Guía básica de privacidad, anonimato y autodefensa digital para novatXs con smartphones

https://cottonio.no-ip.org/hacklab/

http://hacksturias.net

Versión 0.1

Índice

Prefacio:

A lo largo de estos últimos años, hemos asistido en España al despertar de una población más concienciada con los problemas sociales, más reivindicativa, más activista, más consciente de la necesidad de la transparencia en organismos públicos y de un "OpenGov". Por desgracia, la respuesta de unas instituciones arcáicas y reacias al cambio también han acarreado represalias físicas o legales para quienes, de una forma u otra, todavía hoy se empecinan en que las cosas mejoren y evolucionen.

El crucial papel de internet en este tipo de luchas a favor de la justicia considero que ya no es necesario describirlo aquí, pues durante estos años he podido leer grandes textos acerca como pueden ser -y no pretendo hacer Spam- "el Kit de la lucha en Internet", de Margarita Padilla, o "Ciberactivismo" de Mario Tascón y Yolanda Quintana.

Internet ha sido básico a la hora de informar de forma inmediata cuando algo está sucediendo, mostrando como la información puede dispersarse de forma viral, en progresión geométrica a golpe de click. Julian Assange, fundador de Wikileaks mantiene que, una de las mejores formas de hacer justicia es evidenciando la injusticia y, quizás, tu mismX no puedas ir en persona a una manifestación, o a alguna otra acción reivindicativa, pero difundiendo lo que emane de allí estás poniendo tu granito de arena para que no se censure, para que se conozca la injusticia.

No obstante existe un fenómeno previo al nacimiento de todas estas luchas hacia la evolución de una sociedad más justa: es el fenómeno del "Oversharing" que, como su propio nombre en ingles indica, se trata de la compartición de excesiva información personal a través de canales de comunicación abiertos para todo el mundo. En internet compartimos muchas de nuestras vivencias, las fotos de eventos a los que asistimos, comentarios con cierta complicidad con nuestros amigos que no deberían salir de nuestro círculo íntimo y mucha otra información más que, a la hora de la verdad, solo sirve de munición para un estado cada día más consciente de la utilidad de la monitorización constante sobre internet a la hora de perseguir y desmantelar las corrientes de pensamientos disidentes para con el orden establecido.

Hoy por hoy, la excusa barata del "es que yo no tengo nada que ocultar" ya ha quedado desbaratada pues no se trata de que tengas algo que ocultar, es que no tienen porqué monitorizarte si no estás planeando hacer nada malo, amén de que hay empresas enriqueciendose a costa de comercializar tus actividades en internet. Lo que comunmente se conoce como "bigdata" y que es una de las formas más lucrativas de operar servicios masivos en internet que existen a día de hoy.

Durante estos años, he tenido la oportunidad de organizar e impartir varios eventos "cryptoparty", pequeños talleres de privacidad y anonimato básicos donde la gente aprendia el uso de criptografía aplicada en forma de software para un uso mas sano de internet, así como la asimilación de hábitos mas seguros a la hora de conectarte a la red de redes, con lo cual he tenido la oportunidad de enriquecerme de la experiencia de otras personas, así como ellas lo han hecho de mis conocimientos. Sin entrar en detalles muy técnicos, ni profundizar, voy a tratar de que esta guía sea lo más abierta posible, aunque que quede claro que hay mucho más que aprender.

No voy a hacer un ensayo acerca de porqué es necesario ser protectores de nuestra vida íntima, pues existe información exahustiva en internet que refleja perfectamente como funcionan las cosas, así pues, si llegados a este punto, piensas que estoy equivocado, o soy un exagerado, te invito a que pares automáticamente de leer esta guía, busques por internet alguno de los términos que he utilizado en este prefacio, y si todavía no has tomado conciencia de a que me refiero, no malgastes más tu tiempo leyendo los siguientes capítulos. De todas manera te advierto que, pudiera ser, utilice expresiones que te resulten chocantes e, incluso, que te generen cierto miedo o recelo.

Usar un teléfono movil de por si es ya someterse a un riesgo, aunque no hagas absolutamente nada con él, pues quieras o no, la localización de tu posición mediante las diferentes celdas que componen una red de telefonía, es una técnica muy depurada. Los teléfonos móviles son unas de las mejores máquinas de monitorización que existen. No obstante, eso no quiere decir que no haya que recurrir a ellos. Despues de todo, para eso estamos aquí.

Así mismo, quiero inistir de nuevo en una advertencia, antes de que nadie intente echarnos la mano al cuello. Esta guía va enfocada a usuarios básicos de smartphones. Gente cuyo uso del sistema se limita a disfrutar de la experiencia de usuario que su movil salido de fábrica puede ofrecerle. Si eres un usuario más avanzado y con conocimientos técnicos, lamentamos decirte que hemos diseñado esta guía para tratar de ser lo más asimilable posible, y que no entraremos a profundizar en complejos asuntos técnicos sobre privacidad y anonimato, ni tampoco en todas las opciones de que disponen muchas de estas aplicaciones y que, lo sabemos, son estupendas.

De hecho, si aún disponiendo de conocimientos, decides enmarcarte en la tarea de revisar todo este documento, probablemente encuentres conceptos o definiciones que no son las más acertadas: Somos conscientes de ellos, pero aún así, quisimos plasmarlo de esta manera pues, aunque no sea una definición exacta, consideramos en ese momento que era la más entendible y aproximada para el gran público.

También somos conscientes de que existen otras técnicas y aplicaciones distintas que quizás son capaces de lograr lo mismo, incluso de forma más efectiva, así que, por favor, abstente de criticarnos pues, aunque lo sabemos, en su momento creímos que lo que a continuación viene era lo más sencillo y amigable, y que, además, pudiera ser exportable a otras plataformas como ordenadores de sobremesa. De hecho, todo lo aquí utilizado permite la interconexión con personas que están en ordenadores. Todos los programas aquí explicados tienen su alternativa para GNU / Linux o Windows, y que nos permitiran comunicarnos globalmente. No son tecnicas exclusivas de smartphones. No obstante, y aunque lo intentamos, en algunos casos dar la información suficientemente “mascada” rozaba lo imposible, así que os invito, a aquellos a los que los conceptos expuestos os suenen raros, a que una vez finalizada la lectura de este documento, uséis internet para ampliar más aún vuestros conocimientos.

Todas las aplicaciones, técnicas y hábitos explicados aquí son completamente legales y de libre uso, prueba de ello es que todo se descarga desde el programa de aplicaciones de Google. No obstante y dado que no podemos estar presente para asistir a todos los usuarios, queremos dejar claro que no nos responsabilizaremos de ningún daño derivado de haber puesto en funcionamiento nada de lo aquí expuesto.

La verdad es que podría dedicar páginas y páginas enteras a desarrollar de una manera muchisimo más amplia todos estos asuntos relacionados con privacidad y anonimato, incluso alternativas al uso de GooglePlay pero, por desgracia, esto es lo que nos ha salido tras pasar la tijera sobre todo el materíal que nos gustaría haber includo. Sea como fuere, te deseo que te sea util y, sobre todo, que a partir de ahora, tus hábitos de uso de smartphones sean mucho más saludables gracias a los conceptos. Este manual se licencia como cultura libre: Usalo, distribuyelo, modificalo...

iGNUrante, miembro del HacksturLab

Consideraciones y consejos básicos sobre privacidad y anonimato:

El primer punto que me gustaría desarrollar es que privacidad y anonimato NO SON LO MISMO. Haciendo una definición barata, pero clarificadora para con estos dos conceptos, podríamos decir que la privacidad es la capacidad que tenemos para realizar actividades sin que nadie, ajeno a nosotros, sea consciente de que estamos realizándolas, mientras que, por su parte, el anonimato es la barrera que evita que se sepa quien está detras de la realización de una determinada actividad, que no necesariamente tiene porqué ser privada. Teniendo claro estos conceptos es importante, a partir de aquí, diferenciar el porqué vamos a tomar algunas de las medidas que vamos a tomar a lo largo de este documento.

La mejor defensa que alguien puede tener para contra la represión en caso de actividad online es la "negación plausible". ¿como podríamos interpretar la negación plausible? Pues como una técnica de inteligencia que nos permite negar el conocimiento de una determinada información, o de algún dato. Dicho de manera práctica: Nadie podría probar con absoluta certeza y sin el más resquicio de duda que has sido tu la persona que ha realizado algúna actividad.

El primer paso que todo ciudadano que debería dar es proceder al compartimentado de su identidad. La compartimentación de información es otra técnica de inteligencia desarrollada durante la 2ª guerra mundial que evita la acumulación de excesiva información fuera de un nucleo de control, en este caso, nosotros mismos como individuos. ¿en que consiste el compartimentar tu identidad? Pues en disponer de diferentes cuentas para distintas actividades. Por ejemplo podrías tener un perfil en twitter donde conectas con tus amigos íntimos, planeas actividades lúdicas con ellos y realizas un uso personal de redes sociales y, así mismo, disponer de otra cuenta, totalmente desvinculada de la anterior en la misma red social, usando un nick o pseudónimo que no se pueda relacionar con la primera y donde publicas tus comentarios sobre la actualidad política, conectas con otros círculos de amigos y conocidos independientes de los primeros, y subes fotografías de manifestaciones, o realizas cualquier otro tipo de actividad distinta. Por eso, si aún no lo has hecho, te invito a que vayas pensando desde ya en ir creando diferentes cuentas de email y de cualquier otro servicio online que uses en internet

El compartimentado de tu identidad es esencial de cara a evitar, entre otras cosas, que se generen perfiles fantasmas sobre tí. ¿y que es un perfil fantasma? Te estarás preguntando... Pues un perfil fantasma es toda aquella información adicional que los proveedores de servicios como pueden ser facebook, se guardan para sí mismos y que, aunque no seas consciente de ello, o ni tan siquiera tengas una cuenta alli registrada, cada día aumentan más y más, en base a fotografías, los comentarios que te dejan tus amigos con detalles adicionales, las fotos donde se te etiquetan aunque no hayas subido tu, tus intereses, los enlaces que compartes... Es importante para evitar caer víctima del "bigdata". Es muy problable que, aún sin tener una cuenta en alguna de esas redes sociales, exista un perfil fantasma sobre ti en base a técnicas de reconocimento facial sobre las fotografías que tus amigos suben y a los comentarios que allí se vierten.

