Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Análisis del modelo de seguridad y propuesta de configuración segura para dispositivos Android

Grado en Ingeniería Mecánica

ALUMNO: Carlos Sánchez de Toca Rodríguez

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2018-2019

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Análisis del modelo de seguridad y propuesta de configuración segura para dispositivos Android

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

La seguridad informática es un asunto que ha ido adquiriendo especial importancia en las últimas décadas. Las medidas para proteger la información que los dispositivos electrónicos almacenan deben evolucionar a la misma velocidad con la que se descubren sus vulnerabilidades. Dada la relevancia de los *smartphones* en la vida cotidiana y profesional, es necesario reflexionar sobre si estos están protegidos de manera adecuada de las amenazas que hoy en día no dejan de aparecer.

En este TFG se analiza el modelo de seguridad del principal sistema operativo empleado en móviles: Android. A su vez, se estudian todas las medidas a implantar en un *smartphone* Xiaomi Mi A2 Lite para conseguir una configuración más segura y garante de la privacidad del usuario. Esta configuración segura se ha estudiado desde distintos puntos de vista, como el de la seguridad física, la seguridad en las redes de comunicaciones o en las aplicaciones.

Con el objetivo de validar dicha configuración, se estudian diversas aplicaciones utilizadas habitualmente en pruebas de seguridad. También se realiza una recopilación de buenas prácticas que minimizan la exposición del dispositivo. Finalmente, se exponen las conclusiones extraídas, así como unas líneas futuras que permitirían ampliar este trabajo, algunas de las cuales proponen extrapolar estas medidas a otros sistemas operativos o estudiar la protección de los emergentes dispositivos del llamado *Internet de las cosas.*

PALABRAS CLAVE

Android, seguridad, *smartphone*, privacidad, Google

AGRADECIMIENTOS

Me gustaría agradecer a todos los profesores, civiles y militares, el esfuerzo dedicado a mi formación, especialmente a mis tutores, que me han acompañado y apoyado durante esta última etapa en mi recorrido por la Escuela Naval Militar. También he de agradecer a mis compañeros de promoción su constante entusiasmo, que siempre me transmitieron y que hizo más llevaderos los momentos más agitados y difíciles.

No debo olvidar a mis compañeros de la C5 y C2, por aguantar los “Ok Google” y por prestarme sus teléfonos, sabiendo que posiblemente no volviesen a verlos. Por último, agradecer a mis padres la educación que me dieron y me ha permitido lograr mis objetivos hasta ahora.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto y motivación

No es disparatado imaginarse un *smartphone* o una tablet como pequeños ordenadores y, como tal, las amenazas a las que se enfrentan son, en muchos aspectos, parecidas. Existen amenazas a estos dispositivos tanto físicas como de software, pudiéndose comprometer la información que estos almacenan.

La rápida difusión que han sufrido *smartphones* y tablets junto con el colosal aumento de sus capacidades ha provocado que se hayan convertido en objetivo de los ciberdelincuentes. Estos ataques han aumentado de forma exponencial estos últimos años y se espera que esta tendencia continúe. Es por ello que la necesidad de mantener el *smartphone* seguro se ha vuelto una necesidad de primer orden.

El mercado de los *smartphones* no ha dejado de crecer desde su aparición. Según cifras de Ditrendia para 2017 [1], se estima que actualmente dos tercios de la población mundial ya disponen de estos dispositivos (4,9 mil millones de personas), encontrándose España en el top mundial con un 88% de usuarios móviles. Este mismo informe confirma que en 2016 las búsquedas en Internet realizadas desde *smartphones* superaron por primera vez las realizadas desde ordenadores y así se ha mantenido desde entonces. Se espera que el mercado de teléfonos inteligentes siga aumentando, aunque a menor ritmo que en años anteriores, como el del resto de dispositivos conectados o *wearables*, un 23% hasta alcanzar en 2021 los 16.000 millones y en 2025 se calcula un número superior a los 75.000 millones.

En el caso de las tablets, se observa un estancamiento de mercado desde 2015. La expansión de estos aparatos no ha sido tan grande ni tan global como los teléfonos inteligentes. La distribución de tablets a nivel mundial es muy heterogénea: por ejemplo, en China la cantidad de usuarios no alcanza el 2%, frente al 75% en España o el 66% de Australia [2]. En definitiva, las ventas de tablets siguen cayendo. En la realidad no han conseguido desbancar a los móviles, que en ocasiones son hasta más potentes y cómodos, ni tampoco a los ordenadores, que siguen teniendo más capacidad y más posibilidades que las tablets.

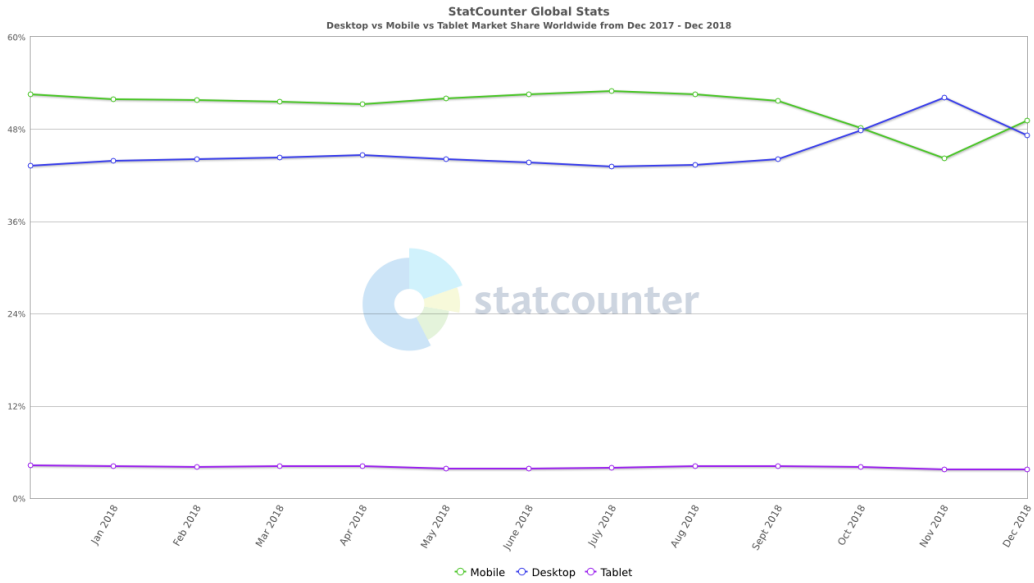

Figura 1-1 Gráfica comparativa del mercado de móviles, ordenadores y tablets en 2018 [2]

Debido a la mayoritaria presencia de los teléfonos inteligentes frente a las tablets (véase Figura 1-1), este TFG se centrará en el análisis de seguridad en móviles.

Existen multitud de fabricantes de *smartphones*, aunque la inmensa mayoría de ellos no cuenta con sistema operativo propio. Como se observa en la Figura 1-2, el sistema operativo líder en el mundo y por mucho es Android con más de un 70% de usuarios. IOS de *Iphone* aparece con algo más de un cuarto de los *smartphones* a nivel mundial, destacando en los países ricos del primer mundo como Noruega, Suecia, Suiza o Estados Unidos. El resto de sistemas operativos (SO) juntos apenas suman un 3%, no siendo ninguno de ellos predominante en ningún país.

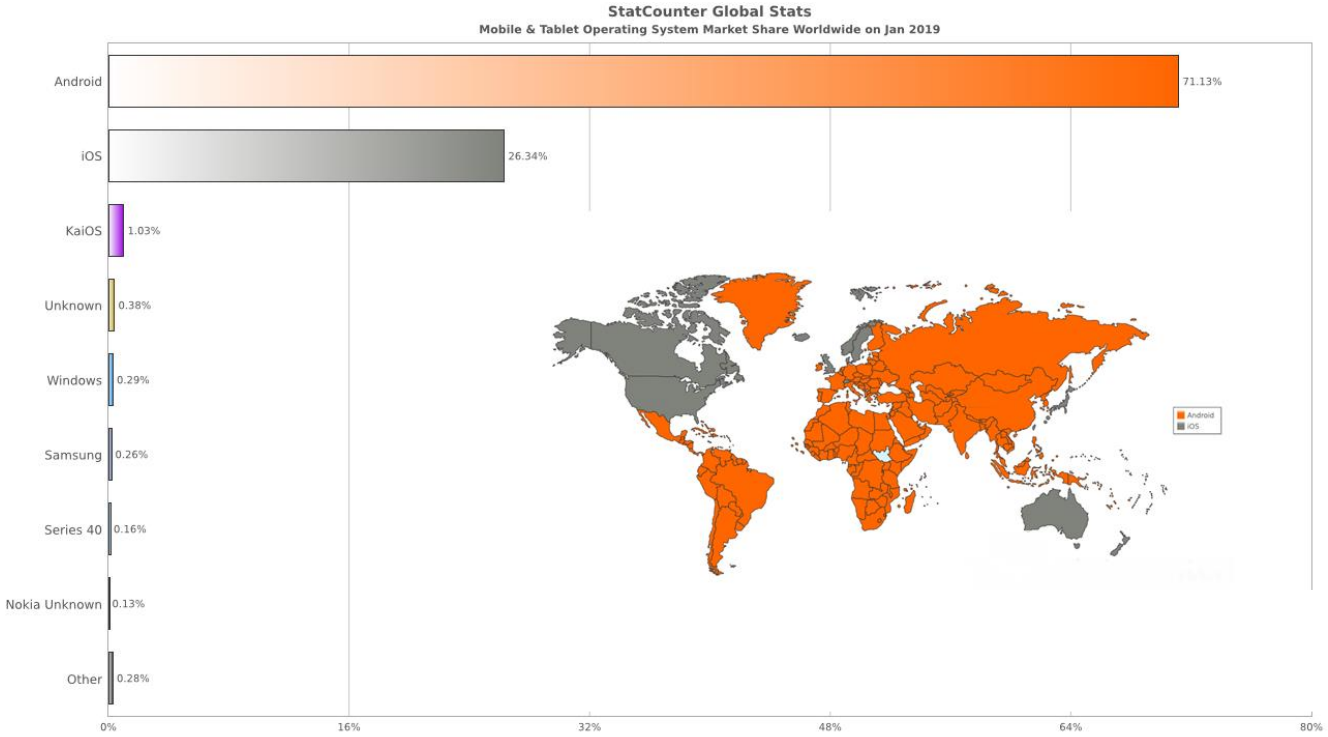

Figura 1-2 Gráfico y mapa de mercado de distribución de SO por países [2]

Debido a la aplastante diferencia entre Android y el resto de competidores, para este TFG se decide analizar un dispositivo con este sistema operativo. De entre los diferentes fabricantes que trabajan con Android, se escogió un teléfono Xiaomi para el estudio.

Xiaomi es un fabricante de origen chino. Si bien normalmente trabaja con una versión muy personalizada de Android, conocida como MIUI, desde un acuerdo con Google en 2017 comenzó a trabajar con una versión diferente de Android: Android One. Android One es una versión sin apenas personalización (y, por tanto, más ligera) de Android. Xiaomi arrasó con el *smartphone* Xiaomi Mi A1, que montaba este SO, y desde entonces no ha dejado de crecer en el mercado mundial, siendo a día de hoy el tercer fabricante con más ventas en España [2]. Debido a la emergente popularidad de Xiaomi y a la proyección futura que tiene Android One, se decidió utilizar el Xiaomi Mi A2 Lite, versión modernizada del Xiaomi Mi A1.

Figura 1-3 Teléfono Xiaomi Mi A2 Lite y principales características [3]

1.2 Objetivos

El objetivo principal del presente TFG consiste en tratar de proponer la configuración más adecuada, desde el punto de vista de la seguridad, de un teléfono móvil con un sistema operativo Android, comprendiendo previamente este SO. El cumplimiento de este propósito se asienta sobre la siguiente lista de objetivos intermedios:

- Realizar una revisión exhaustiva de los estudios y trabajos en el ámbito del TFG.
- Identificar los distintos tipos de amenazas a la seguridad que afectan a los dispositivos móviles y conocer los principales medios por los que actúan.
- Analizar la arquitectura del sistema operativo y explicar las características que componen el *modelo de seguridad de Android* y que garantizan la protección de los usuarios.
- Analizar la información que recopila Google de los usuarios Android para evaluar el riesgo que supone para la privacidad de los mismos y proponer medidas que limiten dicha exposición.
- Explicar detalladamente los pasos a seguir para conseguir una configuración adecuada del dispositivo y presentar una serie de buenas prácticas del usuario para maximizar la seguridad.
- Evaluar, mediante el uso de aplicaciones de seguridad, el nivel de protección alcanzado con la configuración.

1.3 Organización de la memoria

En el presente capítulo se ha expuesto el marco en el que se desarrolla este TFG y los objetivos que se pretenden alcanzar. A su vez, se ha presentado el *smartphone* (Xiaomi Mi A2 Lite) con el que se va a trabajar y las principales razones por las que se ha escogido.

En el segundo capítulo, se profundiza en el concepto de seguridad informática para. a continuación, explicar la importancia de ésta, presentando el nivel de concienciación de las instituciones de gobierno, de las empresas y del usuario particular. Posteriormente, se comentan los distintos sistemas operativos existentes para móviles, desarrollando más en detalle el que trae instalado el Mi A2 Lite. Se muestran las principales amenazas a las que están expuestos los *smartphones*, así como los medios que aprovechan los ciberdelincuentes para llevar a cabo sus ataques. Para finalizar, se citan distintas iniciativas que existen a día de hoy en el ámbito de este trabajo.

El tercer capítulo es el más extenso, y en él se desarrolla principalmente el trabajo propuesto, explicándose el modelo de seguridad propio de Android y las medidas para establecer una configuración más segura del dispositivo, atendiendo a cuatro aspectos: seguridad física, seguridad en las comunicaciones, seguridad de aplicaciones y localización.

En el siguiente capítulo se presenta, de una forma resumida, mediante tablas, todas las medidas anteriormente propuestas y los objetivos que buscan cada una de ellas, constituyendo el conjunto de recomendaciones una completa guía de buenas prácticas. A continuación, se exponen los distintos intentos con los que se probó dicha configuración en el teléfono de estudio.

Se cierra este TFG con un quinto capítulo donde se tratan las conclusiones extraídas, con unas líneas futuras para posibles trabajos posteriores. En último lugar figura la bibliografía, donde aparecen las fuentes consultadas.

2 ESTADO DEL ARTE

En este capítulo se pretende aclarar los conceptos de seguridad informática y el porqué de su importancia, así como el nivel de concienciación que existe a nivel institucional, empresarial y particular. También se expone la situación actual del mercado de *smartphones*, analizando los distintos sistemas operativos. A continuación, se explicarán las principales amenazas a la seguridad de dispositivos móviles y los principales medios por los que actúan. Finalmente se hablará de los distintos trabajos y estudios realizados en este ámbito.

2.1 Seguridad informática

2.1.1 Definición

La seguridad informática, ciberseguridad o seguridad tecnológica de la información es la disciplina dentro de la telemática que, mediante todo tipo de herramientas, técnicas, directrices, leyes, sistemas y prácticas seguras, se encarga de preservar la infraestructura computacional. La ciberseguridad se basa tanto en la protección de software como de hardware, así como de redes de ordenadores, para garantizar que se cumplen las distintas características de seguridad de los sistemas de información establecidas por la Organización Internacional de Estandarización en la ISO 27001: Sistemas de Gestión de la Seguridad de la Información [4]:

- ***Confidencialidad***: garantía de que únicamente los usuarios que están autorizados a ello acceden a la información. Se evita así la divulgación de dicha información restringida.
- ***Disponibilidad***: característica que garantiza que el acceso a la información será posible siempre que sea necesario.
- ***Integridad:*** concepto que busca evitar que la información sea modificada o alterada por un tercero no autorizado.

Estos tres pilares pueden verse complementados por los conceptos de autenticidad, fiabilidad y responsabilidad. La ciberseguridad puede abordarse desde diferentes perspectivas [5]:

- ***La seguridad física y la lógica***: Esta forma de clasificar, centrada en el recurso que se debe proteger, diferencia entre la defensa del aparato físico (hardware), tanto de incendios, accidentes, como de amenazas externas más relacionadas con el robo y fallos eléctricos de la defensa del software y la información almacenada en el equipo.
- ***La seguridad activa y pasiva***: Esta clasificación está más centrada en las medidas de protección. Se diferencia entre dos tipos de medidas. Las activas son los medios proactivos que buscan proteger el equipo de fallos o amenazas en hardware y software. Un ejemplo serían los antivirus o la encriptación. Las medidas pasivas buscan minimizar los daños en el caso de que

las activas no consigan detener la amenaza. Un ejemplo serían las copias de seguridad, que nos garantizan que no perderemos la información.

- ***La seguridad de software, de hardware y de red***: Esta clasificación es la más común. No es incompatible con las demás, de hecho suelen utilizarse para complementarse. Esta clasificación es ligeramente más específica que la primera que se analizó. Además, se incluye la seguridad de red, para la definición de protocolos y herramientas en la protección del equipo conectado a una red corporativa o incluso doméstica.

2.1.2 Importancia

Como ya se ha comentado previamente, en la actualidad existe una total dependencia de las nuevas tecnologías en todos los ámbitos, desde el empresarial o público al personal.

La importancia de la seguridad informática se hace evidente con los datos sobre la cantidad de ciberataques a nivel mundial. Se estima que cada día se llevan a cabo más de un millón de ataques. El Instituto Nacional de Ciberseguridad (INCIBE) publicaba en [6] a principios de 2018 que durante el año 2017 habían resuelto 123.064 ataques, de los cuales 116.642 (casi el 95%) fueron dirigidos a empresas y ciudadados, y el resto se reparten entre operadores estratégicos y la RedIRIS. Además, INCIBE informa de haber avisado de más de 18.000 nuevas vulnerabilidades. Para el año 2018 el presupuesto para esta institución fue de más de 23 millones de euros, y casi dos tercios fueron destinados a servicios de seguridad y concienciación.

Esta cifra permite hacerse una idea de que el Gobierno de España está concienciado de la importancia de la ciberseguridad. España cuenta desde 2013 con una Estrategia de Ciberseguridad Nacional [7], que actualmente se encuentra en pleno proceso de actualización para hacer frente a las amenazas emergentes. Para garantizar los distintos objetivos de dicho plan se estableció, entre otros, una Política de Ciberseguridad Nacional (Figura 2-1) que sigue la línea de su equivalente a nivel UE: Estrategia de Ciberseguridad de la Unión Europea [8].

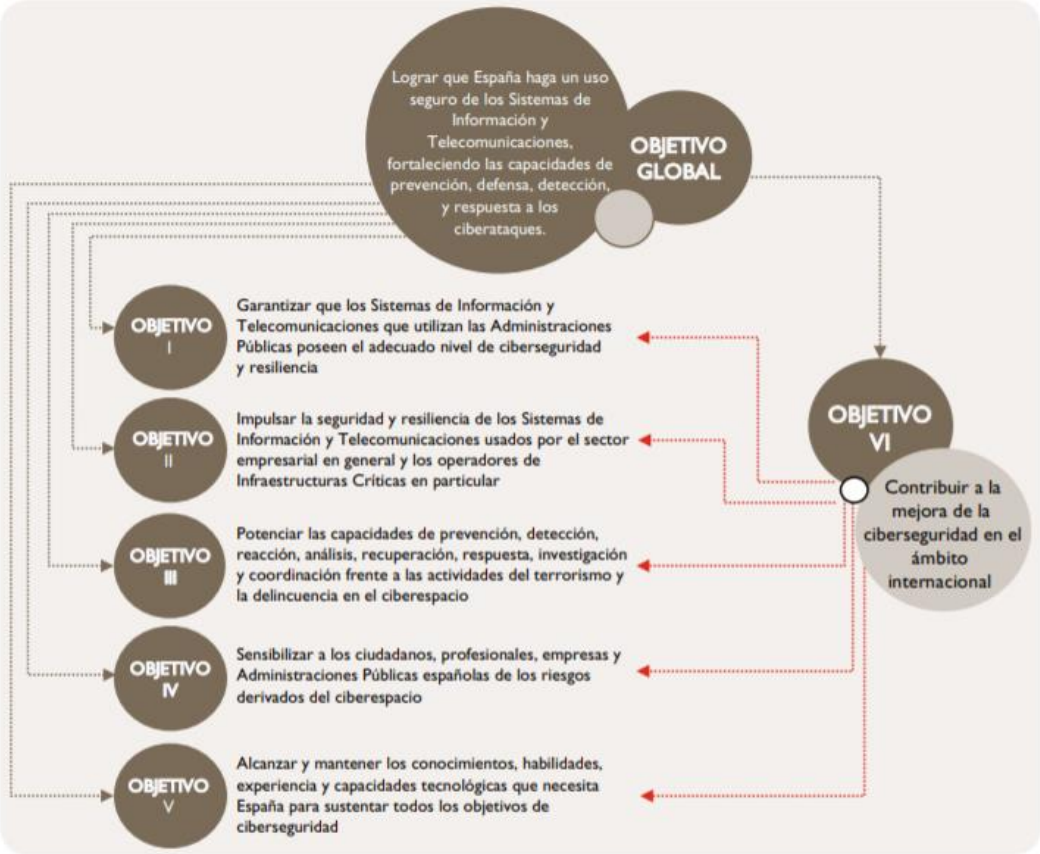

Figura 2-1 Objetivos de la Estrategia de Ciberseguridad Nacional [7]

La primera línea de acción indicada por este documento es la de disponer de "capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas". En este ámbito cabe destacar el punto en que se establece que se fomentará la cooperación entre los distintos organismos con responsabilidades en seguridad cibernética, especialmente el CERT (*Computer Emergency Response Team*) del Centro Criptológico Nacional (CCN), el CERT de Seguridad e Industria y el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD).

Este último, el MCCD, nace también en 2013 por la Orden Ministerial 10/2013, y muestra el compromiso de las FAS con la ciberseguridad, al considerarse éste como un factor crítico para los intereses nacionales. Actualmente, y desde la firma del convenio de colaboración entre el MCCD y el CNI (Centro de Inteligencia Nacional) en 2016, estos organismos trabajan en íntima cooperación, desmostrando de nuevo la relevancia e importancia de este asunto [9].

La preocupación por mantener a salvo la información también se hace patente a nivel empresarial. Según el *International Business Report* [10], el 32% de las empresas españolas admiten haber recibido al menos un ataque durante 2017. Este porcentaje es muy similar a la media mundial. Si bien esta situación es alarmante, la consultora Accenture en su informe de ciber resiliencia de 2018 [11] muestra que el 84% de estos ataques a empresas en España fueron detenidos. Sin embargo, el 65% de las empresas que participaron en la encuesta aún no disponían de un plan propio de ciberseguridad, mientras que el 35% ya planeaban duplicar su inversión en este ámbito. En definitiva, hay una clara tendencia hacia un aumento en la inversión y las medidas de ciberseguridad por parte de las empresas, ya que se constata que el número de ataques aumenta mucho cada año.

Por último, se plantea la importancia de la seguridad informática para el usuario común. Si bien se podría pensar que un usuario particular es menos susceptible de sufrir ciberataques, éste no es el caso. Lo cierto es que la concienciación de la población respecto a este tema es mucho menor que en los casos mencionados previamente. Esto podría deberse al hecho de que para un potencial atacante un usuario particular es mucho menos interesante que una gran empresa. Sin embargo, es infinitamente más fácil realizar ataques a dicho usuario, y el premio no es en absoluto despreciable, ya que se pueden dar casos de robos de información bancaria, robo de identidad, etc. Por todo esto es por lo que actualmente existen gran cantidad de programas de concienciación por parte del Gobierno y organismos dependientes.

La rápida expansión de dispositivos *IoT* (*Internet of things*) [12] produce que éstos sean fuente de gran cantidad de ataques, ya que los *hackers* aprovechan las frecuentes vulnerabilidades de estos y la facilidad de rastreo de los mismos (buscando servicios abiertos a gestión remota en Internet). Los ataques más comunes son los de denegación de servicio, y afectan sobre todo a *routers*, cámaras IP, etc. De hecho, según un informe de F5 labs [13], España sufrió en la primera mitad de 2018 aproximadamente el 80% de los ataques a esta clase de dispositivos.

2.2 Seguridad en dispositivos móviles

Este apartado comienza con el concepto de sistema operativo, así como los más importantes a día de hoy en *smartphones*, con el fin último de justificar la elección del sistema operativo Android para este TFG. El resto de componentes que aseguran el correcto funcionamiento y la seguridad del *smartphone* serán comentados más en detalle en el Capítulo 3.

2.2.1 Sistemas operativos móviles

Un sistema operativo (software de sistema) es el principal software de un dispositivo electrónico. Es el conjunto a su vez de todos los programas que permiten la correcta gestión del hardware así como la interactuación con el usuario final. Se podrían resumir las funciones básicas de un sistema operativo en cinco: suministro de interfaz al usuario, la administración de recursos, la administración de archivos, la administración de tareas y el servicio de soporte y utilidades.

Al igual que un ordenador requiere de sistema operativo como Windows o Linux para funcionar, encontramos la misma necesidad en los teléfonos inteligentes. Desde el punto de vista de la seguridad, se podría decir que el sistema operativo, al ser un elemento crítico, es el primer eslabón en la defensa del dispositivo.

En el mundo de los teléfonos inteligentes encontramos gran variedad de SO. A continuación se describen los más importantes: (véase Figura 1-2):

- ***Windows 10 mobile*** [14]**:** Diseñado por Microsoft para móviles y tablets, anteriormente conocido como *Windows phone*. Su núcleo es Windows NT y su código es cerrado. Su baja participación en el mercado hizo que esta compañía dejase de diseñar funciones y hardware para dispositivos móviles desde finales de 2017. Hoy en día, se centran en crear aplicaciones compatibles con Android e IOS, y mantener los dispositivos existentes con parches de mantenimiento.

- ***Tizen (Samsung en Figura 1-2)*** [15]**:** Este sistema operativo es el resultado del proyecto construido sobre la plataforma Linux de Samsung basada en HTML5. En la conocida como Asociación Tizen colaboran importantes compañías como Samsung, Intel, Panasonic o Huawei. Al ser un proyecto *open-source* (permite la colaboración en el desarrollo a cualquiera), nos encontramos con un SO flexible muy adaptable a todo tipo de dispositivos desde *smartphones* a televisiones (estos últimos especialmente). Sin embargo, las posibilidades que ofrece el Wear OS de Google [16] (Android para *wearables*) han hecho que cada vez más fabricantes opten por este sistema, abandonando cada vez más Tizen. El propio Samsung, que invirtió especialmente en Tizen para evitar la total dependencia que tiene de Google, planea instalar en su próxima generación de *smartwatches* el SO basado en Android.

