nivel mundial, por países y en función del porcentaje de usuarios atacados por malware móvil, observamos que el listado lo encabezan Irán, Bangladesh y Nigeria.

País*	%**
Irán	44,24
Bangladesh	42,98
Nigeria	37,72
India	36,08
Argelia	35,06
Indonesia	34,84
Pakistán	32,62
Tanzania	31,34
Kenia	29,72
Filipinas	26,81

No es de extrañar que el listado lo sea encabezado por países con conflictos sociales, políticos y religiosos en más auge. De hecho históricamente cuando hay conflictos hay ciberataques.

5. Fuentes de divulgación

Vivimos en la era de la información, una era en la cual se puede tener acceso a un gran cúmulo de información, facilitándonos así, en teoría, la obtención de conocimiento. A niveles de seguridad, ésta información también se encuentra presente y los usuarios podrían estar correctamente informados.

En la realidad no es así, y es que la información es poder pero el exceso de información sumado a una mala estructuración y enfoque de la información, provocan la desinformación. Ya en 1970, el escritor y científico americano Alvin Toffler, realizaba una investigación sobre los excesos en la información o *information overload*, donde relacionaba la evolución tecnológica con la sobrecarga de información llegando a la conclusión que los usuarios sobreinformados posponían las decisiones de lo aprendido o bien realizaban un enfoque erróneo.

A raíz de lo comentado, en la actualidad nos encontramos que los usuarios pueden estar informados sobre seguridad TIC, pero que la sobrecarga de la misma hace que no realicen un uso correcto de la seguridad.

La tecnología avanza con una rapidez abismal, como consecuencia muchos sectores se encuentran siempre atrasados provocando consecuencias negativas. Este planteamiento se observa sobretodo con las leyes, ya que se tarda excesivamente en adaptar el sistema legislativo a las nuevas tecnologías provocando situaciones ilógicas. Y es que las leyes enfocadas a las nuevas tecnologías, tales como la RGPD, suelen llegar tarde y con un enfoque poco determinante. Esto ocurre también en educación, hoy en día deberíamos tener asignaturas sobre tecnología o seguridad tecnológica ya desde edades tempranas, en España debería iniciarse en la educación secundaria obligatoria o incluso en la primaria.

Las empresas de dispositivos tecnológicos, deberían incorporar de manera muy visual manuales de buenas prácticas, un sistema parecido al que disponemos en los trípticos de la medicina tradicional, para así, advertir correctamente a los usuarios del buen uso de los dispositivos y ser conscientes que la herramienta que adquieren tiene sus peligros tanto a nivel laboral, como personal, como económico o bien como de salud.

Los usuarios deberían ser conscientes de dónde pueden obtener información sobre seguridad de dispositivos móviles, y saber encontrarla en organismos oficiales o bien en las propias URL de las marcas de dispositivos.

A nivel de organismos oficiales o empresas , podemos observar iniciativas muy interesantes, como la reciente de INCIBE, donde el pasado 21 de febrero nos mostró el recurso educativo comenzamos con seguridad, una manera de acercar a la ciberseguridad o al internet seguro a niños de entre 5 y 8 años. Al igual que dispone de unidades didácticas, recursos educativos para fomentar el buen uso de internet y de las nuevas tecnologías.

Desde el blog de la oficina de seguridad del internauta también se dispone de numerosos recursos informativos donde obtener información.

En conclusión podemos decir que no es falta de información lo que tiene el usuario, sino falta de enfoque o de facilidad en encontrarla, además de un sistema educativo y legislativo incapaz de adaptarse en consonancia o de avanzarse a la evolución de las tecnologías.

5.1. Estudio estadístico

Con tal de contrastar, de forma más cercana, todos los datos, informaciones y estadísticas externas aportadas en éste documento y en referencia a los usuarios, se ha realizado un encuesta analítica a una pequeña muestra poblacional.

La encuesta se ha realizado con las herramientas gratuitas proporcionadas por Google, la herramienta *Google Forms*. De éste modo la distribución se puede realizar de forma muy sencilla y la interacción del usuario es realmente cómoda, ya que pueden realizar la encuesta tan sólo pulsando sobre la URL facilitada, desde cualquier dispositivo y lugar.

La encuesta es anónima y no se ha almacenado ningún dato privado de los encuestados. Se ha distribuido en cascada a usuarios de proximidad social, éstos lo han distribuido a otros contactos y así sucesivamente, llegando a una muestra de 111 usuarios encuestados.

A pesar de no ser una muestra considerable al contrastarlo con el número de usuarios de teléfonos móviles, podemos afirmar que los resultados son igualmente relevantes y confirman los datos aportados en éste documento y que han sido, a su vez, contrastados con fuentes externas de información.

En éste punto mostraremos los aspectos más relevantes de la encuesta, el completo de la encuesta y sus respuestas se podrán observar en los Anexos 1 y 2 respectivamente.

La encuesta se divide en cinco secciones, una sección de preguntas generales como Edad o Sexo, una segunda sección con preguntas sobre dispositivos móviles, una tercera sobre aplicaciones, una cuarta sobre aplicaciones de mensajería instantánea y finalmente, una quinta sobre tecnología en general.

De la encuesta observamos que un 99,1% de los encuestados dispone de teléfono móvil. Podemos decir que, una mayor parte de los encuestados muestra interés por informarse sobre tecnología a grandes rasgos sin detallar en información específica.

El 90,9% de los encuestados hacen uso de aplicaciones móviles, casi el 81% lee los comentarios de otros usuarios sobre las aplicaciones, para evaluar si hacer uso o no de la misma. Prácticamente ningún de los encuestados suele rechazar los permisos y la mitad los suele leer. El 85,5% de los encuestados no leen el texto legal, y prácticamente nadie suele rechazarlo.

Un alto porcentaje de los encuestados está correctamente informado sobre técnicas de *phishing*, y son precavidos con la mensajería instantánea.

A nivel de conexión a redes *WIFI*, un 30% suele conectarse a cualquier red pública y un 58,2% a cualquier red privada.

Uno de los datos más relevantes de la encuesta es la referente a la divulgación de información de seguridad TIC. Un 88,2% entiende que es insuficiente.

5.2. Conclusiones del estudio estadístico

Tras el análisis de los datos estadísticos de la encuesta, podemos concluir lo siguiente:

- Tras los grandes ataques de seguridad de los últimos años y en concreto, el ataque *WannaCry* de 2017, los usuarios son más desconfiados con los mensajes que reciben desde mensajería instantánea. Además ha provocado que los usuarios tengas más conocimiento sobre los ataques mediante ingeniería social como puede ser el *phishing*.

- Las nuevas tecnologías están plenamente consolidadas y están en auge. Los usuarios hacen uso de ellas pero siguiendo unas pautas inadecuadas que pueden provocar ser objetivo de malware. Hay mucha información sobre seguridad TIC, pero se encuentra dispersa, en grandes cantidades y en su mayor parte en lenguaje específico. En la encuesta se muestra cómo los usuarios ponen más atención en lenguaje coloquial y mucha menos atención en lenguaje específico. Es obvio que hay que llegar al usuario de una manera más directa y más adecuada.

Tras preguntar a los usuarios sobre como divulgarían la información sobre seguridad TIC, tras múltiples respuestas, indican que se podría informar sobre seguridad en el momento de la compra de un dispositivo móvil, que se podría informar mediante mensajería instantánea o que la información fuera más apta al lenguaje de usuario.

Una de las conclusiones a las que llegamos, tal como se ha indicado, es el lenguaje que se usa para llegar al usuario, y éste podría ser similar al lenguaje que se usa con opiniones de otros sectores como hoteles, viajes, restaurantes, cine, entre muchos otros. En concreto, con las aplicaciones móviles, se podría disponer de un método de puntuación basado en un sello de calidad, con una puntuación, por ejemplo del 1 al 5, de aplicación insegura a segura. Un sistema muy visual que sirviera para que el usuario tenga conocimientos sobre la aplicación que va adquirir y en caso que se decida por hacer uso de la misma, sea consciente de las precauciones que debe tomar.

Podría ser un sistema del siguiente tipo, de menos a más seguro:

Mencionar que se hará uso de éste sistema de puntuación en informe final del análisis de la aplicación *Android*.

6. Análisis forense de una APK. (Aplicación Android)

Se realizará un análisis forense de una aplicación *Android*, con el objetivo de realizar un estudio minucioso del comportamiento, un análisis de vulnerabilidades y una revisión de código, para que, con ello, sea de utilidad para fines de desarrollo de aplicativos o bien para ser conocedores del comportamiento real de la misma.

Para llevar a cabo éste análisis, en primer lugar se realizará una pequeña introducción sobre la estructura particular de las aplicaciones *Android* y mostraremos que herramientas se usarán para preparar el entorno de laboratorio. Posteriormente se realizará el análisis y su correspondiente informe final.

6.1 Introducción

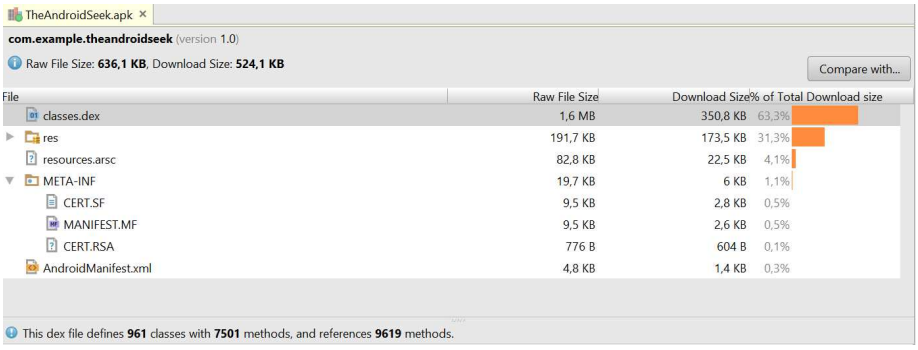
6.1.1 Aplicaciones Android

Las aplicaciones *Android* se ejecutan una vez compiladas desde los archivos con extensión .apk (*Android Application Package*), un paquete exclusivo para los sistemas operativos *Android* y que no son más que comprimidos *.zip* con distinta extensión que son contenedores de archivos *.java.*

Al desensamblar el archivo *.apk*, se puede observar la siguiente estructura:

- *META-INF*: En éste directorio nos encontramos varios archivos: *MANIFEST.MF, CERT.RSA* y *CERT.SF*
  - *MANIFEST.MF*: Es el manifiesto de la aplicación.
  - *CERT.RSA*: Se trata del certificado de la aplicación.
  - *CERT.SF*: Se trata de un listado de recursos necesarios y su clave *sha-1*.
- *LIB*: En éste directorio nos encontramos código compilado específico del software o procesador que contiene directorios como armeabi, x86 o mips entre otros.
- *RES*: Directorio que contiene recursos no compilados en resources.arsc
- *ASSETS*: Contiene recursos de aplicaciones, los assets de la aplicación.
- *AndroidManifest.xml*:Manifiesto adicional, archivo que contiene en formato *.xml* la información de las clases, versión, nombre, librerías o derechos de acceso.
- *Classes.dex*: Contiene las clases compiladas, el código java, en formato *.dex* que puede ser interpretado por la máquina virtual *Dakvik* o bien por *Android Runtime*.
- *Resources.arsc*: Contiene los recursos precompilados.

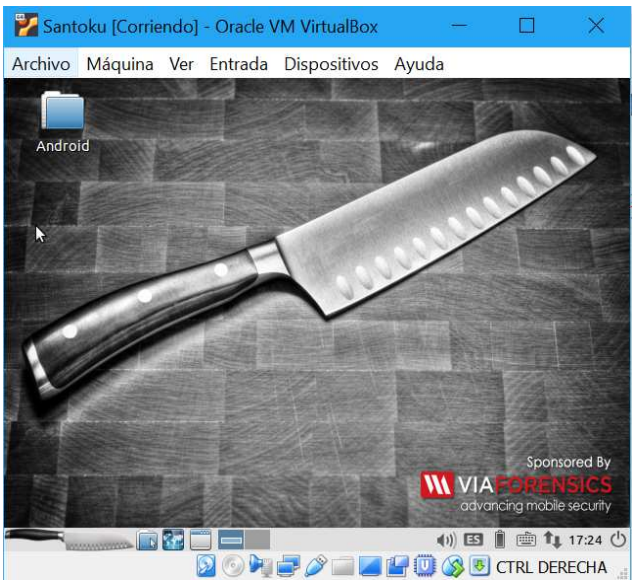
Es importante ser conocedor de la estructura de *.apk* para poder analizar en profundidad la aplicación, como veremos aplicando técnicas de ingeniería inversa, tales como *apkTool*, se podrá observar dicha estructura y se podrá navegar a través de los ficheros con tal de obtener información relevante.



6.1.2 Recursos para el análisis.

Con tal de realizar dicha auditoría o análisis forense, mencionaremos los recursos utilizados para ésta gestión.

En primer lugar se ha usado una imagen de *Linux* llamada *Santoku*, emulada en una máquina virtual a través de VirtualBox.



Santoku Linux es una distribución basada en *Linux* directamente diseñada para auditar teléfonos móviles. Esta imagen dispone del software necesario para realizar análisis forense y análisis de seguridad, es decir, los recursos necesarios para realizar una auditoría a una aplicación móvil.

Dentro de éste entorno, hemos usado las siguientes aplicaciones:

- *Androguard*: Se trata de una herramienta para realizar ingeniería inversa o *reverse engineering* para realizar un análisis exhaustivo del *.apk*. Se trata de un *framework* desarrollado en *Python* que nos permitirá descompilar la aplicación para realizar un estudio o análisis estático del código. Con Androguard podremos usar varias características tales como *androlyze, androsim, androaxml, androdd, androarsc o androaxml* entre otras.

    - *Androdd*: Con esta utilidad podemos realizar una extracción de todo el código *.java*, para poder navegar archivo por archivo del código.
    - *Androaxml*: Con ésta utilidad *Androaxml* podemos extraer en un fichero la información del *AndroidManifest.xml*
    - *Androapkinfo*: Obtenemos información sobre la clase principal o *Main Activity*, tales como permisos, ficheros, servicios entre otros.

- *Dex2jar*: Utilidad de ingeniería inversa que convierte *.dex* a *.jar*
- *JD-GUI*: Visor con estilo clásico de un *IDE*, que permite visualizar el código en un entorno más confortable.

Fuera del entorno de *Santoku-Linux*, se ha usado *Android Virtual Device Manager*, software que se puede localizar al instalar *Android Studio* o *Eclipse* con los recursos *Android*, ambos se tratan de un IDE para programar en *Android* y en particular, *Android Studio*, es el recurso oficial de *Android* para sus

desarrolladores. El *AVD*, o bien el mencionado *Android Virtual Device Manager*, se trata de una herramienta para virtualizar o emular dispositivos móviles. Con este recurso podremos emular un dispositivo móvil, instalar un *.apk* y lanzarlo en ésta emulación para poder realizar un estudio dinámico de la aplicación móvil. Si lo unimos al depurador de *Android Studio*, podremos observar las funcionalidades, sus acciones y sus reacciones.