Siempre suelo poner un ejemplo al respecto en todos mis eventos "cryptoparty" para ejemplificarlo: Imagina que eres un activista por los derechos de los animales y, cada poco, realizas publicaciones en facebook u otras redes sociales, de animalitos en adopción de una protectora / refugio en la que participas activamente. Notarás, al cabo de un tiempo que, por alguna magia ignota, en la esquina de anuncios de facebook, twitter o google plus comienzan a salirte anuncios de veterinarios, tiendas online de mascotas y muchas otras cosas más relacionadas con los animales ¿por que sucede eso? Porque existen programas corriendo en el trasfondo de esos servicios que, minuciosamente, se encargan de buscar y registrar en bases de datos esos patrones de conducta, realizando lo que en inglés se conoce como "data mining" : Eso es el bigdata, el estudio de tus aficiones para, entre otras cosas, la comercialización de las mismas en base a vender a esas tiendas online espacios

publicitarios. Ahora imagina que, diariamente estás hablando de todos tus intereses y actividades en una sola cuenta. Estarás dándole a esa empresa proveedora de servicios carta blanca para comercializar con la casi totalidad de tu vida, de tus gustos y aficiones

Pero no solo es básico compartimentar de cara a evitar que jueguen con tu vida privada. También es una buena barrera defensiva ante posibles acciones represivas contra tu persona física. Tener diferentes círculos de actividad en diferentes cuentas, independientes, dificulta el rastreo y la creación de perfiles ideológicos por parte de cuerpos y fuerzas de seguridad del estado, así como una posible visita de un coche patrulla para buscarte, pues no serás más que un nick que siempre habla de los mismos temas. No obstante no es suficiente con compartimentar, es por eso por lo que debes seguir leyendo:

Para la creación de cuentas / compartimentado en redes sociales no son pocos los servicios que te piden, previamente, una cuenta de email para enviarte una verificación y, aunque como ya he dicho, es importante tambien compartimentar los emails, la mejor opcion a la hora de registrarte es utilizar cuentas de email desechables:

Existen proveedores de cuentas de correo que, al cabo de un tiempo (minutos) eliminan la cuenta y toda la información contenida y recibida en ella. Estos servicios nos dan una baza mas para la irrastreabilidad de nuestra identidad personal en el caso de haber adquirido un alterego online en forma de nick o pseudonimo. Crear nuestras cuentas utilizando estos servicios es una barrera más a tener en cuenta. A continuación se linkan algunos proveedores -hay muchos más- de esas cuentas de correo desechables:

• http://10minutemail.com/

• http://getairmail.com/

• https://www.guerrillamail.com/es/

Restringe, en la medida de lo posible, el acceso a tu información personal. Si ha acontecido lo peor y, por lo que sea, acabas siendo expuesto en todos los medios de prensa como si fueras un trofeo, está muy en voga comenzar a publicar de forma masiva tus fotos compartidas en internet para vender más periódicos o ganar audiencia a costa de tu persona, así pues, si decides subir fotografías personales a internet, toma en consideración las siguientes precauciones :

1. Bloquea, en las opciones de tus cuentas personales en redes sociales, el acceso a aquellas personas que NO conozcas y que no hayas autorizado, a tus contenidos tweets, comentarios y fotografías en esa cuenta personal

2. No es buena idea ser etiquetado o nombrado en ninguna fotografía, ni etiquetar o nombrar tu a nadie que salga en la misma. Podría ayudar para crear perfiles a quien monitoriza constantemente

3. Si subes una fotografía, desfigurar las caras de aquellos que salen, es una buena política., y sí acaso le interesa, hacerle llegar el original a esa persona por otras vías más seguras Existen aplicaciones que ya realizan este trabajo por ti y hablaremos de ellas más adelante.

4. Desactiva la geolocalización en las redes sociales. Esto es imperativo e importantisimo. Nunca dejes que sepan desde donde escribes, pues ese tipo de actividades genera datos que no te convienen para nada por tu seguridad. Si tienes que subir una información acerca de algo que está sucediendo en algún lugar, mejor geolocalizala mediante un hashtag (#)

Así mismo, es importante conocer la existencia de lo que, comunmente se llaman buscadores “zero-logs”. Esto son buscadores cuya utilización no queda registrada en sus servidores y, además, tienen una politica de privacidad que se opone radicalmente a la creación de perfiles fantasma de tus búsquedas en base a metadatos. ¿y que son los metadatos? Te estarás preguntando... Explicandolo de forma clara aunque no del todo exacta, los metadatos es la información adicional que tus actividades online dejan tras de sí, tales como marca y modelo del teléfono, la hora y la fecha a la que se realizó la conexión y muchos otros datos sensibles más que, para la mente aguda y motivada a la hora de desenmascararte, pueden ser de muchísima utilidad. Por eso, si de verdad quieres empezar a tomar verdadera concienca de tu anonimato, comienza a utilizar algunos de estos buscadores:

https://duckduckgo.com/ que es un motor de búsqueda abierto, potente y que, además, dispone de app para Android y tiene muchísimas posibilidades más, descritas, por ejemplo, aquí: http://www.emezeta.com/articulos/duckduckgo-guia-buscador-alternativo

https://www.startpage.com/ que consiste en una especie de pantalla protectora para obtener resultados de google eliminando, previamente, cualquier tipo de información.

También es importante tener claro que, si vas a hacer activismo, o, simplemente te preocupa tu privacidad, NUNCA USES EL TELÉFONO PARA LLAMAR O MANDAR SMS, utiliza internet para comunicarte, a través de las herramientas que relataré a lo largo de esta guía. En España existe el sistema SITEL, que es el que permite a los cuerpos y fuerzas de seguridad del estado monitorizar -teoricamente solo con una orden judicial, en la práctica yo no me lo creo- las comunicaciones de tu teléfono, con la colaboración obligatoria de tu proveedor de servicios, donde quedará registrado a quien llamas o mandas SMS y cual es su contenido. Este punto es importante pues, una de las primeras medidas que podrían tomar contra ti es pincharte el teléfono

Otra cosa que tienes que tener clara son tus prioridades. A lo largo del tiempo que he dedicado a impartir eventos cryptoparty, me he encontrado con persona con teléfonos de gama media-baja, cuyo espacio en memoria es cláramente restringido y, aunque las aplicaciones que aquí expongo no son especialmente grandes y corren en cualquier teléfono independientemente de su potencia, para muchas de esas personas les resultaba un dilema muy grande tener que desinstalar aplicaciones “guays” solo para poder almacenar en su teléfono unas, aparentemente, inservibles aplicaciones para mantener su seguridad en internet. Si tienes problemas de espacio en tu teléfono por ser de gama media-baja, y te cuesta discernir entre la utilidad de disfrutar de privacidad y anonimato o de juegos en tu movil, solo te puedo dar dos consejos, cómprate un teléfono mejor, o replantea tus prioridades y preguntate ¿por que seguir leyendo esta guía?

Pasando ya a otro tipo de consideraciones rápidas, de cara a tu actividad online deberías tener en cuenta las siguientes expuestas en este “Negatorio” de consejos breves no solo si vas a hacer activismo, sino por pura protección personal:

NO des información personal en internet porque es público, cualquiera podría leer lo que escribes, también la policía, y NO menciones tu participación en grupos de activismo online, en la vida real.

NO incluyas información personal en tu nombre de pantalla. Una fotografía o tu nombre real son, en mi opinión, un error. Siempre es mejor recurrir a un pseudónimo y un avatar.

NO facilites información personal, tu dirección aproximada (calle, barrio...) o de dónde eres en ningun sitio de internet.

NO menciones tu género, tatuajes, cicatrices, piercings u otras características físicas llamativas

NO menciones tu profesión, hobbies o aficiones en varias cuentas a la vez

NO menciones si tienes una relación sentimental.

NO menciones tu participación con otros grupos activistas o círculos de personas con los que contactas a través de otras cuentas ó perfiles

NO menciones congresos en los que has estado o participado en tus cuentas de activismo
.
NO menciones tus estudios, universidad, etc..

NO te conectes siempre a la misma hora. Intenta hacerlo de forma alternativa.

NO hagas a la vez inicios de sesión y cierre en Facebook, Twitter e IRC, pueden ser comparados y así identificarte mediante otras cuentas.

NO actualices nunca tus programas o aplicaciones mediante wifis públicas o durante manifestaciones a menos que estés conectado a través de una VPN. Hazlo siempre desde tu casa y redes de confianza. De otro modo podrías ser víctima de un honeypot para instalar en tu teléfono aplicaciones como Finfisher, de monitorización policial, o ser víctima de sistemas de vigilancia como Stingray

NO tengas tu teléfono cerca cuando estés hablando de situaciones o de asuntos de tu vida lejos del teclado (AFK), nunca se sabe si alguien puede estar usando tu microfono para escucharte

NO utilices programas de acceso remoto a tu teléfono que permitan, en caso de pérdida o extravío, acceder remotamente y borrar su contenido o localizarlo mediante GPS. Al igual que puedes acceder tu, alguien más podría acceder. Si ya no tienes teléfono asumelo: Procurate uno nuevo y da gracias que has seguido todos los consejos de esta guía básica.