- ***KaIOS:*** Este sistema operativo de código abierto está diseñado por la empresa Kai Technologies [17]. Es de los pocos SO que siguen creciendo actualmente, hasta el punto de recibir inversiones de Google para habilitar aplicaciones de Google apps en sus plataformas. Está diseñado sobre HTML5, como una variante del Firefox SO [18], para dispositivos sencillos e IoT. Una de sus principales ventajas es que, al estar basado en HTML5, cualquier aplicación es ejecutable desde un navegador. El máximo exponente de móvil con este sistema operativo es el conocido *banana phone* de Nokia, el Nokia 8810 4G.

- ***IOS:*** Siendo su propietaria la multinacional Apple Inc [19], este sistema operativo aparece por primera vez en 2007. Proviene de macOS que deriva a su vez de Darwin BSD, siendo por tanto un sistema tipo Unix. Este sistema operativo parcialmente abierto cuenta ya con su duodécima versión. Está programado en C, C++, Objective-C y Swift. Dispone de su propia tienda de aplicaciones (Apple Store) aunque permite aplicaciones de Google como Maps y de su propio navegador Safari.
  Es, a día de hoy, el segundo más utilizado en todo el mundo, después de Android, con más del 20% de usuarios. En el mercado de tablets es claramente el más utilizado, habiéndose adaptado para el exitoso Ipad.

- ***Android:*** Es un sistema operativo desarrollado por Google, que compró la empresa Android Inc. en 2005. Está presente en móviles, tablets, relojes, televisores y automóviles de todo el mundo. La versión más básica de Android se conoce como *Android Open Source Project* (*AOSP*), que es accesible a un gran número de fabricantes como Samsung, Huawei, HTC, Motorola, etc.
  En septiembre de 2008 salió al mercado la primera versión estable de este SO, el en HTC Dream. Desde su aparición, el sistema operativo ha ido sufriendo actualizaciones y mejoras

para adaptarse a las necesidades de sus clientes. Cada una de estas versiones recibe el nombre (en inglés) de un postre típico. Actualmente se está implantando la novena versión: Android 9 *Pie* (tarta). Debido al peso que tiene este SO en el TFG, cuenta con un apartado más adelante en el que se explica con más detenimiento (véase apartado 3.1).

2.2.1.1 Android One

Android One [20] es una versión del sistema operativo Android, creada en 2014 y pensada para mercados emergentes de Asia, principalmente de la India. Google se asoció con fabricantes de estos países para ofrecer *smartphones* de gama baja y así expandir enormemente la venta de plataformas Android [21].

La principal característica de esta versión es que se parece mucho a la versión de Android *stock*, es decir, la versión que Google desarrolla para sus propios dispositivos Pixel o Nexus. Al ser Android un código abierto, los distintos fabricantes de móviles utilizan esta versión de *stock* y la modifican, añadiendo aplicaciones o servicios propios, creando la conocida capa de personalización. Éste es el motivo de que Android parezca distinto según la marca. Android One se libera de esa capa, obteniendo un sistema operativo menos pesado, pudiéndose instalar en móviles con menor capacidad y aún así funcionar correctamente.

El hecho de que cada fabricante modificase con más o menos libertad la versión de *stock* llevó a lo que se conoce como *fragmentación* de Android. El principal problema viene a la hora de actualizar el SO, ya que si para un dispositivo de Google la actualización llega muy rápidamente, para otros fabricantes el proceso es más complejo, llegando a demorarse meses. Este problema es crítico cuando dicha actualización resuelve alguna vulnerabilidad del sistema, dejando al usuario desprotegido durante demasiado tiempo. Para solucionar la fragmentación, se puso en marcha el Proyecto Treble [22] que busca separar el sistema operativo de la parte que depende del fabricante, para poder actualizarlo de forma más frecuente.

En Android One, al ser una versión mucho más pura, este problema es mucho menor. La rapidez con la que llegan las actualizaciones y la escasez de aplicaciones preinstaladas por el fabricante (que ocupan espacio de almacenamiento y requieren más capacidad de los teléfonos) son los principales factores que han hecho que Android One sea todo un éxito, hasta el punto de convertirse en el principal programa de Google para *smartphones*. El testigo en cuanto al sector de gama baja ha sido tomado por Android Go.

2.2.2 Amenazas

A continuación se citan los distintos riesgos a los que se enfrentan los usuarios de los *smartphones*. Esta lista está centrada en las amenazas de software principalmente, no incluyéndose el robo del dispositivo o su pérdida, el desgaste o el mal funcionamiento por uso inadecuado. Los usuarios maliciosos buscan principalmente lo siguiente:

- ***Robo de credenciales:*** Consiste en la adquisición de contraseñas, tanto de cuentas como del propio aparato, por parte de un tercero no autorizado, dejando desprotegida información sensible, ya sea para robarla, eliminarla o compartirla, o simplemente inutilizar el equipo atacado.
- ***Robo de información personal***: Entre la información que se obtiene de estos ataques se encuentran conversaciones, documentos, imágenes, registro de llamadas, registro del navegador. Un atacante podría hacer chantaje con la información robada, o establecer exigencias para recuperar la información. Son ataques que atentan contra la privacidad del usuario y a la confidencialidad. Los *malware* tipo *Ramsonware* bloquean el acceso del usuario a la información y exigen dinero a cambio del desbloqueo.
- **Suplantación o *spoofing*:** problema que amenaza principalmente la seguridad en redes, al hacerse pasar el atacante por el usuario, para toda clase de actos maliciosos. Destaca el *spoofing* en correo electrónico para SPAM, en IP, DNS, etc. También se entiende por

suplantación el hacerse pasar por una página web con el objetivo de conseguir información del usuario atacado.

- ***Daños económicos*:** se pretende conseguir beneficio económico. Esto contempla las suscripciones no autorizadas a servicios de pago, las llamadas o SMS a números de alto coste, robo de información durante las transacciones, falsos antivirus, o chantaje a empresas o usuarios particulares.
- ***Denegación de servicio (DoS):*** el atacante busca la inutilización o degradación de un servicio. Los objetivos que se persiguen son muy variados: conseguir el reinicio del equipo, llenar el espacio de almacenamiento, sobrecarga de red…
- ***Control remoto:*** el usuario malicioso accede al control del dispositivo, muchas veces sin saberlo el propietario, para utilizarlo dentro de una botnet (red de equipos infectados o controlados). Una vez hecho esto, se puede usar el teléfono para mandar información a un centro de mando y control, para reenviar información, spam o para ataques DoS, entre otros.
- ***Vigilancia:*** seguimiento remoto de la actividad del teléfono. Con las capacidades que tienen hoy en día los móviles un *hacker* podría conocer la ubicación del propietario, saber lo que busca en Internet, con quién habla o chatea, acceder a su vídeo y audio, etc.
- ***Modificación de datos o Tampering:*** no solo ataca la integridad de las comunicaciones, sino que el atacante puede introducir código dañino en aplicaciones legítimas que puede afectar al funcionamiento del teléfono.

2.2.3 Vectores de ataque

Una vez analizado lo que busca del usuario el atacante, se procede a investigar las múltiples opciones que este tiene para lograrlo:

- ***Vulnerabilidades del sistema:*** Son fallos en la programación del SO o las aplicaciones que ponen en riesgo la seguridad del dispositivo, comprometiendo la integridad, confidencialidad o disponibilidad del mismo. Estos errores, hasta que no se corrigen, son motivo de muchos ataques llegando a ser algunos críticos.
- ***Ingeniería social:*** conjunto de actividades que buscan engañar al usuario. Se basa en el principio de que el ser humano es el eslabón más débil de la cadena de seguridad y es corrompible. Los ataques por este método pueden llegar por llamadas telefónicas en las que el atacante se hace pasar por alguien de servicio técnico para conseguir una contraseña, o abriendo un enlace malicioso que llega por correo electrónico, y sobretodo mediante las redes sociales. Los ataques tipo *phishing* utilizan técnicas de ingeniería social.
- ***Navegador web:*** algunas apps integran un navegador a través del cual se puede descargar y posteriormente ejecutar código dañino sin que el usuario sea consciente.
- ***Redes Wi-Fi:*** Es común que el usuario se conecte a redes gratuitas poco seguras, que podrían ser una trampa para realizar ataques tipo *Man in the Middle* (MitM). En estos ataques, el usuario malicioso es capaz de interceptar el tráfico de red, pudiendo llegar a descifrarlo o modificarlo, además de obtener cierta información del dispositivo conectado. Un ejemplo sería *Krack*, que es el conjunto de diez vulnerabilidades, que infecta tanto puntos de acceso como equipos, que consiguió romper la seguridad de WPA2 [23].
- ***Bluetooth:*** aunque se trate de una red inalámbrica de proximidad, existen ataques como BlueBorne (2017) que explotaba ciertas vulnerabilidades y que permitían realizar MitM, tomar control del dispositivo, o enviar *malware* sin interactuar con el usuario, simplemente por el hecho de tener activado Bluetooth. Este ataque explota ocho vulnerabilidades (más en el caso de dispositivos IoT) y afecta a muchos SO, incluidos IOS y Android 7.1.2 [24]. Sigue siendo un problema importante debido a la cantidad de equipos sin soporte y sin las actualizaciones necesarias.
- ***NFC (Near Field Communication) o comunicación de campo cercano***: esta tecnología de comunicación inalámbrica de corto alcance (10 cm) está presente en muchas actividades del

día a día, como en las tarjetas de transporte público o en el pago *contactless*. Los problemas de seguridad van de la mano de la tecnología que utiliza, la radio frecuencia. Al ser una onda radio, ésta puede ser interceptada. Los principales ataques son los de *eavesdroping* (escucha discreta), retransmisión (*relay attack*) con lo que se conseguiría aumentar el alcance de este medio, y los de modificación de la información. Algunos ejemplos serían *Sidechannel Attack* o *Cryptanalitic attack*, que explotan el bajo nivel de encriptación existente debido al poco alcance de esta tecnología [23].

- ***Rooteado***: Este proceso otorga al usuario el acceso a distintas capas del software y permite controlar completamente el dispositivo [25]. Por lo general, se realiza para poder instalar una ROM distinta en el dispositivo, borrar aplicaciones de fábrica o instalar cierto tipo de aplicaciones. Este proceso es poco recomendable a nivel de seguridad, ya que no solo el usuario puede hacer cambios irreversibles que podrían hacer que el equipo dejase de funcionar, sino que las aplicaciones maliciosas consiguen mucha más facilidad para realizar ataques de todo tipo.

2.3 Estudios y trabajos realizados en este ámbito

Dada la importancia que tiene este asunto, es lógico encontrar multitud de proyectos, estudios, libros, manuales, guías o artículos sobre el tema. A continuación se presentan algunos de los muchos ejemplos de los que se ha obtenido información de referencia para este TFG:

- ***Guías de Seguridad de las TIC del CCN*** [26]: Tal y como indica el Director del CNI, Félix Sanz Roldán, en diciembre de 2018: "la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad [27], conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad."

  Existe en la actualidad una serie de guías clasificadas según el tipo de información que proporcionan. Dentro de la familia 400 Guías Generales (véase Figura 2-2), se encuentra una dedicada especialmente a dispositivos Android versión 7: *CCN-STIC 453E: Seguridad de dispositivos móviles Android 7.x* [28]. Esta guía explica, entre otros, distintos aspectos acerca de cómo configurar un móvil de la familia Nexus de Google. Otra guía interesante dentro de esa misma familia es *CCN-STIC 456 Cuenta de Usuario Servicios Aplicaciones Google para Dispositivos Móviles Android*, relevante para este TFG en varios puntos que afectan a la seguridad de las cuentas de Google [29].

Documento	Publicado	Actualizado
CCN-STIC-455D Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 12.x	Nov 2018	Nov 2018
CCN-STIC-455C Guía Práctica de Seguridad en Dispositivos Móviles iPhone iOS 11.x	Nov 2018	Nov 2018
CCN-STIC 456 Cuenta de Usuario Servicios Aplicaciones Google para Dispositivos Móviles Android	Sep 2018	Sep 2018
CCN-STIC 453E Seguridad de Dispositivos Móviles Android 7.x	Sep 2018	Sep 2018
CCN-STIC-496 Sistemas de comunicaciones móviles seguras	Jun 2018	Jun 2018
CCN-STIC-453D Seguridad de dispositivos móviles Android 6.x	Jun 2018	Jun 2018
CCN-STIC-470I1 PILAR - Manual de Usuario v7.1	May 2018	May 2018
CCN-STIC-470I2 PILAR - Continuidad Manual de Usuario v7.1	May 2018	May 2018
CCN-STIC-472G PILAR Basic - Manual de Usuario v7.1	May 2018	May 2018
CCN-STIC-473F µPILAR - Manual de Usuario v7.1	May 2018	May 2018

Figura 2-2 Guías CCN-STIC Serie 400 [26]

- ***Informes y trabajos:*** existen multitud de empresas o instituciones que realizan informes de seguridad, ya sea para beneficio propio o para uso público. Una de las principales es la propia web de Android que publica desde agosto de 2015 de forma mensual (lo que demuestra el compromiso de esta plataforma con sus usuarios en materia de seguridad) un boletín de seguridad (*Android Security Bulletin)* [30] en el que menciona vulnerabilidades encontradas así como herramientas para arreglar posibles fallos del sistema.

  A nivel nacional, aparece de nuevo la figura del CCN, que publica informes anuales sobre ciberseguridad, como el que se puede ver en [24], en el que se analizan las principales amenazas que aparecieron en el año anterior y posibles tendencias en los ataques de ciberdelincuencia. El CCN también publica informes más concretos sobre algunas tecnologías, como, por ejemplo, de NFC [23].

  En cuanto a trabajos e investigaciones, se pueden encontrar infinidad de documentos que tratan sobre cada aspecto de este sistema operativo, desde trabajos realizados por alumnos a otros realizados por académicos de universidades de gran prestigio, sin olvidar los que realizan las consultoras y empresas de seguridad. Ha sido de especial ayuda el trabajo *Seguridad en smartphones: Análisis de riesgos, vulnerabilidades y auditorías de dispositivos* [31], sobre todo en cuanto al estudio sobre las amenazas a las que están expuestos los dispositivos de esta plataforma. Otro trabajo destacable es *Seguridad en redes y sistemas: Técnicas y conceptos sobre hacking y pentesting* [32], que ofrece un enfoque diferente en lo relativo a las amenazas (no tan centrado en móviles), pero sobre todo ofrece información sobre cómo defender los sistemas de los ataques.
- ***Libros:*** muchos autores han visto una gran oportunidad en todo lo relacionado con Android. Si bien es cierto que, por lo general, la mayoría de libros tratan más sobre el desarrollo de aplicaciones y de código en general, casi siempre hay algún apartado sobre seguridad. Algunos ejemplos de libros específicos en seguridad de Android, utilizados como referencia en este TFG, serían: *Android security internals* de Nikolay Elenkov [33] en el que autor analiza muchos aspectos de la seguridad hasta Android 4.4 así como describe la estructura completa del sistema operativo. Otro ejemplo es *Android Hacker´s Handbook* [34], escrito por varios autores expertos como Joshua J. Drake o Pau Oliva Fora. En él se explican los riesgos asociados a este sistema operativo y cómo defenderse de una manera muy técnica. También se comentan diversos métodos de búsqueda de vulnerabilidades y *exploits* desarrollados para ello.

- ***Sitios web:*** una parte importante de la investigación se realiza a través de este medio. Aparte de las web oficiales, en Internet existen muchas fuentes de información. Pese a que en algunas de ellas la información no siempre está bien contrastada y, por tanto, no son demasiado fiables, existen foros de considerable prestigio, como la plataforma multinacional *StackOverflow* [35]. Este sitio web es utilizado por una amplia comunidad de desarrolladores para solucionar problemas a la hora de programar o tratar diferentes temas. En esta plataforma se realizan análisis sobre ciertas vulnerabilidades o ataques destacados, se exponen ejemplos de cómo funcionan y se debate sobre posibles soluciones.

3 DESARROLLO DEL TFG

Este cápitulo aborda la seguridad en los dispositivos Android. Primero se explicará la estructura del sistema operativo (apartado 3.1), seguido del apartado 3.2, centrado en el modelo de seguridad de Android, para después tratar el tema de la seguridad desde distintas perspectivas: seguridad en las aplicaciones (3.3), seguridad en acceso al dispositivo (3.4) y seguridad en las comunicaciones (3.5). Finalmente habrá un apartado dedicado únicamente a la localización (3.6), por su especial importancia en la privacidad.

A lo largo de todo el capítulo se hace referencia al teléfono empleado durante el desarrollo de este TFG: el Xiaomi Mi A2 Lite, al que pertenecen la mayoría de las capturas.

3.1 Arquitectura de Android

Es posible presentar la arquitectura de Android en cinco capas bien diferenciadas (véase Figura 3-1), que no han sufrido muchas modificaciones desde su creación. La más interna es el kernel de Linux, y la más externa la que contiene las aplicaciones del sistema (*System Apps*), pasando por la capa de abstracción de hardware (HAL por sus siglas en inglés*: Hardware Abstraction Layer*), las bibliotecas C/C++ nativas y el tiempo de ejecución de Android (ART), y la infraestructura de la API de Java. A continuación se explicará cada una de estas capas con más detalle [31] [33] [34] [36] [37].

3.1.1 Kernel de Linux

El kernel es el núcleo de cualquier sistema operativo, en este caso, de Linux, en el que se basa no solamente Android, sino también otras distribuciones como, por ejemplo, Debian o Arch. En esta capa se encuentran todos los drivers que sirven para controlar los distintos componentes del hardware, como la cámara, la pantalla, la memoria, etc. La versión que se tenga instalada en el dispositivo depende del procesador que disponga. El teléfono analizado cuenta con la versión 3.18.120 (se puede comprobar en *Ajustes>> Información del teléfono>> Versión de Android*).

Es posible instalar un kernel distinto en el dispositivo, a veces a través del propio fabricante. Dado que es poco común que se actualice de esta forma el núcleo Linux, es importante mencionar que existe la posibilidad de realizarlo de forma manual. Es un proceso complejo y depende mucho del móvil con el que se esté trabajando. La instalación manual de un nuevo kernel, debido a la peligrosidad que conlleva, está totalmente desaconsejada.

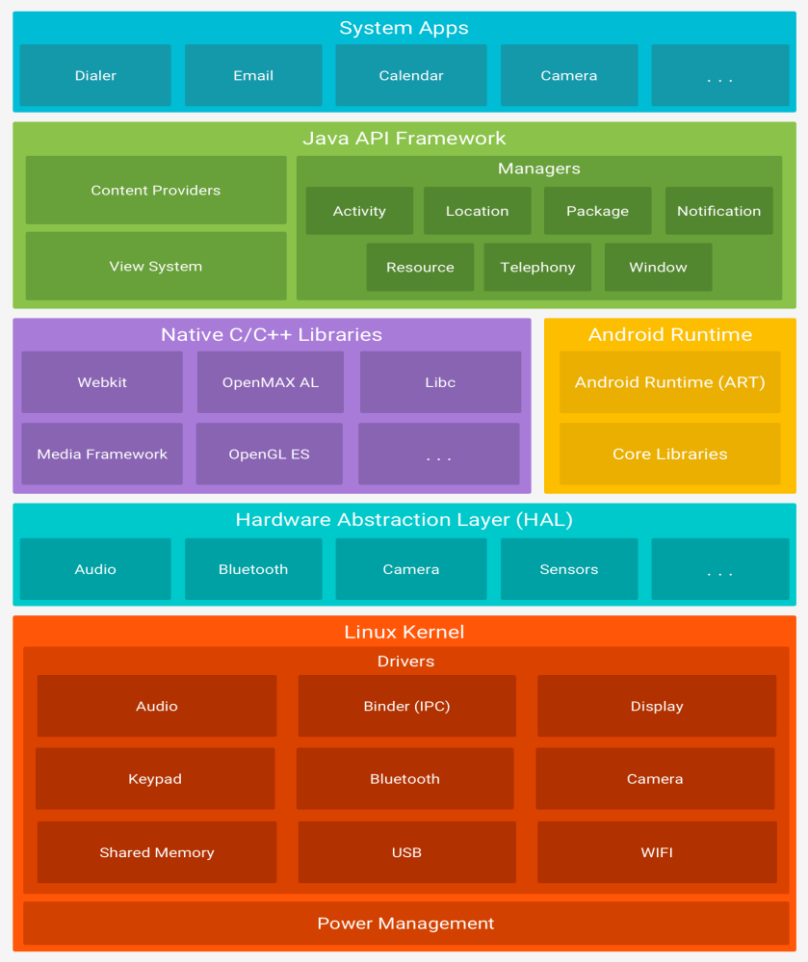

Figura 3-1 Arquitectura de la plataforma Android [36]

3.1.2 Capa de abstracción de hardware (HAL)

Las aplicaciones del sistema utilizan *HAL* para acceder a los drivers del sistema. Contiene un conjunto de librerías *C/C++*. Cada una de estas librerías implementa una interfaz para cada componente del hardware (*Bluetooth*, audio, cámara, DRM, entrada, gráficos, medios, sensores, periféricos, TV, automóvil y almacenamiento externo). Estas interfaces separan las implementaciones de los *vendors* (fabricantes de hardware) de la infraestructura del sistema operativo. Esto aparece por primera vez en Android 8, como medida para facilitar y agilizar las actualizaciones del sistema, como parte del Proyecto Treble contra la fragmentación de Android. Las *HAL* se almacenan en una partición del dispositivo, permitiendo que se actualice el sistema operativo sin necesidad de reconstruirlas.

3.1.3 Librerías Nativas C/C++

Esta capa contiene diversas librerías, escritas en código *C/C++*, y se compilan sobre el hardware del dispositivo, razón por la cual cada fabricante tiene la responsabilidad de instalarlas. Cada una de ellas garantiza el funcionamiento de distintas tareas, que se repiten frecuentemente, para evitar que haya que codificarlas cada vez. Un ejemplo sería la *Media Framework*, que permite reproducir vídeos e imágenes, o SQlite, para bases de datos.

3.1.4 Android Run Time

Desde Android 5.0, cada aplicación lleva a cabo sus procesos en sus propias instancias de ART. El ART está pensado para ejecutar varias máquinas virtuales, con archivos de código .DEX (creado y optimizado para Android). Compila Java en este tipo de código para que el sistema pueda ejecutarlos.

Hasta Android 4.4 (*KitKat)*, las aplicaciones (igualmente escritas en Java) se ejecutaban en una máquina virtual llamada Dalvik. Las aplicaciones que funcionan en ART, por lo general, funcionan en Dalvik, pero a la inversa puede no ser así.

En cuanto a las librerías del núcleo (*Core libraries)*, están desarrolladas en su mayoría en Java, aunque también las hay en código nativo. Son necesarias para que las aplicaciones y servicios del sistema funcionen correctamente.

3.1.1 Java API framework (infraestructura de aplicaciones)

Todas las funciones del SO están disponibles a través de interfaces de programación de aplicaciones (APIs por sus siglas en inglés) escritas en Java. Son la base para el funcionamiento de las aplicaciones, ya que recopilan multitud de funciones y servicios del sistema. Los principales servicios del sistema (*System services*) aparecen en la Figura 3-1, destacando *Content Providers* (proveedores de contenido), que permiten que las aplicaciones accedan a datos de otras aplicaciones (como una aplicación de mensajería a *Contactos*, por ejemplo) o el bloque de *Managers* (administradores). Este bloque incluye, entre otros, el administrador de sensores, el administrador de pantalla (*Windows)* o el administrador de notificaciones. De no existir esta capa, el desarrollador de cada aplicación debería compilar cada una de las funciones que necesitase su aplicación. En lugar de eso, puede llamar directamente a estas funciones, ahorrando tiempo y espacio en el dispositivo.

3.2 Modelo de seguridad de Android

La seguridad del sistema se implementa a lo largo de toda la arquitectura del mismo [38]. Se basa en tres pilares principales: *modelo de permisos, sandbox* y *firma de aplicaciones*.

3.2.1 Modelo de permisos de Android

Un punto central de la arquitectura de seguridad se basa en establecer restricciones a las operaciones que una aplicación puede realizar. Estas restricciones se consiguen mediante el uso de permisos.

En versiones previas, existía el modelo de permisos en *tiempo de instalación*, que consistía en que la aplicación solicitase al usuario los permisos que requería, antes de la descarga e instalación de la misma. El usuario, en este momento, decidía si aceptaba o no descargarlo bajo esas condiciones. Una vez descargada, el usuario no tenía potestad para denegar los permisos, salvo por medio de la eliminación de la aplicación. Los permisos requeridos podían consultarse en la *Play Store*, pudiendo conseguir información adicional sobre los mismos al pulsar sobre un permiso en concreto. También era posible a través del menú de *Aplicaciones*.

Para garantizar un mejor control sobre los permisos, así como un mayor conocimiento sobre los permisos de una aplicación, por parte del usuario, se cambió al modelo de permisos *en tiempo de ejecución* (desde Android 6.x). Cada permiso es gestionado individualmente y en el momento en que la aplicación requiere hacer uso de la función en cuestión.

Las aplicaciones con un nivel de API igual o superior a 23 (asociado a Android 6.x), no solicitan ningún permiso para instalarse, y por defecto, no tienen ningún permiso concedido de forma predeterminada. En el momento en que la aplicación se ejecuta, ésta va solicitando al usuario los permisos que requiere, y éste decide si concederlos o no. Si se rechazan, es posible que la aplicación deje de funcionar o que algunas de sus funcionalidades no lo hagan correctamente. De hecho, no es el sistema el que limita el funcionamiento de las aplicaciones, si no ellas mismas, que pueden decidir no ejecutarse si no se conceden todos los permisos.

A la vez que se instauró el nuevo modelo de permisos, Google distribuyó los permisos en tres categorías: permisos peligrosos, permisos estándar y permisos de *Acceso especial de aplicaciones*.

Los permisos estándar son aquellos que, según Google, aunque necesitan funcionalidades fuera de su entorno de ejecución, no suponen un riesgo para la seguridad del usuario. El usuario del dispositivo no autoriza este tipo de permisos, sino que el sistema los concede en el momento en el que la aplicación lo declara en su *manifiesto* (*Manifest*). El *manifest* es un archivo en el cual el desarrollador expone las configuraciones básicas de la aplicación (se encuentra en la raíz de ésta). Ejemplos de permisos estándar serían el acceso a Internet o el uso del *Bluetooth*.

Los permisos peligrosos son aquellos que conceden acceso a información sensible o confidencial del usuario, por lo que requieren de su consentimiento expreso.