Se ha usado la herramienta *WireShark* para esnifar la red, es decir, realizar un estudio de la red con la aplicación en marcha.

Finalmente se han usado dos recursos de análisis en profundidad online de aplicativos móviles *Android*, que son los siguientes:

- *VirusTotal*: Herramienta online de detección de malware. A través de varios motores de búsqueda, analiza el fichero subido y muestra si hay alguna detección. También muestra datos de análisis estático.

- *APKScan*: Herramienta online que muestra un reporte completo con los siguientes datos: Información general, información del *AndroidManifest*, información de virus a través de *Virus Total*, capturas de pantalla dinámicas de la aplicación, actividad de disco, actividad de red, de llamadas y de SMS automáticos entre otros

6.1.3 Aplicación objetivo.

La aplicación objetivo del análisis, es la aplicación llamada *theAndroidSeek*, aplicación desarrollada como trabajo final de carrera por el autor del presente documento, sujeto a una licencia *Creative Commons*: *Licencia Creative Commons*. Evidentemente, al ser el autor de ésta aplicación, quedo autorizado a realizar la auditoría.

El trabajo en sí, se puede localizar en la siguiente URL: http://hdl.handle.net/10609/22881

TheAndroidSeek es una herramienta de geolocalización, desarrollada en 2013, que tiene como objetivo dar soporte a excursionistas. La aplicación permite, en momentos de urgencia, enviar un mensaje a un contacto con su posición geográfica con tal que sea localizable en momentos que, el excursionista, se ha perdido. La aplicación también permite localizar con *GMaps*, posiciones geográficas con la latitud y la longitud, herramienta que permitiría interpretar el mensaje recibido por un usuario para observar, en modo mapa, la posición de un excursionista.

La herramienta también dispone de otras características como, muestra de rutas GR (senderos de Gran Recorrido) y teléfonos de interés.

6.1.4 Objetivo del análisis.

El objetivo del análisis a realizar se basa en un estudio detallado de una aplicativo móvil. Se realizará una auditoría completa de seguridad mediante técnicas forenses y técnicas propias de análisis de vulnerabilidades, privacidad y malware, con tal que, el desarrollador sea conocedor del posible mal funcionamiento, introducción de código malicioso, vulnerabilidades o aspectos negativos y pueda realizar las modificaciones y actualizaciones oportunas, para que, la aplicación sea lanzada con éxito y con una alta fiabilidad.

Se trata de realizar una auditoría de seguridad con similitudes a una auditoría de certificación ISO pero a pequeña escala y enfocado a una aplicación móvil en concreto.

El objetivo del análisis, no es tan sólo para beneficio del desarrollador, sino que, evidentemente también es en beneficio de los usuarios.

Tal como hemos visto en el punto cuatro de éste documento, el apartado fuentes de divulgación y en concreto con las datos estadísticos observados del comportamiento de los usuarios, éstos se interesan en leer los comentarios de una aplicación para decidir si descargarla o no. Éste comportamiento de contraste en los productos o servicios lo podemos observar extrapolado a muchos otros sectores como en la compra online (comentarios en los productos, como en *Amazon*), cine (estrellas sobre la calidad de una película, como en la URL de *metacritic* o bien en revistas del sector), restauración (opiniones sobre un restaurante, como en *tripadvisor*) entre muchos otros. Y es que para los usuarios, éste contraste es importante a la hora de decidir si comprar o no comprar, usar o no usar. Éste concepto, tal como hemos visto anteriormente, podría extrapolarse a la seguridad de las aplicaciones móviles, así pues, con una nota sobre la seguridad de una aplicación, podría servir para informar al usuario sobre si el aplicativo es seguro, es seguro pero con menciones o bien es totalmente inseguro.

En conclusión, este análisis o auditoría de seguridad tiene como objetivo informar sobre el estado de seguridad de una aplicación, tanto para desarrolladores como para usuarios.

6.2 Proceso de análisis

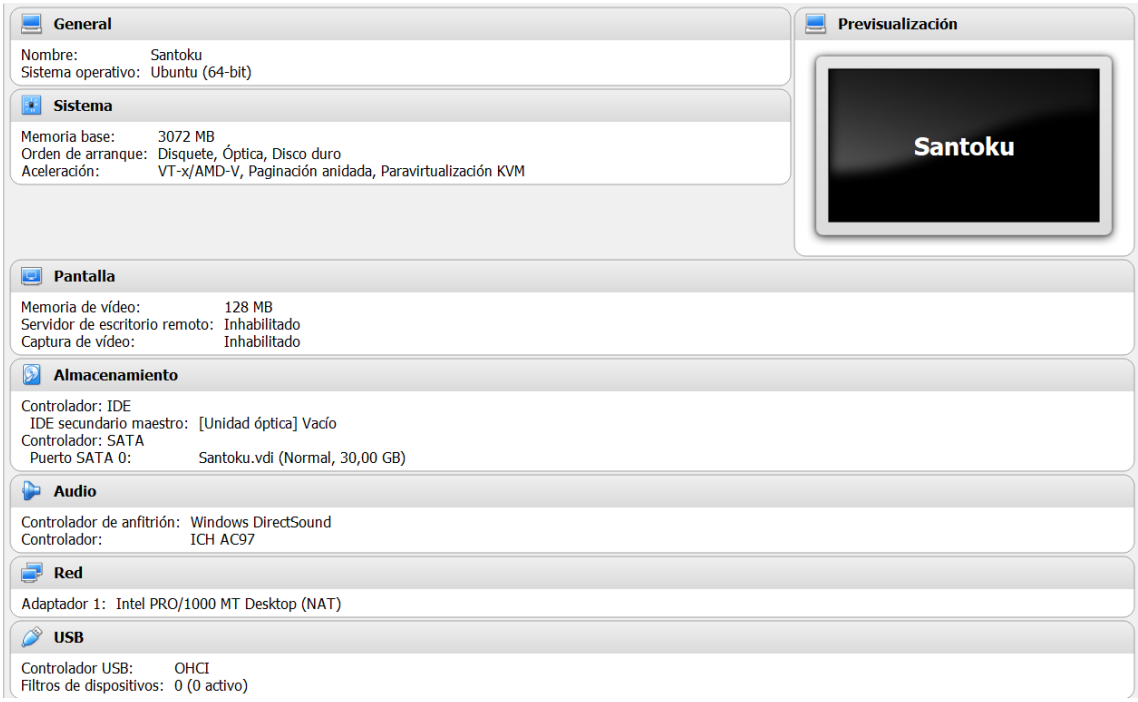
6.2.1 El entorno de laboratorio

A continuación se mostrará el proceso de instalación/creación del entorno de laboratorio. Mencionar que las herramientas online, básicamente nos hemos redirigido a su correspondiente URL para hacer uso de ellas.

- *Virus Total*: https://www.virustotal.com/gui/home/upload
- *APKScan*: https://apkscan.nviso.be/

En cuanto a *Santoku-linux*, se ha descargado una imagen de ésta versión de Linux en formato *.iso* desde la URL de https://santoku-linux.com/

Ésta imagen se ha cargado en *VirtualBox*, que es un software de virtualización. Se ha creado un entorno virtual con sistema operativo base *Ubuntu* de 64 bits, memoria base de 3072MB y 30Gb de espacio.



Una vez creado el entorno virtual, se ha cargado el fichero *.iso* y se ha instalado el sistema operativo *santoku-linux*, con un proceso de instalación estándar sin nada a destacar.

Las herramientas usadas desde *santoku-linux* ya vienen precargadas en ésta imagen, con lo cual se ha evitado todo el proceso de instalación de cada una de las herramientas disponiendo de inmediato de las mismas.

Tanto la herramienta *Android Studio* como *Wireshark* se han descargado desde sus páginas oficiales y se ha realizado, también, un proceso de instalación estándar sin nada a destacar.

6.2.2 Análisis

Se mostrarán los pasos realizados en ésta auditoría de seguridad y los resultados de los mismos.

En primer lugar se realiza un reconocimiento de la aplicación a nivel de usuario, se realizan las pruebas con un *Samsung s3 Mini*, (el dispositivo que en primera instancia se usó para presentar la aplicación) y posteriormente se realiza un seguimiento a través de *avd* y *Android Studio*.

- Desde Samsung s3 Mini

  Observamos un comportamiento normal de la aplicación que dispone de un diseño antiguo, aunque éste aspecto estético no es relevante a nivel de seguridad del aplicativo.

Nos encontramos con cuatro opciones, que a continuación detallaremos lo más relevante y a grandes rasgos, con tal de comprender el funcionamiento del aplicativo:

- *Cerca punts de interés:* Pulsando esta opción aparecerá un mapa geolocalizando la posición y dará varias opciones interactuando con el botón menú del dispositivo móvil: *1.Llocs:* Se muestra un listado de sitios de interés que se marcaran en el mapa. 2.*TipusMapa:* Se muestra varias opciones de visualización del mapa. 3.*NetejaMapa:* Limpia las marcas realizadas en el mapa. *4.Rutes*: Se muestra un listado de rutas de interés que se marcaran en el mapa.

- *Cerca usuari:* En ésta opción el usuario puede enviar a un contacto, de su listado de contactos del dispositivo, la posición vía SMS. A su vez, el usuario receptor, puede copiar el contenido del SMS y pegarlo en ésta opción del aplicativo para poder visualizar la posición del emisor.

- *Telefons d'interés:* Esta opción te permite llamar a los teléfonos de interés que aparecen en éste listado.

- *Ajuda:* Texto de la ayuda.

Navegando por las funcionalidades indicadas del aplicativo, destacamos lo siguiente:

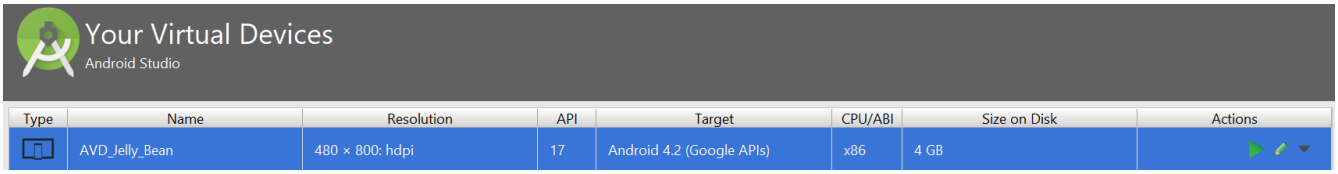
1. Se observan listados estáticos, se deduce ésta afirmación ya que son listados que no cargan, no se conectan a ninguna base de datos para actualizar los listados y siempre se encuentran los mismos ítems. Esto nos lleva deducir que se dispone de una base de datos *sql-lite* interna o bien información almacenada en estructura de datos.

A priori, éste factor puede resultar negativo, a futuro, para el rendimiento de la aplicación, ya que, si hipotéticamente se ampliara la información de dichos listados, éstos ampliarían el tamaño del aplicativo pudiendo afectar a una correcta experiencia de uso.

2. Se observa que tras el envío de la posición vía SMS, no hay registro del envío de éste SMS en ninguna parte del dispositivo.

- Desde Avd

Se configura una virtualización de dispositivo móvil con las siguientes característica

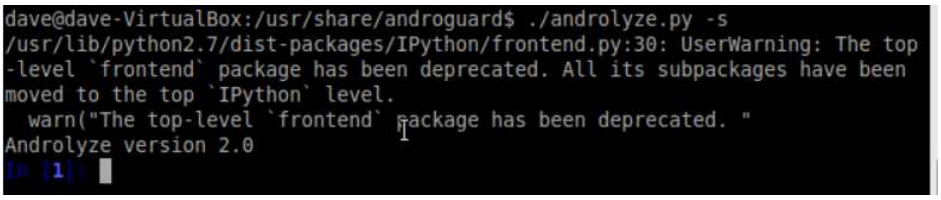


Se realizan pruebas también con una versión de *Android* superior a la *Jelly Bean*, en concreto la versión *Nougat*.

Mencionar que, no se destaca nada diferente de éstas pruebas respecto a las realizadas desde dispositivo móvil.

A continuación se realizará un análisis estático mediante ingeniería inversa, se accederá a *santoku-linux* y se empezará usando *Androguard*.

Para ello, en primer lugar, desde una *Shell* de *Linux*, y desde la ruta de *Androguard*, iniciaremos sesión con la utilidad de *androlyze*, que a partir de una nueva *shell* podremos obtener datos de archivos, permisos o funcionalidades del código.



Una vez abierta, se empieza la comunicación con ésta *Shell*, así que apuntamos el análisis sobre la *.apk* destinataria con la función *AnalizeAPK*. Mencionar que, se llama al decompilador *DAD* que es el predeterminado y estándar que viene incorporada en la instalación de *Androguard*.

```
In [1]:
a,d,dx=AnalyzeAPK("/home/dave/Desktop/Android/TheAndroidSeek.apk",decompiler="dad")
```

Una vez llamada ésta función, se realizan llamadas a estos datos almacenados, con listado de comunicación y respuesta que veremos a continuación.