POR ÚLTIMO, LEE LA GUÍA AL COMPLETO ANTES DE INSTALAR NADA Y DESCONFÍA

SIEMPRE DE TODO: LA CRIPTOGRAFÍA PUEDE DAR UNA FALSA SENSACIÓN DE

SEGURIDAD Y, AUNQUE AYUDARÁ MUCHÍSIMO A EVITAR QUE TU PRIVACIDAD Y

ANONIMATO SE VEAN COMPROMETIDOS TAN FACILMENTE, PIENSA QUE LA

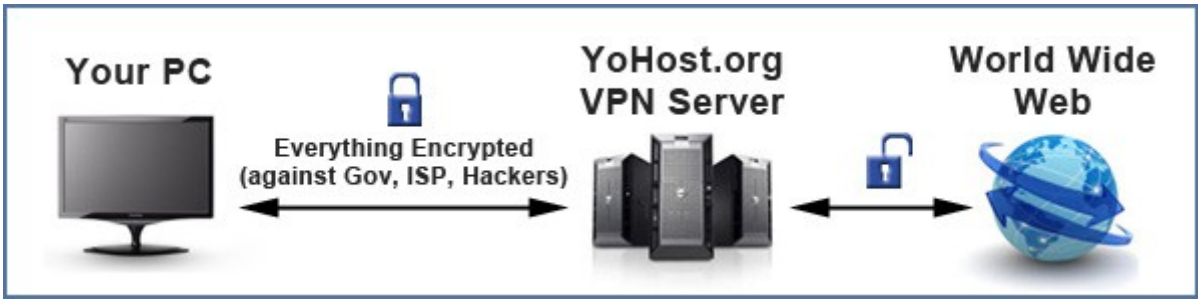
PARANOIA ES TU MEJOR MECANISMO DE DEFENSA

Ofuscando tu IP: VPN & Tor / Orbot:

Para aquellos que no lo sepan, todos los dispositivos conectados a día de hoy a internet disponen de una dirección IP. Una IP, poniendo un simil cotidiano es como un número de teléfono que los distintos ordenadores del mundo utilizan para comunicarse entre sí y realizar las transmisiones de datos. Por eso es MUY importante saber ofuscar tu IP: Porque, de otro modo, estás declarando abiertamente quien eres y desde donde te conectas, y a cualquier cuerpo de seguridad le resultará muy facil encontrarte.

Afortunadamente existen numerosas opciones a día de hoy para ocultar tu ip, así pues voy a exponer dos de las más habituales, como son el uso de una VPN o de la red Tor. Estos dos métodos son excepcionales porque, además de hacer que tu conexión, aparentemente, provenga desde cualquier otra parte del mundo excepto desde tu teléfono, realizan la transmisión de datos cifrada, de manera que ni tu proveedor de telefonía, ni la policía si te tiene monitorizado, podría saber que estás haciendo online, pues no pueden ver el contenido de tus comunicaciones. El uso de estas herramientas no solo es bueno de cara a hacer activismo, es una práctica muy sana si estás usando wifis públicas de bibliotecas, cafeterías, o símplemente puntos de acceso abiertos que te encuentres por la calle, pues nunca se sabe quien podría estar controlando dichos accesos, y quizás haya alguien intentando espiar comunicaciones, pues con un mínimo de interes, para cualquier cracker es sencillo hacerlo. No solo eso, te aportará ventajas a la hora de evadir la censura si tu conexión a internet está “capada” y se te restringe el acceso a determinadas páginas web o servicios de internet.

VPN:



Una VPN, explicado de forma coloquíal, es un tipo de conexión que crea un tunel cifrado de datos con un proveedor de servicios de privacidad. Una conexión directa con otro ordenador, protegida mediante criptografía que la hace ilegible, tal y como muestra el diagrama. Una vez que nuestra información ha llegado al proveedor de servicios, ya se transmite a internet de forma normal, de manera que, cuando alguien intente rastrear tu actividad, llegará a un callejón sin salida al no poder superar la barrera de tu proveedor de VPN que, con casi total seguridad, además, estará en otro país con otra legislación distinta y al que cualquier solicitud de datos por parte de España le resultará irrisoria... Una VPN no solo mejora tu privacidad haciendo ilegible mediante criptografía cualquier tráfico de internet que tu proveedor o la policía quieran monitorizar, también mejora tu anonimato pues el destinatario final de la información nunca podrá saber desde donde se la han enviado
Aunque existen proveedores de VPN gratuitos, mi recomendación, si te tomas en serio tu privacidad, o si vas a hacer activismo de relativa importancia o riesgo y necesitas anonimato, es que pagues por ella. Despues de todo, un buen proveedor de servicios de VPN, entre otras cosas, si pagas, te ofrecerá distintos paises desde donde aparentar que estás conectado y, lo más importante, te protegerá bajo una estricta póliza de no guardar dato alguno sobre tu persona. Un proveedor de VPN normal ronda entre los 30 y 50 euros al año, normalmente no tiene límites de ancho de banda o de megabytes y, además, lo puedes usar en distintas plataformas a la vez (o sea, además de en tu movil, también en tu ordenador de sobremesa). Podría entrar a hablar de muchos más detalles, tales como el protocolo a usar (PPTP, OpenVPN...) para transmitir y encriptar los datos, o de si se

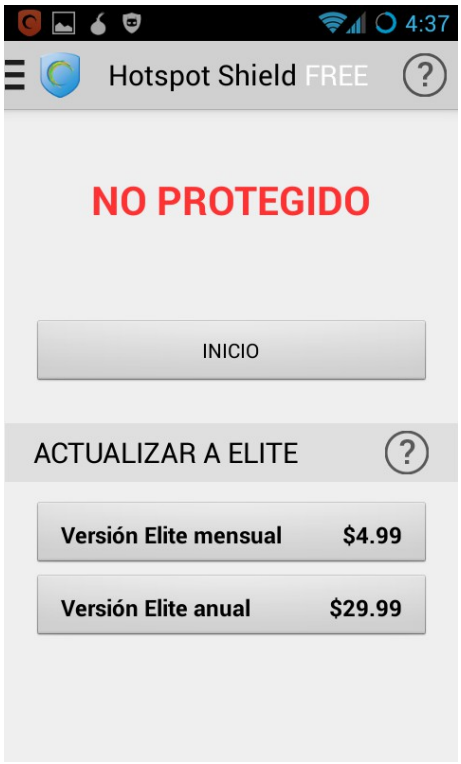
licencia como software libre, aunque no lo considero relevante y, si además tienes inquietud, te invito a que busques información por tu propia mano usando los buscadores anteriormente mencionados

A continuación expongo dos de las aplicaciones más utilizadas en Android. Una de ellas es gratuita y funciona muy bien, aunque existe el riesgo de que el proveedor de servicios esté recolectando algún dato tuyo. Dispone por supuesto de versión de pago, en el que ya entonces te aseguras que no guardarán registro alguno. Y otra, que es la que yo utilizo, que es de pago, y que para ejemplificar como funciona de forma genérica, servirá muy bien. Nótese que no quiero hacer, bajo ningún concepto, apología de algún proveedor determinado, esto son solo ejemplificaciones basadas en mi experiencia y disponibles en "Google Play". HAY MUCHOS MÁS PROVEEDORES IGUAL DE BUENOS

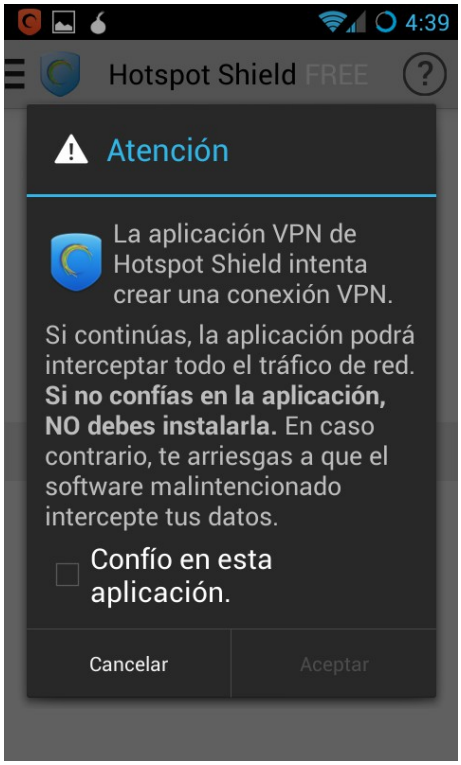
HotSpotShield: Gratuita, aunque no confiable del todo
Salvo que, obviamente pagues (retiene datos en caso contrario)
Aún así es una buena salvaguarda. Mejor que nada

PrivateInternetAcces: De pago y con buena póliza de privacidad

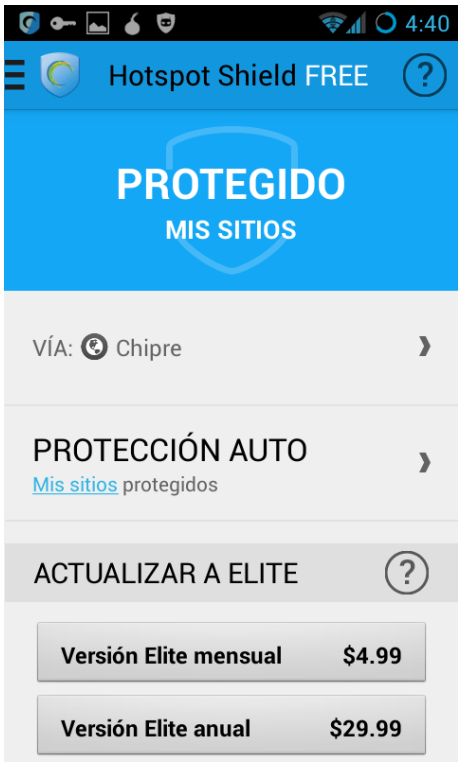
En la pantalla de presentación nos informan de algunas ventajas