El tercer tipo de permisos, conocido como *Acceso especial de aplicaciones*, sirve para establecer excepciones en algunas aplicaciones respecto al comportamiento de Android. Se recomienda tener especial cuidado con las aplicaciones que utilizan alguno de estos permisos, ya que muchos *malware* los suelen solicitar debido a las posibilidades que brindan.

Adicionalmente, en junio de 2014, la tienda de aplicaciones de Google (*Play Store*) creó los grupos de permisos, para simplificar su gestión y petición. Cada tipo de permiso queda recogido dentro de una unidad mayor que agrupa todos los permisos con capacidades o funciones relacionadas entre sí.

Desde entonces, lo que anteriormente eran unos 150 permisos, pasaron a aglutinarse en 12 grupos. Este sistema supuso, para muchos, una pérdida de seguridad importante. Por ejemplo, una aplicación que requiera hacer llamadas solicitará el permiso CALL_PHONE. Con este modelo, a la aplicación no sólo se le otorgará este permiso, sino el grupo de permisos relacionados con *Teléfono* al completo. Otro ejemplo, más crítico, sería una aplicación de Linterna, que necesite acceso al *flash*, englobado dentro de Cámara. Ésta solicitará acceso a la cámara para sus funciones (la cámara es un permiso considerado peligroso), pero a su vez conseguiría permisos para hacer fotografías o vídeos. En la Tabla 3-1, se muestran algunos de estos grupos de permisos (los considerados peligrosos), los permisos que recogen y los riesgos asociados.

Grupo de Permisos	Permisos	Peligros/Riesgos
Calendario	*READ_CALENDAR* *WRITE_CALENDAR*	El acceso a Calendario puede delatar la rutina del usuario o sus próximos eventos
Cámara	*CAMERA*	Permite hacer fotografías o grabar vídeos
Contactos	*READ_CONTACTS* *WRITE_CONTACTS* *GET_ACCOUNTS*	Una aplicación podría compartir la agenda completa, empleada para *spam*
Ubicación	*ACCESS_FINE_LOCATION* *ACCESS_COARSE_LOCATION*	Permite rastrear los movimientos del usuario
Micrófono	*RECORD_AUDIO*	Permite registrar toda clase de sonidos, incluidas llamadas o conversaciones
Teléfono	*READ_PHONE_STATE* *CALL_PHONE* *READ_CALL_LOG* *WRITE_CALL_LOG* *PROCESS_OUTGOING_CALLS*	Se autoriza a realizar prácticamente cualquier función, incluido llamadas, o compartir el registro de llamadas

SMS	*SEND_SMS* *RECEIVE_SMS* *READ_SMS* *RECEIVE_MMS*	La aplicación podría enviar mensajes *Premium* o leer mensajes con información sensible, como códigos de confirmación de compra
Almacenamiento	*READ_EXTERNAL_STORAGE* *WRITE_EXTERNAL_STORAGE*	Permite leer y escribir en la memoria del teléfono, pudiendo hasta borrar archivos
Sensores Corporales	*BODY_SENSORS*	Puede compartir información de las constantes vitales del usuario a empresas como aseguradoras

Tabla 3-1 Permisos peligrosos y riesgos asociados

3.2.2 Entorno de ejecución de las aplicaciones

Gracias al entorno de ejecución de las aplicaciones o *sandbox*, cada aplicación realiza sus operaciones de forma aislada, para protegerse de posibles aplicaciones maliciosas. Android aprovecha la protección basada en Linux, asociando a cada aplicación un UID (Identificador de usuario único), que luego utiliza para identificar y aislar la aplicación y sus recursos en un proceso separado.

El *Sandbox application* se configura a nivel del kernel. El kernel refuerza la seguridad entre aplicaciones, impidiendo que una pueda interactuar con otra sin los privilegios de usuario. Por ejemplo, el sistema operativo evitará que una aplicación lea datos de otra, sin el adecuado permiso. Debido a que el *sandbox* se encuentra en el kernel, este modelo de seguridad se extiende al resto de capas superiores.

Romper la seguridad de este mecanismo no es imposible, pero para ello habría que comprometer la integridad del kernel de Linux. Este entorno de ejecución proporciona la seguridad de que una aplicación comprometida por una vulnerabilidad no perjudicará a otras.

Para garantizar una correcta comunicación entre procesos que podrían necesitarse mutuamente, se implementa el mecanismo de *comunicación entre procesos* (*IPC*, por sus siglas en inglés, *Inter-Process Communication*). Así, las aplicaciones pueden compartir ficheros, memoria, colas de mensajes, etc. Android desarrolla *Binder*, basado en OpenBinder [39], para conseguir este propósito.

3.2.3 Firma de aplicaciones

Todas las aplicaciones, para que puedan instalarse, deben ir firmadas de forma privada por su desarrollador. Cada dispositivo puede comprobar que una aplicación va firmada a través del certificado público asociado a la firma privada del desarrollador. Con la firma se garantiza que sólo las actualizaciones con la misma firma sean aceptadas, además de ser necesaria para que la aplicación pueda acceder a otras. Si las aplicaciones están firmadas por la misma autoridad, tienen la posibilidad de ejecutarse en el mismo *sandbox*.

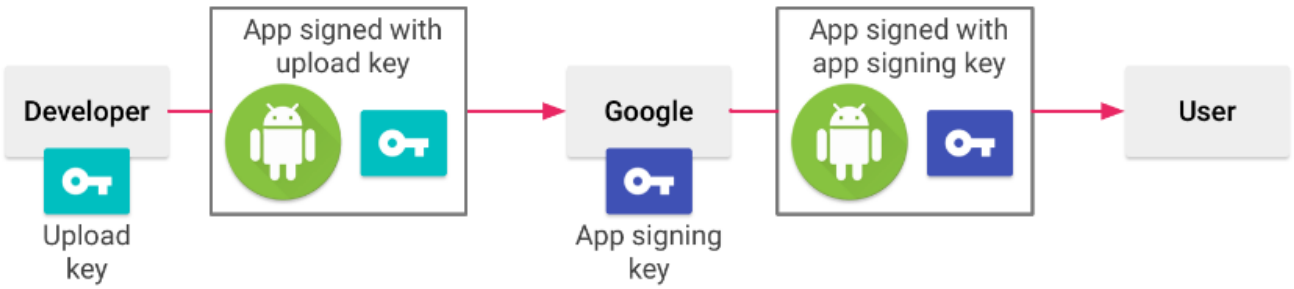

Figura 3-2 Firma de aplicaciones según el procedimiento de Google Play [36]

La Figura 3-2 muestra el método tradicional de firmado de aplicaciones o esquema de firmado *APK V1*. Este método requiere que el desarrollador haya obtenido previamente la clave de subida (*upload key*), con la que el sistema identificará al desarrollador, para que luego Google genere la clave para firmar la aplicación. Este procedimiento no evita que la aplicación sea maliciosa o tenga algún problema, ya que su misión es simplemente vincularla con un desarrollador en particular.

3.3 Seguridad en aplicaciones

El principal motivo de la exitosa expansión de *smartphones* es su versatilidad. La razón de esto se debe en gran parte a la posibilidad de descargar aplicaciones que permiten realizar infinidad de funciones: juegos, comunicaciones, gestión de cuentas y archivos, etc. En este apartado se tratará la procedencia de estas aplicaciones, el riesgo que conlleva descargar aplicaciones de fuentes no oficiales, así como los permisos sobre el teléfono que éstas pueden tener, si así se autoriza.

3.3.1 Aplicaciones de Google Play Store

Google Play [40] es una plataforma de distribución digital de aplicaciones principalmente para dispositivos Android. También se trata una tienda online a través de la cual Google ofrece distintos servicios. Dentro de Google Play se encuentran distintas aplicaciones (no confundir con la aplicación Servicios de Google Play), como Play Música, Play Películas, etc. Estas aplicaciones vienen instaladas de fábrica, y en muchos fabricantes no se pueden eliminar. La principal de todas ellas es Google Play Store o *Play Store*, que es la que comúnmente se conoce como *Google Play*, ya que es la que cuenta con todas las aplicaciones de Google (incluidas las mencionadas previamente). Según AppBrain, a fecha de realización de este TFG, existían más de 2,5 millones de aplicaciones publicadas en la Play Store [41]. Google tiene la potestad para retirar las aplicaciones si éstas no se adaptan a sus exigencias o si, directamente, son maliciosas.

Para descargar una aplicación de Google Play, es tan sencillo como abrir la aplicación de *Play Store* y buscar el nombre de la que se está buscando. Si no se busca ninguna en particular, existe un desplegable, que organiza por categorías todas las existentes (véase Figura 3-3). Las aplicaciones de *Acceso beta* son aquellas que aún están en desarrollo y pueden ser inestables, por lo que es preferible evitarlas. En este TFG se utilizará la aplicación *Twitter* como ejemplo.

Figura 3-3 Categorías de aplicaciones en *Play Store*

Al intentar descargar una aplicación, se entra en un menú (véase Figura 3-4) que proporciona cierta información sobre la misma: número de descargas, puntuación de los usuarios y número de opiniones, y la clasificación PEGI con la edad mínima para utilizarla. Si se pulsa sobre *Más información*, aparece una explicación más detallada de cómo funciona la aplicación (véase Figura 3-4), las novedades si se ha actualizado recientemente, e información adicional sobre el control parental recomendado, si contiene anuncios o permite realizar pagos, etc. Se puede observar quién es el desarrollador y si la versión está actualizada. Pero posiblemente el factor más importante a la hora de determinar si se debe o no instalar una aplicación es ver los permisos que ésta solicita, a través del botón de *Permisos de la aplicación.*

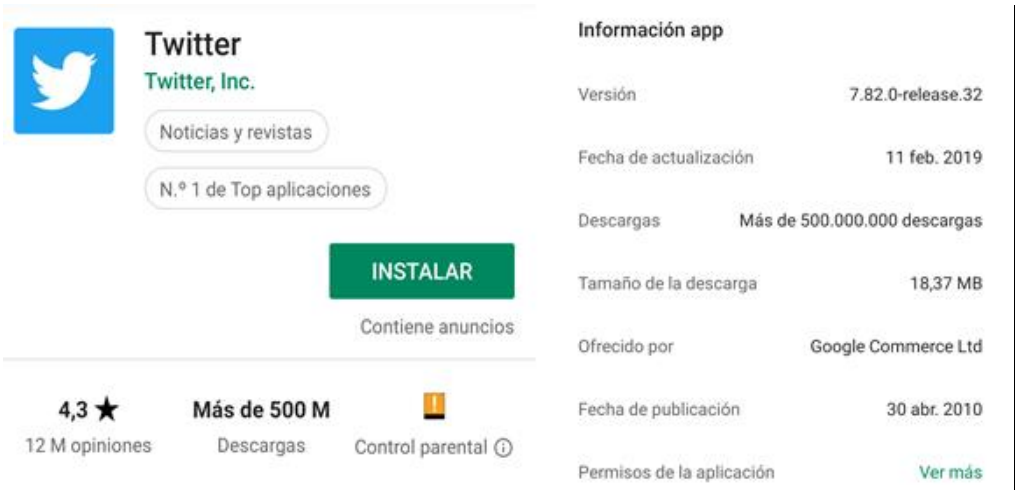

Figura 3-4 Aplicación *Twitter* en *Play Store*

Esta aplicación requiere muchos de los permisos analizados en el apartado 3.2.1 (véase Figura 3-5). Es importante analizar cuidadosamente que los permisos que va a solicitar la aplicación van acorde a la función que va a desarrollar, y buscar permisos peligrosos que parezcan sospechosos. Cada uno de estos permisos viene acompañado de una breve descripción del uso que se va a hacer. De todas formas, ningún permiso, como ya se ha mencionado, será concedido hasta que la aplicación lo requiera y lo otorgue el usuario.

Figura 3-5 Permisos que puede llegar a solicitar *Twitter*

El usuario puede activar y desactivar los permisos que la aplicación necesita a través del menú *Ajustes>>Aplicaciones y notificaciones>>Todas las aplicaciones>>Twitter>>Permisos.* De esta forma, se puede otorgar algún permiso sensible momentáneamente y luego retirarlo cuando se considere que ya no es necesario para el correcto funcionamiento de la aplicación, como se puede observar en la Figura 3-6.

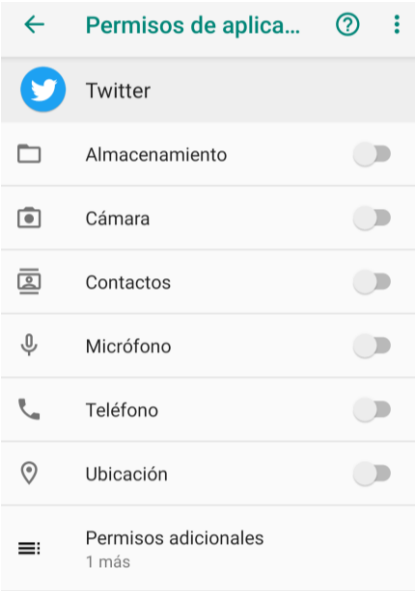

Figura 3-6 Permisos concedidos a *Twitter* desde el menú *Aplicaciones*

Una de las principales ventajas de Google Play es que cuenta con el sistema *Google Play Protect*, que se encarga de garantizar la seguridad en el dispositivo y de las aplicaciones. *Google Play Protect* analiza diariamente 50.000 millones de aplicaciones [42] y descartan aquellas que no cumplen con la política de Google. Este sistema no sólo comprueba las aplicaciones antes de subirlas a Google Play, sino que también las aplicaciones presentes en el dispositivo, avisando de las que sospecha que son dañinas y eliminando aquellas que se conoce que son software malicioso. Se encuentra activado de forma predeterminada en el dispositivo, aunque se puede desactivar en el menú *Ajustes>>Seguridad y ubicación>> Google Play Protect*. En este menú se puede ver la última comprobación y las aplicaciones que se analizaron. Se recomienda mantener activa la opción de *Buscar amenazas de seguridad* y activar *Mejorar detección de aplicaciones dañinas*, desactivada inicialmente, para permitir a Google analizar las aplicaciones descargadas en fuentes distintas a *Play Store*. En la Figura 3-7 se muestran estas opciones activadas.

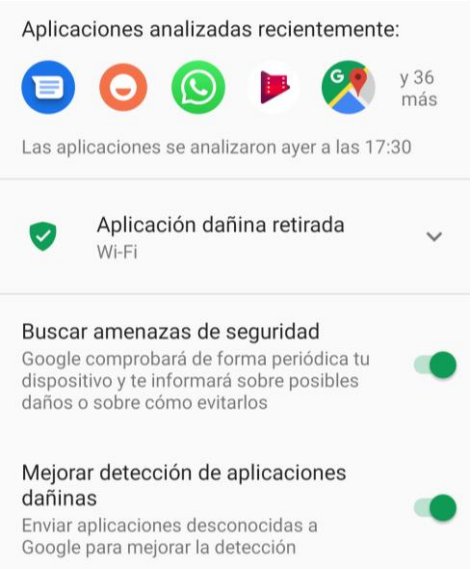

Figura 3-7 Menú de *Google Play Protect*

3.3.2 Aplicaciones de orígenes desconocidos

Las aplicaciones en Android se instalan mediante archivos ejecutables en formato APK. Por tanto, cualquier archivo de este tipo puede ser ejecutado en un dispositivo Android. La plataforma de Google descrita previamente no es la única forma de obtenerlos.

Se considera aplicación de origen desconocido a cualquiera que no provenga de Google Play. No por no ser de Google significa que la aplicación sea maliciosa, aunque la probabilidad es más alta. Por eso, Android no permite de forma predeterminada que se instalen este tipo de aplicaciones, principalmente para evitar que alguna aplicación legítima en el dispositivo pueda descargar otras maliciosas sin conocerlo el usuario. Sin embargo, se puede configurar el teléfono para permitir su instalación. En versiones anteriores, existía un apartado dentro del menú de *Seguridad*, que directamente habilitaba la opción de instalar aplicaciones de origen desconocido. Actualmente, esta opción se considera un permiso de acceso especial, que cualquier aplicación podría solicitar. Lo más común es querer instalar alguna aplicación que no se encuentre en *Google Play* sino en otro mercado, como por ejemplo *Uptodown* [43], al que se accede a través del navegador. Por ello, se debe acceder al menú de *Acceso especial* descrito en el apartado 3.2.1 y conceder a la aplicación de navegador (en este caso *Chrome*) este permiso.

Desde el punto de vista de la seguridad, no se recomienda habilitar esta opción, para no aumentar la probabilidad de ser infectado por algún tipo de *malware*, y utilizar aplicaciones de *Play Store*, donde se comprueba quién es el desarrollador y se realizan pruebas de seguridad a las aplicaciones.

3.4 Seguridad en el acceso al dispositivo

A lo largo de este apartado se comentarán todas las medidas propias con las que cuenta el Xiaomi Mi A2 Lite para protegerse del acceso no autorizado de una tercera persona, además de explicar cómo se deben configurar y cuáles son más efectivas que otras, considerando también la comodidad y la accesibilidad.

3.4.1 Inicio con SIM e inicio seguro

El PIN de la tarjeta SIM bloquea la tarjeta e impide que se puedan realizar llamadas telefónicas, utilizar los datos, etc. En definitiva, priva de los servicios de operador al teléfono movil.

La tarjeta SIM viene bloqueada de forma predeterminada con un *PIN* que se encuentra grabado en en el soporte de la misma (aquí también se encuentra el *PUK*). Después del primer desbloqueo, se ha de cambiar este *PIN*, para evitar que alguien con acceso a la tarjeta pueda desbloquearla. Al iniciar el teléfono, antes de poder acceder al mismo, se requerirá que se desbloquee la SIM. Se disponen de tres intentos al introducir el código. De ser erróneo, la tarjeta se bloqueará, impidiendo su uso en cualquier dispositivo. Sería necesario introducir el *PUK*, que es un código de ocho dígitos pensado para estas situaciones. Si se ha olvidado el *PUK*, no se recomienda intentar desbloquearlo, ya que si se introduce un valor equivocado diez veces, la tarjeta quedará inutilizada de forma permanente. En lugar de esto, se debe contactar con el servicio técnico de la compañía para que se facilite este código.

Este *PIN* representa una primera defensa del teléfono, ya que a no ser que se extraiga la SIM, es necesario introducirlo para acceder al dispositivo (solo una vez al iniciar o cuando se introduce la tarjeta). No solo eso, ya que también protege en caso de que se robe la tarjeta, ya que si no se desbloquea, no se podrán utilizar sus servicios, evitando que un usuario malicioso llame a números de alto coste, use SMS Premium, etc.

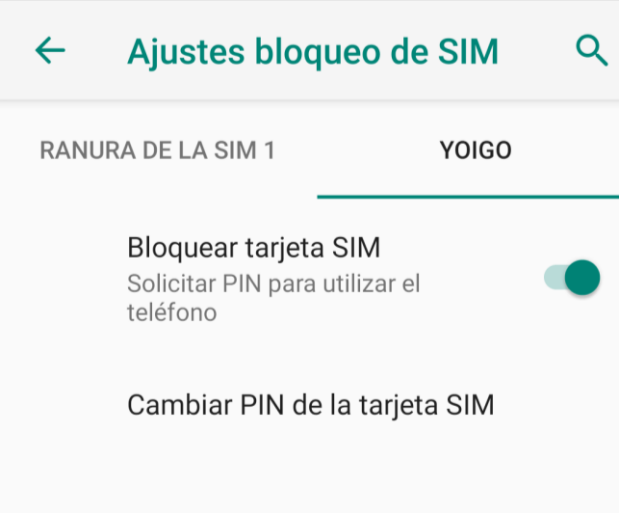

Figura 3-8 Ajustes de bloqueo de la tarjeta SIM

Sin embargo, existe la posibilidad desactivar este bloqueo, como se muestra en la Figura **3-8**. De hacerlo, la tarjeta y teléfono quedarán desprotegidos de las amenazas descritas anteriormente. La única ventaja reside precisamente en que no se bloquea el uso de los datos móviles. Un ladrón podría pensar en apagar el móvil para evitar que se le pueda localizar, pero en el momento que lo encienda cuando considere que esté en un lugar seguro, si no está activado el bloqueo de SIM, los datos móviles se activarán de forma automática y se le localizaría. Eliminar dicho bloqueo puede parecer lógico por este motivo, y además teniendo en cuenta que a día de hoy no es tan fácil robar la SIM de forma rápida y discreta. Por tanto, el usuario debe valorar los riesgos y ventajas de cada opción, considerando cómo lo usa. De forma más general, se recomienda tener este bloqueo activado.

Como protección extra, y si se ha decidido mantener el bloqueo SIM, se recomienda establecer un PIN que sea solicitado antes de encender el dispositivo y el arranque del sistema operativo. Esta opción se llama *inicio seguro* (véase Figura 3-9) y se establece al configurar la pantalla de bloqueo (véase el apartado 3.4.2). Si se activa, se bloquea todo tipo de llamadas y notificaciones; no se puede acceder a ninguna función del dispositivo. Es una eficaz defensa de la información personal del propietario.

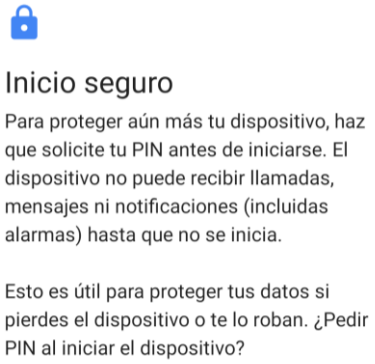

Figura 3-9 Configuración de Inicio seguro

3.4.2 Bloqueo de pantalla

Para acceder a la configuración de bloqueo de pantalla, se ha de entrar en el menú de *Ajustes >> Seguridad y ubicación >> Bloqueo de pantalla (Seguridad del dispositivo).* Antes de poder acceder a modificar los parámetros de este menú, es necesario introducir la contraseña, *PIN* o patrón actual, como medida de protección contra un tercero con acceso a la pantalla desbloqueada que pueda

modificar y privar así de control al propietario. Si no había ningún tipo de seguridad, no se requerirá *PIN* para acceder a estos ajustes, permitiendo que cualquiera pudiese cambiarlos. Existe una vulnerabilidad, que algunos fabricantes ya han corregido (Xiaomi no), por la que un atacante puede evitar escribir el *PIN* o contraseña para cambiar de modo de bloqueo: si se bloquea la pantalla estando dentro del menú para cambiar este parámetro, después de desbloquearla, incluso tiempo después, se desbloquea directamente en este menú, posibilitando que se pueda modificar sin conocer la contraseña. También se puede acceder sin permiso desde el menú de aplicaciones recientes, si no se cerró la aplicación de Ajustes después de utilizarla. Una vez dentro del menú aparecen las opciones de la Figura 3-10.

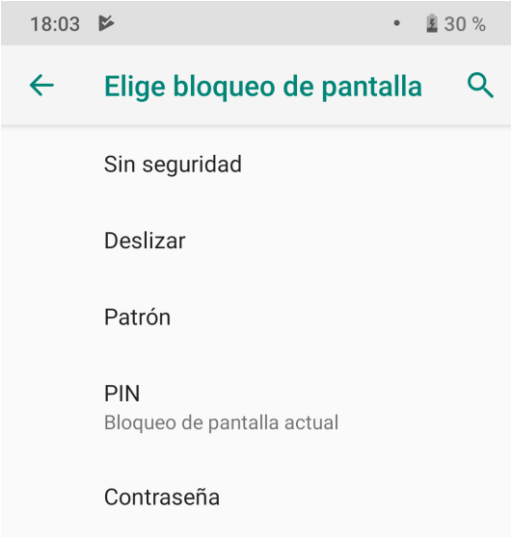

Figura 3-10 Diferentes sistemas de bloqueo de pantalla

Sin seguridad es un modo que directamente elimina la pantalla de bloqueo, por lo que simplemente pulsando el botón de encendido se accede a la pantalla de inicio. Por razones obvias, este modo está completamente desaconsejado, pese a ser extremadamente cómodo a la hora de acceder al móvil.

Otra forma, prácticamente igual de insegura que la anterior y por ello desaconsejada, consiste en emplear *Deslizar*. La principal diferencia con el modo *sin seguridad* es que ahora sí existe una pantalla de bloqueo previa a la de inicio. Tiene por tanto mejor accesibilidad que este, ya que a través de esta pantalla se puede acceder a algunas aplicaciones directamente, como la cámara o el asistente de Google. Si este modo está activado, aparecerá un candado abierto (Figura 3-11) en la parte inferior de la pantalla, dando una idea a un delincuente del nivel de protección del dispositivo, volviéndolo muy llamativo para un potencial ladrón.

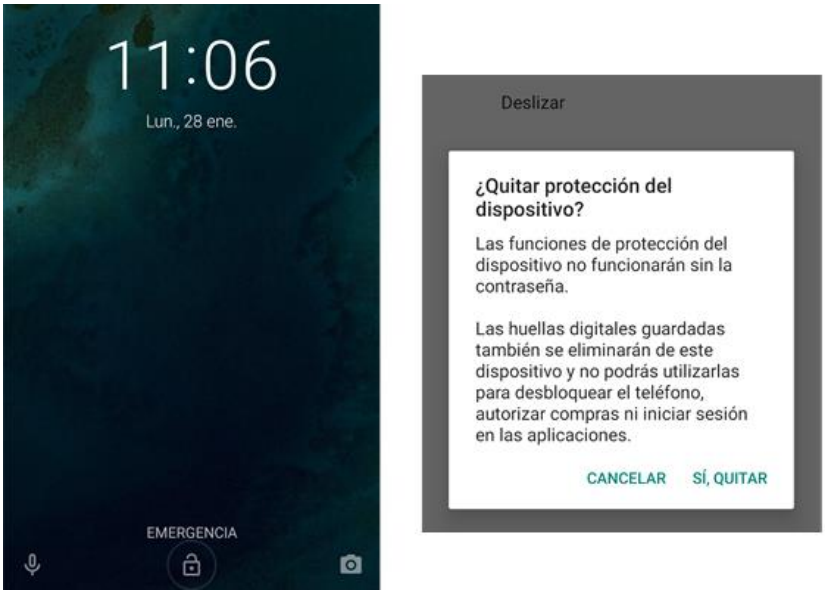

Figura 3-11 Pantalla de bloqueo en modo *Sin seguridad o Deslizar* y mensaje de aviso.