Se obtiene el nombre del paquete:

```
In [2]: a.get_package()
Out[2]: u'com.example.theandroidseek'
```

Se obtienen los permisos de la aplicación:

```
In [3]: a.get_permissions()
Out[3]:
['com.example.theandroidseek.permission.MAPS_RECEIVE',
 'android.permission.INTERNET',
 'android.permission.ACCESS_NETWORK_STATE',
 'android.permission.WRITE_EXTERNAL_STORAGE',
 'com.google.android.providers.gsf.permission.READ_GSERVICES',
 'android.permission.ACCESS_COARSE_LOCATION',
 'android.permission.ACCESS_FINE_LOCATION',
 'android.permission.READ_CONTACTS',
 'android.permission.SEND_SMS',
 'android.permission.CALL_PHONE']
```

Se obtiene el listado de actividades:

```
In [4]: a.get_activities()
Out[4]:
['com.example.theandroidseek.MainActivity',
 'com.example.theandroidseek.CercaLlocInteres',
 'com.example.theandroidseek.CercaUsuari',
 'com.example.theandroidseek.Telefons',
 'com.example.theandroidseek.Ajuda',
 'com.example.theandroidseek.IntroCoord',
 'com.example.theandroidseek.MostrarUsuariPerdut',
 'com.example.theandroidseek.Ubicacions',
 'com.example.theandroidseek.NomsDeRutes']
```

Se obtiene sobre las versiones del código, de *sdk* y del objetivo *sdk*:

```
In [5]: a.get_androidversion_code()
Out[5]: u'1'

In [6]: a.get_androidversion_name()
Out[6]: u'1.0'

In [7]: a.get_min_sdk_version()
Out[7]: u'8'

In [8]: a.get_max_sdk_version()

In [9]: a.get_target_sdk_version()
Out[9]: u'17'
```

Se obtiene datos del manifiesto:

```
In [10]: a.get_android_manifest_axml()
Out[10]: <androguard.core.bytecodes.apk.AXMLPrinter instance at 0x7f4fbd3ccef0>

In [11]: a.get_android_manifest_axml().get_xml()
Out[11]: '<?xml version="1.0" encoding="utf-8"?>\n<manifest android:versionCode="1"
android:versionName="1.0" package="com.example.theandroidseek"
```

```
xmlns:android="http://schemas.android.com/apk/res/android">\n\t\n\n\t<permission
android:name="com.example.theandroidseek.permission.MAPS_RECEIVE"
android:protectionLevel="0x00000002">\n</permission>\n\t\n\n\t<uses-feature
android:glEsVersion="0x00020000" android:required="true">\n</uses-
feature>\n\t\n\n\t<uses-permission
android:name="com.example.theandroidseek.permission.MAPS_RECEIVE">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.INTERNET">\n</uses-permission>\n\t\n\n\t<uses-
permission android:name="android.permission.ACCESS_NETWORK_STATE">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="com.google.android.providers.gsf.permission.READ_GSERVICES">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.ACCESS_COARSE_LOCATION">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.ACCESS_FINE_LOCATION">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.READ_CONTACTS">\n</uses-permission>\n\t\n\n\t<uses-
permission android:name="android.permission.SEND_SMS">\n</uses-
permission>\n\t\n\n\t<uses-permission
android:name="android.permission.CALL_PHONE">\n</uses-permission>\n\t\n\n\t<uses-sdk
android:minSdkVersion="8" android:targetSdkVersion="17">\n</uses-
sdk>\n\t\n\n\t<application android:allowBackup="true" android:debuggable="true"
android:icon="@7F020018" android:label="@7F060015"
android:theme="@7F080001">\n\t\t\n\n\t\t<meta-data
android:name="com.google.android.maps.v2.API_KEY" android:value="@7F06001C">\n</meta-
data>\n\t\t\n\n\t\t<activity android:label="@7F060015" android:name="MainActivity"
android:screenOrientation="1">\n\t\t\t\n\n\t\t\t<intent-
filter>\n\t\t\t\t\n\n\t\t\t\t<action
android:name="android.intent.action.MAIN">\n</action>\n\t\t\t\t\n\n\t\t\t\t<category
android:name="android.intent.category.LAUNCHER">\n</category>\n\t\t\t\t\n\n\t\t\t</in
tent-filter>\n\t\t\t\n\n\t\t</activity>\n\t\t\n\n\t<activity
android:name="CercaLlocInteres">\n</activity>\n\t\t\n\n\t<activity
android:name="CercaUsuari"
android:screenOrientation="1">\n</activity>\n\t\t\n\n\t<activity
android:name="Telefons">\n</activity>\n\t\t\n\n\t<activity
android:name="Ajuda">\n</activity>\n\t\t\n\n\t<activity android:name="IntroCoord"
android:screenOrientation="1">\n</activity>\n\t\t\n\n\t<activity
android:name="MostrarUsuariPerdut">\n</activity>\n\t\t\n\n\t<activity
android:name="Ubicacions">\n</activity>\n\t\t\n\n\t<activity
android:name="NomsDeRutes">\n</activity>\n\t\t\n\n\t</application>\n\t\n\n</manifest>
\n'
```

Se obtiene el nombre de la firma:

```
In [12]: a.get_signature_name()
Out[12]: 'META-INF/CERT.RSA'
```

Se obtiene la firma:

```
In [13]: a.get_signature()
Out[13]:
'0\x82\x03\x04\x06\t*\x86H\x86\xf7\r\x01\x07\x02\xa0\x82\x02\xf50\x82\x02\xf1\x02\x01
\x011\x0b0\t\x06\x05+\x0e\x03\x02\x1a\x05\x000\x0b\x06\t*\x86H\x86\xf7\r\x01\x07\x01\
xa0\x82\x01\xe90\x82\x01\xe50\x82\x01N\xa0\x03\x02\x01\x02\x02\x04Q~\xb3*0\r\x06\t*\x
86H\x86\xf7\r\x01\x01\x05\x05\x00071\x0b0\t\x06\x03U\x04\x06\x13\x02US1\x100\x0e\x06\
x03U\x04\n\x13\x07Android1\x160\x14\x06\x03U\x04\x03\x13\rAndroid
Debug0\x1e\x17\r130429175138Z\x17\r430422175138Z071\x0b0\t\x06\x03U\x04\x06\x13\x02US
1\x100\x0e\x06\x03U\x04\n\x13\x07Android1\x160\x14\x06\x03U\x04\x03\x13\rAndroid
Debug0\x81\x9f0\r\x06\t*\x86H\x86\xf7\r\x01\x01\x01\x05\x00\x03\x81\x8d\x000\x81\x89\
x02\x81\x81\x00\xb9\x11\xd8aAl\xec\x015\x947\xf0\x16^|bG$\xa0\xf8\xf8P\xecC/\xd3\xcf\
x03\xc6\x1ds\x16o\xc6*\xb1K\xbb@xo\x9c\xde\x8b\x93\xc3\x9c\xa8k\xe2}%\x0b\xddA\xe3B&\
```

```
x05\xd4nS\xdd6\xde3e\xdf\x967\xd8m\xd2\xf7\xea4\xb7\xbckC_\x1d\x93\xb7\x96\x85GrU\x82
\xdc\xea\xd4\x18Ja\'\x00Ce*h\x87\'z\xa4\nn\xc9\xaa\x92\x8bu\r\xbaN\xbaE\x8eD\xe7\x8dq
\xdd\xa9\x84q\xf5\x02\x03\x01\x00\x010\r\x06\t*\x86H\x86\xf7\r\x01\x01\x05\x05\x00\x0
3\x81\x81\x00q,\xb5\x9b#Y>\xeb\x03#dqJGW"\xafC<x\xcb\xa9\x1d\xad\x92\xa7\xa5\xe4
\xd1v\xf7i;\x97]\xaf\xa3]\xee\xcc\xf7\xd8\xa3\xf7\x03C\xb1u\x89\x97\xa1f!\xe5\x02mhw\
xf9\xe6\xc1\xea\x1e\n\x10\x0e\xf2\x9eH\xa9Oy\x1d\xd5\xe8\x9b\xb7\xdeSh\xee\x12<\xbby\
x0e\x17N?\x9b?x=\x10\xfbj\xfc\x81\x9e\xb5\xa4\xef\xf7\x0f#\xbd\x1da\x88H\xf3\xd0\xffg
\t\xee\xcd\xe5\xf0@-
wU/\xa9V.1\x81\xe40\x81\xe1\x02\x01\x010?071\x0b0\t\x06\x03U\x04\x06\x13\x02US1\x100\
x0e\x06\x03U\x04\n\x13\x07Android1\x160\x14\x06\x03U\x04\x03\x13\rAndroid
Debug\x02\x04Q~\xb3*0\t\x06\x05+\x0e\x03\x02\x1a\x05\x000\r\x06\t*\x86H\x86\xf7\r\x01
\x01\x01\x05\x00\x04\x81\x80\x1dJ\x91FK\x95\xc8\x9c\xcd|\x84[\xfas\xde\x9fn\x84\xe31R
?\xe0v\xb6\x1a\x14\xc3\xf7\x15\xc8\x1f$u\x97j\xf5E\n\x85\x06\xb0;\x85$n\x11$FH\xd3/\x
c7\xfd\xc3\x1c\x83\xee\x93g\xa9+\x03.X\xff\'\xd7O\x8d\x84\x1e\xc0_\xaf\xa4\xa5\xe9\xe
f-\t\'\x00\xcdt\xd6
0\x1d\xa1\xd0\xea\xb0\xf1\xa0\x8b\xb8\xe0\x8eNO\xc8~\xd5\'\xb4\xc7\x02\x88/\x06WW\xe5
GN\x12\x88h.\xd7\xa4\xf0\x111\x9a%g'
```

Se obtienen los archivos de la aplicación:

```
In [14]: a.get_files()
Out[14]:
['res/color/common_signin_btn_text_dark.xml',
 'res/color/common_signin_btn_text_light.xml',
 'res/drawable/common_signin_btn_icon_dark.xml',
 'res/drawable/common_signin_btn_icon_light.xml',
 'res/drawable/common_signin_btn_text_dark.xml',
 'res/drawable/common_signin_btn_text_light.xml',
 'res/layout/activity_main.xml',
 'res/layout/ajuda.xml',
 'res/layout/cerca_lloc_interes.xml',
 'res/layout/cerca_usuari.xml',
 'res/layout/custom_dialog.xml',
 'res/layout/intro_coord.xml',
 'res/layout/mapa_mostra_usuari_perdut.xml',
 'res/layout/noms_rutes_list.xml',
 'res/layout/noms_rutes_list_item.xml',
 'res/layout/telefons.xml',
 'res/layout/telefons_item.xml',
 'res/layout/ubicacions_list.xml',
 'res/layout/ubicacions_list_item.xml',
 'res/menu/info_ubicacio_usuari.xml',
 'res/menu/main.xml',
 'res/menu/menu_cerca_lloc.xml',
 'res/menu/menu_cerca_usuari.xml',
 'res/menu/menu_principal.xml',
 'AndroidManifest.xml',
 'resources.arsc',
 'res/drawable-hdpi/common_signin_btn_icon_disabled_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_disabled_focus_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_disabled_focus_light.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_disabled_light.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_focus_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_focus_light.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_normal_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_normal_light.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_pressed_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_icon_pressed_light.9.png',
 'res/drawable-hdpi/common_signin_btn_text_disabled_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_text_disabled_focus_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_text_disabled_focus_light.9.png',
 'res/drawable-hdpi/common_signin_btn_text_disabled_light.9.png',
 'res/drawable-hdpi/common_signin_btn_text_focus_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_text_focus_light.9.png',
 'res/drawable-hdpi/common_signin_btn_text_normal_dark.9.png',
```

```
 'res/drawable-hdpi/common_signin_btn_text_normal_light.9.png',
 'res/drawable-hdpi/common_signin_btn_text_pressed_dark.9.png',
 'res/drawable-hdpi/common_signin_btn_text_pressed_light.9.png',
 'res/drawable-hdpi/ic_launcher.png',
 'res/drawable-hdpi/layout_menu.png',
 'res/drawable-hdpi/layout_menu2.png',
 'res/drawable-mdpi/common_signin_btn_icon_disabled_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_disabled_focus_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_disabled_focus_light.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_disabled_light.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_focus_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_focus_light.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_normal_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_normal_light.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_pressed_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_icon_pressed_light.9.png',
 'res/drawable-mdpi/common_signin_btn_text_disabled_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_text_disabled_focus_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_text_disabled_focus_light.9.png',
 'res/drawable-mdpi/common_signin_btn_text_disabled_light.9.png',
 'res/drawable-mdpi/common_signin_btn_text_focus_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_text_focus_light.9.png',
 'res/drawable-mdpi/common_signin_btn_text_normal_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_text_normal_light.9.png',
 'res/drawable-mdpi/common_signin_btn_text_pressed_dark.9.png',
 'res/drawable-mdpi/common_signin_btn_text_pressed_light.9.png',
 'res/drawable-mdpi/ic_launcher.png',
 'res/drawable-xhdpi/common_signin_btn_icon_disabled_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_disabled_focus_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_disabled_focus_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_disabled_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_focus_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_focus_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_normal_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_normal_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_pressed_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_icon_pressed_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_disabled_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_disabled_focus_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_disabled_focus_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_disabled_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_focus_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_focus_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_normal_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_normal_light.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_pressed_dark.9.png',
 'res/drawable-xhdpi/common_signin_btn_text_pressed_light.9.png',
 'res/drawable-xhdpi/ic_launcher.png',
 'res/drawable-xxhdpi/ic_launcher.png',
 'classes.dex',
 'META-INF/MANIFEST.MF',
 'META-INF/CERT.SF',
 'META-INF/CERT.RSA']
```

Se obtiene la clase principal:

```
In [15]: a.get_main_activity()
Out[15]: u'com.example.theandroidseek.MainActivity'
```

Se obtienen los nombres de las clases:

```
In [16]: d.get_classes_names()

 'Landroid/support/v4/widget/CursorAdapter;',
 'Landroid/support/v4/widget/EdgeEffectCompat$BaseEdgeEffectImpl;',
```

```
'Landroid/support/v4/widget/EdgeEffectCompat$EdgeEffectIcsImpl;',
'Landroid/support/v4/widget/ScrollerCompat$ScrollerCompatImplIcs;',
'Landroid/support/v4/widget/SearchViewCompat$SearchViewCompatHoneycombImpl$1;',
'Landroid/support/v4/widget/SearchViewCompat$SearchViewCompatHoneycombImpl$2;',
'Landroid/support/v4/widget/SearchViewCompat$SearchViewCompatStubImpl;',
'Lcom/example/theandroidseek/Ajuda;',
'Lcom/example/theandroidseek/CercaLlocInteres;',
'Lcom/example/theandroidseek/CercaUsuari;',
'Lcom/example/theandroidseek/MostrarUsuariPerdut;',
```

A partir de la sentencia anterior, se puede apurar más y consultar el código clase a clase con la sentencia: `d.get_class('Lcom/example/theandroidseek/MostrarUsuariPerdut;').source()`

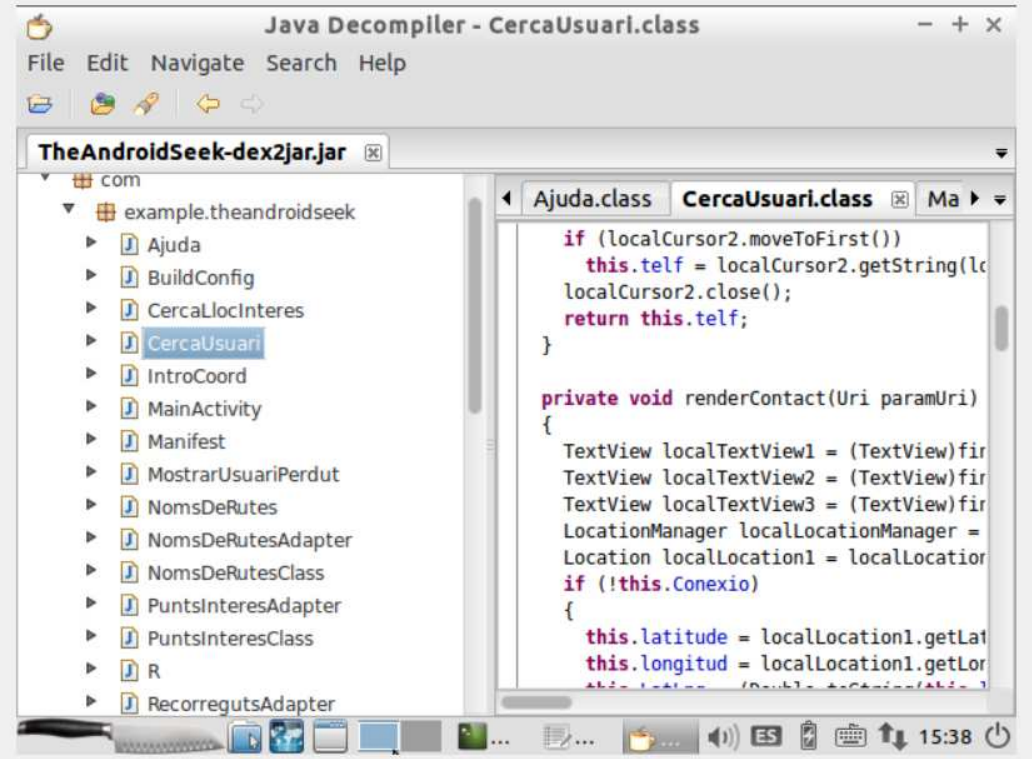
Se verá más al detalle algunos aspectos del código en un análisis posterior.