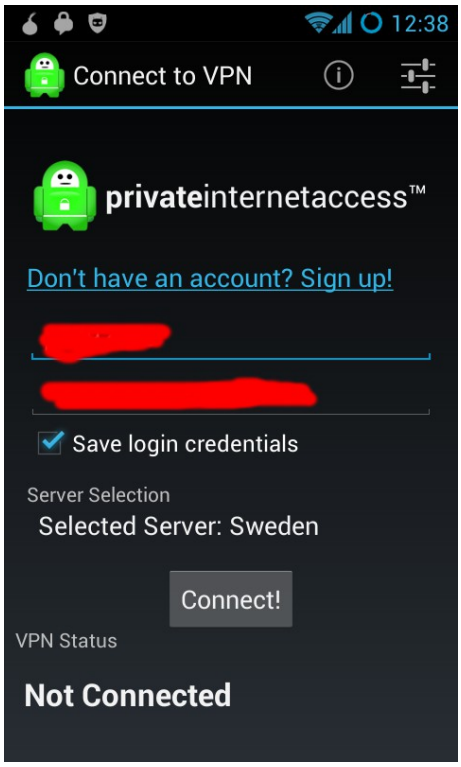
La app nos indica que aún no está contectada y el precio si deseas la versión mejor. Tan solo presiona "Inicio"



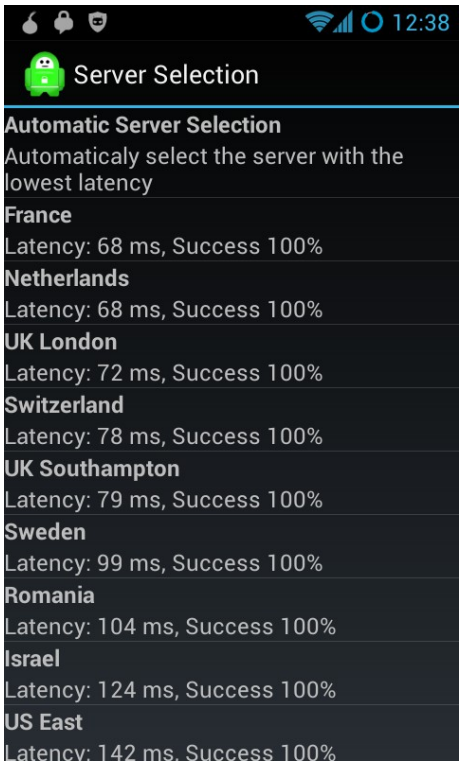
La app nos pide permiso para modificar nuestra conexión a internet. Obviamente le diremos que sí confiamos



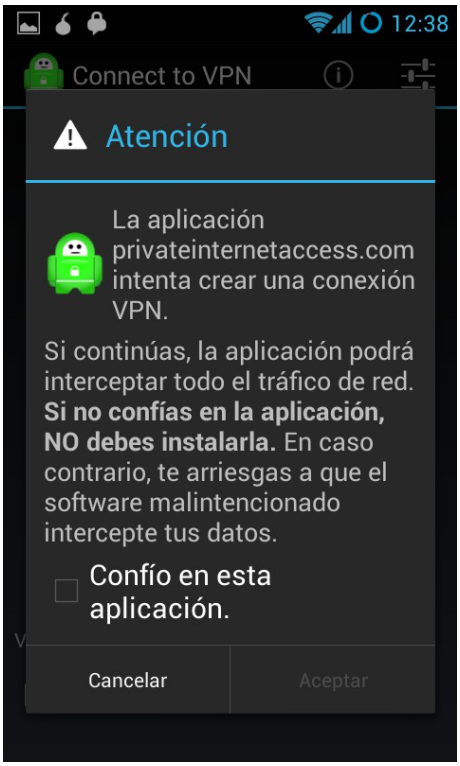
Ya estamos conectados y protegidos. Si presionas en la sección "Via.." te dejará escoger otros países como UK, o USA



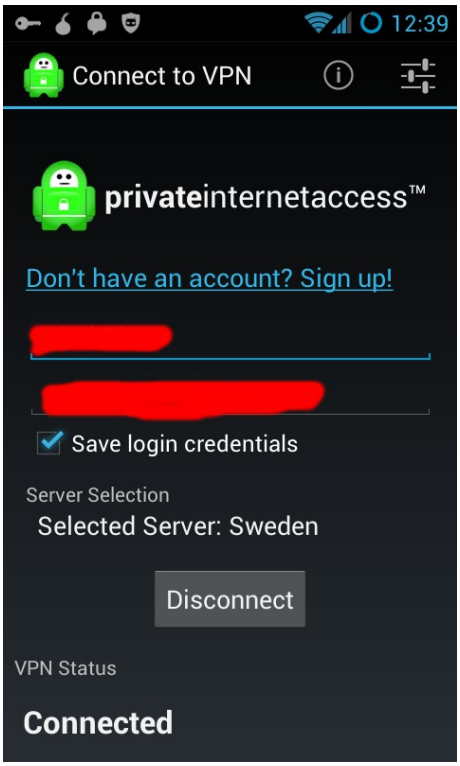
Respecto de la otra app, Privateinternetacces, este es su inicio Pantalla principal donde podemos crear una cuenta e introducir nuestro login y password



Si presionas en "Selected Server" nos saldrán varios Paises a elegir, así como su latencia (ping). Cuanto mas baja sea, mejor.



Antes de liarla parda, la app nos pide permiso para conectarse



¡Conectado! Fuck the police!. Así de facil es...

Tor:

El proyecto Tor es una red de decenas de miles de voluntarios de todo el mundo que comparten parte de su conexión a internet para crear un entramado digital donde es posible evadir la censura, evitar ser rastreado y garantizar el mayor anonimato. Además todas las conexiones dentro de la red Tor van cifradas, con lo cual nadie podrá monitorizarte de forma exitosa. El uso de la red Tor es totalmente gratuito y abierto para todo el mundo, y han depurado de tal manera su uso que cualquier persona puede disfrutar de ella en casi cualquier plataforma (Android, Windows, GNU/Linux, MacOS X...).

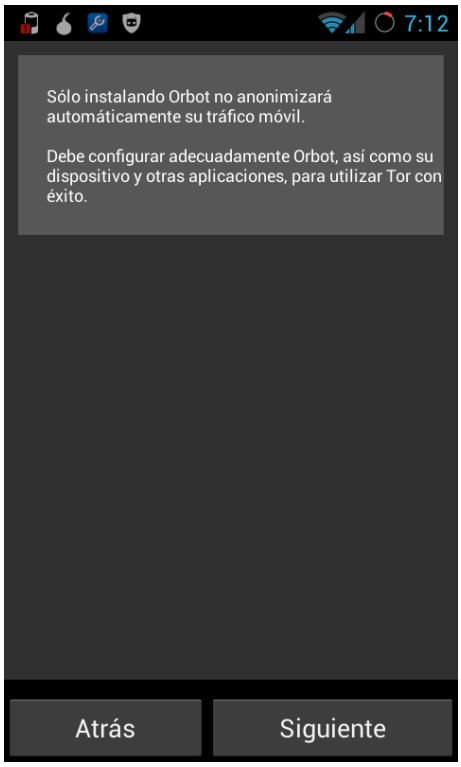
Es interesante que sepas, además, que de tanto en cuanto -minutos- tu conexión a la red Tor se reconfigura y renegocia así, de cara a alguien que intente rastrearte, estarías, aparentemente, cambiando de país cada pocos mínutos: Una auténtica pesadilla para el “gran hermano”. Es una buena alternativa si tu economía no te permite contratar una VPN, pues es igualmente seguro a la hora de protegerte de miradas ajenas por parte de la policía o tu proveedor de telefonía y, además también mejora tu anonimato. ¡Y si combinas Tor con una VPN es todavía AUN mejor!

El proyecto Tor es software libre, con lo cual cualquiera puede auditar su código fuente en busca de puertas traseras o posibles fallas. Esa es una buena baza de cara a confiar en este software

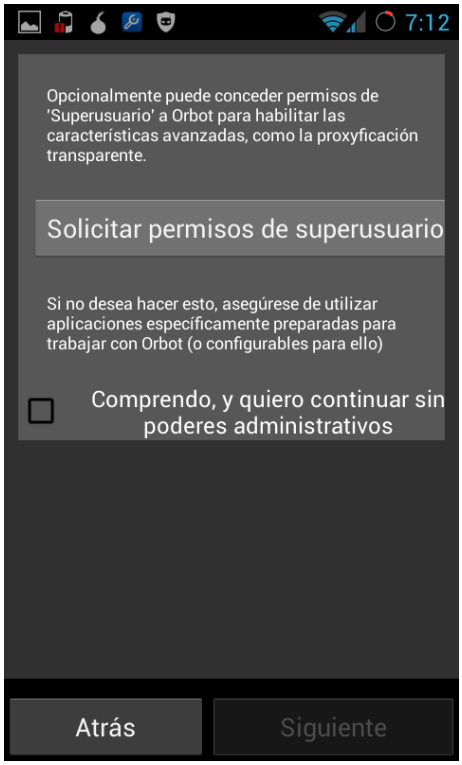
Realmente el proyecto Tor está tan sumamente “mascado” que considero innecesario ponerme a explicar de forma técnica el como funciona, así que te invito a que visites su página web y leas esta breve explicación sobre como funciona.