El resto de métodos de desbloqueo tiene ya un mayor grado de protección. El primero que aparece es *Patrón.* Esta opción consiste en una matriz de nueve puntos, con la posibilidad de unirlos al deslizar el dedo por la pantalla y crear así el patrón. Tiene ciertas restricciones: la longitud mínima del patrón ha de ser de al menos cuatro puntos, y no se puede pasar por el mismo punto más que una vez. Esto limita el número de posibilidades a 389.112. En versiones previas a Android 6 los patrones se almacenaban dentro del sistema, cifrados con un hash *SHA-1* sin semilla, lo que permitía a un usuario con acceso root acceder a la carpeta donde se guardaban y descifrarlo con relativa facilidad.

Este tipo de contraseña ha sido objeto de numerosos estudios, ya que es típico de dispositivos móviles. El resultado de la inmensa mayoría de ellos es que este método es realmente inseguro. Un estudio de 2017 realizado por la Academia Naval de Estados Unidos y la Universidad de Maryland [44] comprobó que aproximadamente dos de cada tres individuos situados a poco menos de dos metros, eran capaces de repetir un patrón de seis puntos viéndolo solo una vez. Con ese mismo número de dígitos, el *PIN* obtuvo mucho mejor resultado: solo uno de cada diez era capaz de repetirlo.

Existen posibilidades para intentar mejorar la viabilidad de este método. La principal y recomendada es la desactivación de *Mostrar el patrón dibujado.* De esta manera, eliminamos la posibilidad de que alguien observe momentáneamente la figura final del patrón y posteriormente la repita. Para desactivarlo basta con entrar en el menú mencionado previamente y pulsar en el ajuste *Mostrar el patrón dibujado.* Otra opción de mejora de la seguridad podría ser generar patrones más complejos, utilizando todos los puntos disponibles. Si bien empeora la comodidad en el desbloqueo, es cierto que resulta más difícil a un atacante recordarlo.

Un estudio conjunto de la Universidad Lancaster, la Universidad de Bath y la Universidad del Noroeste (China) [45] creó una forma de ataque que conseguía descifrar el patrón en los cinco primeros intentos. El ataque consiste en grabar al atacado desde una distancia aproximada de dos metros (el estudio plantea múltiples espacios públicos, en los que consiguen su objetivo en todos), para luego procesar el vídeo. Por el simple movimiento de los dedos, el programa es capaz de obtener la geometría del patrón. Por si fuera poco, se comprobó que el patrón, cuanto más complejo fuese (Figura 3-12), más fácil resultaba para el programa descifrarlo. Por todo esto, se recomienda elegir otra opción de bloqueo de pantalla.

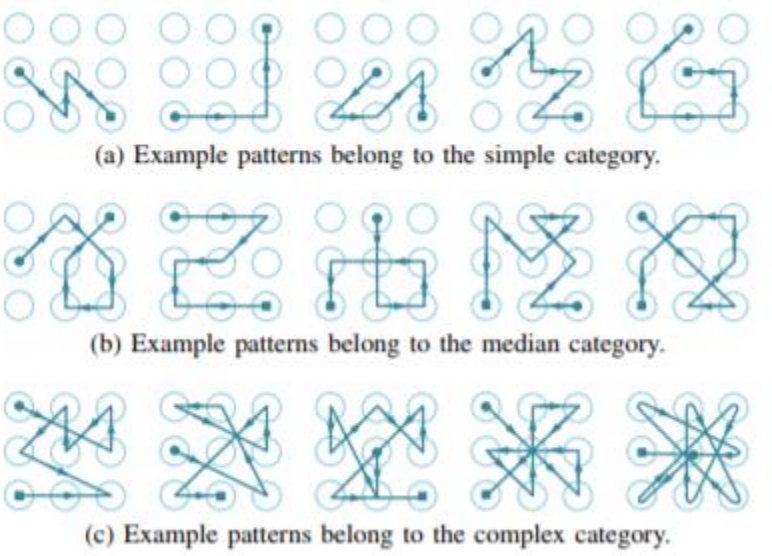

Figura 3-12 Ejemplos de patrones simples (a), intermedios (b) y complejos (c) [45]

Está comprobado que la opción de establecer un *PIN* para la pantalla de bloqueo es más segura que el patrón, aunque aún es posible reconocerlo analizando los movimientos del dedo. Android establece una restricción, por la que la longitud del *PIN* debe ser superior a cuatro dígitos y como máximo de dieciséis. Antes de la versión 6 de Android, también la información sobre el *PIN* se almacenaba en la base de datos pero, en este caso, cifrado con semilla, dándole un plus de seguridad. Se recomienda que el *PIN* escogido sea distinto al *PIN* de la tarjeta SIM.

Finalmente, la elección de establecer una contraseña para acceder al teléfono constituye la opción más segura y, por tanto, es la recomendada. Tiene la misma restricción en cuanto a longitud que el *PIN*, pero permite caracteres alfanuméricos, diferenciando entre mayúsculas y minúsculas. Se recomienda no establecer una contraseña que esté directamente relacionada con el propietario (nombre, mascota, etc), así como evitar las que sigan algún patrón o cualquiera de la lista de las más utilizadas [46]. En el dispositivo de estudio no existe la posibilidad de impedir que la letra pulsada durante el desbloqueo no aparezca durante unos segundos. De poderse, se recomienda inhabilitar esta opción, ya que permite a un tercero ver lo que se está escribiendo, facilitando que la pueda descifrar.

Por otro lado, también existe la posibilidad de desbloquear el teléfono a través de la huella dactilar del propietario. Para poder registrar huellas digitales es necesario que previamente se haya establecido *PIN*, *patrón* o *contraseña*, no permitiendo su uso en el caso de *sin seguridad* o *deslizar* (en el dispositivo utilizado), por motivos de seguridad. Otros fabricantes sí que permiten que se utilicen, pero recomiendan que si se decide establecer un método no seguro de desbloqueo, no se registren huellas dactilares. Para poder añadir huellas (hasta un máximo de cinco, como se puede observar en la Figura 3-13), primero se ha de introducir la contraseña de desbloqueo, para evitar que un usuario malicioso pueda introducir sus huellas. Una vez dentro del menú, basta seguir las instrucciones sobre cómo colocar el dedo.

Este método aparece con soporte nativo a partir de Android 6.x. Previamente existía en algunos fabricantes, aunque en ocasiones con debilidades de seguridad. En algún caso, la representación de la huella se almacenaba en ficheros sin cifrar, facilitando que un usuario malicioso pudiera acceder a ella, con mayor facilidad si el teléfono estuviese *rooteado*. Dado que la huella puede utilizarse para acceder a ciertas aplicaciones o para comprar, se trataba de un problema crítico. La principal característica de este sistema es su conveniencia y facilidad en el desbloqueo, aunque debido a la cantidad de veces que el usuario toca objetos a lo largo del día (incluso el propio teléfono) dejando su huella, un atacante con la debida técnica podría sustraerla y utilizarla para acceder al dispositivo. Existen diversas vulnerabilidades en este sistema [47], la mayoría resueltas a día de hoy. Dada la excelente acogida por

parte de los usuarios, cada vez se están implementando mejores sistemas de reconocimiento dactilar, que mejoren la experiencia para estos, ya que en ocasiones ocurre que el sistema no funciona si el dedo está sucio o se tiene la mano húmeda. Muchos fabricantes han optado en los últimos meses por introducir un detector de tipo óptico en la misma pantalla, lo que a primera vista parece futurista, y que se encuentra todavía en proceso de análisis por parte de Google. Lo que sí que apunta a ser un éxito son los sensores de ultrasonidos, que siempre son capaces de analizar la huella y son muy difícilmente engañables por reproducciones.

El usuario debe valorar si compensa disponer de este método más inseguro pero de gran comodidad. Incluso en el caso de utilizarlo, se debe seleccionar un mecanismo secundario (*contraseña*, *PIN*, etc), ya que el sistema por huella digital se bloquea tras cinco intentos fallidos al encender el dispositivo o tras un periodo largo de inactividad.

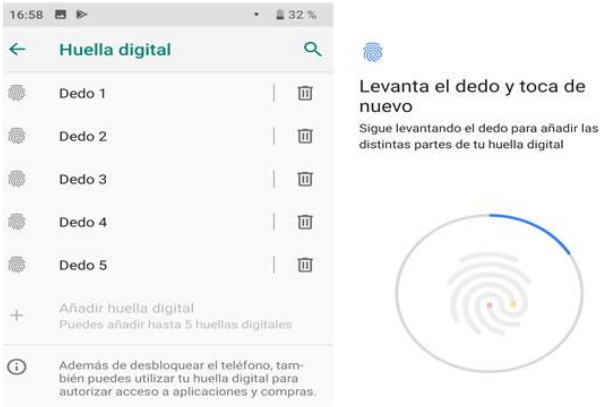

Figura 3-13 Proceso de configuración de la Huella digital

3.4.3 Smart Lock

A finales de 2014 Google presentó la versión de Android 5.0 *Lollipop* que incluía ambiciosos cambios. Entre ellos destaca *Smart Lock*, que a lo largo de los años ha sufrido muy pocas variaciones. Es una herramienta de seguridad inteligente que permite el desbloqueo del dispositivo si se cumplen ciertas condiciones. Aparece preinstalada en todos los dispositivos Android desde 5.0, aunque está desactivada por defecto. Es un complemento a la seguridad que ofrece el *PIN* o la contraseña, no configurable si el teléfono tiene un método inseguro de bloqueo (*sin seguridad* o *deslizar)*.

Las ventajas de esta herramienta son bastante obvias. Que el dispositivo se desbloquee solo al llegar a casa, que no se bloquee si se está trabajando con un equipo de confianza o que se desbloquee con solo mirarlo, son algunas de las llamativas opciones que ofrece *Smart Lock*, que además parecen mejorar la seguridad del dispositivo. Sin embargo, antes de analizar con detalle cada una de estas opciones, es necesario aclarar que, en ningún caso, mejoran la seguridad del móvil, es más, pueden convertirse en una seria amenaza contra la misma si no se utiliza correctamente.

Antes de poder configurar *Smart Lock*, al tratarse de una herramienta de seguridad, es necesario disponer de un PIN, contraseña o patrón, que será demandado antes de acceder al menú. Una vez dentro (*Seguridad y ubicación del dispositivo*) aparece el desplegable de la Figura 3-14.

Figura 3-14 Posibilidades que ofrece *Smart Lock*

- ***Detección corporal**:* este sistema no permite técnicamente el desbloqueo. Su función es evitar que el teléfono se bloquee mientras éste detecte que está en movimiento o cuando el usuario lo sostiene. Si, por ejemplo, el usuario deja el móvil en una mesa, este programa debería proceder a su bloqueo. Google avisa de que puede tardar hasta un minuto en bloquearse en este caso, e incluso de cinco a diez minutos en caso de subirse a un coche o a un autobús. Debido a esto, Google insiste en bloquear el dispositivo manualmente si es preciso. Sin embargo, esto no ocurre en todos los casos. Se configuró el teléfono de prueba de forma que se suspendiese la pantalla a los treinta minutos de inactividad. Más tarde, se habilitó esta opción, que debería bloquear el móvil en cuanto se depositase en algún lado. El resultado fue que no se cumplieron los tiempos determinados por Google, sino que esperó los treinta minutos antes de apagar la pantalla.

Otro problema de este sistema es precisamente su forma de actuar: no se bloquea si está en movimiento. En caso de robo, el ladrón tendría acceso libre al dispositivo, lo que supone un grave problema de seguridad (Figura 3-15). Esto ocurre en la mayoría de dispositivos, aunque es cierto que algunos modelos de gama alta son capaces de detectar el patrón de movimiento del propietario, bloqueándose si detecta que ha cambiado, sospechando de un robo.

Figura 3-15 Advertencia de Android respecto a *Detección corporal*

Este sistema requiere acceso al acelerómetro del teléfono y almacena la información en el propio dispositivo. Si se desactiva, todos los datos serían automáticamente borrados.

- ***Sitios de confianza***: este método es capaz de detectar, a través de los medios de ubicación del móvil, si se encuentra en alguno de los sitios de confianza que el usuario ha añadido (casa, trabajo, etc). De ser así, el dispositivo no se bloquea, evitando tener que introducir el patrón siempre que se quiera acceder.

Pese a que el sistema activa el modo de *Alta precisión* o el de *Ahorro de batería* (véase apartado 3.6.1), Google avisa de que la ubicación puede no ser exacta, dándose los mejores resultados al estar conectados a una red Wi-Fi, llegando a permitir que el teléfono se desbloquee a 80 metros de la ubicación registrada. En la Figura 3-16, los puntos azules indican esta distancia máxima, pero con el móvil de prueba se llegó a desbloquear incluso a más del doble de esta (Círculo rojo).

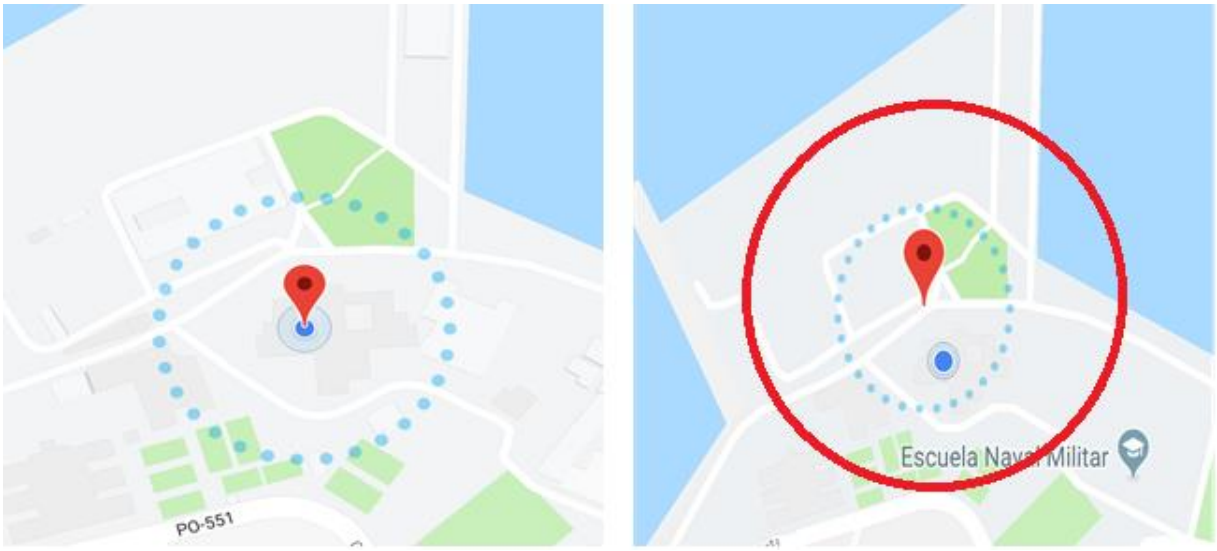

Figura 3-16 Diferencia entre el límite teórico y real de la ubicación en *Smart Lock*

Nada parece indicar que este programa tenga en cuenta la altura a la que se encuentra el teléfono, por lo que no es capaz de diferenciar entre encontrarse en el primer piso o en la azotea de un gran edificio. Además, se advierte al usuario de que las señales de ubicación son perturbables o modificables con el equipo adecuado.

- ***Dispositivos de confianza:*** permite el desbloqueo y la negación de bloqueo si el llamado dispositivo de confianza permite que así sea. Valdría cualquier dispositivo *Bluetooth*, como los altavoces del coche, un reloj inteligente o un teclado *Bluetooth*. Según el tipo de dispositivo, habrá que desbloquear primero una vez antes de que funcione correctamente.

Si se decide aplicar este sistema, se ha de tener extremo cuidado con los dispositivos de confianza elegidos. Se recomienda evitar todos aquellos que acompañen siempre al equipo, como un teclado en el caso de una tablet. Si se robase el dispositivo de confianza junto con el teléfono a proteger, este quedaría desbloqueado exponiendo toda la información al atacante. Es importante saber que la señal *Bluetooth* puede ser imitada y que su rango puede ser variable, con un máximo de 100 metros de alcance.

- ***Reconocimiento facial***: una vez configurado, cada vez que se encienda la pantalla, el móvil intentará, a través de la cámara frontal, reconocer el rostro del usuario, desbloqueando el *smarphone* si la cara supera con éxito el análisis. Si no es capaz de reconocer la cara, se deberá introducir la contraseña. Es un método muy eficaz y rápido, aunque Google avisa de que alguien parecido al usuario podría desbloquearlo. Se realizó una prueba con el Xiaomi miA2 Lite con diez personas de la misma edad y sexo y ninguno salvo el propietario legítimo fue capaz de desbloquearlo. El reconocimiento depende, en gran medida, de la calidad de la cámara frontal, pudiendo ser más inseguro en móviles de gama más baja.

El principal problema llega cuando se intenta desbloquear el teléfono con una fotografía. El móvil de prueba se desbloqueaba sin problema al exponer la cámara tanto a una fotografía impresa como a una en la pantalla de otro móvil. Para solucionar este problema, en algunos dispositivos existe un filtro que analiza el movimiento de la cara para diferenciar entre fotografía y realidad, pero de nuevo estos son fácilmente engañables con un vídeo o un *gif animado*. La calidad de este servicio depende, en gran medida, del fabricante y de la gama del teléfono, siendo francamente más fiables en teléfonos de gama alta.

Para configurar este sistema, se debe pulsar la opción de *Reconocimiento facial* y seguir las indicaciones y advertencias, como buscar un lugar con la luz adecuada y mantener los ojos a la misma altura. Después de esto, solo hay que mantener la cara en el círculo que aparece en pantalla mientras el teléfono obtiene capturas de la misma (véase Figura 3-17)

Figura 3-17 Pantalla mostrada mientras se crea el patrón facial

Para mejorar la eficacia, existe la posibilidad de *Mejora el reconocimiento facial*, para garantizar que funciona en distintas situaciones, como la falta de luz, barba, gafas, etc. El resultado a la prueba de fotografías es el mismo, así que no se puede confirmar que sea una mejora en cuanto a seguridad. Es más, dado que se pueden añadir rasgos diferentes, posibilita que mayor número de personas con esos rasgos puedan acceder al móvil.

- ***Voice Match:*** es la aplicación que permite principalmente gestionar el Asistente de Google a través de la voz para búsquedas en Internet. También existe la posibilidad de activar el desbloqueo por reconocimiento de voz, siendo necesario para esto tener activado dicho asistente. Al intentar activar esta opción, aparece un mensaje que ya avisa de que alguien con voz parecida a la del propietario puede acceder al teléfono. Si se decide utilizar este sistema, desaconsejable desde un punto de vista de seguridad, sería necesario entrar en el ajuste de *Voice Match*, activar *Acceder con Voice Match*, para dar permiso al asistente y, posteriormente, activar *Desbloquear con Voice Match*. Si no se había realizado previamente, será necesario crear un modelo de voz, para que el dispositivo sea capaz de generar un patrón con la voz que escuche. Para ello basta con aceptar el aviso que informa de que esta opción es insegura, y decir en voz alta cuatro veces la fórmula utilizada para llamar al asistente: "Ok, Google". Cada vez que se quiera desbloquear el teléfono por este método, se deberá pronunciar dicha fórmula, y en el caso de que no sea capaz de reconocer la voz, el móvil tendrá que ser desbloqueado de forma manual.

Como se mencionó previamente, la calidad de estos servicios depende bastante de la calidad de la plataforma en sí. Para comprobar este servicio, se han realizado diversas pruebas para ver cómo reaccionan móviles de distintos fabricantes y precios, todos ellos Android. La mayoría de los móviles testados se desbloqueaban con voces de distintas personas (nunca en el caso de distinto género). La misma prueba se llevó a cabo, esta vez probando el reconocimiento facial, y los resultados fueron más tranquilizadores, ya que salvo el J5 de Samsung (que no dispone de este sistema) todos negaron el acceso a usuarios distintos. Sin embargo, muchos de ellos sí que se desbloquearon al ser expuestos a una imagen o vídeo de la cara del propietario.

En la Tabla 3-2 se muestra *Sí* si se desbloqueó en la prueba, *No* si no lo hizo y *X* si el móvil no tiene esa capacidad.

			Desbloqueo mediante			
Dispositivo	Fabricante	Versión Android	Voz distinta	Cara distinta	Imagen	Vídeo
mi A2 Lite	Xiaomi	9	Sí	No	Sí	Sí
J5	Samsung	8	Sí	X	X	X
S9 +	Samsung	8	No	No	No	No
3T	One Plus	8	No	No	No	No
3	One Plus	8	Sí	No	Sí	Sí
Moto G5	Motorola	8	Sí	No	Sí	Sí

Tabla 3-2 Resultados del análisis de *Smart Lock* en distintos teléfonos

Los resultados de la prueba confirman que el buen funcionamiento de *Smart Lock* no depende en gran medida de la versión de Android, sino que principalmente depende del fabricante y del *smartphone* en sí. Una mejor cámara o un mejor micrófono son la clave a la hora de garantizar un buen servicio.

3.4.4 Configuración de la pantalla de desbloqueo

En este apartado se tratará de explicar la importancia de la configuración de la información que se muestra en la pantalla antes de acceder al teléfono. Algunas aplicaciones pueden mostrar notificaciones, llegando a desvelar información sensible, como mensajes personales, códigos, etc. Incluso es posible desactivar algunas funciones desde el menú de configuración de ajustes rápidos. En algunos casos, un mal ajuste de estos parámetros puede llegar a ser crítico.

Se partirá de la configuración por defecto, analizando las distintas opciones disponibles desde la pantalla de desbloqueo. Comenzando de arriba abajo, se puede observar a la izquierda de la pantalla *Falta la tarjeta SIM*, de introducirse, aparecería el nombre de la compañía contratada. Las aplicaciones que tengan permiso para ello podrán indicar, con un símbolo característico, que hay notificaciones nuevas. En la parte derecha aparece el estado de diversas funciones del sistema como la cobertura, la batería, *Bluetooth* y Wi-Fi (si están activados) o si el móvil está en silencio o no. En el centro aparece la hora y la fecha, y más abajo se encuentran tres símbolos: el micrófono, para utilizar el Asistente (requiere desbloquear el teléfono), el candado, que indica si el teléfono está desbloqueado o no, y la cámara, que permite sacar fotografías de forma rápida sin necesidad de acceder al móvil (no permite la visualización de las imágenes obtenidas).

Estos parámetros podrían ayudar a un ladrón al desvelar ciertos aspectos de seguridad. Pero el principal riesgo de esta pantalla es que permite el acceso al menú de ajustes rápidos, permitiendo activar y desactivar los parámetros que aparezcan. Por defecto, aparecen los que se pueden ver en la Figura 3-18. En algunos casos, como puede ser la *Linterna*, sí que es cómodo poder hacer uso de esta función sin necesidad de desbloquear el dispositivo. Pero el hecho de que permita desactivar la Wi-Fi, el *Bluetooth*, los datos móviles o directamente poner el *Modo avión*, constituyen una importante brecha de seguridad. Si un atacante tuviese acceso físico al teléfono, podría desactivarlos, haciendo imposible

hacer uso de servicios como *Encuentra mi dispositivo*, por lo que no se podría bloquear de forma remota o acceder a la ubicación del móvil.

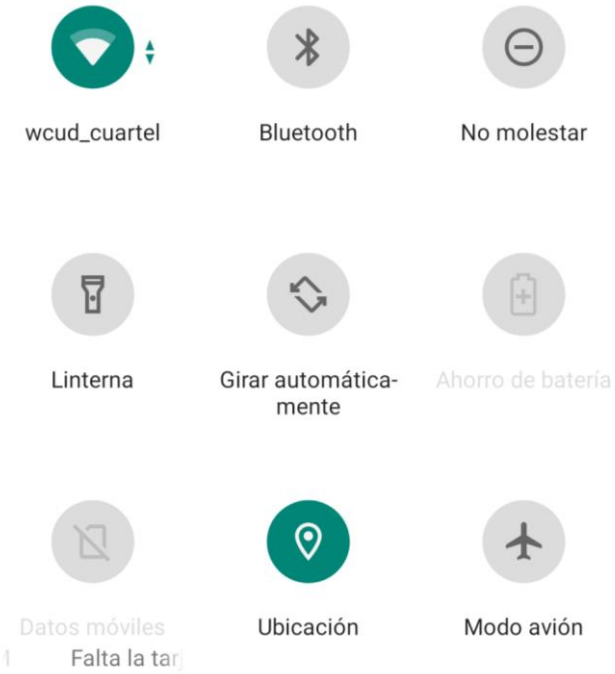

Figura 3-18 Menú de ajustes rápidos de la pantalla de bloqueo

Otros parámetros pueden añadirse a este menú, para lo que hace falta acceder al teléfono, deslizar el dedo hacia abajo para abrir dicho menú y pulsar el botón con forma de lápiz. Se pueden añadir a la pantalla de desbloqueo el control de la ubicación, el de zona Wi-Fi, Invertir colores, Ahorro de datos, y Luz nocturna. El de ubicación se recomienda no añadirlo, por los motivos anteriormente explicados. Es más, para garantizar la seguridad del dispositivo en caso de pérdida o robo, se han de retirar, como mínimo, los controles sobre Wi-Fi, *Bluetooth*, datos móviles y el modo avión.

Precisamente, las versiones a partir de Android 7.x no permiten que algunas de las funciones accesibles desde ajustes rápidos se modifiquen sin autenticación por parte del usuario, solventando así el problema. Sin embargo, algunos fabricantes (entre ellos, Xiaomi) no tienen este aspecto contemplado en su ROM (salvo para la función *Enviar* de Xiaomi). En el teléfono de estudio, no existe la posibilidad de activar este extra de seguridad, por lo que la única opción para no comprometer la seguridad es realizar el proceso detallado previamente.

3.4.5 Gestión remota del dispositivo

Un usuario particular puede acceder a gestionar de forma remota su dispositivo a través del servicio *Encuentra mi dispositivo*. Esta función, que en Android 4.4 era una aplicación, ahora es un recurso integrado de *Google Play Protect.* Actualmente esta función se encuentra activada por defecto y es posible realizar modificaciones en la misma a través del menú *Seguridad y ubicación.*

Este servicio necesita de ciertos requisitos para poder funcionar:

- Necesita comunicación con los servidores de Google, para lo que requiere tener conexión a una red Wi-Fi o a una red de datos móviles. En caso de no tener conexión, las órdenes que se le envíen al teléfono quedarán a la espera y se ejecutarán cuando éste se conecte. Debido a este requisito, es evidente que no funcionaría en caso de estar el móvil apagado o en modo avión. Asimismo, es necesario que la *Ubicación* esté activa.
- Administrador de dispositivos activo: *Aplicaciones y notificaciones>> Avanzado>> Acceso especial de aplicaciones>> Aplicaciones de admin. de disp.* En este menú aparecen todas las

aplicaciones con este permiso. Se debe comprobar que el servicio está activado y verificar que no existe ninguna aplicación con este permiso sin que seamos conscientes. En este teléfono, de forma predeterminada la aplicación *Google Pay* (permite el pago por NFC y gestionar cuentas bancarias) tiene dicha autorización y, dado que no se pretende utilizar, se debe desactivar.