Con la sentencia *a.show()* se puede observar un reporte de algunos aspectos ya observados con las llamadas anteriores, al no ser de momento relevante, se podrá observar dicho reporte en el Anexo 1 de éste documento.

Mencionar también que con la utilidad *Androaxml* se puede extraer en un fichero la información del *AndroidManifest.xml*

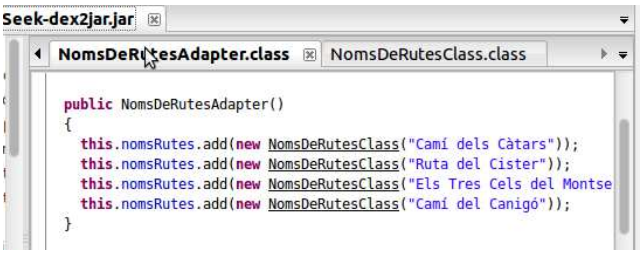
Para disponer del código de forma más visual, se ha combinando *dex2jar* y *JD-GUI*, así que, en primera instancia se obtiene el código *.java* para posteriormente visualizarlo en un entorno más dinámico

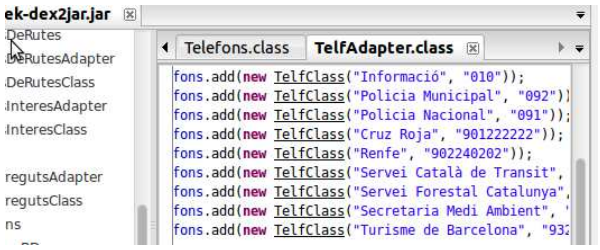
```
dave@dave-VirtualBox:/usr/share$ sudo d2j-dex2jar /home/dave/Desktop/Android/
TheAndroidSeek.apk
[sudo] password for dave:
dex2jar /home/dave/Desktop/Android/TheAndroidSeek.apk -> TheAndroidSeek-dex2j
ar.jar
```



De la revisión de código se destaca lo siguiente:

- Se confirma que la aplicación tiene los datos almacenados en estructura de datos, se encuentran en el propio código.





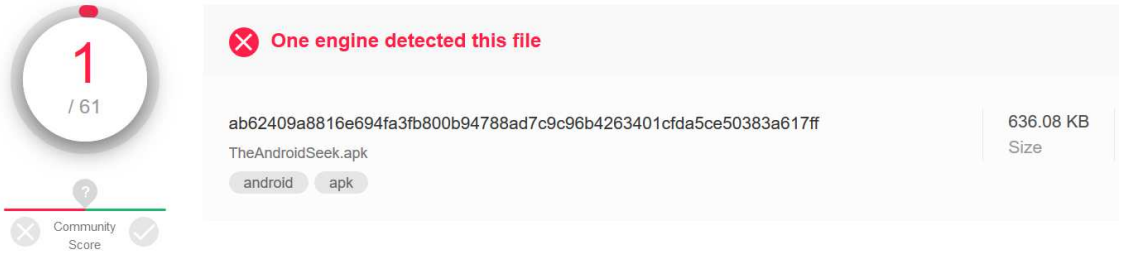
- El aplicativo dispone del código para la realización de una pequeña base de datos interna en *SQLLite*, pero que no se llega a usar.

De hecho al revisar el código, no se aprecia ni que se haga una llamada a ésta clase ni que se llegue a crear la base de datos.

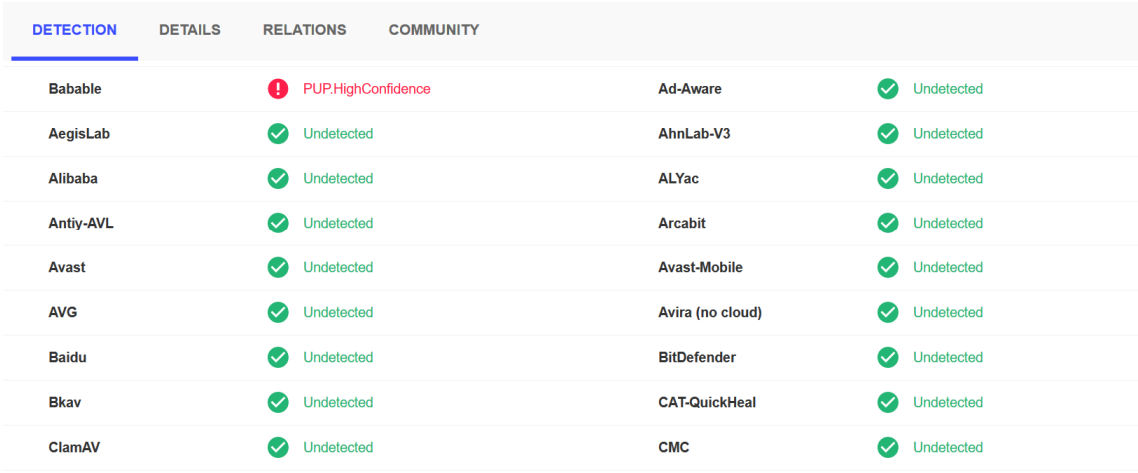
- Se observa, además del código de creación de base de datos mencionado, muchas clases que no se usan, y que son innecesarias para el funcionamiento de la aplicación.

A continuación, se realizan pruebas con herramientas online, empezando por la búsqueda de posible código malicioso con *VirusTotal*.

Tras subir el fichero, nos muestra la siguiente información:



La aplicación analizada, ha aparecido en uno de los 61 motores de búsqueda:



DETECTION DETAILS RELATIONS COMMUNITY

Babable	PUP.HighConfidence	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
Bkav	Undetected	CAT-QuickHeal	Undetected
ClamAV	Undetected	CMC	Undetected

Desde *Babable* detectan *PUP.HighConfidence*, en éste caso al tratarse sólo de 1 caso de 61, podría tratarse de un falso positivo, de que la *.apk* se encuentra mal firmada o algún permiso potencialmente peligroso. Tras el análisis realizado con *Androguard* y como comprobaremos en el análisis mostrado a continuación, ésta alarma podría también tratarse de los permisos de Contacto y SMS del aplicativo.

Desde *VirusTotal* también nos facilitan la siguiente información:

Información de las propiedades básicas del fichero en sí, tales como su tipo, la codificación del MD5, la codificación SHA-1, el tamaño del fichero entro otros.

Basic Properties

MD5	f47e2315d36e5fad64d390e288f5ccdd
SHA-1	8c98ccddde3a44f1b7c5f54f224dc293b66a1b27
SHA-256	ab62409a8816e694fa3fb800b94788ad7c9c96b4263401cfda5ce50383a617ff
SSDEEP	12288:VMR6Nnc6tN9XqKb1NMxtftsUWD3XZ2ecSLFrvc9:ssXtHXBotftsUWDZOSZ
File type	Android
Magic	Zip archive data, at least v2.0 to extract
File size	636.08 KB (651341 bytes)

Por otro lado, nos facilita información de los ficheros que contiene e información *Android* en sí como datos de la versión y del certificado

Bundle Info

Contents Metadata

Contained Files	96
Uncompressed Size	1.93 MB
Earliest Content Modification	2013-05-19 15:57:34
Latest Content Modification	2013-06-10 18:14:14

Contained Files By Type

PNG	66
XML	25
UNKNOWN	4
DEX	1

Contained Files By Extension

PNG	66
XML	25
MF	1
RSA	1
SF	1
DEX	1

Android Info

Summary

Android Type	APK
Package Name	com.example.theandroidseek
Internal Version	1
Displayed Version	1.0

Certificate Attributes

Valid From	05:51 PM 04/29/2013
Valid To	05:51 PM 04/22/2043
Serial Number	517eb32a
Thumbprint	9ef6b39e89c2a53343499e42bbff88a300737673

Certificate Subject

Distinguished Name	C:US, CN:Android Debug, O:Android
Common Name	Android Debug
Organization	Android
Country Code	US

A continuación nos muestra datos de los permisos, que saltan advertencias en algunos de ellos tales como los permisos de realizar llamadas o de SMS. También nos facilita la información de las actividades que tiene el aplicativo.

Permissions

- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_FINE_LOCATION
- android.permission.CALL_PHONE
- android.permission.INTERNET
- android.permission.READ_CONTACTS
- android.permission.SEND_SMS
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.ACCESS_NETWORK_STATE
- com.example.theandroidseek.permission.MAPS_RECEIVE
- com.google.android.providers.gsf.permission.READ_GSERVICES

Activities

com.example.theandroidseek.MainActivity
com.example.theandroidseek.CercaLlocInteres
com.example.theandroidseek.CercaUsuari
com.example.theandroidseek.Telefons
com.example.theandroidseek.Ajuda
com.example.theandroidseek.IntroCoord
com.example.theandroidseek.MostrarUsuariPerdut
com.example.theandroidseek.Ubicacions
com.example.theandroidseek.NomsDeRutes

Finalmente se usará la herramienta online *APKScan*, que aportará más información sobre la aplicación. Como ésta herramienta nos facilita mucha información duplicada respecto a la herramienta online anterior, se mostrará tan sólo la información relevante.

La herramienta muestra una pequeña emulación en formato de animación de la interacción del usuario con la aplicación, aunque en éste caso la interacción es automática con un *bot* de la herramienta. Además, se muestra un pequeño reporte de la actividad de la aplicación.

Disk activity

Accessed files

Filename	/proc/1261/cmdline
Filename	/data/data/com.android.gallery3d/shared_prefs/com.android.gallery3d_preferences.xml
Filename	/proc/1248/cmdline
Filename	/proc/meminfo
Filename	/proc/1346/cmdline
Filename	/data/data/com.android.vending/shared_prefs/finsky.xml
Filename	/proc/1233/cmdline
Filename	/dev/input/event0
Filename	/proc/1321/cmdline
Filename	/proc/1303/cmdline
Filename	/proc/1275/cmdline
Filename	/data/data/com.android.music/shared_prefs/Music.xml
Filename	/proc/1314/cmdline
Filename	/proc/1195/cmdline
Filename	/proc/1319/cmdline

Automatically placed calls and text messages

Placed phone calls

No phone calls were placed automatically.

Sent SMS messages

No text messages were placed automatically.

Cryptographic activity

Used encryption keys

No cryptographic activity detected.

Encryption operations

No cryptographic activity detected.

Decryption operations

No cryptographic activity detected.

Information leakage

Network information leakage

No network information leakage detected.

SMS information leakage

No SMS information leakage detected.

File information leakage

No file information leakage detected.

Con todos estos datos recogidos, podemos llegar a las siguientes conclusiones a nivel de seguridad y rendimiento:

- Según la interacción con la aplicación, la herramienta tiene tres funcionalidades. Geolocalización del usuario y muestra de puntos de interés cercanos. Geolocalización del usuario y envío de su localización vía SMS a otro usuario de su lista de contactos. Muestra de teléfonos para contactar.

- Código y funcionalidades sin actualizar que pueden provocar incompatibilidades con algunas versiones de *Android* y algunos dispositivos. El aplicativo por ejemplo usa el antiguo botón menú, obsoleto en muchas terminales.

- Tras el envío de coordenadas por SMS, el teléfono no registra en ningún lado éste envío, quedando opaco al usuario.

- Que la aplicación solicita para funcionar ciertos permisos con carácter obligatorio y que son permisos sensibles tales como permisos de localización, de realización de llamadas, de envío de SMS, de lectura de contactos y de escritura en almacenaje externo, siendo éste último, un permiso innecesario para el funcionamiento de la *app* al igual que el permiso de llamadas, ya que finalmente éstas llamadas se realizan fuera de la aplicación.

- La aplicación dispone de código en desuso y que no es relevante para el funcionamiento del aplicativo.

- La aplicación almacena la información que muestra en el propio código en una estructura interna de datos.

- No se dispone ni se ha realizado ninguna actualización desde junio del 2013.

- Tras análisis de código malicioso, tan sólo salta una alarma de 61 motores de búsqueda.

- No se detectan actividades automáticas dentro de la aplicación del tipo mensajes automáticos o llamadas automáticas.

- La aplicación no cumple con el reglamento RGPD del 25 de mayo del 2018, y no se informa al usuario del uso de sus datos privados.

Estas conclusiones, son en parte, lo que se mostrará en el informe final.

6.3 Reporte del informe

6.3.1 Contenido del informe

Una vez realizadas las pruebas específicas para el análisis de la aplicación móvil y tras sacar unas primeras conclusiones, es el momento de realizar el informe final. Éste debe ser tan simple y directo como sea posible, facilitando la información más relevante del estudio y mostrando como se ha llegado a grandes rasgos a éstos resultados.

Éste informe de auditoría dispondrá de los elementos fundamentales de una auditoría de seguridad que a su vez, éste esquema básico, está también relacionado con un informe forense sencillo.

En nuestro caso serán los siguientes cuatro puntos:

- Introducción: Breve descripción del documento.

- Resumen ejecutivo: Es recomendable mostrar de un vistazo general unas primeras conclusiones del informe, destacando tanto algunos de los aspectos negativos como también algún aspecto positivo.

- Metodología usada: En éste punto se mostrará una breve explicación de la metodología usada. Qué herramientas se han usado para llevar a cabo el estudio. También se informará de cualquier sistema de identificación del caso hallado así como su nivel de criticidad de actuación. En nuestro caso, además, se usará un pequeño sistema de puntualización de criticidad de forma visual para el usuario.

- Evidencias o constataciones: Se mostrará en formato tabla y de forma muy visual las evidencias encontradas.

- Recomendaciones: Éste será el último punto del informe donde se indicarán las posibles acciones a seguir para solventar las posibles evidencias de mal funcionamiento o vulnerabilidades.

6.3.2 Informe final

1. Descripción

Éste documento constata el análisis realizado sobre la aplicación *TheAndroidSeek*. Se han analizado, mediante herramientas de análisis forenses y de análisis de vulnerabilidades, las políticas de seguridad, las vulnerabilidades, las características principales y el código de la aplicación. Se ha contrastado el documento *OWASP Top 10 2016*, última versión conocida del documento destinado a tener las aplicaciones móviles seguras.

2. Resumen Ejecutivo

En el presente documento se mostrarán características poco recomendables para la publicación de ésta aplicación, tales como, código y características no actualizadas a entornos y funciones actuales, escasa información sobre las políticas de seguridad y privacidad del uso de la aplicación o bien permisos innecesarios y de riesgo elevado.

Mencionar que, tras interactuar y revisar el código, se puede constatar que la aplicación, no está destinada para fines poco éticos y es una aplicación de utilidad pero bajo la confianza del buen hacer de los usuarios.