Tor / Orbot en el Google Play para instalar

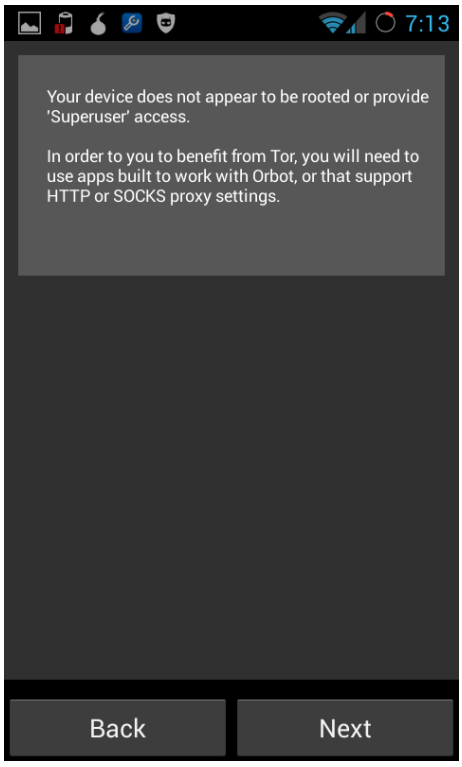
Una vez instalado y ejecutado por primera vez, nos sale este tutorial. Paso uno: Seleccion de idioma



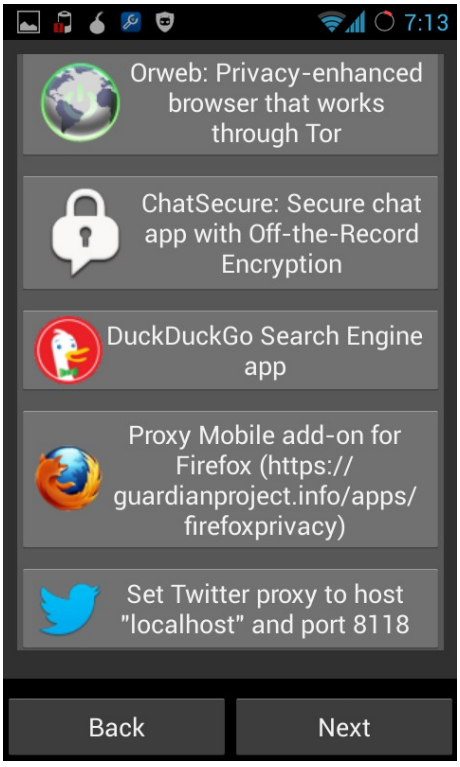
Aviso para “navegantes”, muy importante



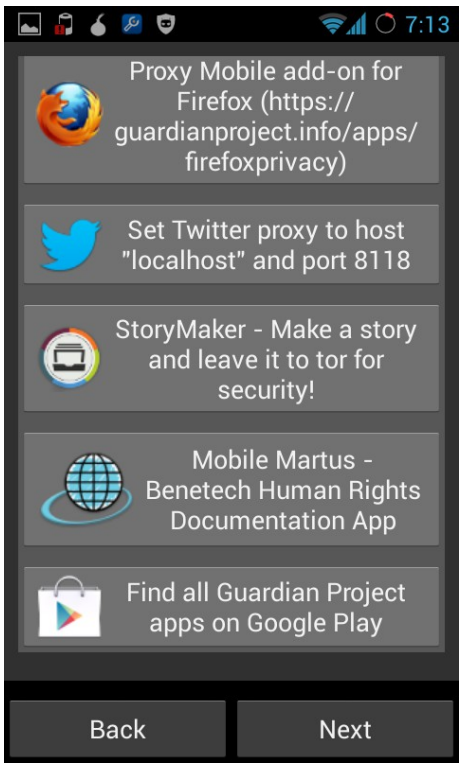
Si tu teléfono está “rooteado” (cosa que dudo, y si no sabes lo que es, mejor aún, para no liarte) podrás activar opciones “chuliguays” en Tor / orbot. No obstante, mi consejo, por batería y seguridad, es que actives la casillla de “comprendo y quiero continuar SIN poderes administrativos” o sea, sin usar superuser



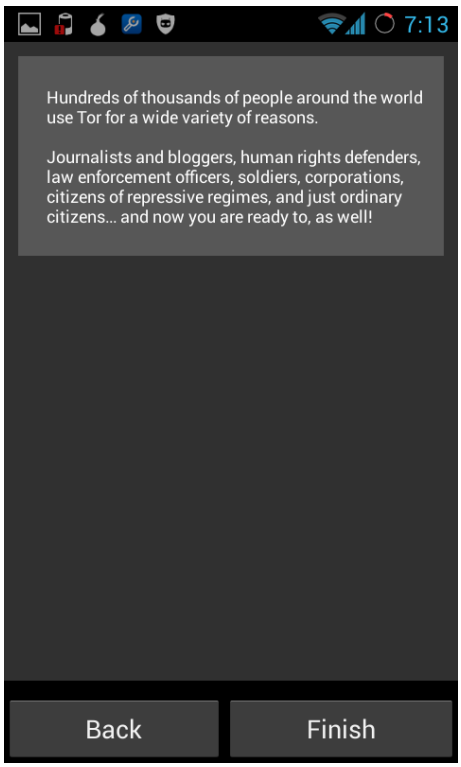
El propio programa nos avisa de que vamos “a pelo”



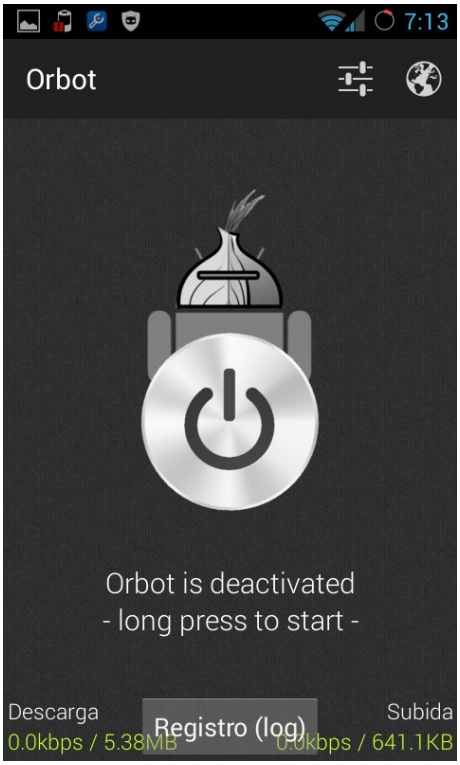
A continuación nos muestra algunas de las apps propuestas para utilizar con tor/orbot de manera segura, tras su protección...



Más apps que se pueden combinar con Tor, o que provienen de los creadores del proyecto Orbot

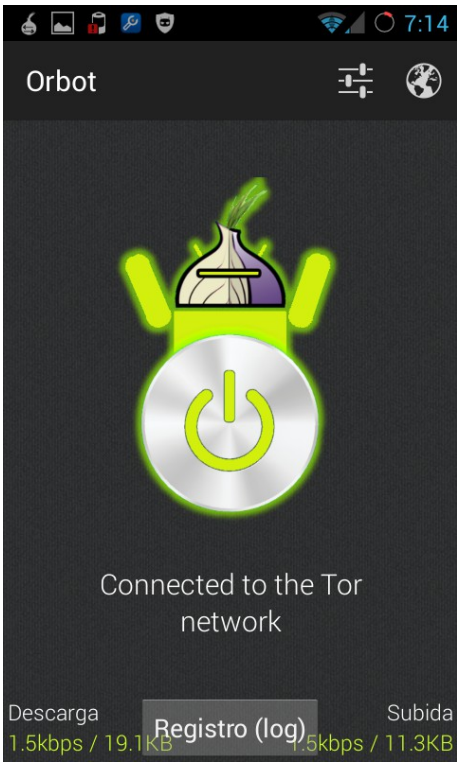


Una breve explicación de quien puede ser el perfecto candidato a ser usuario de Tor / Orbot. Gente con buenas razones para mantener su anonimato y velar por su privacidad. ¡Ya casi terminamos!



Para empezar a usarlo, presiona durante unos segundos el botón de power de la pantalla

“Estamos trabajando en ello” que diría Chemari Aznar
Se está conectando, no toques nada



¡Estamos conectado a la red tor! Ya puedes salir
Notarás que un logotipo de una cebolla ha empezado a ser visible en la barra de notificaciones de tu movil

Navegadores: Firefox con Proxymobile

Como ya he dicho al principio de esta guía, conviene que la leas al completo ANTES de instalar nada, por eso, antes de instalar Tor / Orbot, es esencial tener instalado el navegador Firefox, así podremos instalar, durante el tutorial de tor, el plugin de Proxymobile, que nos permitirá hacer que nuestra navegación web (a través de Firefox) se realice de forma anónima, dificilmente rastreable.

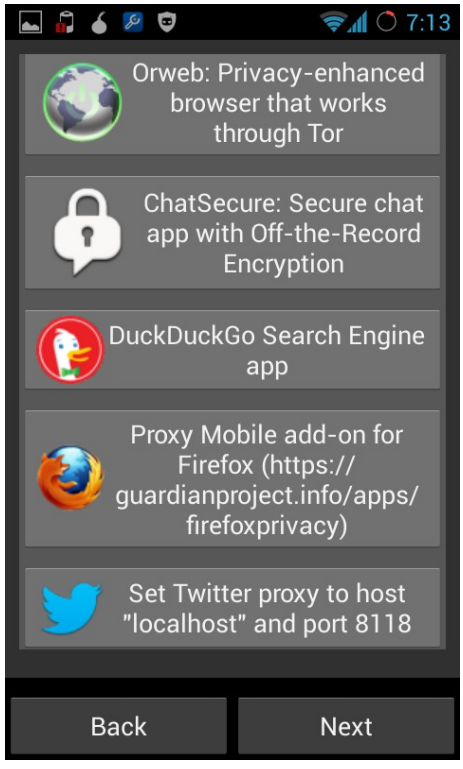
El navegador Firefox para Android es parte de la fundación Mozilla, por lo que su licencia de software es Open Source, es decir, de código abierto, lo cual es muy positivo

Como habrás visto en el paso previo, el proyecto Tor, en su selección de apps, también menciona el navegador Orweb, diseñado ex profeso para usar la red Tor por defecto pero, como es un proyecto que aún le queda mucho por evolucionar y no te permitirá disfrutar de la experiencia que firefox sí te va a permitir, te recomiendo que siguas mis consejos de forma estricta e instales Firefox en lugar de Orweb.

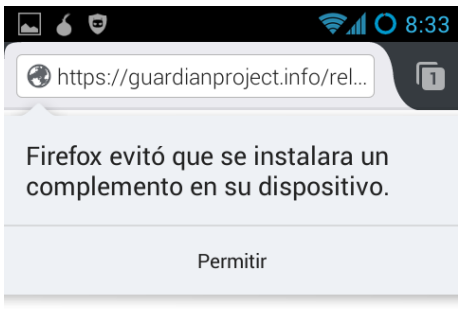
Disponer del navegador Firefox es esencial para un apartado del siguiente capítulo, el referente a redes sociales, en especial en la parte relacionada con Facebook, pues la app de twitter está mejor diseñada y tiene su propia forma de hacer funcionar tor, que más adelante veremos

A continuación expongo la secuencia, paso a paso, de como proceder a su instalación y puesta en funcionamiento.