- Se debe tener iniciada una cuenta de Google en el dispositivo (básico para aprovechar correctamente los servicios de Google y lo más común es tenerla iniciada siempre).

Existen varias formas de utilizar este servicio. Se puede descargar la aplicación de *Play Store*, lo que permitirá acceder a otros dispositivos móviles a través de otro dispositivo Android. Otra forma sería acceder a la URL *https://myaccount.google.com/find-your-phone*, gracias a la cual, iniciando sesión de Google en cualquier dispositivo electrónico, se puede acceder a las funcionalidades de *Encuentra mi dispositivo*. Esta última será la que se utilice en el presente TFG, por ser la más común (no requiere descargarse la aplicación y permite su uso en cualquier dispositivo).

Una vez se accede vía Internet a la función *Encuentra mi dispositivo*, introduciendo correo electrónico y contraseña, aparece el menú de la Figura 3-19. Si se hace click en *Hacer sonar*, el móvil recibirá la orden de sonar y la ejecutará al máximo volumen, aunque se encuentre en modo silencio, hasta que se desbloquee el teléfono. Es útil en caso de pérdida, pero no tanto si el móvil ha sido robado, ya que se puede detener el sonido apagando y encendiendo la pantalla varias veces, o automáticamente después de cinco minutos.

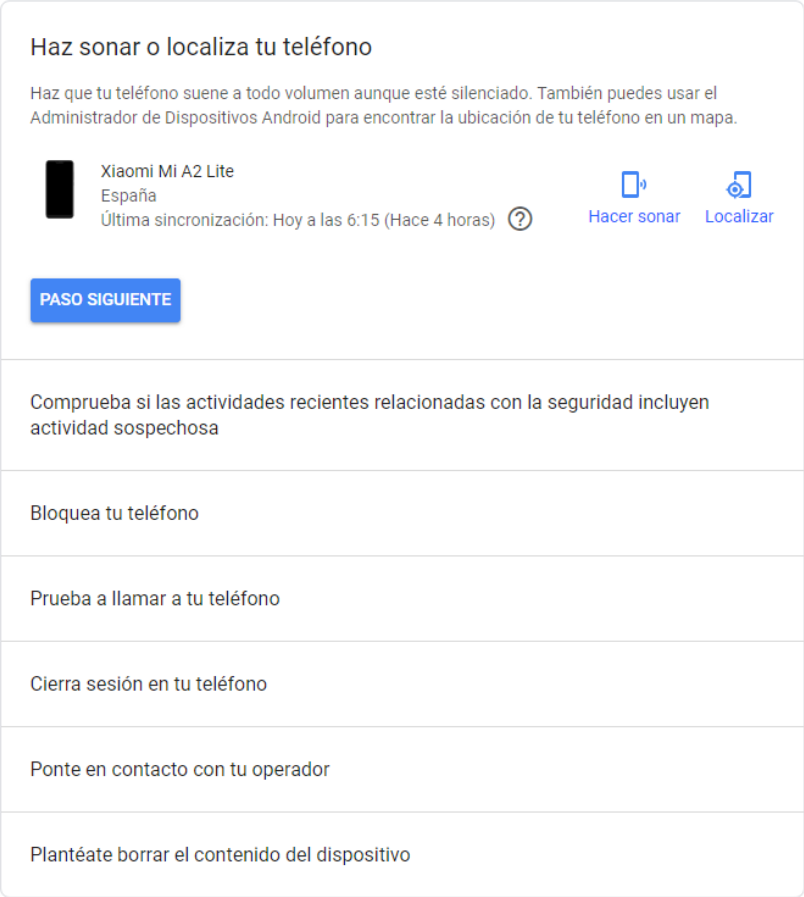

Figura 3-19 Menú de *Encuentra mi dispositivo*

Si se pulsa en localizar, se abrirá una pestaña (véase Figura 3-20) que mostrará en *Google Maps* la posición del teléfono, pudiendo aumentar para mayor exactitud. En el lado izquierdo de la pantalla se observa información sobre el teléfono: IMEI/MEID (código único de identificación del móvil), la última conexión (se refiere a la última vez que se sincronizó alguna de las aplicaciones de Google), el estado de la batería y, si es el caso, la red Wi-Fi a la que está conectado. Es importante refrescar esta

información, lo que nos permitirá conocer la situación en tiempo real o que sigue conectado. A su vez, desde dicha pestaña es posible efectuar algunas de las órdenes también disponibles en la Figura 3-19.

Volviendo a la captura de la Figura 3-19, existe la posibilidad de comprobar las actividades más recientes efectuadas pulsando en *Paso siguiente*. Se incluye toda la información relevante para la cuenta de Google como puede ser el registro de una nueva cuenta de correo electrónico o un teléfono como contacto de recuperación o el intento de acceso a la cuenta desde otro dispositivo. Una vez analizada la información, se permite denunciar alguna actividad sospechosa y, si es el caso, se propondrá cambiar la contraseña para garantizar que el usuario es el único con acceso a la cuenta (la nueva contraseña no impediría el uso del teléfono al atacante, solo restringe el acceso a Google). Para evitar cambiar la contraseña, se puede cerrar la sesión remotamente.

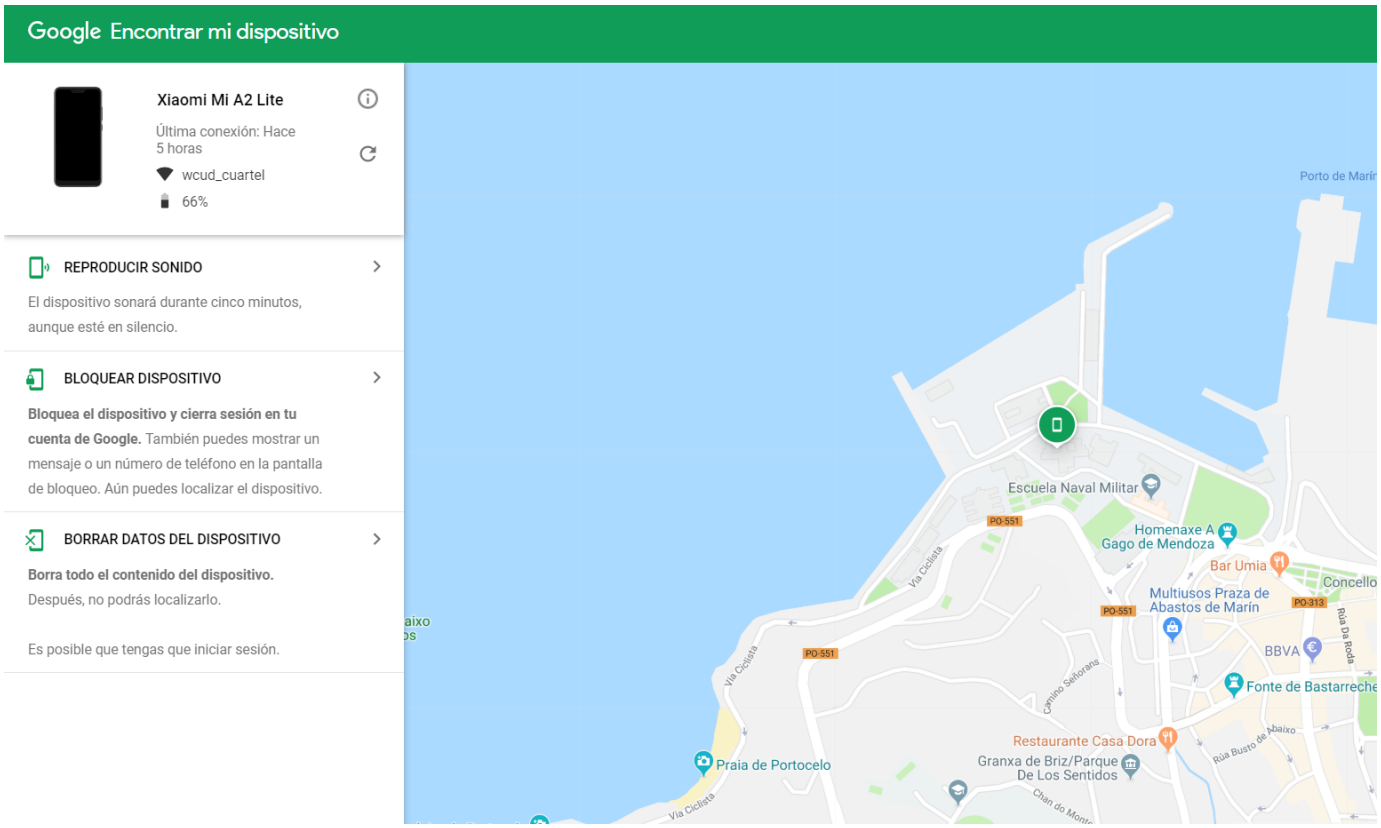

Figura 3-20 Localización del teléfono por *Encuentra mi dispositivo*

La opción de bloquear el teléfono es útil suponiendo que el teléfono tuviese un método inseguro de bloqueo, ya que permite establecer una contraseña de forma remota (Figura 3-21). Si ya se disponía de una contraseña, *PIN* o patrón, por mucho que se introduzca una contraseña nueva, ésta no cambiará. Los métodos alternativos de desbloqueo (*Smart Lock* o huella dactilar) quedan desactivados en este modo. También se puede introducir un mensaje en la pantalla y un número de contacto para facilitar que se devuelva el teléfono al propietario.

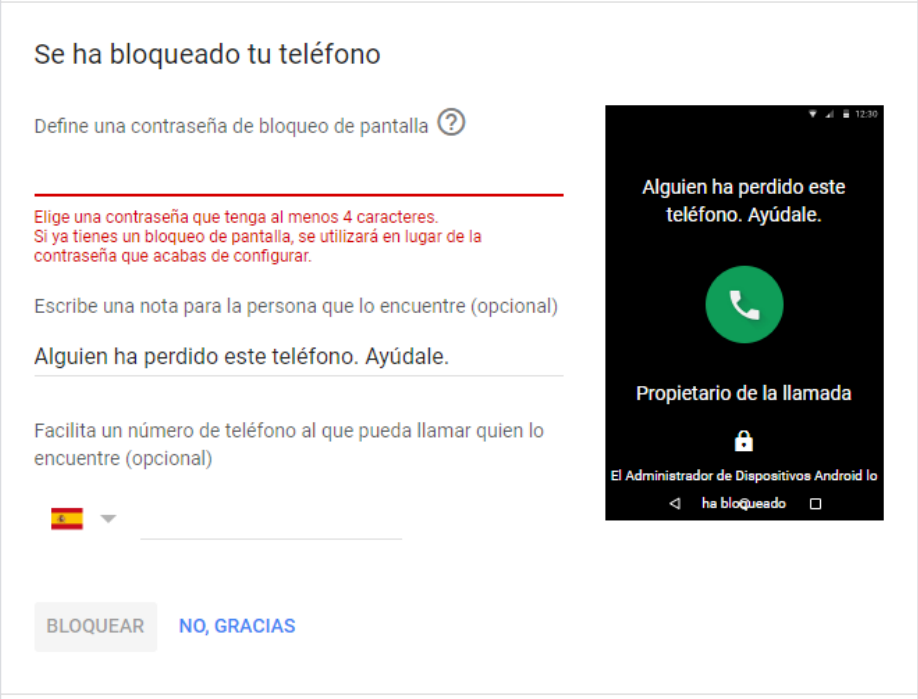

Figura 3-21 Bloqueo remoto del dispositivo

Se recomienda llamar al operador de telefonía, ya que es capaz desactivar la SIM y desviar las llamadas al número que se le indique. Así se evita que un atacante experto suplante la identidad, robe información o utilice servicios telefónicos Premium. El operador, además, tiene la capacidad de bloquear el teléfono, inhabilitando la conexión de teléfono y datos, para evitar el uso inapropiado del mismo. Este bloqueo se realiza indicando el IMEI y, aunque es efectivo, el desbloqueo en caso de recuperación del teléfono es largo, así que no debe considerarse como primera opción.

Como última opción, cuando se es consciente de que no se va a recuperar el teléfono o que éste almacena información especialmente sensible, es posible borrar el contenido del móvil. Se han de tener siempre presentes los avisos de Google: "Es posible que no podamos borrar por completo todas las tarjetas de memoria de tu dispositivo. La función Encontrar tu móvil y el Administrador de Dispositivos Android ya no podrán localizar, hacer sonar ni bloquear tu teléfono. Perderás de forma permanente el acceso a toda la información del dispositivo de la que no se haya hecho ninguna copia de seguridad en Google". El teléfono realizará un reseteo de fábrica pero, al contar con el mecanismo FRP (*Factory Reset Protection)*, el ladrón no podrá instalarlo de cero y usarlo como si fuera suyo. Esta protección está activada siempre que haya una cuenta de Google iniciada en el dispositivo. Tras un reseteo de fábrica, se le solicitarán al usuario unas credenciales enviadas a la cuenta del anterior propietario.

A estas alturas es posible darse cuenta de que esta funcionalidad resulta inútil en caso de que el teléfono se quede sin batería o peor, que el ladrón lo apague consciente de que puedan encontrarlo. Por este motivo, algunos fabricantes como Samsung han comenzado a introducir medidas como que el teléfono solo pueda ser apagado manualmente a través de la huella o un *PIN*. Android no incluye esta medida de forma nativa, por lo que el Xiaomi mi A2 es vulnerable en este aspecto.

3.5 Seguridad en las comunicaciones

En este apartado se estudiará cómo se garantiza la seguridad en el uso de redes Wi-Fi, USB y *Bluetooth*. Supone un aspecto muy importante ya que, a día de hoy, los *smartphones* son los principales medios utilizados para la comunicación.

3.5.1 Bluetooth

Se trata de una tecnología inalámbrica de corto alcance (máximo 100 metros teóricos) utilizada principalmente para el control remoto de otros dispositivos o para la transferencia de datos. Su éxito se debe principalmente a su bajo consumo de batería y al hecho de no necesitar una infraestructura de red, como si ocurre con el Wi-Fi o los datos de telefonía móvil. Actualmente, *Bluetooth* se divide en *Bluetooth Basic Rate / Enhanced Data Rate/ High Speed (BR/EDR/HS)*, conocido como el clásico, con velocidades de transmisión de hasta 24Mbps y *Bluetooth Low Energy (Bluetooth LE)*, de menor consumo de batería con hasta 3Mbps [48].

Bluetooth cuenta con su propia arquitectura de seguridad [49], que se basa en la generación de claves (a través de un *PIN)*, almacenamiento y autenticación de las mismas, cifrado y firma de datos. Algunos aspectos de seguridad varían en función del tipo de *Bluetooth*. Pese a todo esto, sigue siendo una tecnología muy aprovechada por delicuentes, que explotan vulnerabilidades, que a día de hoy siguen apareciendo (véase apartado 2.2.2).

Android no permite modificar demasiados parámetros de esta función en sus dispositivos (véase Figura 3-22). Desde *Ajustes rápidos* se puede activar y desactivar la interfaz. Desde el menú propio de *Bluetooth* únicamente aparece la opción de vincularse a nuevos dispositivos y el nombre del teléfono. Se recomienda cambiar el nombre que aparece por defecto (en este caso *Mi A2 lite*), ya que desvela el fabricante y modelo del mismo, facilitando pistas a un posible atacante. Desde el momento en que se activa, el móvil intenta conectarse de forma automática a aquellos dispositivos a los que se vinculó una vez (sigue un orden alfabético para ello). Si se quiere vincular a un nuevo dispositivo, se comienza un rastreo de todos los que estén al alcance. En el momento que empieza a buscar, el móvil será visible para todos ellos. Este aspecto no es configurable desde Android 6.

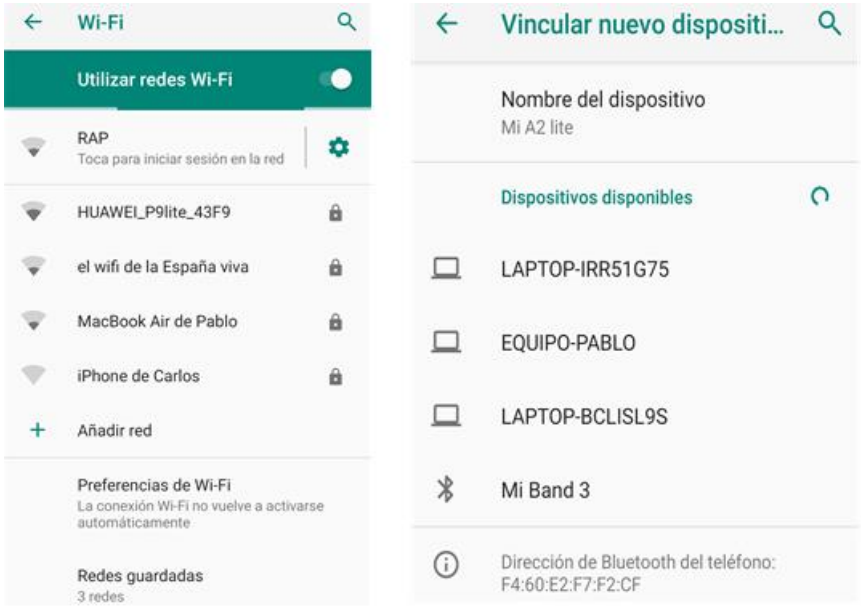

Figura 3-22 Menús de configuración Wi-Fi y *Bluetooth*, respectivamente

Como recomendación general se recomienda únicamente activar *Bluetooth* cuando se requieran sus servicios, si bien esto no garantiza la total invulnerabilidad frente ataques. Solo debe vincularse con dispositivos de plena confianza, teniendo en cuenta que el momento más susceptible de ataques *MitM* es el emparejamiento, durante el cual se comparten las claves.

3.5.2 Wi-Fi

Wi-Fi [50] es posiblemente la tecnología más común y popular para la conexión a Internet o la transferencia de datos. Ofrece mejores velocidades que el *Bluetooth*, así como mayores alcances y, consecuentemente su uso conlleva un consumo mayor.

Wi-Fi también puede ofrecer mejores prestaciones de seguridad, dependiendo del tipo de red que se utilice. Una red *abierta* no dispone de mecanismos de seguridad; las redes *WEP* solicitan contraseña, pero desde 2001 se consideran inseguran. Las redes tipo *WPA y WPA2*, que además cifran el tráfico, tampoco son seguras al haberse conseguido vulnerar su protocolo de seguridad. Actualmente se están implantando las redes *WPA3*, que por el momento son seguras.

Android permite mayor grado de configuración que en el caso de *Bluetooth* (Figura 3-22), si bien han desaparecido algunos parámetros según han ido actualizando la versión de Android. Para realizar ajustes, se puede acceder directamente desde el menú de *Ajustes rápidos*. En este menú, aparecen todas las redes disponibles (excepto las ocultas). Si el móvil está conectado ya a una red, se permitirá visualizar información como la intensidad de la señal, la seguridad, la dirección IP, DNS, etc. Se permite cambiar el modo en el que se conecta a la red: *Detectar automáticamente*, *Tratar como red de uso medido* o *de uso no medido*. Si se trata de una red habitual y de confianza, la opción más cómoda es que se conecte automáticamente. Por lo general, no se recomienda modificar los parámetros de *Proxy* ni el de *Ajustes de IP* (establece el protocolo de asignación de direcciones IP, normalmente *DHCP*).

Volviendo a la captura de la Figura 3-22, al ajuste *Preferencias de Wi-Fi*, se recomienda desactivar *Activar Wi-Fi automáticamente* y *Notificaciones de redes abiertas*, para minimizar la interacción del dispositivo con redes desconocidas. Tampoco es recomendable *Instalar certificados*, y se debe sospechar de aplicaciones que soliciten instalar su propio certificado.

Figura 3-23 Menú *Preferencias de Wi-Fi*

Adicionalmente, se deben evitar las redes públicas abiertas, que no requieren contraseña para acceder, que son frecuentemente creadas y utilizadas por ciberdelincuentes para ataques *MitM*, aprovechando la red de escasa seguridad y sin cifrar.

3.5.3 USB

Universal Serial Bus (USB) es una tecnología de comunicación entre dispositivos a través de cables. En el caso de teléfonos móviles, se utiliza principalmente para conectarse al ordenador o para introducir dispositivos de almacenamiento externo. Este apartado se centra en la conexión a ordenadores debido a todas las posibilidades que ofrece (véase Figura 3-24 Opciones de conexión USB): *Transferencia de archivos*; *Compartir conexión USB*, para compartir de un dispositivo a otro la conexión a Internet; *MIDI* (*Musical Instrument Digital Interface*) para instrumentos musicales principalmente; *PTP*, para fotos en caso de fallo de la transferencia de datos*; Sin transferencia de datos*, para cargar el teléfono. Estas opciones no son compatibles entre sí y no se pueden utilizar simultáneamente.

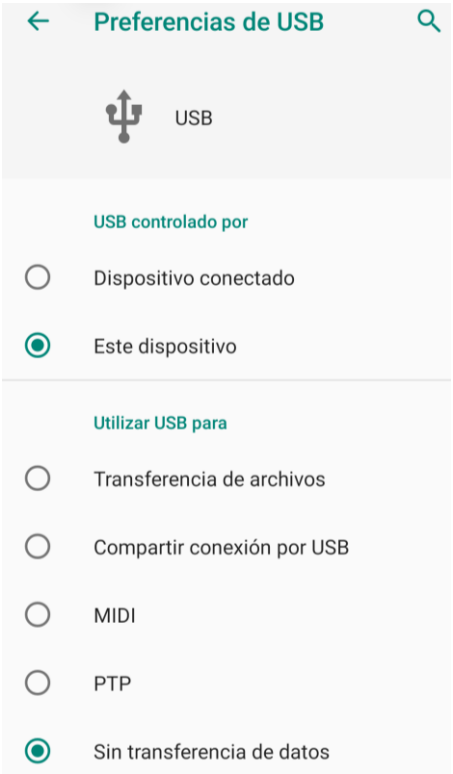

Figura 3-24 Opciones de conexión USB

Al conectarse por primera vez al ordenador, la opción *Sin tranferencia de datos* se encuentra establecida de forma predeterminada. El teléfono no será visible por el ordenador en este modo. Para cambiar de modo de funcionamiento es necesario desbloquear el móvil y seleccionar el deseado.

Cambiar la forma predeterminada con la que se conecta el dispositivo requiere desbloquear (en el caso de Xiaomi) las *Opciones de desarrollador*, un menú oculto pensado para facilitar algunas funciones a los desarrolladores de aplicaciones. Para desbloquear este menú, se ha de entrar en *Ajustes>>Información del teléfono* y pulsar repetidas veces sobre *Número de compilación*, hasta que aparezca que efectivamente se ha desbloqueado. Este nuevo menú aparece dentro de *Sistema>> Avanzado* y despliega multitud de funciones, donde la mayoría quedan fuera del ámbito de este trabajo. Ahora sí que se podrá modificar las preferencias de USB. Incluso si se cambia a, por ejemplo, *Transferencia de archivos*, el ordenador no reconocerá el móvil hasta que éste no se haya desbloqueado al menos una vez después de la conexión.

Sin embargo, el menú de *Opciones de desarrollador* ofrece otras funciones a través de USB. Los desarrolladores las utilizan para instalar sus aplicaciones o depurarlas. Activar la *Depuración por USB* proporcionará acceso a algunas funciones avanzadas mediante *Android Debug Bridge* (*ADB*), que es una herramienta con una lista de comandos. Antes de conectarse a un ordenador en modo depuración,

es necesario que se cree una relación de confianza entre ordenador y el móvil, mediante el mensaje de la Figura 3-25. No se debe autorizar esta conexión de forma predeterminada, ya que alguien con acceso al ordenador podría ejecutar comandos *ADB* sin necesidad de desbloquear el móvil.

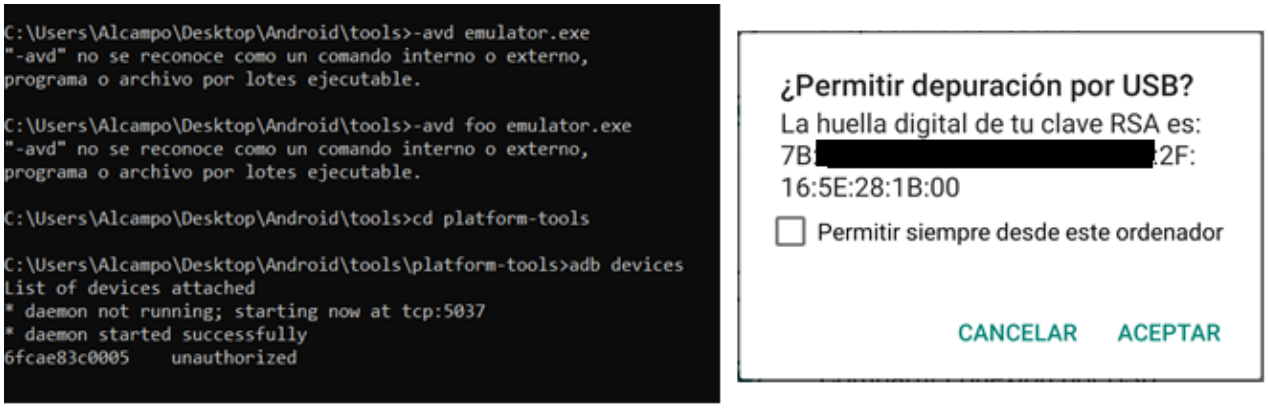

Figura 3-25 Dispositivos disponibles para acceso a depuración USB

Estos comandos están disponibles mediante la instalación de una suite que existe para distintas plataformas (*Windows, Linux*, etc) y se pueden descargar en la página oficial de Android [51]. Los comandos *ADB* pueden llegar a ser peligrosos si no se dominan. El motivo más común por el que suele utilizar estos comandos es para acceder al gestor de arranque y al modo *recovery*, que permite instalar una *ROM* distinta, resetear de fábrica el teléfono, actualizar el sistema operativo, etc. Dada la potencia de estas funciones, se recomienda no utilizarlas si no se tiene clara su forma de funcionamiento, ya que en algunos casos se borra el contenido del teléfono de forma automática. Además, tener habilitadas estas funciones aumenta el riesgo de que un atacante pueda acceder y dañar el dispositivo. Solo se debe activar la depuración para acciones concretas, después de la cuál se debe *Revocar autorizaciones de depuración USB* para que el ordenador tenga que solicitar acceso a depuración la próxima vez que se conecte.