3. Metodología usada

En primer lugar se realizará un análisis a nivel de usuario en dos entornos controlados, uno físico y otro virtual, mediante un dispositivo móvil y una virtualización *AVG* vía *Android Studio*. Se interactuará en ambos casos con todas las funciones del aplicativo.

En segundo lugar se realizarán técnicas de ingeniería inversa para poder desglosar el ejecutable de forma que se puedan cotejar datos sobre el aplicativo y realizar un estudio del código. Estas técnicas se realizarán en dos caminos, uno con un entorno de laboratorio usando una imagen de *Linux*, versión *Santoku*, dónde se usará en gran medida la herramienta *Androguard* y en concreto su utilidad *Androlyze* para poder analizar mediante *shell* el *apk*. Posteriormente mediante *dex2jar* y *JD-GUI*, se extraerá con el

primero el código de tal manera que lo podremos leer con el segundo. En el segundo camino aprovecharemos las herramientas online *VirusTotal* y *ApkScan* para complementar éste análisis.

Finalmente, y en tercer lugar, con las mismas herramientas *VirusTotal* y *ApkScan* se realizará un análisis de código malicioso y posibles funcionamientos erróneos.

Esto se basa en el siguiente modelo de puntuación según los casos encontrados:

id	Nivel	Explicación
1	A título informativo en éste momento.	Es recomendable que sea gestionado en una actualización planificada y no es recomendable que sea ignorado. A nivel de usuario no es importante.
2	Ligeramente Importante	Ha de ser gestionado en la próxima actualización planificada, pero no ha de ser ignorado. A nivel de usuario es poco importante.
3	Moderadamente importante	Ha de ser gestionado en la próxima actualización planificada. A nivel de usuario es importante.
4	Importante	Se ha de resolver lo antes posible. A nivel de usuario es muy importante.
5	Crítico	Necesita una resolución inmediata con carácter urgente. A nivel de usuario es de alta gravedad.

4. Constataciones

Caso	id	Puntuación usuario
Código y funcionalidades sin actualizar que pueden provocar incompatibilidades con algunas versiones de Android y algunos dispositivos	4	
Tras el envío de coordenadas por SMS, el teléfono no registra en ningún lado éste envío, quedado opaco al usuario.	5	
Solicitud de permisos innecesarios	2	
Código en desuso y que no es relevante para el funcionamiento del aplicativo	1	
La aplicación almacena la información que muestra en el propio código en una estructura interna de datos.	3	
La aplicación no cumple con el reglamento RGPD del 25 de mayo del 2018, y no se informa al usuario del uso de sus datos privados.	5	

A nivel de usuario se valoraría el global de la aplicación: 

5. Recomendaciones

Tras lo mostrado en el presente documento, se recomienda tomar las siguientes acciones:

- Incorporar con carácter inmediato un texto legal que cumpla con la normativa *RGPD*.
- Adecuar en la medida de lo posible el código para todos los dispositivos móviles y versiones *Android*.
- Adecuar el código con carácter inmediato para que el usuario tenga un mayor control sobre los SMS enviados desde la aplicación.
- La versión final de la aplicación debe ser totalmente transparente para no confundir su uso con usos de carácter delictivo.
- Reestructuración de forma más actual y más recomendada el almacenaje de datos a mostrar.

7. Conclusiones

Los ataques a dispositivo móviles se encuentran en constante crecimiento sin una visión clara que ponga freno a los mismos. El gran volumen de móviles en activo, el elevado uso que se hace de los mismos y la gran cantidad de información personal que contienen, los convierten en un objetivo potencial para los ciberdelincuentes.

Se concluye que, a pesar de disponer de excesiva información en Internet sobre seguridad en dispositivos móviles y de instrucciones sobre buenas prácticas en el uso de los mismos, este tipo de información no llega correctamente a los usuarios, ya que, su lenguaje específico dificulta tanto la comprensión como la atención. Ocurre un caso similar al de los textos legales, unos textos que no aportan nada al usuario y que tan sólo sirven para salvaguardar el interés empresarial.

Las nuevas tecnologías evolucionan exponencialmente y el resto de organizaciones deben adaptarse e incluso adelantarse a éstos hechos, es decir, tanto educación, como cultura, como leyes y normativas deben entender el estado actual y a la sociedad, en el entorno de las nuevas tecnologías, para así, poder llegar correctamente a los usuarios.

Se ha comprobado que, por muy buenas maneras que tengan los desarrolladores, el tipo de uso que hace un usuario de una aplicación móvil, puede ser causante de una vulneración de la seguridad. Con lo cual, las aplicaciones deberían de estar de alguna manera certificadas para la correcta información del usuario.

En definitiva, se evidencia que se está presentando un cambio social, que actualmente el cambio ya se encuentra en la sociedad, que hay riesgos en seguridad para los usuarios, y todas las vertientes deben adaptarse a ésta tendencia.

8. Glosario

Gesture Builder: herramienta para desarrolladores que sirve para gestionar eventos de gestos, con la funcionalidad que mediante gestos se puedan realizar interacciones.

NFC: (*Near Field Communication*): tecnología inalámbrica que sirve para realizar pagos mediante el teléfono móvil.

SIP: (*Session Initiation Protocol*) o bien en castellano, protocolo de inicio de sesión, es un protocolo que tiene como finalidad ser un estándar para la gestión de sesiones interactivas dónde intervengan elementos multimedia.

VOIP: Protocolo de internet o voz. Recursos que permiten que las señales de voz viajen por internet.

Dalvik: Máquina virtual que utiliza la plataforma para dispositivos móviles *Android.*

Phishing: Engaño al usuario mediante ingeniería social.

Malware: Programa malicioso.

SHA-1: Familia de funciones hash publicadas por NIST. Destinado para funciones de encriptación.

Framework: Entorno de trabajo, conjunto estandarizado de criterios para resolver un problema.

IDE: (*Integrated Development Enviaronment*) aplicación informática que sirve a los desarrolladores para realizar sus funciones de programación.

Sql-lite: Sistema de gestión de base de datos.

Shell: Intérprete de comandos.

MD5: Algoritmo de reducción criptográfico.

Bot: En castellano, robot, se trata de un programa informático para automatizar funciones de usuario.

9. Bibliografía

Enlaces Información TFM

[1] Wikipedia – Telefonía móvil.

https://es.wikipedia.org/wiki/Telefon%C3%ADa_m%C3%B3vil

[2] Wikipedia – Teléfonos inteligentes.

https://es.wikipedia.org/wiki/Tel%C3%A9fono_inteligente

[3] Blog – Historia de la informática – Historia de los smartphones

https://histinf.blogs.upv.es/2012/12/03/smartphones/

[4] Xataka móvil – Historia de los smartphones

https://www.xatakamovil.com/n/la-historia-del-smartphone-narrada-por-sus-hitos-del-salto-a-la-pantalla-tactil-a-tener-todos-los-gadgets-en-uno

[5] Blog - smartphone avance tecnológico

http://smartphoneavancetecnologico.blogspot.com/p/historia-y-evolucion-del-smartphone.html

[6] Statista – Base de datos estadística - Estadísticas teléfonos inteligentes

https://es.statista.com/estadisticas/636569/usuarios-de-telefonos-inteligentes-a-nivel-mundial--2019/

[6] Statista – Base de datos estadística - Ventas teléfonos inteligentes

https://es.statista.com/estadisticas/521667/numero-de-smartphones-vendidos-en-el-mundo-al-usuario-final/

[7] Comercios Electrónicos – Estadísticas smartphones

https://www.comercios-electronicos.com/estadisticas-uso-movil-2018-como-afectara-a-tu-negocio-y-lo-que-debes-saber-sobre-las-app-para-el-futuro-tus-ventas/

[9] El país – Actualidad tecnológica - Información Mobile Congress

https://elpais.com/tecnologia/2018/02/27/actualidad/1519725291_071783.html

[10] Wikipedia – Sistemas operativos móviles

https://es.wikipedia.org/wiki/Sistema_operativo_m%C3%B3vil

[11] Wikipedia – Android

https://es.wikipedia.org/wiki/Android

[12] Xataka móvil – Noticias sistema operativo Android

https://www.xatakamovil.com/sistemas-operativos/asi-como-android-se-ha-comido-mercado-diez-anos

[13] Xataka móvil – Historia sistema operativo Android

https://www.xatakandroid.com/sistema-operativo/historia-y-evolucion-de-android-como-un-sistema-operativo-para-camaras-digitales-acabo-conquistando-los-moviles

[14] Blog – Historia de la informática – Información Android

https://histinf.blogs.upv.es/2012/12/14/android/

[14] Android Authority – Historia de Android

https://www.androidauthority.com/history-android-os-name-789433/

[15] Wikipedia - iOS

https://es.wikipedia.org/wiki/IOS#Seguridad

[16] Statista – Base de datos estadística – Ventas Apple

https://es.statista.com/estadisticas/473921/ventas-apple-ios-espana/

[16] Wikipedia – Windows Phone

https://es.wikipedia.org/wiki/Windows_Phone

[17] Xataka Moviles – Final de Windows Phone

https://www.xataka.com/moviles/windows-10-mobile-dira-adios-definitivamente-diciembre-2019

[18] Xataka Moviles – Final de Windows Phone

https://www.xatakamovil.com/sistemas-operativos/windows-10-mobile-tiene-fecha-para-su-fin-soporte-actualizaciones-acabaran-diciembre

[19] Blog facilethings – Sobrecarga de información

https://facilethings.com/blog/es/information-overload

[20] My computer – Problemas de los smartphones

https://www.muycomputer.com/2018/07/14/smartphones-restaurados-problemas/

[21] Revista Semana – Enfermedades uso tecnología.

https://www.semana.com/tecnologia/tips/articulo/enfermedades-producidas-exceso-tecnologia/373968-3

[21] Empresa Blancco – Estadísticas seguridad móvil

https://www.blancco.com/resources/rs-state-of-mobile-device-repair-security/

[22] Statista – Base de datos estadística – Consumo y uso smartphones

https://es.statista.com/temas/4086/consumo-y-uso-de-smartphones-en-espana/

[23] Xataka – Historial smartphones

https://www.xataka.com/moviles/como-eran-los-sistemas-operativos-de-los-smartphones-de-2007

[24] Statcounter – Estadísticas móviles

http://gs.statcounter.com/os-market-share/mobile/worldwide

[25] Proteccion Online, Noticias - Privacidad

http://www.protecciononline.com/%C2%BFque-pasa-con-tu-privacidad-cada-vez-que-usas-tu-smartphone/

[26] Xataka - Privacidad

https://www.xataka.com/privacidad/tu-smartphone-te-delata-asi-siguen-tus-pasos-las-empresas-y-las-agencias-de-inteligencia

[27] Información Tecnológica FayerWayer – David Gerrold y la privacidad

https://www.fayerwayer.com/2018/03/david-gerrold-smartphone-privacidad/

[28] Redes Zone – Seguridad y privacidad

https://www.redeszone.net/2019/03/02/smartphone-maxima-seguridad-privacidad/

[29] Unocero - Fragmentación

https://www.unocero.com/entretenimiento/que-es-la-fragmentacion-en-android-y-por-que-es-dificil-terminar-con-ella/

[30] La Vanguardia – Divulgación seguridad Incibe

https://www.lavanguardia.com/vida/20190311/46971462211/el-incibe-lanza-una-campana-de-concienciacion-sobre-los-riesgos-de-internet.html

[31] Oficina Seguridad Internauta - Privacidad

https://www.osi.es/es/actualidad/blog/2018/10/24/tecnologias-emergentes-y-privacidad-que-debemos-hacer

[32] Oficina Seguridad Internauta – Buenas practicas

https://www.osi.es/es/actualidad/blog/2018/10/10/tu-tambien-puedes-fomentar-entre-tus-conocidos-buenas-practicas-de

[33] Oficina Seguridad Internauta – Puesta a punto móvil

https://www.osi.es/es/actualidad/blog/2018/08/29/puesta-punto-de-tu-movil

[34] Oficina Seguridad Internauta – Ciberseguridad Noticias

https://www.osi.es/es/actualidad/blog/2018/12/05/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se-deben-errores

[35] Oficina Seguridad Internauta – Ciberseguridad Noticias

https://www.osi.es/es/actualidad/blog/2018/11/07/te-fias-del-dispositivo-de-tu-amigo

[36] Oficina Seguridad Internauta – Ciberseguridad Noticias, pagos con móvil

https://www.osi.es/es/actualidad/blog/2018/06/20/pagos-con-el-movil-lo-que-necesitas-saber

[37] Oficina Seguridad Internauta – Ciberseguridad Noticias

https://www.osi.es/es/actualidad/blog/2018/05/23/que-informacion-se-oculta-detras-de-una-foto

[38] Kaspersky – Noticias – Seguridad Móviles

https://latam.kaspersky.com/resource-center/threats/mobile

[39] Kaspersky – Noticias – Ataques SMS

https://latam.kaspersky.com/resource-center/threats/sms-attacks

[40] Kaspersky – Noticias – Seguridad Móviles

https://latam.kaspersky.com/resource-center/preemptive-safety/tips-for-mobile-security-smartphone

[41] Incibe - Vulnerabilidades

https://www.incibe-cert.es/alerta-temprana/vulnerabilidades

[42] Wikipedia - Vulnerabilidades

https://es.wikipedia.org/wiki/Vulnerabilidad#En_informática

[43] Centro Criptográfico Nacional – Informe Anual 2018

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3464-ccn-cert-ia-04-19-informe-anual-2018-dispositivos-moviles/file.html

[44] Secure List – Evolución del malware 2018

https://securelist.lat/mobile-malware-evolution-2018/88378/

[45] Kaspersky – Noticias – Seguridad Móviles - Monitor

https://encyclopedia.kaspersky.es/knowledge/monitor/

[46] StackExchange – Reporte Auditoria

https://security.stackexchange.com/questions/29642/what-should-a-security-audit-report-include

[47] Pentest – Reporte Auditoria

http://www.pentest-standard.org/index.php/Reporting

[48] OWASP - Proyecto abierto de seguridad de aplicaciones web

https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Mobile_Threat_Model#Controls

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Mobile_Threat_Model#Controls

[49] e-book - Mobile Application Penetration Testing-

https://books.google.es/books?id=Y0XiCwAAQBAJ&pg=PA136&lpg=PA136&dq=androlyze+all&source=bl&ots=ZmzGt-50qP&sig=ACfU3U2lpYNUvWSZuuJ3ZquGoT9JipiwZQ&hl=es&sa=X&ved=2ahUKEwjNqNGH88LiAhXd6eAKHfZ4BTIQ6AEwCHoECAkQAQ#v=onepage&q=androlyze%20all&f=false

[50] Documentación androguard

https://buildmedia.readthedocs.org/media/pdf/androguard/latest/androguard.pdf

[51] Hacking Ético – Auditar app móviles

https://hacking-etico.com/2016/02/25/auditando-aplicaciones-en-android/

[52] Incibe – Herramientas forenses para móviles

https://www.incibe-cert.es/blog/herramientas-forense-moviles

https://www.incibe-cert.es/blog/utilidades-para-analizar-apks

[53] Androguard – Información uso androguard

https://androguard.readthedocs.io/en/latest/intro/gettingstarted.html

[54] Santoku-Linux – Guía

http://santoku-linux.com/howto/installing-santoku/installing-santoku-in-a-virtual-machine/