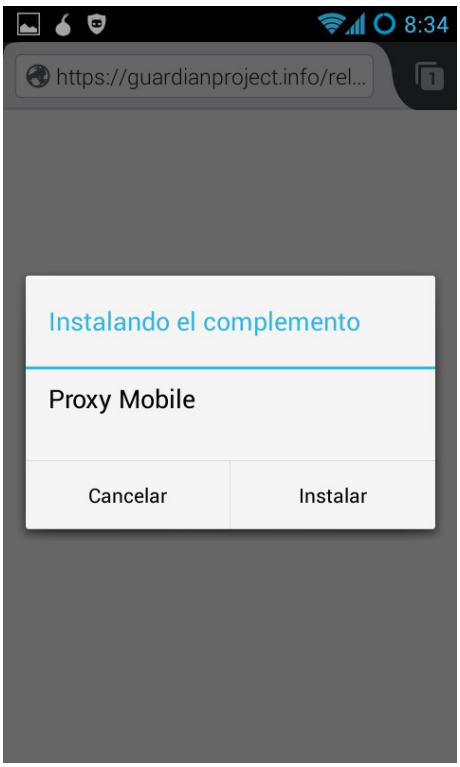
Vista del navegador Firefox en Google Play para instalar



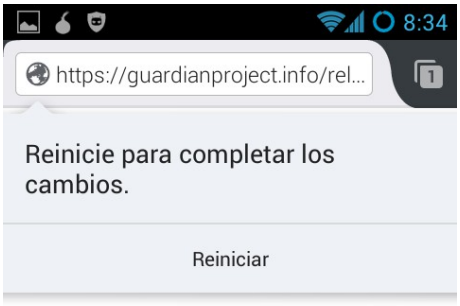
Si te fijas, esta es la misma captura de pantalla del tutorial de tor. Como verás, además de Firefox también dispones del navegador orweb, sin embargo, llegados a estepaso en el anterio tutorial, haz click en “proxy mobile add-on for firefox” y se te abrirá



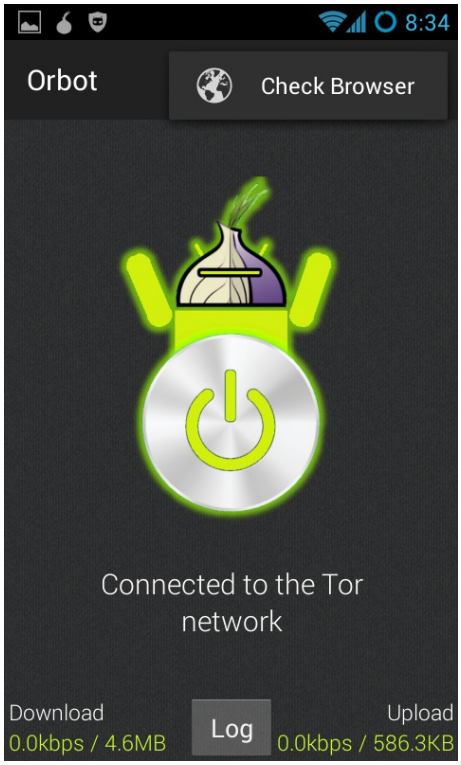
Quizás te salga este aviso al querer instalar el add-on Obviamente, debes permitir que se instale



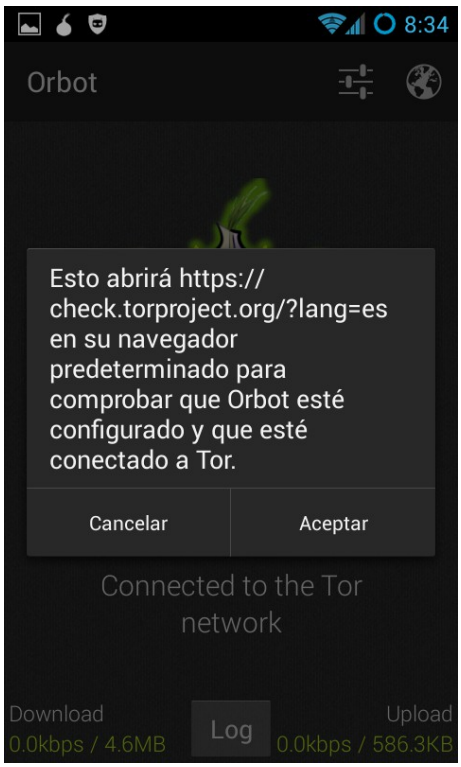
Al haberle dado permiso comenzará a descargar el Plugin, cuando esté finalizado, te saldrá este aviso. Solo hay que darle a “instalar”.



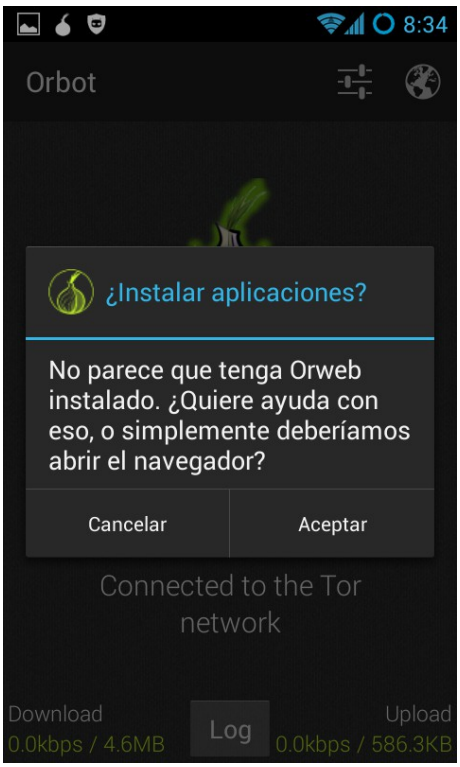
Cuando ha terminado de instalar, él mismo nos pedirá reiniciar el navegador. Solo es hacer click



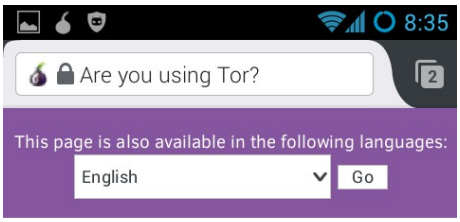
Ahora vamos a comprobar que efectivamente Tor está Funcionando en nuestro Firefox, para ello, en Orbot Presionaremos el globo terraqueo que hay arriba a la derecha de la pantalla y seleccionaremos “Check browser para ejecutar Firefox

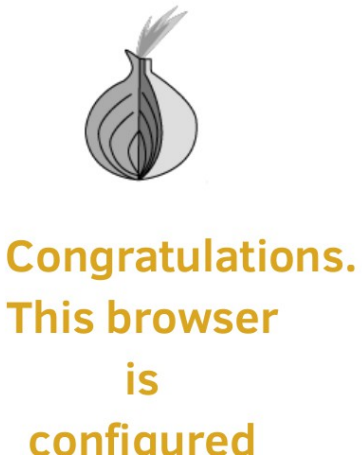


Orbot nos avisa que va a realizar una comprobación sobre si nuestro navegador es el adecuado, Presiona “aceptar



Como NO hemos instalado Orweb, en este paso hay que seleccionar “Cancelar” para que busque a Firefox





Si lo hemos hecho todo bien se abrirá Firefox y, tras unos segundos nos mostrará este mensaje de enhorabuena

Redes Sociales: Twitter y Facebook

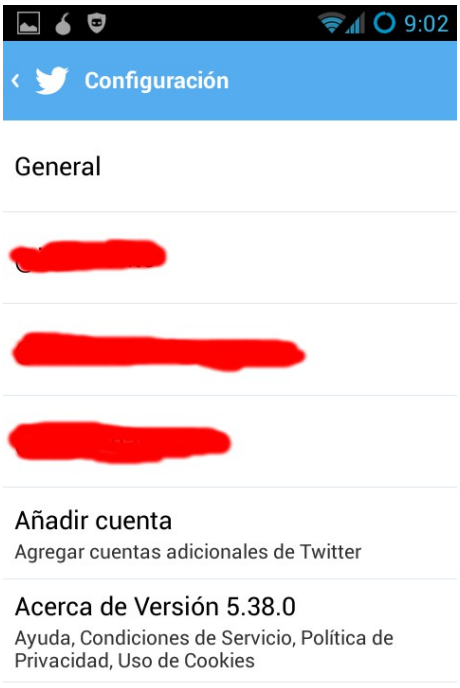
Aunque soy marcadamente proclive a abandonar el uso de estas redes sociales propietarias (es decir, con intereses economicos tras de sí) y no tan respetuosas para con tu privacidad, en favor de alternativas más OpenSource, distribuidas y seguras como GNUSocial, Pump.io o Diaspora, entiendo que lo mayoritario manda y, aunque os lanzo un guante a que os informéis usando buscadores éticos acerca de estas alternativas de redes sociales, los siguientes pasos que voy a explicar van relacionados con dos de los más grandes peces gordos en ese negocio que es el social media: Twitter y facebook.