3.6 Localización

La localización es una herramienta que utiliza datos obtenidos del teléfono para intentar identificar o situar el dispositivo en un mapa. Existen infinidad de aplicaciones que emplean esta funcionalidad y que se utilizan día a día, como las recomendaciones para llegar a un lugar, indicar la ubicación a unos amigos, encontrar restaurantes por la zona, etc. Pero, en muchas ocasiones, el usuario no es consciente de cómo funciona este servicio y qué ocurre con la información de ubicación. En este apartado, se pretende aclarar el funcionamiento de los sistemas de ubicación y explicar cómo configurar el teléfono para maximizar la privacidad del propietario.

3.6.1 Formas de localizar el dispositivo

El teléfono dispone de diversos medios para proporcionar ubicación, no únicamente el módulo GPS integrado en él, sino también la Wi-Fi, los datos móviles o el *Bluetooth*. Estos medios son configurables por el usuario, permitiendo desactivar la localización y volver a activarla cuando se requiera su uso. También son configurables las aplicaciones que tienen acceso a este servicio.

El uso del módulo GPS [52] es probablemente el más fácil de entender, ya que su funcionamiento es igual al de un coche, barco, etc. Utiliza la constelación americana de 24 satélites que orbitan la Tierra para triangular la posición. Android es compatible con otros sistemas satelitales como el GLONASS ruso y lo será para el sistema europeo Galileo [53]. Utilizando un mínimo de tres satélites sería posible triangular la ubicación, pero es necesario un cuarto que garantice una correcta configuración de los relojes.

Existen numerosas iniciativas para la geolocalización con Wi-Fi. La propia *Wi-Fi Alliance* certifica el estándar *Wi-Fi Location* [54], pensado principalmente para sustituir al GPS en interiores, donde la cobertura de éste se ve francamente deteriorada. Anteriormente se utilizaban otras técnicas, entre las que destacaba *RSSI* (*Received Signal Strength Indicator*) por su sencillez: mide la intensidad de la señal Wi-Fi que llega al teléfono, y conociendo la ubicación exacta del punto de acceso, se puede estimar la posición. Esta opción no es ni precisa ni económica, ya que necesita muchos *routers* repartidos por el edificio. Sin embargo, *Wi-Fi Location* no utiliza la intensidad de señal sino la velocidad de la onda, que es menos variable. Para obtener la ubicación utiliza un protocolo llamado FTM (*Fine Timing Measurement*). Básicamente, este protocolo utiliza un sistema de pregunta y respuesta para medir el tiempo que tarda en llegar la onda al dispositivo, y con ello la distancia. Con tres puntos de acceso (y conociendo la ubicación exacta de estos) es posible determinar la latitud y longitud en la que se encuentra, y, con un cuarto, se puede hallar la altura, de una manera muy precisa. Los relojes, tanto del dispositivo con los de los puntos de acceso, deben sincronizarse en el orden de nanosegundos. FTM es capaz de diferenciar si la onda llega reflejada o de forma directa, y no se necesita estar conectado a la Wi-Fi en cuestión, ya que obtiene la información necesaria desde el proceso de pre-asociación. Los paquetes están protegidos por cifrado WPA2, manteniendo, en principio, la seguridad y la privacidad.

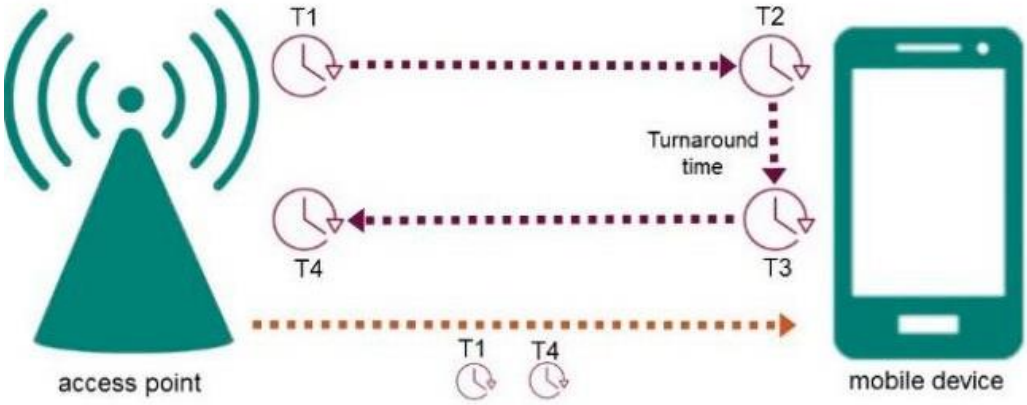

Figura 3-26 Simplificación gráfica del protocolo *Fine Timing Measurement* [54]

Sin embargo, la forma más general por la que los dispositivos Android obtienen la ubicación por Wi-Fi es distinta y mucho menos precisa. Si la configuración establecida lo permite, el teléfono escaneará constantemente las diferentes redes que encuentre y éstas, aunque estén cerradas, compartirán su localización con él. Si se le permite al móvil este tipo de localización, la utilizará aunque la Wi-Fi esté desactivada. En muchos equipos, al activar esta opción, aparece el aviso de que Google podría recopilar información sobre la ubicación de forma anónima para mejora de los servicios.

El teléfono también tiene la capacidad de ubicarse gracias a la telefonía móvil. Para entender este concepto, es necesario conocer cómo se distribuyen las antenas de telefonía. Para poder garantizar un buen servicio, una zona geográfica se divide en celdas (*cells)* y cada una de ellas dispone de su propia torre de telefonía. Los móviles se engancharán a una torre u otra en función de la calidad de señal, por lo que, aunque un teléfono esté conectado a una estación, continuará buscando otras que le den mejor calidad de servicio. Los operadores pueden estimar, por tanto, a través de varias estaciones, una posición del teléfono. Además, se sabe que las estaciones tienen un registro de los móviles conectados a ellas para, por ejemplo, redireccionar una llamada a la estación adecuada, lo que a su vez ayuda en la obtención de la ubicación. La calidad de la ubicación obtenida depende del número de antenas de telefonía, siendo en núcleos urbanos mucho más precisa que en zonas rurales. En la Figura 3-27, se observa la distribución de antenas (puntos azules) en la zona centro de Pontevedra. Debido a la gran cantidad de estaciones, es fácil suponer la gran precisión de la ubicación que se puede obtener.

La información de localización almacenada por las operadoras es confidencial, hasta el punto en que la Policía solo puede obtenerla por orden judicial, cuando se considera que el individuo investigado supone una amenaza contra la integridad física de otra persona. También, por ley, las operadoras deben guardar registro de los últimos doce meses [55]. Esta forma de ubicación es aprovechada por el teléfono pero aunque se deshabilite, las operadoras siguen teniéndolo registrado, incluso si está en modo Avión. La única forma de evitarlo sería apagando el móvil.

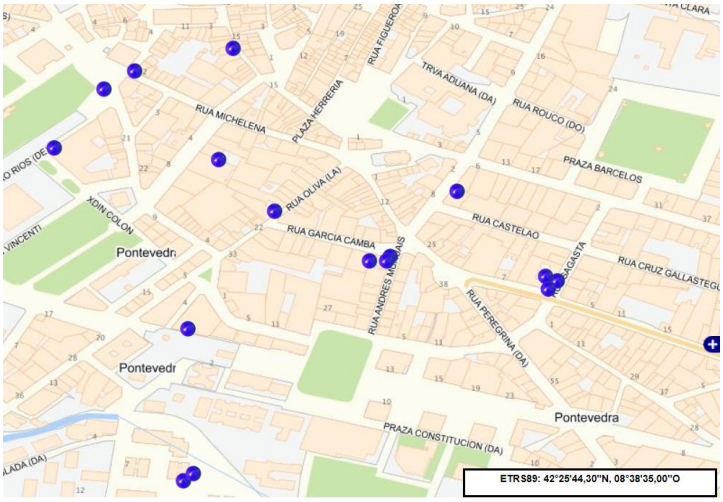

Figura 3-27 Distribución de estaciones de telefonía en el centro de Pontevedra [56]

La combinación de GPS, Wi-Fi y la telefonía móvil, para temas de ubicación, es conocida como *Assisted GPS (A-GPS)*, que sirve precisamente para auxiliar a la información obtenida por el GPS para mejorar la ubicación. No sólo hace uso de los métodos mencionados previamente, sino que también utiliza la conexión de datos para obtener en tiempo real información sobre los satélites y la sincronización de relojes, con el objetivo de agilizar la primera localización del móvil. Al utilizar datos, es posible monitorizar este tráfico, lo que constituye una amenaza.

Adicionalmente, los teléfonos también pueden mejorar la precisión en la localización mediante el uso de *Bluetooth*. El sistema utiliza los diferentes dispositivos *Bluetooth* próximos de la misma forma que se utilizan las antenas de telefonía. Estaba inicialmente pensado para mejorar la localización en locales y sitios cerrados, pero en la actualidad cada vez es mayor la cantidad de *Bluetooth Beacons* (balizas) repartidas por toda la ciudad para potenciar este sistema. De nuevo, no es necesario activar el *Bluetooth* del móvil para que sea posible esta funcionalidad.

Finalmente, el dispositivo móvil cuenta con diversos recursos, como el acelerómetro, la brújula, el barómetro, etc, que a priori no utiliza para ubicarse. Sin embargo, en la Universidad de Princeton se desarrolló un estudio [57] en el cual demostraban que era posible rastrear a un usuario analizando la información que estos medios proporcionaban. En el estudio, se suponía que una aplicación maliciosa era capaz de obtener información. Teniendo en cuenta que el acceso a estos servicios no se considera crítico, existen muchas aplicaciones que tienen acceso a ellos. En dicho estudio, se creó una aplicación llamada PinMe, que combinando esos datos con otros de uso público, como el informe meteorológico o los horarios de transporte público, era capaz de recrear el recorrido del usuario. En la Figura 3-28, la línea negra representa el camino real seguido, obtenido por GPS, y las líneas verde y naranja representan, respectivamente, el camino recorrido andando y conduciendo, según PinMe. La aplicación no necesita, a diferencia de otras aplicaciones, la ubicación inicial del usuario.

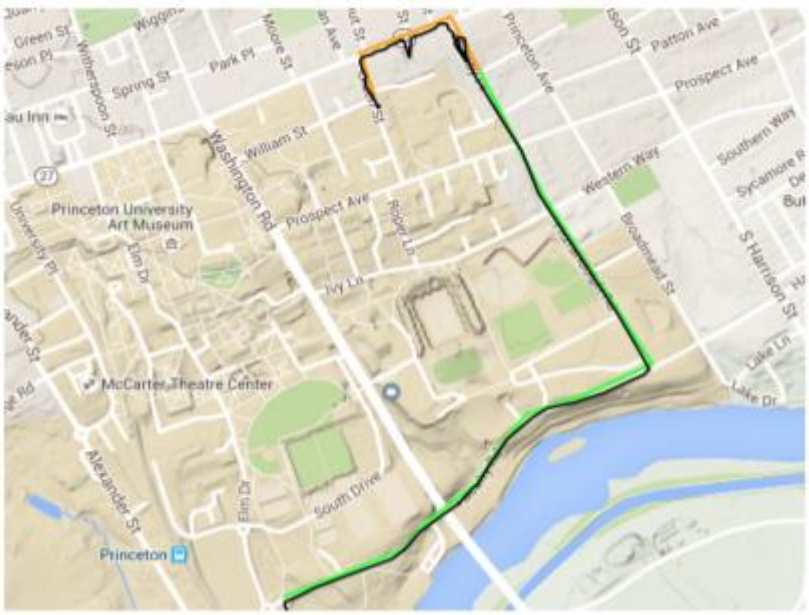

Figura 3-28 Resultado de la prueba de PinMe [57]

Los resultados de este trabajo evidenciaron la facilidad con la que un atacante puede rastrear al usuario. El giróscopo o el acelerómetro, al no entrar dentro de los servicios críticos, no solicitan permiso para ser utilizados, por lo que las aplicaciones pueden hacer uso de estos sin saberlo el propietario, lo que puede llevar a una importante pérdida de privacidad.

Actualmente, no se pueden autorizar permisos a ciertos servicios del sistema, entre ellos los que utilizaba la aplicación PinMe. La solución a este problema de privacidad depende de un cambio el modelo de permisos de Android. A día de hoy, el usuario debe analizar con atención las funcionalidades a las que accede cada aplicación (en Google Play antes de instalar), en busca de alguna irregularidad o sospecha, en cuyo caso no debe descargar dicha aplicación.

3.6.1 Configuración de la ubicación

Este apartado planteará la configuración para dos versiones de Android: versión 9 de Xiaomi mi A2, y la versión 8.1 de Samsung J5, para posteriormente analizar si la actualización mejora o no la seguridad. Esta decisión se debe a numerosos cambios en el menú de ajustes de ubicación que se producen al actualizar a la versión 9, junto con el hecho de que, a fecha de realización de este TFG, únicamente los dispositivos Android One (aún franca minoría) tienen acceso a esta actualización. Debido a que se va a utilizar un dispositivo Samsung, es posible que los nombres en los ajustes varíen entre los distintos fabricantes.

En el Samsung J5, el menú de Ubicación no se encuentra en el menú de seguridad, sino en el de *Conexiones*. Dentro de dicho menú, se encuentra *Método de ubicación*, que permite elegir entre tres opciones de ubicación (véase Figura 3-29: *Precisión alta, ahorro de batería, solo teléfono* (el nombre de las opciones varía ligeramente según el fabricante). La opción *Precisión alta* utiliza GPS, Wi-Fi, redes móviles y *Bluetooth* para garantizar la mejor y más rápida localización. Precisamente para ahorrar batería, el segundo método prescinde del GPS. Y finalmente, el método solo teléfono, utiliza únicamente el módulo GPS. Si se selecciona *Precisión alta*, aparece un mensaje por el cual se avisa al usuario que Google recopilará información de la ubicación periódicamente, de forma anónima, para compartirlo con las aplicaciones y que éstas sean capaces de ubicar más eficientemente. Lo mismo ocurre con *Ahorro de batería.* Google informa de que solo si se activa la ubicación realizará ese registro de localización.

Figura 3-29 Método de ubicación en Samsung J5

Una vez analizado el método de ubicación, por el cual el usuario puede, en definitiva, elegir la precisión con la que quiere que se le ubique, surge la pregunta de para qué sirve el menú *Mejorar la precisión.* Dentro de esta opción se encuentra la búsqueda con Wi-Fi y búsqueda con *Bluetooth* (funciones que ya utilizaban en *Precisión alta).* Ambas opciones proporcionan información sobre su función y funcionamiento. Siempre que se quiere activar alguna de estas medidas, esta información es recordada con un aviso y debe ser aceptada por el usuario. No es necesario activar ni Wi-Fi ni *Bluetooth* para su funcionamiento. Es interesante observar que, en este caso, no se indica que estas búsquedas queden desactivadas cuando el servicio de ubicación se desactive o, dicho de otra forma, las aplicaciones podrían estar usando esta función para conocer la ubicación, sin que el propio usuario requiera conocerla.

Se recomienda activar el servicio de ubicación únicamente cuando se requiera su uso. Desde el punto de vista de la seguridad y privacidad, se recomienda a su vez utilizar el modo *Solo teléfono,* ya que, en la inmensa mayoría de casos, la precisión que proporciona es suficiente, y así se evita que Google pueda rastrear la localización del propietario y la comparta con otras empresas. Lo mismo ocurre con las opciones de mejora de la ubicación. Como se mencionó previamente, el tráfico de datos de estas funciones puede ser analizado por una tercera parte (no el tráfico a los servidores de Google, ya que utiliza protocolos de cifrado), pudiendo obtener información del dispositivo para usos maliciosos.

Volviendo al menú de la captura, la opción muestra qué aplicaciones han accedido recientemente a los servicios de ubicación. Se recomienda realizar un análisis exhaustivo de todas las aplicaciones para asegurar que solo las que lo necesitan tienen permiso para ello, evitando que aplicaciones maliciosas compartan la información de localización.

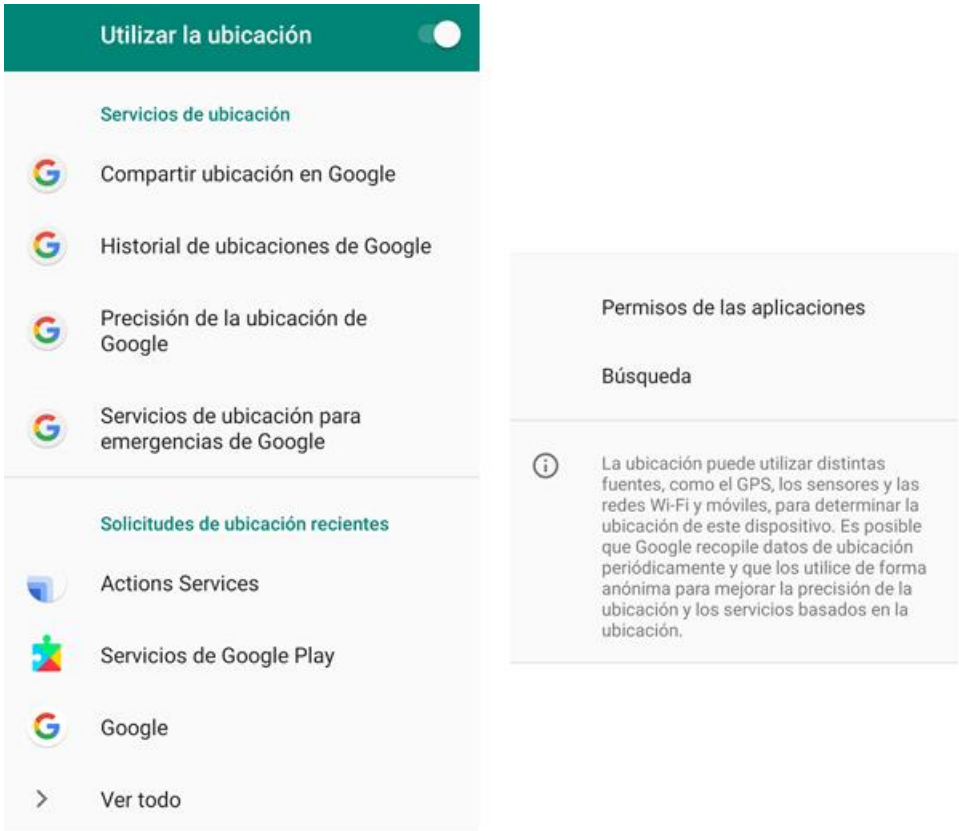

Figura 3-30 Menú de Ubicación Xiaomi mi A2

En la Figura 3-30, se observan los distintos ajustes relativos a la ubicación (en el caso de Xiaomi). Para acceder a este menú, se deben seguir los siguientes pasos: *Ajustes>>Seguridad y Ubicación>>Privacidad (Ubicación).* Como se puede observar en la captura, el menú está orientado a la configuración de los servicios de ubicación de Google. En este apartado no se entrará en detalle en estos servicios, salvo el de *Precisión de la ubicación de Google.* Si se presiona en esta opción, aparece únicamente la posibilidad de activar o desactivar *Mejorar la precisión de la ubicación* (véase Figura 3-31). Esta opción reemplaza al tradicional *Método de ubicación.* Si bien el aviso de que se recopila información sigue vigente, se ha realizado una modificación al mismo: no se especifica que esta función se desactive al desactivar *Ubicación*. De hecho, al apagar el servicio de localización, se comprueba que este sistema sigue activado. El menú de *Búsqueda* es equivalente al de *Mejorar la precisión* de la versión 8.1, sin sufrir apenas modificaciones. Sin embargo, se ha añadido la opción de *Permisos de aplicaciones*, como acceso directo a aquellas aplicaciones que utilizan este servicio, para facilitar un análisis y mejor control sobre ello.

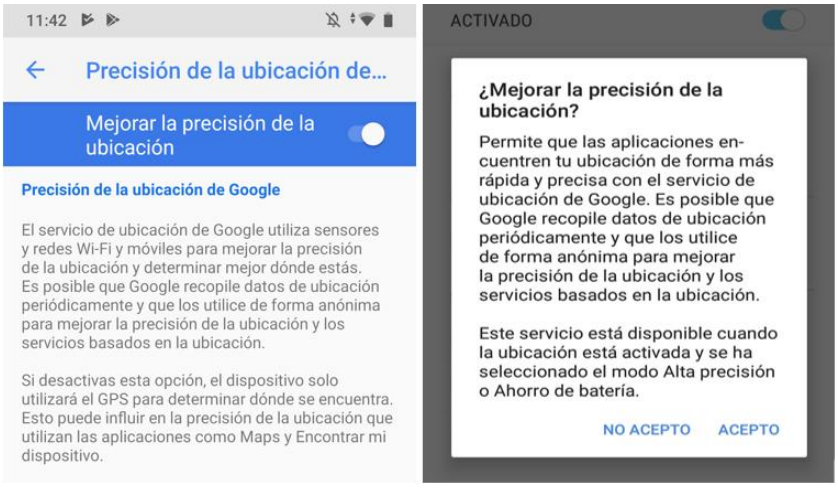

Figura 3-31 Avisos al activar la mejora de precisión (izda: v9 dcha: v8.1)

La conclusión que se extrae de este análisis es que al actualizar a la versión 9 de Android no se mejora la seguridad en la ubicación, sino que, en cualquier caso, la empeora. La versión 8.1 ofrece más información (y de forma reiterada) sobre cómo funcionan los servicios de ubicación. Android 9 ofrece la precisión de localización como un servicio de Google, mientras que en Android 8.1, esta función depende de la configuración propia del dispositivo. Además, Android 8.1 dispone de más métodos de ubicación, que sí se desactivan cuando la *Ubicación* no esta activada. En definitiva, la versión 8.1 se muestra mucho más transparente y no genera dudas sobre el rastreo de Google.

3.6.1 Servicios de ubicación de Google

En este apartado se explicará el funcionamiento de los distintos servicios que ofrece Google basados en la ubicación. Los teléfonos Android permiten su configuración a través del menú de la captura de la Figura 3-30, pero también se pueden configurar desde la aplicación (en el caso, por ejemplo, de Google Maps) o directamente sobre la cuenta de Google. También, se analizarán los distintos problemas que ha supuesto y supone actualmente Google para la privacidad.

- ***Compartir ubicación en Google***: Google permite compartir con otros usuarios la situación en el tiempo a través de distintos dispositivos, entre ellos los *smartphones*. Desde el menú de ubicación (Figura 3-30) no es posible compartir la ubicación, pero sí que da opción a dejar de compartir. La forma más cómoda de utilizar este servicio es a través de Google Maps, instalado de fábrica en todos los dispositivos móviles Android. El proceso se explica a continuación: para acceder a la mayoría de opciones que posee la aplicación, se debe pulsar el icono con tres pequeñas líneas horizontales (véase Figura 3-32). En el desplegable que aparece, se pulsa *Compartir ubicación.* Lo primero que se debe elegir es el tiempo durante el que se desea compartir la localización: se puede elegir entre un tiempo indefinido (hasta que se desactive) o un tiempo determinado, que tiene como mínimo 15 minutos y máximo 3 días. Después, se ha de elegir la forma en la que se va a enviar la solicitud para que accedan a la situación. Google contempla tres formas de hacerlo: en función de si el otro usuario tiene o no cuenta de Google, o por mensajería. En el caso en el que el receptor disponga de cuenta Google, y la aplicación tenga permiso para ver los contactos, se le enviará un correo electrónico con el enlace de ubicación de Google Maps. Si no es el caso, pulsando el icono de puntos de la tercera captura de la Figura 3-32, se podrá copiar en el portapapeles el enlace a través del cual cualquiera puede acceder a la ubicación (máximo 72 horas). De la misma forma, se puede compartir el enlace a través de distintas aplicaciones de mensajería (Mensajes, *Whatsapp*, etc).

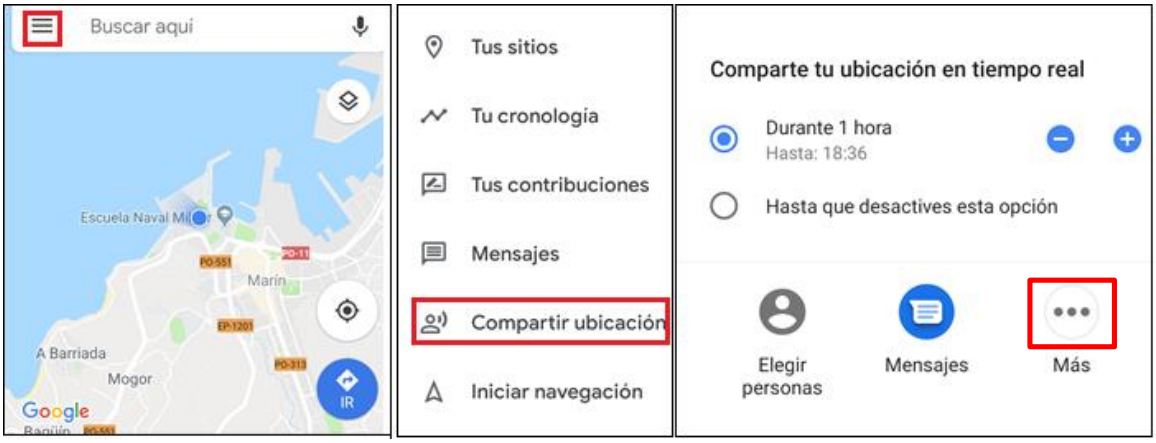

Figura 3-32 Proceso a realizar para compartir ubicación

La utilidad de este sistema es clara, ya sea para indicar a unos amigos cuánto le falta a uno para llegar, o para tener control parental sobre los hijos (existen aplicaciones específicas para ello). Sin embargo, desde el punto de vista de la privacidad, no se recomienda hacer uso de esta función, en ninguno de los dos sentidos. Si se comparte la ubicación con alguien, y a esta persona se le sustrae el teléfono, el ladrón podría localizarle, abriendo un sinfín de posibilidades maliciosas, incluyendo compartir el enlace de ubicación con más gente. De tener que hacer uso de esta función, se recomienda realizarlo durante un breve periodo de tiempo y únicamente con personas de plena confianza.