[55] Technotalkative – Guía ingeniaría inversa

http://www.technotalkative.com/part-1-reverse-engineering-using-androguard/

[56] Incibe – Desarrollo seguro app

https://www.incibe-cert.es/blog/desarrollo-seguro-de-aplicaciones-para-dispositivos-moviles

[57] Android Spain - Fragmentación

https://androidspain.es/que-es-la-fragmentacion-de-android/

[58] Kaspersky – Noticias – Seguridad Móviles - Monitor

https://encyclopedia.kaspersky.es/knowledge/risktool/

[59] Welivesecurity – Noticias – Seguridad Móviles - Malware

https://www.welivesecurity.com/la-es/2017/11/15/malware-multiples-etapas-de-ejecucion-google-play/

[60] Universidad de San Juan – Abstract Guía

http://www.unsj.edu.ar/unsjVirtual/comunicacion/seminarionuevastecnologias/wp-content/uploads/2015/06/06_Control-de-lectura-Abstract1.pdf

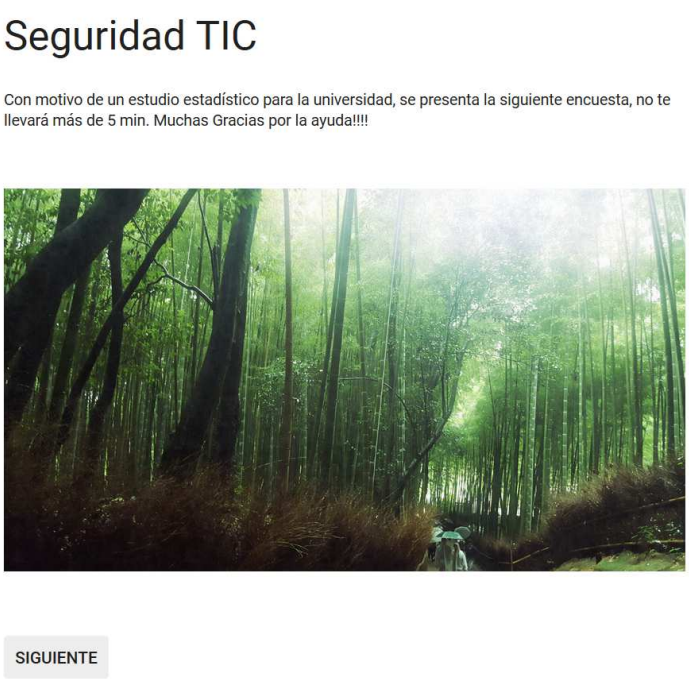
[61] UOC – Material de las asignaturas:

- Análisis Forense
- Auditoria Técnica

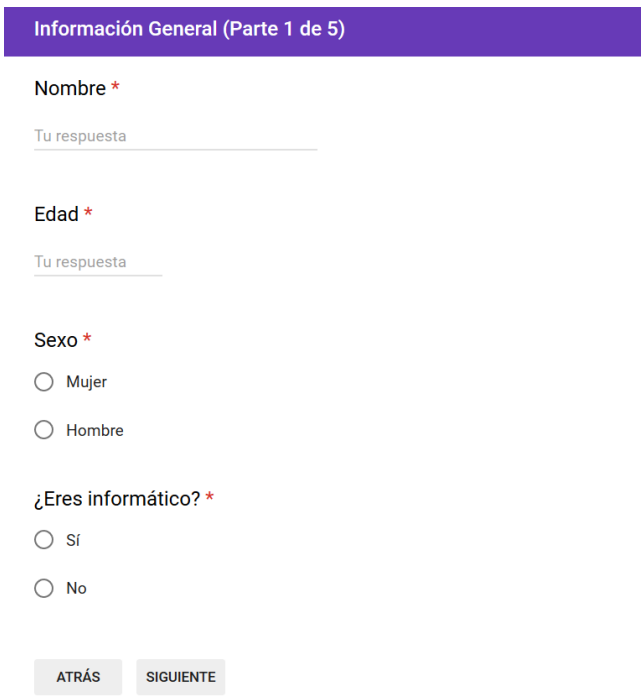
10. Anexos

Anexo 1

La encuesta empieza con una breve presentación y agradecimiento por realizarla.

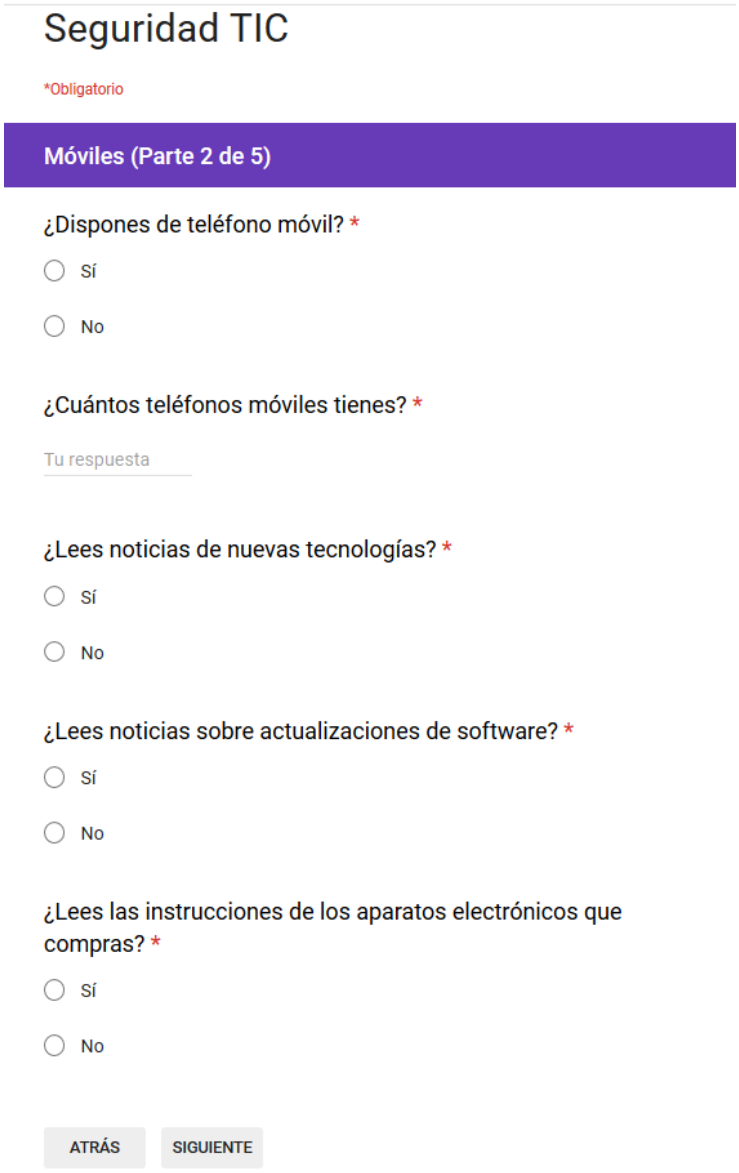


A continuación se solicitan datos generales. Se solicita un nombre para tener, junto a la fecha y hora de realización, un posible id. Mencionar que no se solicitan nombres ni apellidos para que la encuesta sea totalmente anónima. Tampoco se registran datos de usuario de *Google* ni IP del usuario.



El siguiente sector de preguntas se encuentran relacionadas con la tecnología móvil.

Destacar que, todos los campos marcados en asterisco, son preguntas obligatorias. En éste sector, si el usuario no dispone de teléfonos móviles, al cambiar de sector la encuesta queda finalizada para ese usuario, ya que, carece de sentido que siga respondiendo a preguntas sobre uso de teléfonos móviles y aplicaciones.



El siguiente sector de preguntas serán sobre aplicaciones móviles, cómo interactúan los usuarios al elegir una aplicación para usar.

Seguridad TIC

*Obligatorio

Aplicaciones (Parte 3 de 5)

¿Te bajas aplicaciones de la Store de tu teléfono móvil? *

- Sí
- No

¿Lees comentarios sobre la aplicación antes de bajarla?

- Sí
- No

¿Lees los permisos que necesitan las aplicaciones antes de aceptarlas?

- Sí
- No

¿Sueles rechazar los permisos?

- Nunca
- Casi nunca
- A veces
- Casi siempre
- Siempre

¿Lees el texto legal de las aplicaciones antes de usarla?

- Sí
- No

¿Sueles rechazar el texto legal?

- Nunca
- Casi nunca
- A veces
- Casi siempre
- Siempre

¿Te bajas aplicaciones móviles fuera de la tienda oficial? *

- Sí
- No

¿Dispones de antivirus en el móvil? *

- Sí
- No

ATRÁS SIGUIENTE

A continuación, el sector de preguntas es sobre mensajería instantánea. La última pregunta de éste sector, es una pregunta de control, poco relevante para los resultados de la encuesta pero necesaria para detectar posibles encuesta realizadas de forma poco ética.

Mensajería instantánea (Parte 4 de 5)

¿Tienes aplicación de mensajería instantánea? *
- Sí
- No

¿Confías en cualquier mensaje que recibes desde tu aplicación de mensajería instantánea? Por ejemplo, un enlace a una página web recibido por whatsapp
- Sí
- No

¿Hablas con desconocidos en tu aplicación de mensajería instantánea?
- Sí
- No

¿Tienes correo electrónico? *
- Sí
- No

¿Confías en todos los mensajes de correo electrónico que recibes?
- Sí
- No

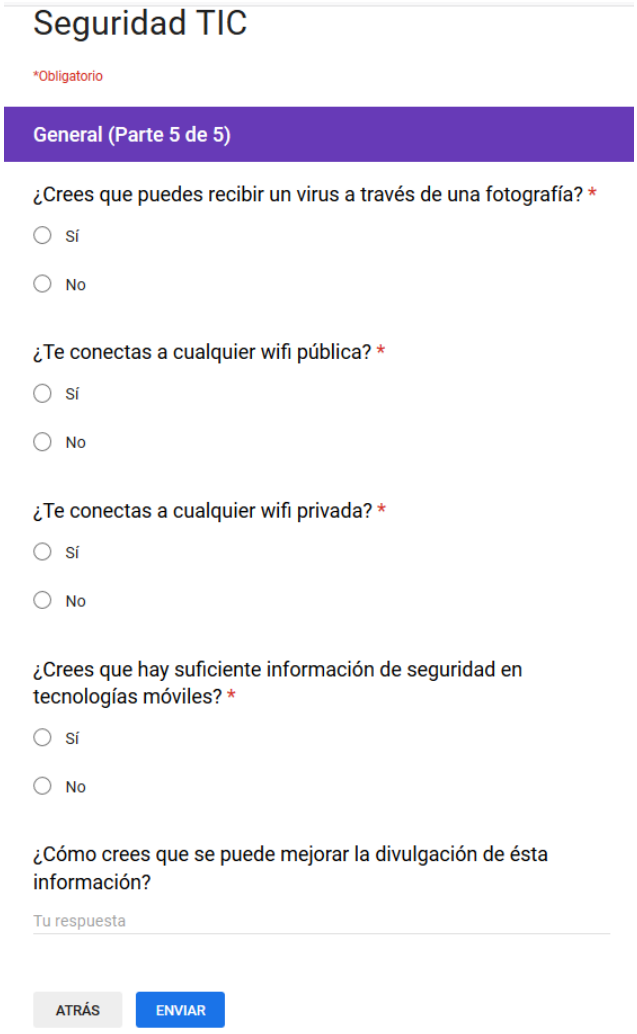
Recibes un correo electrónico de tu compañía eléctrica, ¿analizas el remitente?
- Sí
- No

¿Sabrías explicar que es el phishing? *
- Sí
- No

En caso afirmativo anterior, ¿qué es?
- Técnica para leer el tráfico de datos
- Engaño al usuario mediante ingenieria social
- Tipo de inyección SQL
- Acoso a través de redes sociales
- Envío de cadenas de mensaje a través de mensajería instantánea

ATRÁS SIGUIENTE

Finalizamos con un sector de preguntas generales sobre seguridad TIC. La última pregunta, opcional, se solicita su opinión sobre la forma en que se divulga la información de seguridad TIC.

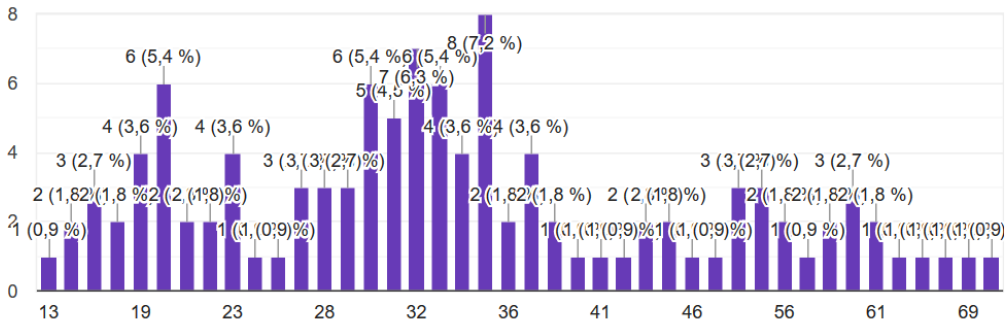


Anexo 2

A continuación mostraremos todas las estadísticas sobre la encuesta realizada.

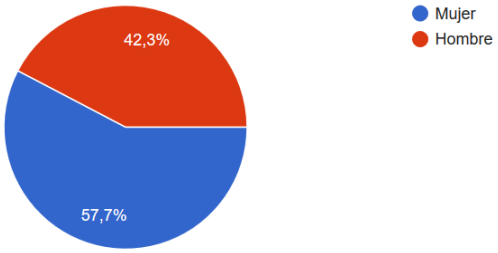
Edad

111 respuestas



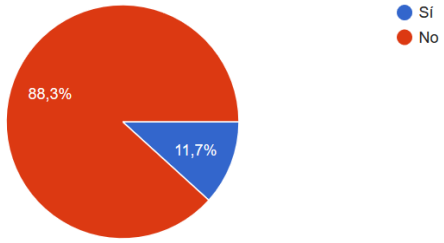
Sexo

111 respuestas



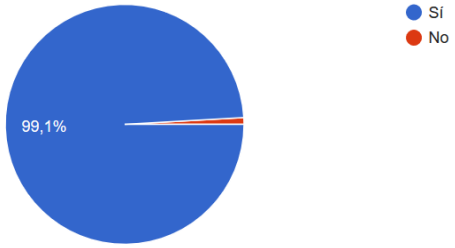
¿Eres informático?