Lo que vamos a aprender aquí es como acceder y utilizar ambas redes sociales de una forma segura y más eficiente para con nuestro anonimato. Ojo, he dicho ANONIMATO, no privacidad, así que si aún no sabes diferenciarlas, te sugiero vuelvas al principio de la guia y vuelvas a empezar

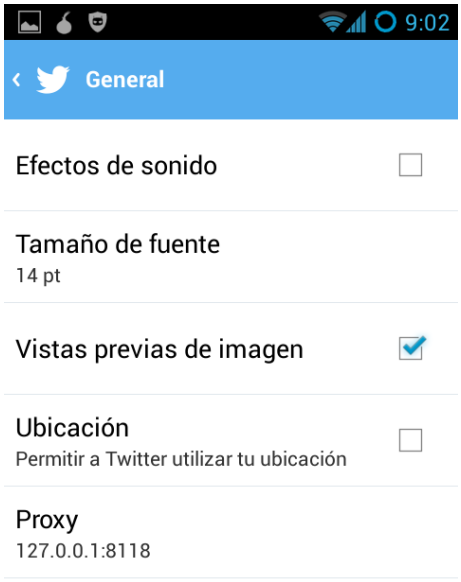
Twitter:

Ya he comentado anteriomente que el cliente oficial de twitter está mucho mejor pensado para ser compatible con el de facebook, con lo cual, para que tu anonimato en twitter esté protegido por el uso de la red Tor tienes que utilizar, obligatoriamente, el cliente de twitter. Otros clientes alternativos, aunque soy consciente de que tienen mejores opciones para interactuar en esta red social, no gozan de la opción en concreto que vamos a utilizar aquí: El proxy http. Así pues, dando por sentado de que ya has instalado, previamente, el cliente oficial de twitter desde el google play, y que ya has configurado tu cuenta de usuario con anterioridad, vamos a proceder a “liar” la madeja de IP's desde las que accedes a twitter. Obviamente, si vás a usar una VPN estas cosas son, en principio, innecesarias, aunque sí muy recomendables:

Desplegamos el menú de opciones de twitter presionando los 3 puntos verticales que están arriba a tu derecha y que te mostrará este menú. Selecciona “Configuración”



Una vez que hemos accedido al menú “Configuración” nos mostrará las cuentas que tenemos registradas y otras opciones, aquí nos interesa el menú “General” Nótese mi compartimentado de identidades al tener tres cuentas distintas registradas aquí.



En este menú es importante, antes de nada, deseleccionar la opción “Ubicación” para NO permitir que twitter pueda geolocalizarnos y añadir nuestra posición a nuestros tweets
Una vez deseleccionado, clickea en la opción “Proxy”
En el primer capítulo mencionaba como era mejor opción utilizar hashtags para marcar la situación, en vez de este Sistema mucho más peligroso (#####!!!)

Una vez has accedido al menú “proxy” rellenalo tal y como se muestra en esta imagen que, si haces algo de memoria, son las mismas que durante el tutorial de Tor / Orbot te pedían para configurar twitter. Una vez hecho esto, ya puedes volver atrás. ¡Estas a traves de la red Tor!

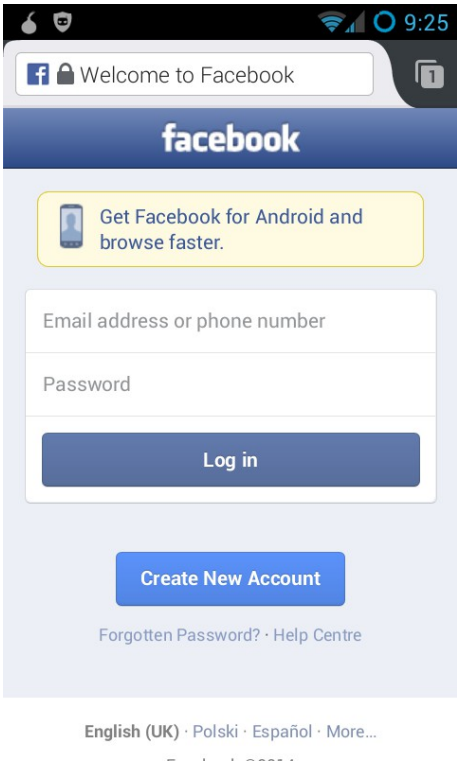
Facebook:

Esta red social es, a mi juicio, uno de los más malignos inventos que ha surgido de internet en la última década. Es una máquina de hacer dinero atroz, endémica y peligrosa. Y todo en base a una sola cosa: Tus datos. Al igual que twitter -aunque esa en menor medida- No te permite subir las fotos de las cenas con tus amigos, o de planear tus eventos solo porque es un grupo de gente amable, sino porque, textualmente, has accedido a que, a cambio de todos esos “favores” puedan someter a analisis hasta el más minimo detalle de tu actividad dentro de sus dominios digitales con el único fin de comercializar con ella. No obstante, su depurada interfaz, estoy de acuerdo, es amigable hasta para el más torpe de los activistas y, puestos a tener que planear un evento viral, es entendible “vender tu alma al diablo” en pro de la difusión masiva. No obstante, y si has seguido todos los pasos expuestos hasta ahora, probablemente hayas ganado muchos enteros de cara a protegerte, así que vamos a ello.

El cliente de facebook es completamente inerte al uso de Tor, no dispone de opcion alguna para configurarse no así al de una VPN que protege la conexión del teléfono en su totalidad (pero no suele ser gratis si la quieres de calidad) así que, como aquí intentamos dar un mínimo de eficacia al menor coste posible, vamos a dar por sentado que NO usas una VPN y que, por ende, NO puedes usar el cliente oficial de Facebook (en caso contrario, ok, utilizalo)

Es por eso que, la única via que tenémos de acceder a facebook es mediante navegador web (¡Albricias! Pero si hace unos capítulos hemos configurado, precisamente, un navegador web movil para que funcione sobre tor...). Creo que con eso queda todo explicado: Usa Firefox con proxy mobile.

Actualmente Facebook está dando pequeños pasos para proteger la privacidad de sus usuarios en una, a mi juicio, campaña de lavado de imagen tras las revelaciones de Snowden que, en realidad, lo que busca es el efecto contrario: Motivar al usuario asustado intentándo hacerle ver lo segura y respetuosa para con tu privacidad y anonimato que es la empresa. Por eso han creado una página web al uso para acceder a través de tor. La dirección web es https://facebookcorewwwi.onion tal cual, más adelante hablaré brevemente de lo que significan los .onion. No obstante, el acceso a esta página web, mientras escribo estas lineas, se encuentra restringido solo a ordenadores de sobremesa, con lo cual te aconsejo que accedas a la misma usando la version normal https://facebook.com a través de Firefox con proxy mobile



Así se ve la version “mobile” de la página principal de facebook a través de Firefox con proxy mobile

Fotografías : ObscuraCam

Subir imágenes a internet es uno de los mayores pelígros que puede existir de cara a ser vigilado, como ayuda involuntaria para quienes monitorizan de forma continuada, así como para ser utilizado de forma ajena a nuestro conocimiento para obtener beneficios económicos.

Cada foto de un evento de activismo al que acudimos: Manifestación, concentración, lo que sea... está, con toda seguridad, siendo monitorizada por las fuerzas de seguridad del estado, que minuciosamente guardan copias de esas mismas fotos en su ordenador a modo de pruebas para, en caso de ser necesario, proceder a la identificación de alguien y su posterior arresto. Así mismo, las grandes redes sociales, como ya he mencionado, aplican programas de reconocimiento facial para crear perfiles fantasmas de nuestras identidades, registrando, de una forma más exaustiva si cabe, el contenido de la fotografía al completo (donde estás, que haces, como vas vestido...)

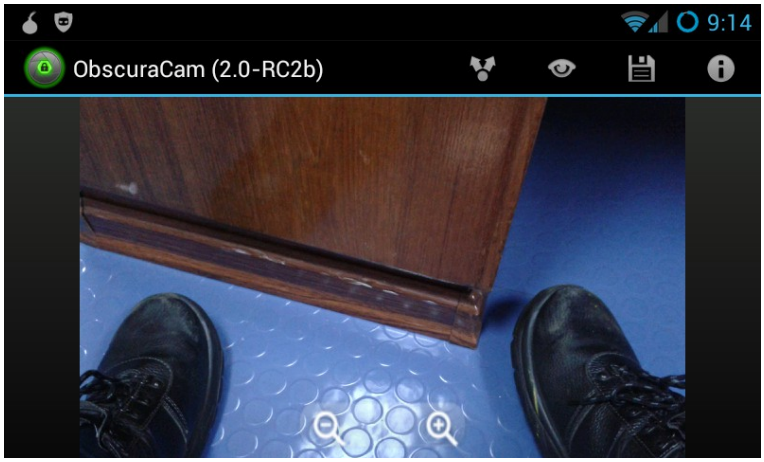
La única forma que tenemos de boicotear estas actividades y, a su vez, poder ayudar de forma "segura" a que otras personas realicen el seguimiento de cualquier evento que estés cubriendo es en base a deformar las caras. Este mecanismo tambien es util con tus fotos personales: Puedes compartirlas en internet de forma protegida y sesgada, mediante el pixelado facial, y si algún amigo quisiera disponer de ellas, buscar otra manera más privada de hacerselas llegar, por ejemplo mediante un lapiz de memoria usb

Pixelando caras evitas que aumenten los perfiles ideológicos de personas que, a lo mejor, ya están fichadas por la policía, y haces más dificil que queden evidencias gráficas de que esas personas han estado allí. De hecho, muy probablemente, la propia policía estén alli grabandote a tí, junto al resto de la gente.