Un posible fallo que tiene este servicio es que el dispositivo no avisa de ninguna forma que se está compartiendo la ubicación con alguien, es decir, se podría estar indicando la situación del propietario sin éste saberlo. Este problema se hace patente en el caso de que se le olvide a uno desactivarlo o, por ejemplo, en el hipotético caso de que alguien cercano al usuario lo active para poder rastrearlo, violando su intimidad. Para este TFG, se le pidió a una persona de confianza el teléfono, con la excusa de consultar un momento la web, aunque realmente se compartió la ubicación a través del método comentado, eliminando posteriormente el mensaje con el enlace en el dispositivo, para no dejar evidencia. El experimento finalizó a las 24 horas, tiempo tras el cual se consideró que la víctima no se daría cuenta de que estaba compartiendo su ubicación, como efectivamente sucedió.

- ***Historial de ubicaciones de Google**:* este servicio de Google permite recoger toda la información de los sitios que se visitan, el recorrido realizado, etc. Google registra todos estos datos para mejorar la experiencia del usuario (no solo para otros servicios de Google, sino para otras aplicaciones), ofreciéndole el informe meteorológico de la zona, para recomendar restaurantes cercanos o para informar del tráfico existente. La opción que aparece en la captura de la Figura 3-30 no es más que un acceso directo a la página de ayuda de Google donde se trata este asunto [58].

  Es posible modificar estos parámetros desde la cuenta de Google, pero de nuevo se va a explicar desde la aplicación de Google Maps. En el menú de la captura Figura 3-32, se pulsa en *Tus sitios>>Ajustes*, lo que abrirá un menú con todos los ajustes sobre contenido personal de las ubicaciones. Se recomienda desactivar todas las opciones que comprometan la privacidad, especialmente las que no se utilicen. En la Figura 3-33, se observa la configuración predeterminada de estos parámetros. Al pulsar el ajuste con el nombre de este apartado, se entrará directamente en la cuenta de Google (sin tener que iniciar sesión), y se permite desactivar el historial para la cuenta en cuestión, o para los dispositivos asociados a la misma. Si se desactiva la primera opción (lo recomendado), saltará un aviso indicando que "este ajuste se pausará en todos los sitios web, las aplicaciones y los dispositivos en los que se haya iniciado sesión con esta cuenta". También se indica, que es posible que la ubicación se siga almacenando en la cuenta de Google a través de otras aplicaciones o servicios, como *Actividad*

en la Web y en Aplicaciones; pausar este servicio no eliminará los datos adquiridos anteriormente. Para eliminar el historial, se debe retroceder hasta el menú de *Contenido personal* (Figura 3-33), y al pulsar se avisará al usuario que de eliminarlo, ni siquiera Google podrá acceder de nuevo a los datos. Debido al peligro que supone para la privacidad, se recomienda eliminarlo completamente.

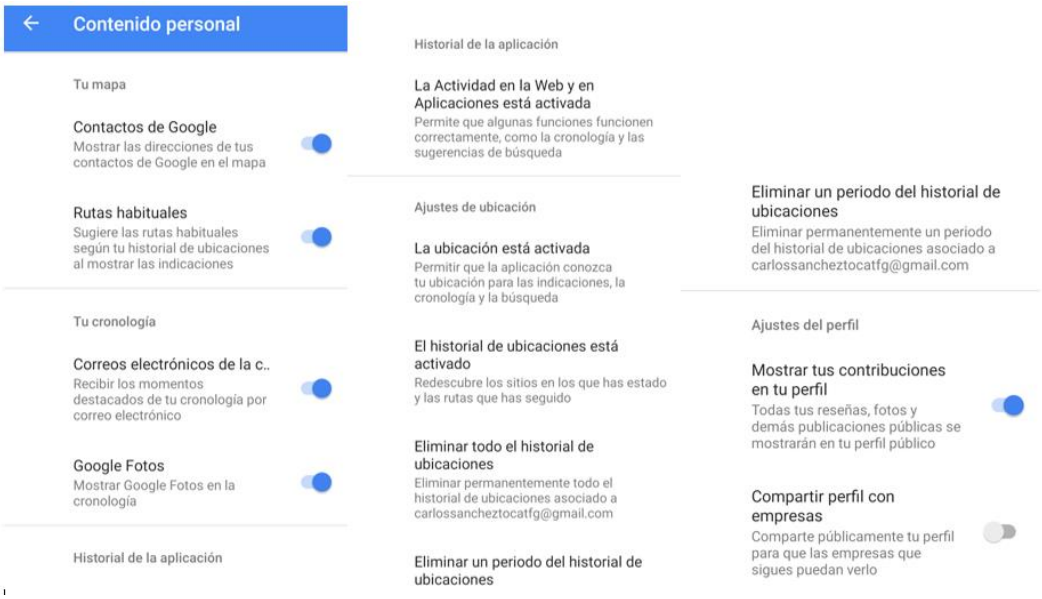

Figura 3-33 Configuración predeterminada de información personal en los ajustes de ubicación.

Existe una opción independiente del historial de ubicaciones llamada *Cronología*, que complementa al historial añadiendo una fecha a cada ubicación. De esta forma, el usuario puede acceder a esta información, los recorridos o sitios visitados. Esta información puede ser utilizada por otras compañías para ofrecer anuncios personalizados, ofrecer servicios o actividades que interesen al usuario, etc.

- ***Servicios de ubicación para emergencias de Google****:* sirve, como su propio nombre indica, para que los servicios de emergencia de cada país (en España, el 112), encuentren la posición del dispositivo con una simple llamada o mensaje. Para ello es necesario que cada país disponga de los medios para ello, siendo posible en España. Este sistema se activa únicamente cuando se contacta con los servicios de emergencia, siendo capaz de activar la ubicación de forma automática si estaba apagada, o incluso los datos móviles. Al finalizar su uso, el teléfono volverá a su configuración previa. Este sistema es diferente e independiente de la forma en la que Google Maps comparte la localización. Por ello, y dado su utilidad en caso de extrema necesidad, se recomienda mantener activado este servicio. Si por algún motivo se desea desactivar, únicamente se debe entrar en el ajuste del menú de la Figura 3-30 y pulsar en el botón para ello.

4 RESULTADOS Y VALIDACIÓN

A lo largo del desarrollo de este TFG, se han estudiado distintos aspectos de la seguridad en teléfonos móviles Android. Estos aspectos se pueden organizar en dos grupos: aquellos que son inherentes al *smartphone*, como la seguridad proporcionada por el sistema operativo, y los que dependen del usuario.

A su vez, este segundo grupo se puede subdividir en otros dos subgrupos: configuración segura y concienciación. Es necesario tanto una adecuada configuración del dispositivo como un mínimo nivel de formación o que el usuario esté concienciado de los riesgos a los que está expuesto.

Este apartado tratará sobre este segundo aspecto de la seguridad, proponiendo una configuración segura del teléfono, considerando tanto la seguridad como la accesibilidad del mismo. En cuanto a concienciación, también se explicarán medidas para evitar ataques de ingeniería social y los errores más comunes de los usuarios. Con el fin de demostrar que de nada sirve una configuración segura si no se utiliza de forma adecuada el dispositivo, se utilizará la aplicación *Mobile Tracker* [59], que usada de forma maliciosa, supone un grave riesgo a la privacidad.

4.1 Configuración segura

A continuación, se expone una serie de tablas resumen que incluyen todas las medidas, descritas y detalladas en el capítulo 3, para establecer en el móvil una configuración que lo proteja en la medida de lo posible. Junto a esta tabla aparecerán un conjunto de recomendaciones o consejos de seguridad, enfocados a que el usuario no cometa errores que le pongan en peligro.

Seguridad en el acceso al dispositivo:

	Medida	Seguridad	Accesibilidad
Bloqueo del dispositivo	Establecer *PIN* previo al arranque	No arranca el sistema operativo	Introducir una vez al encender
	PIN tarjeta SIM	Protección adicional	Introducir una vez al encender
	Sin seguridad	Sin protección	Buena
	Deslizar	Sin protección	Buena
	Patrón	Mala protección	Moderada
	PIN	Mala protección	Moderada

Bloqueo del dispositivo	Contraseña	Buena protección	Mala
	Huella digital	Buena Protección	Buena
	Smart Lock: facial	Protección moderada	Buena
	Smart Lock: voz	Protección moderada	Buena
	Smart Lock: lugar	Mala Protección	Buena
	Smart Lock: movimiento	Mala Protección	Buena
	Smart Lock: Dispositivo	Mala Protección	Buena
Pantalla de desbloqueo	Suspender pantalla después de 15 segundos de inactividad	Buena	Mala
	Suspender pantalla después de 1 minuto de inactividad	Moderada	Moderada
	Suspender pantalla después de 30 minutos de inactividad	Mala	Buena
	Mostrar todo el contenido (notificaciones)	Mala	Buena
	Ocultar contenido sensible (notificaciones)	Moderada	Moderada
	No mostrar (notificaciones)	Buena	Mala

Tabla 4-1 Medidas de protección en el acceso al dispositivo

Buscando un equilibrio entre accesibilidad y seguridad, la configuración recomendada es utilizar un *PIN*, que puede ser complementado con la huella digital. Los pasos a seguir aparecen detallados en los apartados 3.4.1 y 3.4.2.

Medidas adicionales y recomendaciones:

- Cambiar PIN por defecto de la SIM.
- Evitar contraseñas más comunes [46].
- No compartir con nadie la contraseña.
- Evitar contraseñas relacionadas con información personal (fechas, mascotas, etc).
- No utilizar la misma contraseña para distintas cuentas y cambiar cada cierto tiempo.
- No hacer visible patrones o contraseñas mientras se escriben.
- No permitir que se añadan usuarios en la pantalla de desbloqueo.
- Eliminar del menú de *Ajustes Rápidos*: *Bluetooth*, *Wi-Fi*, *Modo avión*, *Datos móviles* y *Ubicación*.
- No dejar sin supervisión el teléfono, sobre todo desbloqueado.

Seguridad en aplicaciones:

	Medida	Objetivo
Google Play	Activar *Buscar amenazas de seguridad*	Permitir a Google informar de daños o peligros en el móvil
	Activar *Mejorar detección de aplicaciones dañinas*	Permitir a Google comprobar que las aplicaciones desconocidas no son maliciosas
	Realizar análisis manuales frecuentemente	Aumentar la probabilidad de detectar peligros
	No desactivar *Google Play Protect*	Permitir la protección de Google
	Descargar únicamente de la *Play Store*	Instalar aplicaciones que han pasado numerosos filtros de seguridad de Google
	No autorizar descargas de aplicaciones de *origen desconocido*	Disminuir el riesgo de infección por *malware*
	No utilizar actualización automática de aplicaciones	Verificar que las actualizaciones no solicitarán nuevos permisos
Permisos de aplicaciones	Conceder únicamente los permisos que se consideren necesarios	No permitir que las aplicaciones accedan a información que no necesitar para su funcionamiento
	No conceder manualmente permisos	Garantizar que solo los permisos que interesan al usuario son concedidos
	Desactivar permisos de aplicaciones cuando ya no se requieran	Evitar el acceso a información o servicios que la aplicación ya no necesite
	Comprobar permisos que solicita la aplicación antes de descargarla	Aumentar la probabilidad de detectar posibles aplicaciones maliciosas
	Comprobar información de la aplicación (desarrollador conocido, número de descargas coherente, etc)	Aumentar la probabilidad de detectar posibles aplicaciones maliciosas
	Realizar análisis frecuentes de las aplicaciones instaladas	Aumentar la probabilidad de detectar posibles aplicaciones maliciosas

Tabla 4-2 Medidas de protección en la seguridad en las aplicaciones

Seguridad en comunicaciones:

Tipo de conexión	Medida	Objetivo
Bluetooth	Activar interfaz solo cuando se necesite	Evitar ataques que explotan este medio
	Intentar utilizar en entorno seguro, especialmente durante la fase de emparejamiento	Evitar ataques *MitM*, especialmente *eavesdropping*
	Cambiar el nombre por defecto por un nombre que no desvele información ni del usuario ni del dispositivo	Evitar facilitar a un tercero información que pueda ayudarle en un posible ataque
	No vincularse a dispositivos desconocidos	Evitar posibles dispositivos maliciosos
	No aceptar archivos ni mensajes no esperados	Evitar ataques de inserción de código
Wi-Fi	Activar interfaz solo cuando se necesite	Evitar ataques que explotan este medio
	Evitar conectarse a redes no seguras (abiertas, WEP, etc)	Evitar que se analice el tráfico y el robo o alteración de la información
	No conectarse a redes desconocidas	Evitar que se analice el tráfico y el robo o alteración de la información
	Desactivar conexión automática a redes abiertas	Evitar conectarse a redes no seguras o maliciosas
	Desactivar *Notificaciones de redes abiertas*	Evitar interactuar con redes desconocidas
	Evitar instalar nuevos certificados y, de hacerlo, únicamente aquellos de confianza	Evitar facilitar a un tercero realizar ataques *MitM*
	Comprobar seguridad de la red	Evitar conectarse a redes no seguras
	No establecer *proxys*	Evitar facilitar a un tercero realizar ataques *MitM*
USB	No conectar a otros dispositivos salvo que se vaya a hacer uso de ellos	Evitar ataques que explotan este medio
	No conectar a dispositivos que puedan estar infectados	Evitar recibir infecciones traspasadas desde el dispositivo conectado
	Establecer como preferencia *Sin transferencia de datos*	Evitar facilitar a un atacante el robo de archivos

USB	No activar el modo *depuración*, salvo por necesidad, y desactivar al finalizar su uso	Evitar facilitar a un atacante ejecutar comandos, robar archivos, etc
	No ejecutar comandos *ADB* sin conocer las posibles consecuencias	Evitar formateos no deseados
	Revocar claves *RSA* al finalizar conexión	Evitar que alguien con acceso al ordenador pueda utilizar el modo depuración

Tabla 4-3 Medidas de protección en la seguridad en las comunicaciones

Medidas adicionales y recomendaciones:

- Evitar descolgar llamadas de números desconocidos. Comprobar en Internet si dichos números se encuentran en la lista de números relacionados con fraude.
- No habilitar a las aplicaciones el acceso a *SMS Premium*.
- No abrir archivos o enlaces no esperados recibidos por SMS.
- Desconfiar de mensajes que afirmen ser urgentes o confidenciales; la mayoría de empresas no solicitan información sensible por correo electrónico. Fijarse en la redacción del mensaje (faltas de ortografía, mal escrito, etc).
- Frente ataques de ingeniería social, sentido común.

Seguridad relacionada con la localización:

	Medida	Objetivo
Ubicación	Mantener siempre activa	Permitir a servicios como *Encuentra mi dispositivo* encontrar el teléfono
	Comprobar regularmente que aplicaciones hacen uso de la ubicación	Encontrar aplicaciones que hacen un uso inadecuado de la ubicación
	Desactivar *Búsqueda de redes Wi-fi*	Evitar que el teléfono interactúe con redes desconocidas
	Desactivar *Búsqueda de dispositivos Bluetooth*	Evitar que el teléfono interactúe con dispositivos desconocidos
	Desactivar *Precisión de la ubicación de Google*	Disminuir la información que Google que recibe del usuario
	Evitar el uso de *Compartir ubicación de Google*	Evitar el rastreo por una tercera parte y la falta de privacidad
	Comprobar regularmente que no se está compartiendo con nadie la localizacón	Evitar el rastreo por una tercera parte y la falta de privacidad
	Desactivar y eliminar *Historial de ubicaciones de Google*, así como la función *Cronología*	Evitar que se guarde en los servidores de Google registro de las ubicaciones y aumentar la privacidad

Ubicación	Evitar compartir o indicar la ubicación en redes sociales	Aumentar privacidad
	Desactivar *Guardar información de ubicación* en la *Cámara*	Impedir que la ubicación quede registrada en los metadatos de las imágenes

Tabla 4-4 Medidas de protección en privacidad y localización

4.2 Herramientas de pentesting

4.2.1 Herramientas tradicionales

Con el fin de conocer cuánta información se puede extraer de un *smartphone* a través de sus conexiones, se utilizó la herramienta *Nmap* [60]. Es una herramienta empleada para evaluar la seguridad de sistemas informáticos, para rastrear puertos o descubrir servicios y servidores en una red. Se realizó una prueba de escaneo *intenso* al Xiaomi Mi A2 Lite y a un ordenador, para comprobar cual de los dos quedaba más expuesto. Los resultados se resumen en la Figura 4-1.

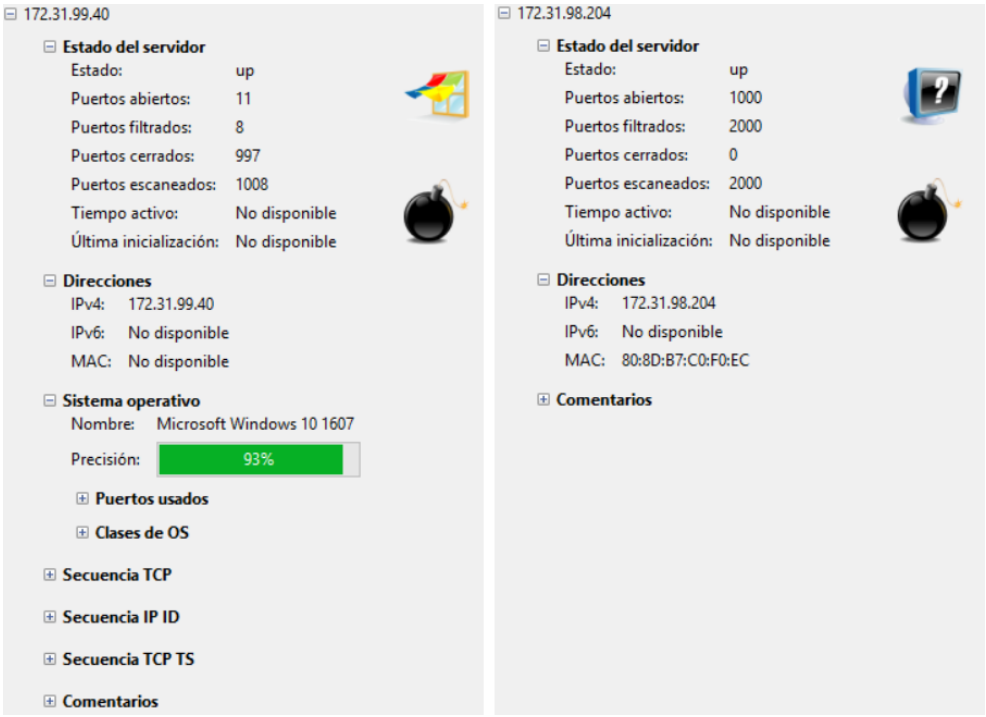

Figura 4-1 Resultados del escaneo *Nmap* en ordenador y *smartphone*

Se puede ver a simple vista que del ordenador (izquierda) se puede extraer más información que del teléfono. Más concretamente, el programa afirma, con una precisión del 93%, que el sistema operativo del ordenador es Windows, mientras que no es capaz de averiguar que SO monta el *smartphone*. Además, mientras que del ordenador se puede saber que puertos son los más utilizados y si están abiertos o no, no se extrae nada al respecto tras el escaneo al móvil. Debido a la escasa utilidad que ofrecían estas herramientas, se decidió utilizar aplicaciones específicas de teléfonos móviles.

4.2.2 Herramientas específicas de móviles

Para comprobar que la configuración comentada previamente realmente protegía al usuario, se realizó una búsqueda de aplicaciones que permitiesen realizar pruebas de penetración, robar información del teléfono, o que pudiesen comprometer la seguridad del dispositivo de alguna forma.

Si bien parecía que este tipo de aplicaciones abundaban en Internet, pronto se comprobó que la gran mayoría no cumplía los requisitos. Algunos ejemplos son:

- *Hackode* [61]: esta aplicación prometía disponer de herramientas para escanear redes, *exploits*, inyectar código. La realidad es que en esta aplicación (versión beta) aún no se han implementado la mayoría de estas funciones.
- *Faceniff* [62]: centrada en el ataque a redes sociales, esta aplicación que asegura que, mediante una sencilla guía, un usuario no experto sería capaz de robar contraseñas de Facebook, Instagram, etc. Sin embargo, antes de poder profundizar más en ella, se requería que el teléfono dispusiese de acceso *root*, por lo que hubo que descartarla.
- *AndroRAT* [63]: es una aplicación de acceso remoto que permite controlar el dispositivo a distancia. De hecho, fue *AndroRAT* una vulnerabilidad descubierta durante un trabajo universitario, que finalmente acabo utilizándose como *malware*. Esta vulnerabilidad fue corregida para versiones posteriores a Android 7, por lo que no se pudo emplear en el móvil estudiado (versión 9).

La aplicación *Andriller* [64] sí que permitió profundizar más en sus funciones. Esta aplicación de pago permite realizar análisis forense de dispositivos, así como romper patrones, *PIN* y contraseñas, extraer información y archivos, descifrar bases de datos de aplicaciones como *Whatsapp* o Facebook, incluso ejecutar algunos comandos *ADB*. Además, cuenta con herramientas interesantes para teléfonos *rooteados*, que no fueron analizadas.

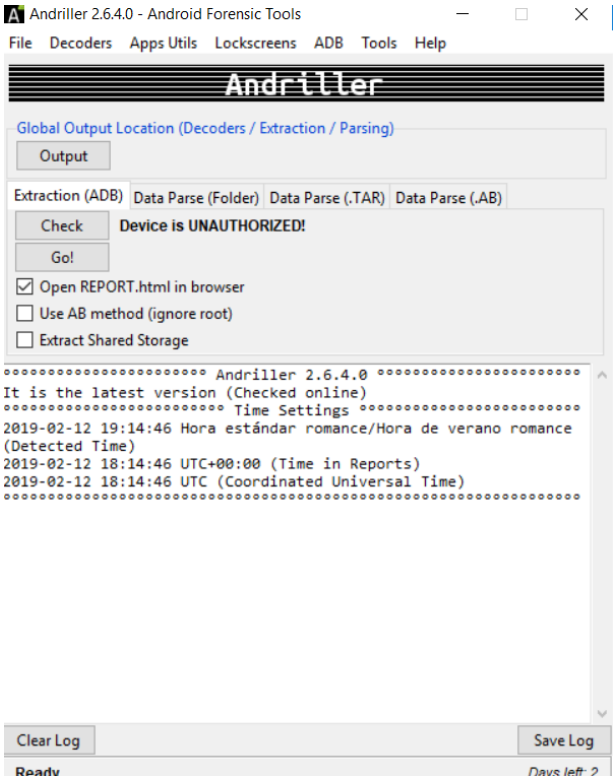

Figura 4-2 Interfaz de *Andriller*

El primer problema que surge al estudiar esta aplicación, es que necesita que se conecte el teléfono al ordenador en modo *depuración*. Esto no se puede conseguir de forma remota, únicamente habiendo desbloqueado el dispositivo y habiendo creado una relación de confianza entre el ordenador y el mismo (véase apartado 3.5.3). Obviando esto, se intentó descifrar el *PIN* del teléfono. Como se puede ver en la Figura 4-3, la aplicación necesita el *hash* de la contraseña, que se almacena en una partición de la memoria no accesible por el usuario, por lo que esta función no resultó útil.

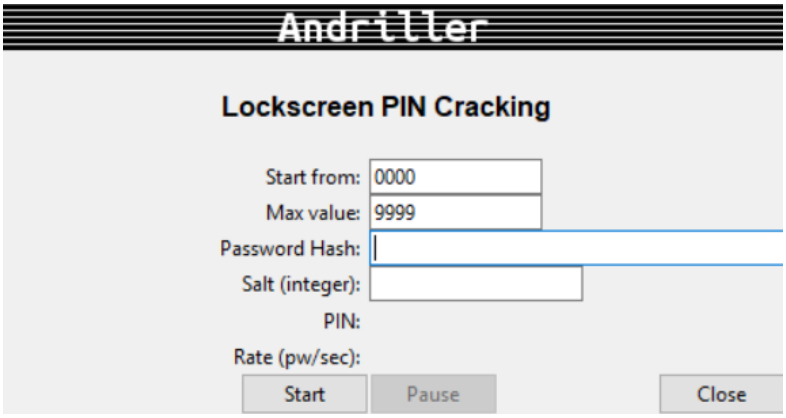

Figura 4-3 Prueba de descifrar *PIN* con *Andriller*

Continuando con las pruebas, se intentó descifrar los archivos almacenados de *Whatsapp*. Estos archivos están actualmente cifrados (.crypt12), pero son accesibles ya que se guardan junto con las demás aplicaciones en el almacenamiento interno el dispositivo. Sin embargo, de nuevo requería una clave que no es accesible en la versión 9 de Android. Sí se han encontrado otras aplicaciones que consiguen descifrar estos archivos, pero como máximo hasta la séptima versión de este sistema operativo.

Al no encontrar aplicaciones que fuesen capaces de burlar la seguridad del móvil para acceder al mismo, se optó por buscar aplicaciones que, una vez instaladas, por engaño u otros métodos, resultasen ser un gran peligro para la privacidad del usuario. Con este enfoque se encontró la aplicación *Mobile Tracker*, cuyo funcionamiento se desarrolla en el siguiente apartado.

4.3 *Mobile Tracker*

Mobile Tracker [59] es una aplicación de vigilancia de pago disponible para Android. En este TFG, se utilizará la versión gratuita *Mobile Tracker Free*. Esta aplicación permite conocer básicamente todo lo que realiza el dispositivo, la información que almacena, la ubicación. Entre sus funcionalidades están: visualizar SMS recibidos y enviados, escuchar llamadas entrantes y salientes, conocer la ubicación en directo, visualizar fotos, vídeos y archivos almacenados, visualizar mensajes de redes sociales o control remoto con un amplio abanico de posibilidades. La vigilancia se realiza a través de la página web de la aplicación, accediendo con una cuenta personal, desde un ordenador, tablet u otro móvil.

Dado que es una aplicación de vigilancia, el usuario del teléfono donde se instala no debe saber que está instalada. La aplicación tiene un proceso de instalación muy sencillo y guía paso a paso para que se le concedan los permisos pertinentes, así como garantizar que quede lo más oculta posible.

El desarrollador vende *Mobile Tracker* argumentando que es ideal para vigilar a los hijos, a los empleados o incluso para grabar los datos propios. No se hacen responsables del mal uso de la misma, y reitera que se deben cumplir las leyes de cada país y de que el usuario del móvil debe ser consciente de que se están registrando sus datos. Antes de usar cualquier aplicación de este tipo, es especialmente importante leer la política de privacidad. En este caso, el desarrollador avisa de que, por ejemplo, los datos del usuario podrán ser reutilizados para enviar correos promocionales o marketing. También explica dónde se almacena la información extraída y durante cuánto tiempo se mantiene.