111 respuestas



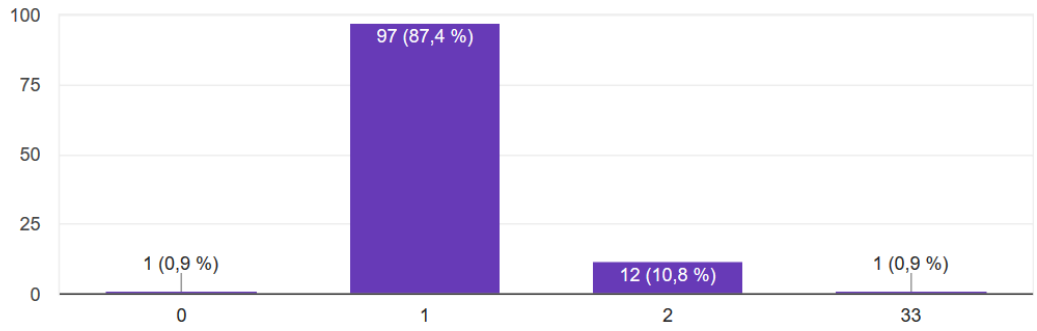
¿Dispones de teléfono móvil?

111 respuestas



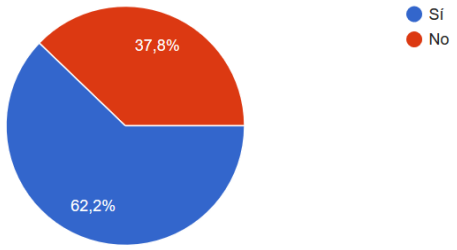
¿Cuántos teléfonos móviles tienes?

111 respuestas



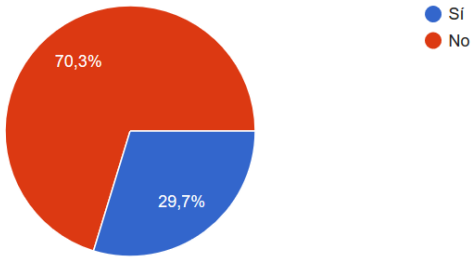
¿Lees noticias de nuevas tecnologías?

111 respuestas



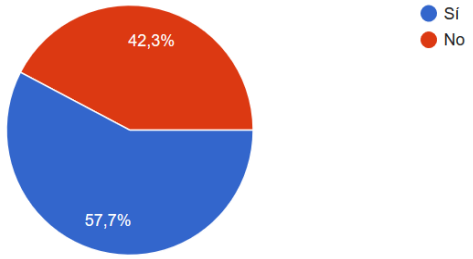
¿Lees noticias sobre actualizaciones de software?

111 respuestas



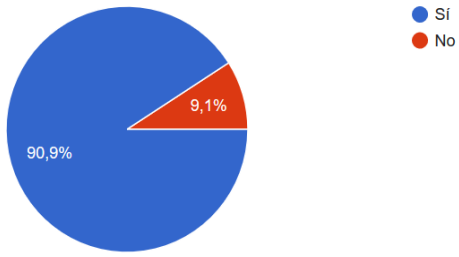
¿Lees las instrucciones de los aparatos electrónicos que compras?

111 respuestas



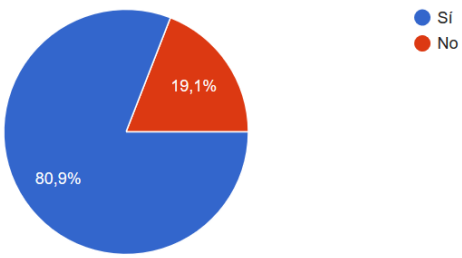
¿Te bajas aplicaciones de la Store de tu teléfono móvil?

110 respuestas



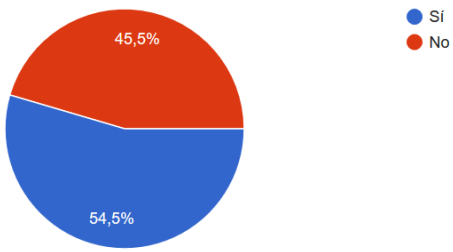
¿Lees comentarios sobre la aplicación antes de bajarla?

110 respuestas



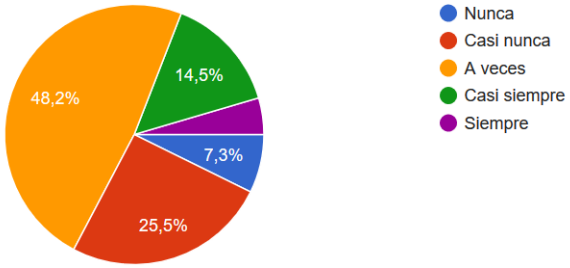
¿Lees los permisos que necesitan las aplicaciones antes de aceptarlas?

110 respuestas



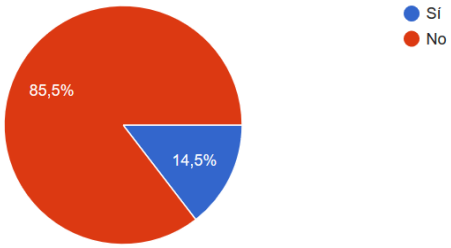
¿Sueles rechazar los permisos?

110 respuestas



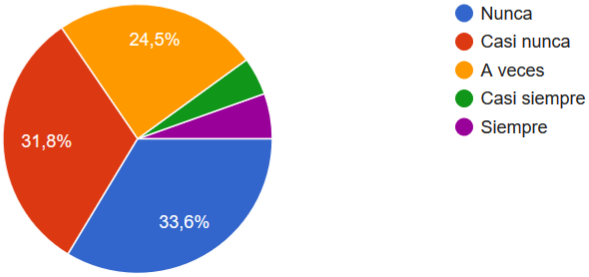
¿Lees el texto legal de las aplicaciones antes de usarla?

110 respuestas



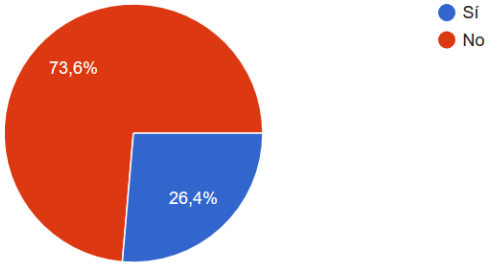
¿Sueles rechazar el texto legal?

110 respuestas



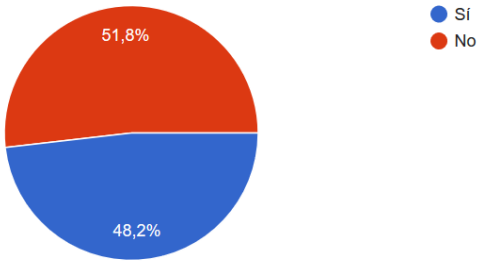
¿Te bajas aplicaciones móviles fuera de la tienda oficial?

110 respuestas



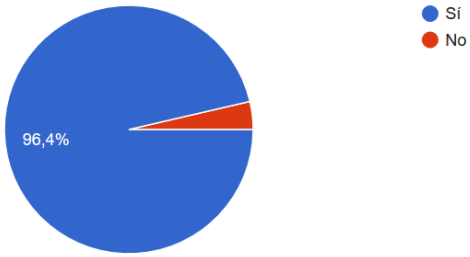
¿Dispones de antivirus en el móvil?

110 respuestas



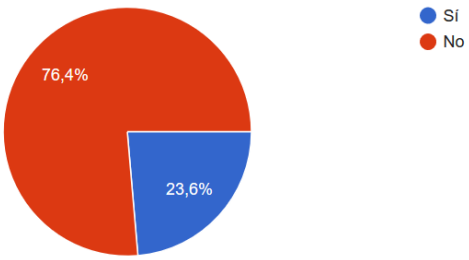
¿Tienes aplicación de mensajería instantánea?

110 respuestas



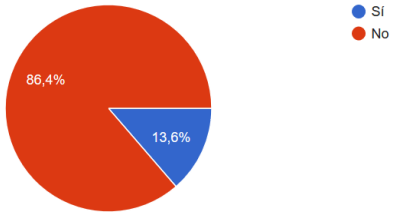
¿Confías en cualquier mensaje que recibes desde tu aplicación de mensajería instantánea? Por ejemplo, un enlace a una página web recibido por whatsapp

110 respuestas



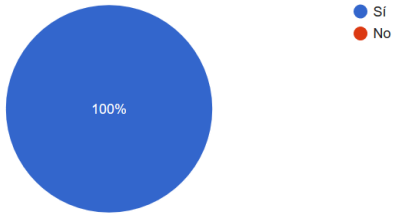
¿Hablas con desconocidos en tu aplicación de mensajería instantánea?

110 respuestas



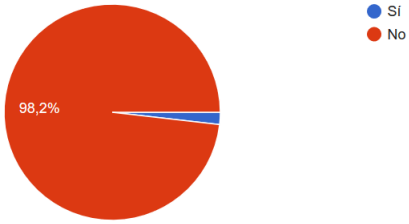
¿Tienes correo electrónico?

110 respuestas



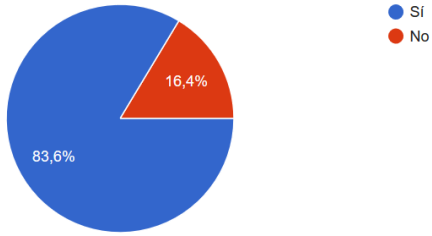
¿Confías en todos los mensajes de correo electrónico que recibes?

110 respuestas



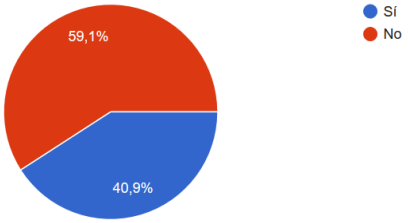
Recibes un correo electrónico de tu compañía eléctrica, ¿analizas el remitente?

110 respuestas



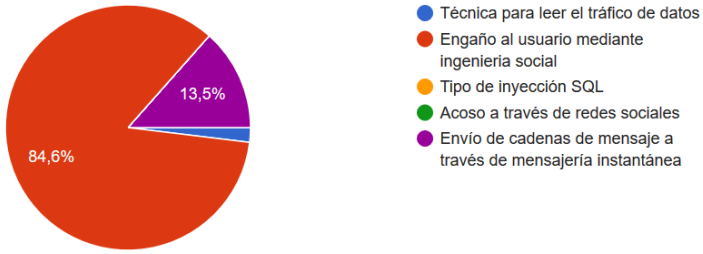
¿Sabrías explicar que es el phishing?

110 respuestas



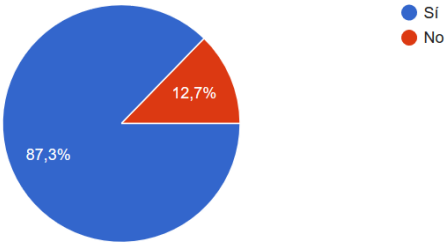
En caso afirmativo anterior, ¿qué es?

52 respuestas



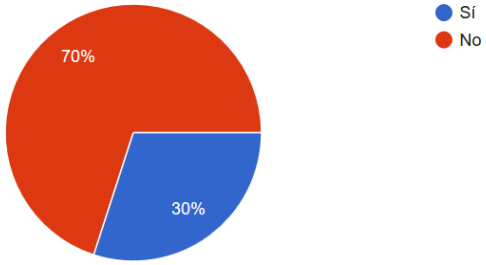
¿Crees que puedes recibir un virus a través de una fotografía?

110 respuestas



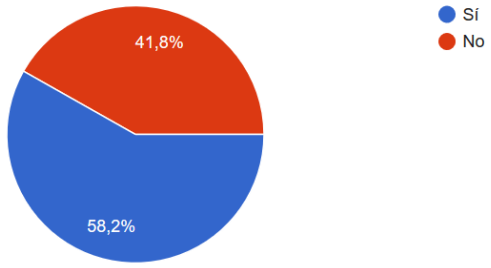
¿Te conectas a cualquier wifi pública?

110 respuestas



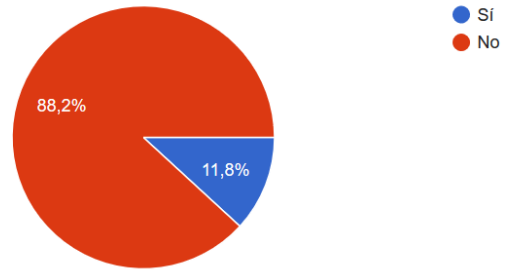
¿Te conectas a cualquier wifi privada?

110 respuestas



¿Crees que hay suficiente información de seguridad en tecnologías móviles?

110 respuestas



Finalmente se ha preguntado a los encuestados como creen que se podría mejorar la divulgación de la información sobre la seguridad TIC. Se mostraran las respuestas textuales, evidentemente sin modificar, de los encuestados que han aportado información.

id	Mensaje
1	Con avisos mediante pantallas emergentes
2	A través de los medios de comunicación
3	Campañas informativa vía postal
4	A través de las redes socislies
5	Hola!! Pues con mas informacion mas resumida
6	Educación
7	En redes sociales
8	Con menos letra pequeña y siendo más claros, educando a la gente en general avisando de los riesgos reales.
9	Formaciones públicas (televisión, radio etc..) y desde pequeño cuando ya tienes acceso por cuenta propia a internet . El propio colegio debería tener una asignatura de informática más global que no solo sea utilizar el Paint o el Word
10	Que los propios proveedores (email, tiendas online, banca...) recuerden al usuario los riesgos que existen y cómo prevenirlos. Y mayores medios para instituciones gubernamentales como la GDT.
11	a traves de las redes sociales y tener mas conocimientos
12	Explicando los peligros a los usuarios a través de charlas gratuïtas o a través de su compañia teléfonica. Seria muy interesante que explicaran como funcionan los virus, como pueden acceder al dispositivo, como analizar el móbil, etc. Mayor información.
13	Quitando las cuentas nocivas
14	Mediante cursos en colegios / universidades.
15	Por wsp
16	A través de personas responsables y profesionales
17	Por whatsapp
18	Por noticias, haciendo los textos más leibles
19	Anuncios televisivos, informar en las redes sociales, etc...
20	Divulgacion en el colegio
21	Mostrar en medios convencionales
22	Anuncios en redes sociales como Facebook o Instagram
23	Exponiendola en redes sociales

24	Información más sencilla de entender
25	Haciendo muchísimas más campañas informativas de las que se hacen.
26	Tenint més informació del que estem fent servir
27	Se puede mejorar con piezas de vídeo donde se ve que pasa cuando te despistas, cuando confías sin leer y recibes un ataque qur te afecta al día a dia
28	Mediante bloqueos
29	Leer todos los mensajes importantes, a pesar de que sean muy largos :v
30	Explicando que supone una conexion y la informacion que se puede conseguir
31	Haciendo saber a los usuarios de los peligros que hay en internet
32	Por canals TV y Radio
33	En escuela, prensa y televisión, en informacions del mobil
34	Haciéndola más didáctica y comprensible para el público general y publicándola en sitios accesibles para mucha gente.
35	Haciéndolo con mensajes fáciles de entender
36	Pues en noticias y diàrios
37	Cuando compras el móvil podrían informarte de todos estos temas, o bien dándote la información por escrito.
38	Mejorar la seguridad
39	Con formación preventiva sobre compartir información, la privacidad y ejemplos reales
40	Con seguridad
41	Por prensa y radio
42	Con más información
43	Haciendo mas charlas explicando la importancia de la seguridad y demostrando la facilidad de infectar dispositivos
44	Redes sociales
45	Información menos técnica y con más consejos
46	Radio, television
47	Ampliandola
48	Comunicandola con sencillez