A continuación se explica el proceso de instalación, poniendo especial énfasis en los permisos y condiciones que necesita. Antes de poder descargarla, se deben cumplir estos requisitos previos:

- Crear una cuenta de *Mobile Tracker*. Es necesario una cuenta de correo electrónico.
- Desactivar *Google Play Protect* (véase apartado 3.3.1). Debido a las características potencialmente maliciosas de la aplicación, el sistema tratará de inhabilitarla o eliminarla.

- Al tratarse de una aplicación no disponible en la *Play Store*, se debe permitir al navegador a descargar *Aplicaciones de origen desconocido* (véase apartado 3.3.2).

Después de esto, y tras aceptar los términos de uso, se podrá descargar el archivo APK. Aparecerá un aviso del sistema indicando que el archivo podría dañar al dispositivo (ocurre siempre que se instala una aplicación de fuentes no oficiales).

Para la configuración, bastaría con seguir los pasos indicados y conceder los permisos que solicite. La aplicación solicitará todos los permisos considerados peligrosos (véase Tabla 3-1), así como los permisos de acceso especial que se ven en la Figura 4-4.

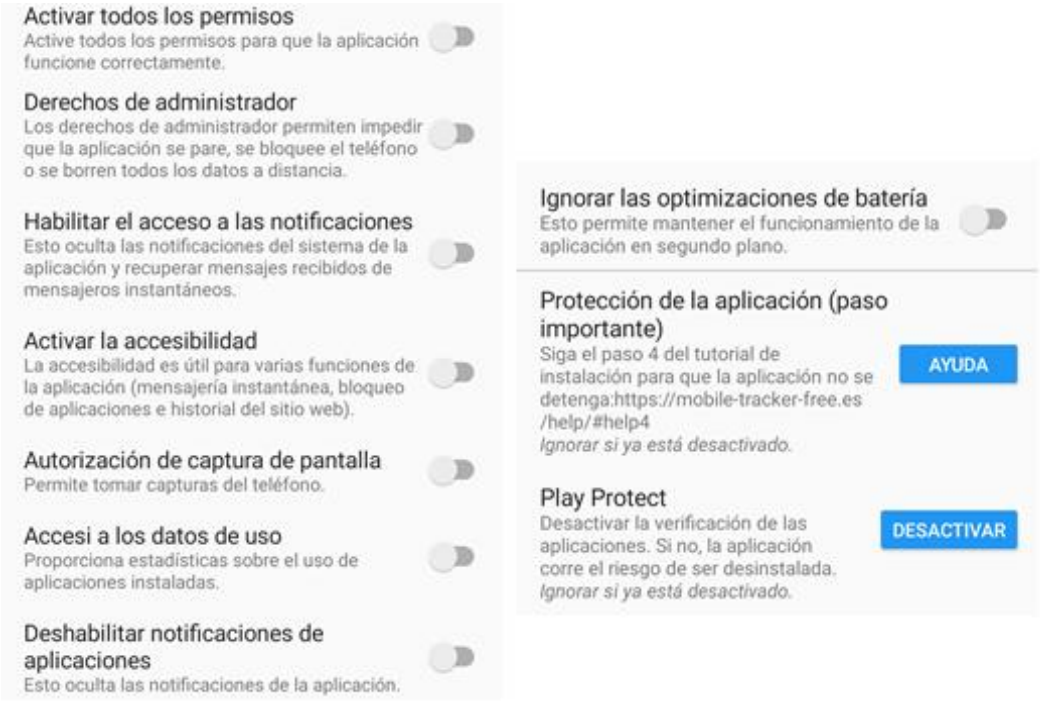

Figura 4-4 Permisos que solicita *Mobile Tracker*

Los *derechos de administrador* le permiten, entre otros, bloquear la pantalla, la cámara y cambiar el bloqueo de pantalla. El a*cceso a las notificaciones* sirve para ocultar las notificaciones de la aplicación, para no dejar constancia de sus acciones. También consigue acceso a las aplicaciones del teléfono y a realizar capturas de pantalla. Al terminar la configuración, la aplicación permite ver utilidades de la misma están autorizadas, para que el usuario pueda fácilmente elegir qué datos registrará (llamadas, capturas de pantalla, SMS, etc).

En el momento de la instalación, la aplicación pasa a llamarse *Wi-Fi*. No aparecerá un acceso directo en la pantalla de inicio, como suele pasar con la mayoría de aplicaciones. Tampoco aparecerá en el menú principal. *Wi-Fi* ni siquiera tiene interfaz de usuario, así que es como una aplicación más del sistema, en las que los usuarios nunca se fijan. Para encontrarla, se debe entrar en el menú de *Aplicaciones y notificaciones*, donde aparecerá en el listado con el resto de aplicaciones y su logo propio.

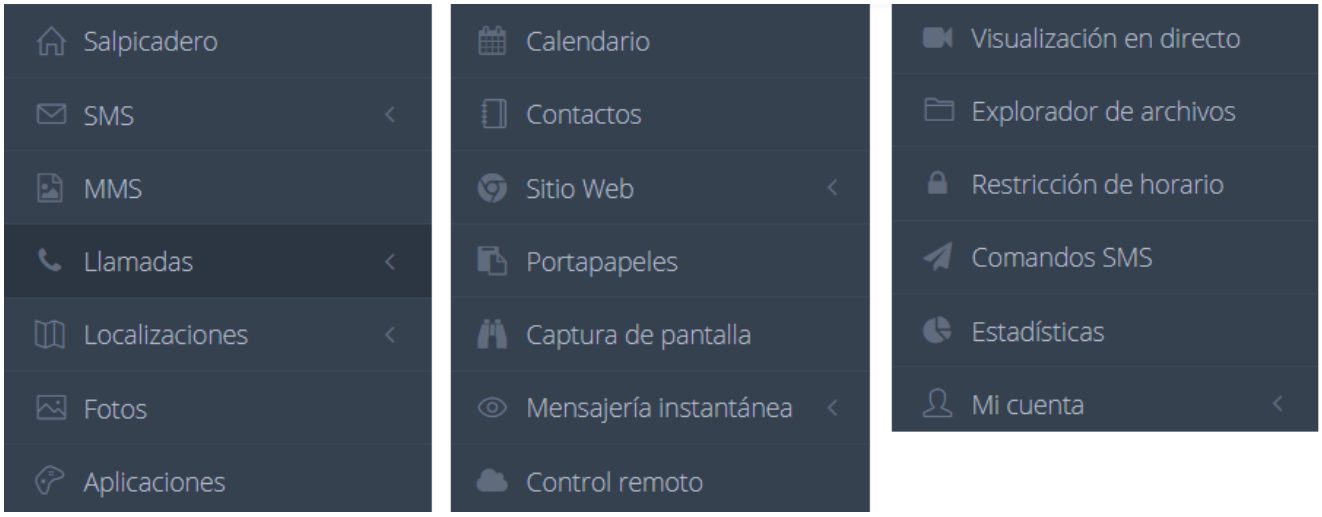

Figura 4-5 Menú de opciones de la página de *Mobile Tracker* [59]

En la Figura 4-5 se pueden observar todas las posibilidades que ofrece *Mobile Tracker*. Las funciones son evidentes, *SMS* permite leer los mensajes del teléfono, *Localizaciones* ver la ubicación en directo en un mapa, desde *Sitio Web* se puede analizar el historial de búsquedas y bloquear páginas, *Explorador de archivos* para buscar datos almacenados en el dispositivo, etc. Las más peligrosas serían *Mensajería instantánea*, *Control remoto* y *Visualización en directo*:

- ***Mensajería instantánea**:* permite visualizar los mensajes recibidos en multitud de aplicaciones de mensajería, como *Whatsapp*, Facebook Messenger, Instagram, Gmail, etc.
- ***Control remoto**:* Permite utilizar ciertas funciones del teléfono, aunque esté bloqueado. Algunas de estas son obtener la localización, grabar audios, obtener fotografías, bloquear aplicaciones como la cámara, eliminar datos del dispositivo, enviar SMS, etc. Además, las fotos o audios obtenidos no se guardan en la memoria del teléfono, sino que se envían directamente al servidor de la aplicación, para evitar dejar ningún rastro. Si el teléfono está *rooteado*, se podrían ejecutar comandos de forma remota, aunque el acceso *root* queda fuera del ámbito de este TFG.
- ***Visualización en directo**:* permite ver en tiempo real y grabar lo mismo que el usuario legítimo. Al permitir que se grabe la pantalla de forma contínua, si el propietario del móvil introdujese una contraseña para acceder al correo, a Facebook, etc, sería extremadamente fácil extraerla, ya que la mayoría de teclados muestran brevemente la letra que se pulsa, y muchos fabricantes no permiten modificar esto en los ajustes del teclado.

Si bien la aplicación no es de por si maliciosa, ya que oficialmente es para vigilar niños o empleados (aunque desde un punto de vista ético esto es francamente cuestionable), sus capacidades hacen que sea muy peligrosa. En apenas unos minutos alguien de confianza puede engañar al usuario e instalarla y mantenerla activa sin que el usuario lo sepa.

En la Figura 4-6 se puede comprobar que la aplicación de mensajería *Whatsapp* tiene prácticamente los mismos permisos que *Mobile Tracker*. Si bien los permisos especiales no son los mismos, si lo es el acceso a la información. En muchos casos, el usuario no es consciente de los motivos por los cuales las aplicaciones solicitan los permisos. Se debe ser muy precavido a la hora de instalarlas, sobretodo aquellas en las que Google no ha realizado un análisis de seguridad (las ajenas a la *Play Store*).

Figura 4-6 Comparación entre los permisos que solicitan *Mobile Tracker* y *Whatsapp*

5 CONCLUSIONES Y LÍNEAS FUTURAS

5.1 Conclusiones

El objetivo principal propuesto al inicio del TFG consistía en el análisis del modelo de seguridad de Android y la implementación de un conjunto de medidas que garantizasen una configuración segura en un *smartphone* Xiaomi Mi A2 Lite. Como objetivo adicional, se ha procurado redactar un documento que sea capaz de resumir de forma comprensible para un usuario no experto, el funcionamiento del sistema operativo Android desde un punto de vista de seguridad, y de cómo conseguir una mayor protección del dispostivo móvil, ya sea particular o empresarial.

A lo largo de este TFG, ha quedado patente que no son demasiado abundantes los parámetros configurables en un teléfono Android (comparado con un ordenador). Sin embargo, el hecho de que el teléfono siempre acompañe al dueño, lo ha convertido en un objetivo muy llamativo para los ciberdelincuentes. Google es consciente de este problema, y por ello trabaja continuamente para mantener el sistema operativo actualizado. Las características de Android estudiadas en este trabajo, junto con las actualizaciones al SO, demuestran que éste es capaz de protegerse de las principales amenazas, también analizadas en este TFG. Si bien el propio sistema operativo es la clave para mantener protegido el móvil, se fue proponiendo en los capítulos 3 y 4 la configuración de aspectos esenciales para la seguridad del mismo.

En cuanto a la validación de las medidas propuestas, apareció el problema de que la mayoría de aplicaciones de *pentesting* requerían realizar el *rooteado* previo al teléfono. Este hecho limitó las aplicaciones disponibles a unas pocas, de escaso interés. Algunas de estas aplicaciones, como Andriller, requerían de tantas facilidades otorgadas por el usuario, que en ningún escenario realista la aplicación sería capaz de hacer peligrar la seguridad del teléfono. Es por ello que se decidió cambiar el enfoque de la amenaza, y se buscaron aplicaciones que, una vez instaladas en el móvil, sí que amenazasen dicha seguridad.

La aplicación estudiada finalmente fue *Mobile Tracker*, una aplicación de rastreo y vigilancia. Se demostró que en apenas unos minutos de descuido, se podía instalar una aplicación que vulnerase totalmente la privacidad del usuario. La conclusión que permitió extraer es que, si bien Android protege de forma muy efectiva frente a aplicaciones maliciosas, el usuario tiene la última palabra, lo que le convierte en la principal amenaza contra su propia seguridad. El usuario no es consciente normalmente ni de los riesgos ni de cómo está configurado su teléfono, lo que le impide detectar variaciones o anomalías en su funcionamiento. Por este motivo, se ha realizado, junto con las recomendaciones de configuración, una lista de buenas prácticas del usuario a modo de concienciación.

El apartado de Localización evidencia que, a día de hoy, el usuario de un *Smartphone* está continuamente siendo analizado. La propia empresa Google utiliza infinidad de datos, obtenidos de nuestras búsquedas, hábitos o ubicación, para ofrecer un mejor servicio o para que terceras compañías enfoquen su publicidad en el usuario correcto. Debido al problema de privacidad que esto supone, se han propuesto distintas modificaciones al funcionamiento normal del dispositivo que consiguen minimizar la información que Google recolecta.

5.2 Líneas futuras

En las próximas líneas se presentarán diferentes ideas sobre cómo profundizar en algunos aspectos de este trabajo o cómo ampliarlo a otro tipo de sistemas:

- El principal problema al que se enfrenta un ciberdelincuente a la hora de atacar un teléfono Android es la aparente necesidad que tiene de disponer de acceso físico al mismo. Un posible trabajo sería analizar, o incluso desarrollar, distintas técnicas de *phising* para engañar a un usuario a descargar una aplicación dañina o insertar código malicioso de forma remota.
- Sería interesante plantear la configuración segura en otros sistemas operativos, por ejemplo, iOS. También se podría analizar otro tipo de dispositivo, como tablets, en el que este sistema operativo es el que tiene mayor éxito. Se podría utilizar este trabajo como base para comparar Android e iOS, desde un punto de vista de la seguridad, con el fin de encontrar el fabricante más adecuado para los empleados de una empresa. Para esto habría que dar un enfoque más corporativo a este TFG, que se ha centrado en usuarios particulares.
- Durante el trabajo se ha mencionado repetidas veces el hecho de que el uso de los dispositivos *IoT* está aumentando muy rápidamente. Por la función que desempeñan, normalmente necesitan estar conectados a la red y a otros dispositivos. En los últimos meses, esta clase de dispositivos ha sido víctima de muchos ataques, debido a que la imposición de medidas de seguridad se realiza a menor velocidad que la expansión de éstos. Un posible trabajo sería analizar la implantación de estos aparatos en una oficina, valorando tanto las ventajas que ofrecen, como el riesgo que suponen para la seguridad de la información.
- Existen aplicaciones avanzadas de *pentesting*, con las que es posible crear un laboratorio de pruebas de seguridad para *smartphones*, que utilizan emuladores, como el propio de *Android Studio*, con los que se podría trabajar sin el menor miedo a dañar un teléfono. Se podrían realizar pruebas de penetración, con el objetivo de romper la seguridad y acceder al móvil. Ejemplos de estas aplicaciones serían *APKtool* [65], una herramienta de ingeniería inversa que permite decodificar los recursos de las aplicaciones para luego reconstruirlos con algunas modificaciones o la aplicación *Drozer* [66] permite buscar vulnerabilidades de otras aplicaciones interactuando directamente con la máquina virtual.

6 BIBLIOGRAFÍA

[1] Ditrendia, «Informe Mobile y en el mundo 2017,» 2017. [En línea]. Available: https://www.amic.media/media/files/file_352_1289.pdf. [Último acceso: 15 01 2019].

[2] Global stats , «Statcounter,» 21 01 2019. [En línea]. Available: http://gs.statcounter.com/os-market-share/mobile-tablet/worldwide/#monthly-201712-201812-map. [Último acceso: 21 01 2019].

[3] Xiaomi, «MI,» [En línea]. Available: https://www.mi.com/es/mi-a1/android-one/. [Último acceso: 21 01 2019].

[4] International Organization for Standarization, «ISO 27000,» 2018. [En línea]. Available: https://www.iso.org/standard/73906.html. [Último acceso: 20 01 2019].

[5] C. Yáñez, «Tipos de seguridad informática,» 11 08 2017. [En línea]. Available: https://www.ceac.es/blog/tipos-de-seguridad-informatica. [Último acceso: 21 01 2019].

[6] Instituto Nacional de Ciberseguridad, «INCIBE,» INCIBE, 03 02 2018. [En línea]. Available: https://www.incibe.es/sala-prensa/notas-prensa/incibe-resuelve-mas-123000-incidentes-ciberseguridad-2017. [Último acceso: 20 01 2019].

[7] CCN-CERT, «Estrategia de Ciberseguridad Nacional,» 2013. [En línea]. Available: https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf. [Último acceso: 24 02 2019].

[8] Consejo de la Unión Europea, «Cybersecurity policies,» 18 10 2018. [En línea]. Available: https://www.consilium.europa.eu/es/policies/cyber-security/. [Último acceso: 21 01 2019].

[9] CCN, «Acuerdo colaboración CCN-MCCD,» EMAD, 26 04 2016. [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/3739-acuerdo-de-colaboracion-entre-el-cni-y-el-ministerio-de-defensa-para-impulsar-dentro-de-la-estrategia-de-seguridad-nacional-la-seguridad-de-la-informacion.html. [Último acceso: 20 01 2019].

[10] Europa Press, «Noticias de Ciberseguridad,» 17 12 2018. [En línea]. Available: https://www.europapress.es/portaltic/ciberseguridad/noticia-espana-fue-objetivo-80-ciberataques-dispositivos-iot-primera-mitad-2018-20181217175221.html. [Último acceso: 21 01 2019].

[11] Accenture, «Estudio de ciberresiliencia España,» 21 11 2018. [En línea]. Available:

https://www.accenture.com/es-es/company-news-release-estudio-ciberresiliencia-espana. [Último acceso: 21 01 2019].

[12] IAC, «Internet of things,» [En línea]. Available: https://www.iac.com.co/que-es-iot/. [Último acceso: 21 01 2019].

[13] F5 Labs, «The Hunt for IoT: Multi-Purpose Attack Thingbots Threaten Internet Stability and Human Life,» F5 Labs, 2018.

[14] Microsoft, «Microsoft,» 21 01 2019. [En línea]. Available: https://www.microsoft.com/es-es/windows/windows-10-mobile-upgrade. [Último acceso: 21 01 2019].

[15] Tizen, «Tizen,» 21 01 2019. [En línea]. Available: https://www.tizen.org/. [Último acceso: 21 01 2019].

[16] Google, «Wear OS,» 21 01 2019. [En línea]. Available: https://wearos.google.com/#hands-free-help. [Último acceso: 2019 01 2019].

[17] Kaios technologies, «Kaiostech Web Oficial,» 21 01 2019. [En línea]. Available: https://www.kaiostech.com/. [Último acceso: 21 01 2019].

[18] Mozilla, «Mozilla,» 08 10 2018. [En línea]. Available: https://developer.mozilla.org/es/docs/Archive/B2G_OS/Architecture. [Último acceso: 21 01 2019].

[19] Apple Inc, «Apple,» 21 01 2019. [En línea]. Available: https://www.apple.com/es/ios/ios-12/. [Último acceso: 21 01 2019].

[20] Google, «Android,» 21 01 2019. [En línea]. Available: https://www.android.com/intl/es_es/one/. [Último acceso: 21 01 2019].

[21] S. Fernández, «Diferencias entre tipos de Android,» 23 12 2018. [En línea]. Available: https://www.xatakamovil.com/sistemas-operativos/que-son-android-go-y-android-one-y-en-que-se-diferencian-de-android-stock. [Último acceso: 21 01 2019].

[22] Android, «Project Treble,» 12 05 2017. [En línea]. Available: https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html. [Último acceso: 21 01 2019].

[23] CCN-CERT, «Informe de Amenazas IA-05/16 Near Field Communication (NFC) VulnerabilidadeS,» CCN, Madrid, 2015.

[24] CCN-CERT, «Informe anual 2017. Dispositivos y comunicaciones Móviles,» 2017.

[25] Kaspersky, «Kaspersky,» 21 06 2017. [En línea]. Available: https://www.kaspersky.es/blog/android-root-faq/13141/. [Último acceso: 21 01 2019].

[26] CCN, «Guía de Seguridad de las TIC- ENS,» 22 01 2019. [En línea]. Available: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html. [Último acceso: 22 01 2019].

[27] CCN-CERT, «Esquema de Seguridad Nacional,» 22 01 2019. [En línea]. Available: https://www.ccn-cert.cni.es/ens.html. [Último acceso: 22 01 2019].

[28] CCN-CERT, «CCN-STIC 453E: Seguridad de dispositivos móviles Android 7.x,» CNI, Madrid, 2018.

[29] CCN-CERT, «CCN-STIC 456 Cuenta de Usuario Servicios Aplicaciones Google para

Dispositivos Móviles Android,» CNI, Madrid, 2018.

[30] Google, «Android Security Bulletin,» 22 01 2019. [En línea]. Available: https://source.android.com/security/bulletin. [Último acceso: 22 01 2019].

[31] A. G. Fernández, Seguridad en Smartphones, TFM Universitat oberta de Catalunya, 2018.

[32] C. J. Jiménez, Seguridad en redes y sistemas, TFG Universitat Oberta de Catalunya, 2016.

[33] N. Elenkov, Android Security Internals, No starch press, 2014.

[34] Joshua J. Drake, Pau Oliva Fora, Zach Lanier, Colin Mulliner, Stephen A. Ridley, Georg Wicherski, Android Hacker´s Handbook, WILEY, 2014.

[35] J. Atwood, «Stackoverflow,» 22 01 2019. [En línea]. Available: https://es.stackoverflow.com/. [Último acceso: 22 01 2019].

[36] Android, «Arquitectura de la plataforma,» 12 02 2019. [En línea]. Available: https://developer.android.com/guide/platform/?hl=es-419. [Último acceso: 12 02 2019].

[37] Android Developer, «Arquitectura de Android,» [En línea]. Available: https://developer.android.com/guide/platform/?hl=es-419. [Último acceso: 18 02 2019].

[38] A. V. Romano, «Descripción y Análisis formal del modelo de seguridad de Android,» Facultad de Ciencias Exactas, Ingeniería y Agrimensura de la Universidad de Rosario, Rosario, Argentina, 2014.

[39] Open Binder Organization, «OpenBinder,» [En línea]. Available: http://ww1.open-binder.org/. [Último acceso: 16 02 2019].

[40] Google, «Google Play,» [En línea]. Available: https://support.google.com/googleplay/answer/4355207?co=GENIE.Platform%3DAndroid&hl=es-419. [Último acceso: 18 02 2019].

[41] AppBrain, «Number of Android Apps on Google Play,» 11 02 2019. [En línea]. Available: https://www.appbrain.com/stats/number-of-android-apps. [Último acceso: 11 02 2019].

[42] Android, «Google Play Protect,» [En línea]. Available: https://www.android.com/intl/es_es/play-protect/. [Último acceso: 18 02 2019].

[43] Uptodown, «Uptodown,» [En línea]. Available: https://www.uptodown.com/android. [Último acceso: 20 02 2019].

[44] A. J. Aviv, «Towards Baselines for Shoulder Surfing on Mobile,» United States Naval Academy, Maryland, 2017.

[45] Lancaster University, Bath University, «Cracking Android Pattern Lock in Five Attempts,» 2017. [En línea]. Available: https://www.lancaster.ac.uk/staff/wangz3/publications/ndss_17.pdf. [Último acceso: 2019 01 28].

[46] T. Foltýn, «Contraseñas más populares,» 19 12 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/12/19/las-25-contrasenas-mas-populares-del-2018/. [Último acceso: 28 01 2019].

[47] FireEye Labs, «Fingerprints On Mobile Devices: Abusing and leaking,» 07 08 2015. [En línea]. Available: https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf. [Último acceso: 28 01 2019].

[48] Bluetooth Organizations, «Bluetooth,» [En línea]. Available: https://www.bluetooth.com/. [Último acceso: 02 21 2019].

[49] CCN, «Guía de Seguridad de las TIC- ENS. Seguridad en Bluetooth,» 2018.

[50] WiFi Alliance, «Discover WiFi,» [En línea]. Available: https://www.wi-fi.org/discover-wi-fi. [Último acceso: 21 02 2019].

[51] Android Studio, «Command line ADB,» [En línea]. Available: https://developer.android.com/studio/command-line/adb?hl=es-419. [Último acceso: 02 23 2019].

[52] U.S. Government, «Global Positioning System,» 09 02 2019. [En línea]. Available: https://www.gps.gov/systems/gps/. [Último acceso: 09 02 2019].

[53] European Global Navigation Satellite Systems Agency, «Sistema de navegación Galileo,» 09 02 2019. [En línea]. Available: https://www.usegalileo.eu/ES/inner.html#data=smartphone. [Último acceso: 09 02 2019].

[54] WiFi Alliance, «WiFi Location,» 05 02 2019. [En línea]. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-location. [Último acceso: 05 02 2019].

[55] Agencia Estatal Boletín del Estado, «Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.,» 14 11 2007. [En línea]. Available: https://www.boe.es/buscar/doc.php?id=BOE-A-2007-18243. [Último acceso: 05 02 2019].

[56] Secretaría de Estado para la Sociedad de Información y Agenda Digital, «Distribución de estaciones de Telefonía en España,» 07 02 2019. [En línea]. Available: https://geoportal.minetur.gob.es/VCTEL/vcne.do. [Último acceso: 07 02 2019].

[57] A. Mosenia, «PinMe: Tracking a Smartphone User around the World,» Universidad de Princeton, 2017.

[58] Google, «Configuración del Historial de ubicaciones,» 07 02 2019. [En línea]. Available: https://support.google.com/accounts/answer/3118687?hl=es. [Último acceso: 07 02 2019].

[59] Mobile Tracker, «Aplicación Mobile Tracker Free,» [En línea]. Available: https://mobile-tracker-free.es/. [Último acceso: 20 02 2019].

[60] Nmap, «Nmap Security Scanner,» [En línea]. Available: https://nmap.org/. [Último acceso: 04 03 2019].

[61] Ravi Kumar Purbey, «Hackode,» [En línea]. Available: https://play.google.com/store/apps/details?id=com.techfond.hackode&hl=en. [Último acceso: 02 23 2019].

[62] Faceniff, «Aplicación Faceniff,» [En línea]. Available: http://faceniff.ponury.net/. [Último acceso: 23 02 2019].

[63] Aplicación de código abierto, «Aplicación AndroRAT,» [En línea]. Available: https://www.ethicalhackingtutorials.com/2017/02/17/download-androrat-full-version/. [Último acceso: 23 02 2019].

[64] Desarrolladores Andriller, «Andriller Forensic Tools,» [En línea]. Available: https://www.andriller.com/. [Último acceso: 23 02 2019].

[65] «Aplicación de seguridad APKtool,» [En línea]. Available: https://apktool.en.lo4d.com/. [Último acceso: 04 03 2019].

[66] MRW labs, «Herramienta de seguridad Drozer,» [En línea]. Available: https://labs.mwrinfosecurity.com/tools/drozer/. [Último acceso: 04 03 2019].