Anexo 3

```
In [40]: a.show()
FILES:
        res/color/common_signin_btn_text_dark.xml data -5da5936
        res/color/common_signin_btn_text_light.xml data -195a3be0
        res/drawable/common_signin_btn_icon_dark.xml data -1488c87f
        res/drawable/common_signin_btn_icon_light.xml data 338f70dc
        res/drawable/common_signin_btn_text_dark.xml data -7d3fd351
        res/drawable/common_signin_btn_text_light.xml data -4184042d
        res/layout/activity_main.xml data 18612a46
        res/layout/ajuda.xml data -35959688
        res/layout/cerca_lloc_interes.xml data -2cb64eb9
        res/layout/cerca_usuari.xml data -5347f652
        res/layout/custom_dialog.xml data -78fdcd8d
        res/layout/intro_coord.xml data 2f824d50
        res/layout/mapa_mostra_usuari_perdut.xml data -26c6cd95
        res/layout/noms_rutes_list.xml data -12c66cdd
        res/layout/noms_rutes_list_item.xml data 33066673
        res/layout/telefons.xml data -3d7a3cfb
        res/layout/telefons_item.xml data -3ab2b358
        res/layout/ubicacions_list.xml data -42b4c32a
        res/layout/ubicacions_list_item.xml data 37cf56eb
        res/menu/info_ubicacio_usuari.xml data 12e4bf4b
        res/menu/main.xml data -605d2293
        res/menu/menu_cerca_lloc.xml data 3720e05d
        res/menu/menu_cerca_usuari.xml data -41f87a94
        res/menu/menu_principal.xml data 58efe71
        AndroidManifest.xml data 6bb34312
        resources.arsc data 1fe89144
        res/drawable-hdpi/common_signin_btn_icon_disabled_dark.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced 6ba2f1d4
        res/drawable-hdpi/common_signin_btn_icon_disabled_focus_dark.9.png PNG image data, 72 x
72, 8-bit/color RGBA, non-interlaced 56aaa937
        res/drawable-hdpi/common_signin_btn_icon_disabled_focus_light.9.png PNG image data, 72 x
72, 8-bit/color RGBA, non-interlaced 56aaa937
        res/drawable-hdpi/common_signin_btn_icon_disabled_light.9.png PNG image data, 72 x 72,
8-bit/color RGBA, non-interlaced 6ba2f1d4
        res/drawable-hdpi/common_signin_btn_icon_focus_dark.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced 2dab6013
        res/drawable-hdpi/common_signin_btn_icon_focus_light.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced -43a0c3be
        res/drawable-hdpi/common_signin_btn_icon_normal_dark.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced 7ea98f7a
        res/drawable-hdpi/common_signin_btn_icon_normal_light.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced 6e1c464e
        res/drawable-hdpi/common_signin_btn_icon_pressed_dark.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced -5a8ad4a9
        res/drawable-hdpi/common_signin_btn_icon_pressed_light.9.png PNG image data, 72 x 72, 8-
bit/color RGBA, non-interlaced -47acb72c
        res/drawable-hdpi/common_signin_btn_text_disabled_dark.9.png PNG image data, 159 x 72,
8-bit/color RGBA, non-interlaced 17e0aaed
        res/drawable-hdpi/common_signin_btn_text_disabled_focus_dark.9.png PNG image data, 159 x
72, 8-bit/color RGBA, non-interlaced 6f060356
        res/drawable-hdpi/common_signin_btn_text_disabled_focus_light.9.png PNG image data, 159
x 72, 8-bit/color RGBA, non-interlaced 6f060356
        res/drawable-hdpi/common_signin_btn_text_disabled_light.9.png PNG image data, 159 x 72,
8-bit/color RGBA, non-interlaced 17e0aaed
        res/drawable-hdpi/common_signin_btn_text_focus_dark.9.png PNG image data, 159 x 72, 8-
bit/color RGBA, non-interlaced 6e5bd43
        res/drawable-hdpi/common_signin_btn_text_focus_light.9.png PNG image data, 159 x 72, 8-
bit/color RGBA, non-interlaced 2d40207c
        res/drawable-hdpi/common_signin_btn_text_normal_dark.9.png PNG image data, 159 x 72, 8-
bit/color RGBA, non-interlaced 7b28e132
        res/drawable-hdpi/common_signin_btn_text_normal_light.9.png PNG image data, 159 x 72, 8-
bit/color RGBA, non-interlaced -64829031
        res/drawable-hdpi/common_signin_btn_text_pressed_dark.9.png PNG image data, 159 x 72, 8-
bit/color RGBA, non-interlaced -d831bc
        res/drawable-hdpi/common_signin_btn_text_pressed_light.9.png PNG image data, 159 x 72,
8-bit/color RGBA, non-interlaced 632a426c
        res/drawable-hdpi/ic_launcher.png PNG image data, 72 x 72, 8-bit/color RGBA, non-
interlaced 4be4c32c
```

```
        res/drawable-hdpi/layout_menu.png PNG image data, 501 x 719, 8-bit/color RGB, non-
interlaced -53167eec
        res/drawable-hdpi/layout_menu2.png PNG image data, 501 x 719, 8-bit colormap, non-
interlaced 6d4c2ac3
        res/drawable-mdpi/common_signin_btn_icon_disabled_dark.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced 6adcd51a
        res/drawable-mdpi/common_signin_btn_icon_disabled_focus_dark.9.png PNG image data, 48 x
48, 8-bit/color RGBA, non-interlaced 2d69d04d
        res/drawable-mdpi/common_signin_btn_icon_disabled_focus_light.9.png PNG image data, 48 x
48, 8-bit/color RGBA, non-interlaced 2d69d04d
        res/drawable-mdpi/common_signin_btn_icon_disabled_light.9.png PNG image data, 48 x 48,
8-bit/color RGBA, non-interlaced 6adcd51a
        res/drawable-mdpi/common_signin_btn_icon_focus_dark.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced 373f3662
        res/drawable-mdpi/common_signin_btn_icon_focus_light.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced 2f93a4f5
        res/drawable-mdpi/common_signin_btn_icon_normal_dark.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced -2b705695
        res/drawable-mdpi/common_signin_btn_icon_normal_light.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced -fa36897
        res/drawable-mdpi/common_signin_btn_icon_pressed_dark.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced 59c4e5dc
        res/drawable-mdpi/common_signin_btn_icon_pressed_light.9.png PNG image data, 48 x 48, 8-
bit/color RGBA, non-interlaced -1a9fad69
        res/drawable-mdpi/common_signin_btn_text_disabled_dark.9.png PNG image data, 106 x 48,
8-bit/color RGBA, non-interlaced -1e92b075
        res/drawable-mdpi/common_signin_btn_text_disabled_focus_dark.9.png PNG image data, 106 x
48, 8-bit/color RGBA, non-interlaced 409d5a57
        res/drawable-mdpi/common_signin_btn_text_disabled_focus_light.9.png PNG image data, 106
x 48, 8-bit/color RGBA, non-interlaced 409d5a57
        res/drawable-mdpi/common_signin_btn_text_disabled_light.9.png PNG image data, 106 x 48,
8-bit/color RGBA, non-interlaced -1e92b075
        res/drawable-mdpi/common_signin_btn_text_focus_dark.9.png PNG image data, 106 x 48, 8-
bit/color RGBA, non-interlaced 22737634
        res/drawable-mdpi/common_signin_btn_text_focus_light.9.png PNG image data, 106 x 48, 8-
bit/color RGBA, non-interlaced -4002d435
        res/drawable-mdpi/common_signin_btn_text_normal_dark.9.png PNG image data, 106 x 48, 8-
bit/color RGBA, non-interlaced -4ddc483
        res/drawable-mdpi/common_signin_btn_text_normal_light.9.png PNG image data, 106 x 48, 8-
bit/color RGBA, non-interlaced 60f83821
        res/drawable-mdpi/common_signin_btn_text_pressed_dark.9.png PNG image data, 106 x 48, 8-
bit/color RGBA, non-interlaced 1e60cd2
        res/drawable-mdpi/common_signin_btn_text_pressed_light.9.png PNG image data, 106 x 48,
8-bit/color RGBA, non-interlaced -6298d5b5
        res/drawable-mdpi/ic_launcher.png PNG image data, 48 x 48, 8-bit/color RGBA, non-
interlaced 2c7af1de
        res/drawable-xhdpi/common_signin_btn_icon_disabled_dark.9.png PNG image data, 96 x 96,
8-bit/color RGBA, non-interlaced 6d7b950
        res/drawable-xhdpi/common_signin_btn_icon_disabled_focus_dark.9.png PNG image data, 96 x
96, 8-bit/color RGBA, non-interlaced 50b8341e
        res/drawable-xhdpi/common_signin_btn_icon_disabled_focus_light.9.png PNG image data, 96
x 96, 8-bit/color RGBA, non-interlaced 50b8341e
        res/drawable-xhdpi/common_signin_btn_icon_disabled_light.9.png PNG image data, 96 x 96,
8-bit/color RGBA, non-interlaced 6d7b950
        res/drawable-xhdpi/common_signin_btn_icon_focus_dark.9.png PNG image data, 96 x 96, 8-
bit/color RGBA, non-interlaced -63df2a9c
        res/drawable-xhdpi/common_signin_btn_icon_focus_light.9.png PNG image data, 96 x 96, 8-
bit/color RGBA, non-interlaced 28715210
        res/drawable-xhdpi/common_signin_btn_icon_normal_dark.9.png PNG image data, 96 x 96, 8-
bit/color RGBA, non-interlaced -1ac9e69d
        res/drawable-xhdpi/common_signin_btn_icon_normal_light.9.png PNG image data, 96 x 96, 8-
bit/color RGBA, non-interlaced -35dd11af
        res/drawable-xhdpi/common_signin_btn_icon_pressed_dark.9.png PNG image data, 96 x 96, 8-
bit/color RGBA, non-interlaced 5c42b01f
        res/drawable-xhdpi/common_signin_btn_icon_pressed_light.9.png PNG image data, 96 x 96,
8-bit/color RGBA, non-interlaced 3a699d26
        res/drawable-xhdpi/common_signin_btn_text_disabled_dark.9.png PNG image data, 211 x 96,
8-bit/color RGBA, non-interlaced -aeda8df
        res/drawable-xhdpi/common_signin_btn_text_disabled_focus_dark.9.png PNG image data, 211
x 96, 8-bit/color RGBA, non-interlaced -73c08b4c
        res/drawable-xhdpi/common_signin_btn_text_disabled_focus_light.9.png PNG image data, 211
x 96, 8-bit/color RGBA, non-interlaced -73c08b4c
        res/drawable-xhdpi/common_signin_btn_text_disabled_light.9.png PNG image data, 211 x 96,
8-bit/color RGBA, non-interlaced -aeda8df
```

```
        res/drawable-xhdpi/common_signin_btn_text_focus_dark.9.png PNG image data, 211 x 96, 8-
bit/color RGBA, non-interlaced 434d065d
        res/drawable-xhdpi/common_signin_btn_text_focus_light.9.png PNG image data, 211 x 96, 8-
bit/color RGBA, non-interlaced -69236a4b
        res/drawable-xhdpi/common_signin_btn_text_normal_dark.9.png PNG image data, 211 x 96, 8-
bit/color RGBA, non-interlaced -546db9ce
        res/drawable-xhdpi/common_signin_btn_text_normal_light.9.png PNG image data, 211 x 96,
8-bit/color RGBA, non-interlaced -b4418f8
        res/drawable-xhdpi/common_signin_btn_text_pressed_dark.9.png PNG image data, 211 x 96,
8-bit/color RGBA, non-interlaced 64d28972
        res/drawable-xhdpi/common_signin_btn_text_pressed_light.9.png PNG image data, 211 x 96,
8-bit/color RGBA, non-interlaced -26331827
        res/drawable-xhdpi/ic_launcher.png PNG image data, 96 x 96, 8-bit/color RGBA, non-
interlaced 2cbb3a81
        res/drawable-xxhdpi/ic_launcher.png PNG image data, 144 x 144, 8-bit/color RGBA, non-
interlaced 38954e74
        classes.dex Dalvik dex file version 035 -71b29e45
        META-INF/MANIFEST.MF ASCII text, with CRLF line terminators 36004600
        META-INF/CERT.SF ASCII text, with CRLF line terminators 61473469
        META-INF/CERT.RSA data 479315f9
PERMISSIONS:
        android.permission.ACCESS_FINE_LOCATION ['dangerous', 'fine (GPS) location', 'Access
fine location sources, such as the Global Positioning System on the phone, where available.
Malicious applications can use this to determine where you are and may consume additional
battery power.']
        android.permission.SEND_SMS ['dangerous', 'send SMS messages', 'Allows application to
send SMS messages. Malicious applications may cost you money by sending messages without your
confirmation.']
        com.google.android.providers.gsf.permission.READ_GSERVICES ['normal', 'Unknown
permission from android reference', 'Unknown permission from android reference']
        android.permission.READ_CONTACTS ['dangerous', 'read contact data', 'Allows an
application to read all of the contact (address) data stored on your phone. Malicious
applications can use this to send your data to other people.']
        android.permission.ACCESS_NETWORK_STATE ['normal', 'view network status', 'Allows an
application to view the status of all networks.']
        android.permission.ACCESS_COARSE_LOCATION ['dangerous', 'coarse (network-based)
location', 'Access coarse location sources, such as the mobile network database, to determine an
approximate phone location, where available. Malicious applications can use this to determine
approximately where you are.']
        android.permission.CALL_PHONE ['dangerous', 'directly call phone numbers', 'Allows an
application to initiate a phone call without going through the Dialer user interface for the
user to confirm the call being placed. ']
        android.permission.INTERNET ['dangerous', 'full Internet access', 'Allows an application
to create network sockets.']
        com.example.theandroidseek.permission.MAPS_RECEIVE ['normal', 'Unknown permission from
android reference', 'Unknown permission from android reference']
        android.permission.WRITE_EXTERNAL_STORAGE ['dangerous', 'modify/delete SD card
contents', 'Allows an application to write to the SD card.']
MAIN ACTIVITY:  com.example.theandroidseek.MainActivity
ACTIVITIES:
        com.example.theandroidseek.MainActivity {'action': [u'android.intent.action.MAIN'],
'category': [u'android.intent.category.LAUNCHER']}
        com.example.theandroidseek.CercaLlocInteres
        com.example.theandroidseek.CercaUsuari
        com.example.theandroidseek.Telefons
        com.example.theandroidseek.Ajuda
        com.example.theandroidseek.IntroCoord
        com.example.theandroidseek.MostrarUsuariPerdut
        com.example.theandroidseek.Ubicacions
        com.example.theandroidseek.NomsDeRutes
SERVICES:
RECEIVERS:
PROVIDERS:  []
```