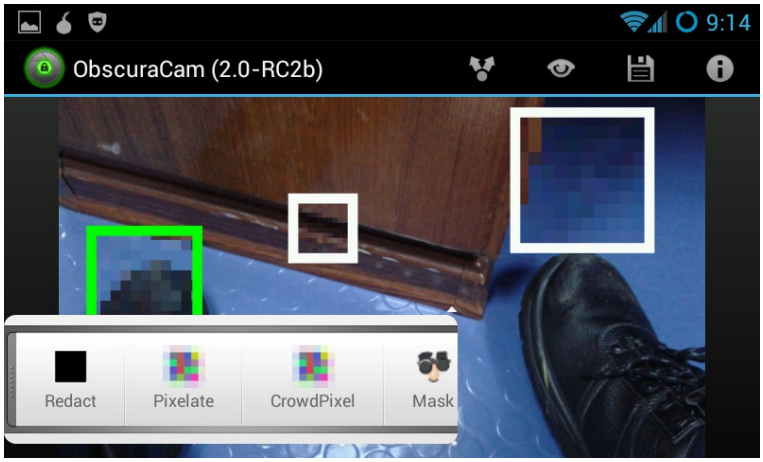
Afortunadamente, en Android, disponemos de una herramienta licenciada como software libre que se puede descargar de forma gratuita desde Google Play: ObscuraCam, cuyo uso veremos a continuación:

Esta es la App tal y como se ve en el google play

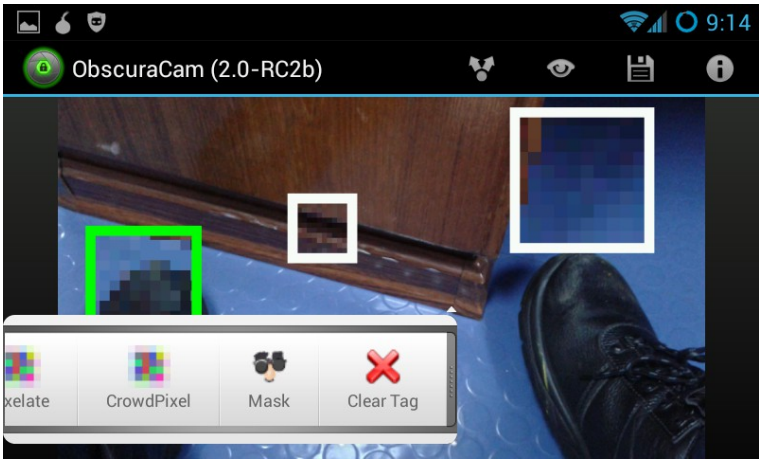
Al ejecutarla, nos ofrece tres opciones: Sacar una foto que nos abrirá la cámara de Android estandar, o bien modificar una foto o video ya existentes



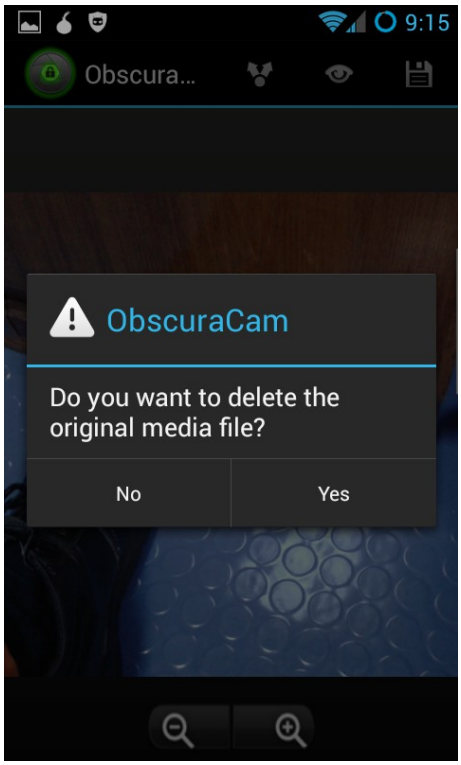
Así se ve una fotografía recién sacada. Atención a las lupas de la parte de abajo, pues son de utilidad



En función del zoom que tengas con las lupas, podremos crear cuadrados pixelados de diferente tamaño, y si los tocas, además te ofrecerá diferentes opciones de pixelado



Tambien podemos poner una máscara tipo “groucho” en las caras o bien, si nos hemos equivocado, eliminar el pixelado. Una vez que has terminado, presiona el disquete de arriba en la esquina para salvar



Al presionar salvar nos dirá si deseamos borrar la foto Original, mi consejo es que NO la borres, pero ojo con cual subas a internet

Mensajería Instantánea : Chatsecure

Hoy en día está de moda usar aplicaciones de mensajería instantanea como Whatsapp, Spotbros o Telegram. Y no son pocas las que, sobre el papel, dicen ofrecer maravillosas características de privacidad en base a su criptografía. Sin embargo, por mi parte, desaconsejo el uso de todo ese tipo de aplicaciones por numerosas razones. La primera es que no son servicios descentralizados, federados donde cada uno pueda montarse su propio servidor, o buscar uno ético, sino que todo va a un servidor central propiedad de una compañía con fines lucrativos. Además, aunque esa compañía no tenga sede fiscal en España, seguro que guarda datos tuyos. No ya por cumplir con un requerimiento legal, sino para seguir aumentando sus perfiles fantasmas gracias a tus metadatos y enriquecerse mediante la comercialización de “big data”. Y por último, aunque diga ofrecer criptografía de alto nivel, en la mayoría de las ocasiones, sinó todas, sus programas no son de código abierto: No se podría auditar como funcionan sus matemáticas. Así mismo, y de remate, está el hecho de que prácticamente todas necesitan de un número de teléfono para verificar tu identidad, y que, tan pronto las ejecutas, para que funcionen, necesitan escanear tu agenda de direcciones de arriba a abajo para cotejar quienes son tus contactos y, por supuesto, almacenar todos esos datos privados tuyos en SUS discos duros ¿donde está la privacidad?. Asi mismo, casi ninguno de esos servicios es multiplataforma: Quiero decir, que estás obligado a usar un smartphone o tablet para utilizarlos. No podrías exportar tu cuenta a un pc para tener, así mismo, posibilidad de seguir chateando cómodamente sentado

Por suerte, existe una alternativa libre, abierta, federada y completamente segura. Se llama protocolo XMPP, y es una forma de mensajería instantánea ya muy desarrollada y cuyas conexiones al servidor van protegidas mediante cifrado, para evitar “mirones”. Además, a estos servicios se les puede añadir uno más. La mensajería OTR (Off The Record) que es un tipo de cifrado adicional diseñado al uso, que se negocia sin intervención alguna del servidor que estés usando. Es decir, es un cifrado punto a punto, realizado automáticamente por nuestros dispositivos.

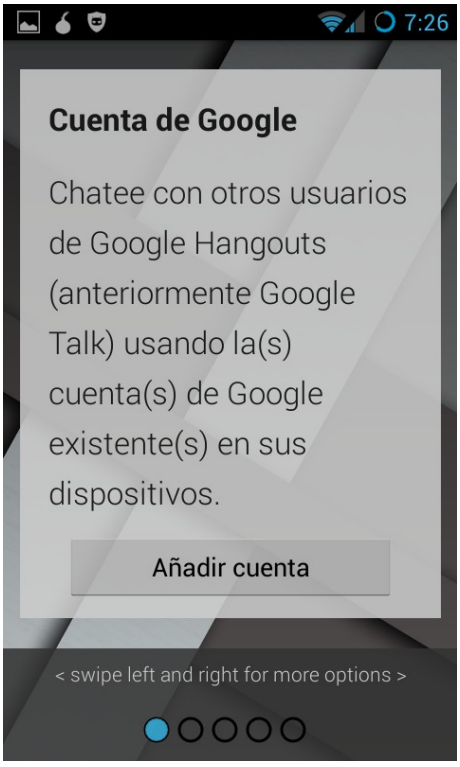
Goza de otras ventajas, además de ser descentralizada / federada, tales como que el cifrado se negocia exclusivamente para cada conversación. Eso significa que, si pasados unos días, volvemos a chatear con una persona, el cifrado será totalmente diferente. De esa manera, si alguien ha conseguido burlar nuestra privacidad, jamás podrá traducir conversaciones realizadas en otro momento. Así mismo podemos verificar la identidad de la persona que está al otro lado mediante un “fingerprint” o huella digital que, si bien no firma los mensajes, sí que sirve para asegurarnos que, en efecto, es la persona deseada la que está al otro lado y no un impostor. Realmente solo necesitas una cuenta de gmail para poder chatear, pues la propia Google es consciente de la eficacia del protocolo XMPP y, de hecho, su programa “gtalk” es lo que usa. No obstante y pese a que nuestras conversaciones estén salvaguardadas por el cifrado OTR, mi consejo es que, más abajo, leas el capítulo relacionado con proveedores éticos de servicio.No obstante puedes estar tranquilo, pues otra ventaja más es que, al renegociarse siempre un cifrado nuevo, el anterior no deja rastro alguno en tu dispositivo una vez que has finalizado la conversación.

El nombre de la aplicación de Android que permite hacer esto se llama chatsecure, y es un proyecto cuyo codigo es abierto para asegurar que no haya nada raro que pueda vulnerar tu privacidad. Esta app ofrece, además, la posibilidad de crear salas de chat en malla, dentro de la misma red wifi, y que no requiere ni de disponer de una cuenta, ni de conexión a internet (ej: Dentro de una conferencia, pabellón o plaza donde haya wifi). La ventaja inherente de ese tipo de chats es que son totalmente incontrolables y espontáneos. Incensurables.

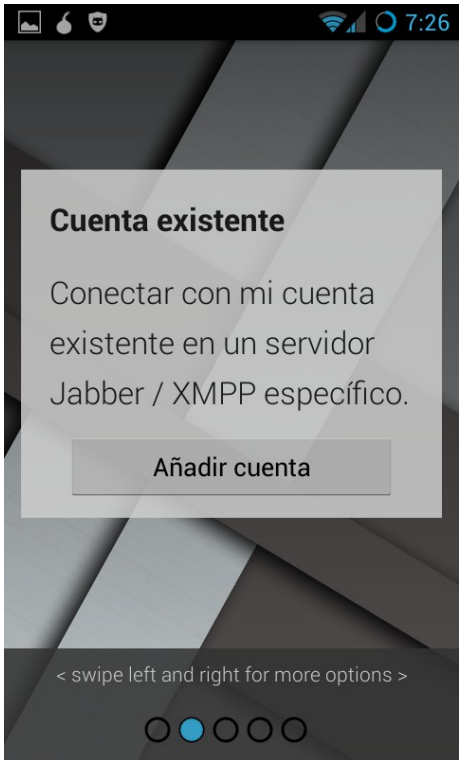
Podría hablar mucho sobre chatsecure y XMPP, no obstante, como lo que busco con esta guía es solo una breve introducción, hablaremos de la comunicación más elemental. La que se puede hacer hasta con una cuenta de gmail. Para ampliar información, como siempre, dispones de internet.

Esta es la app de Chatsecure. Tal y como aparece disponible en el google play para descargar

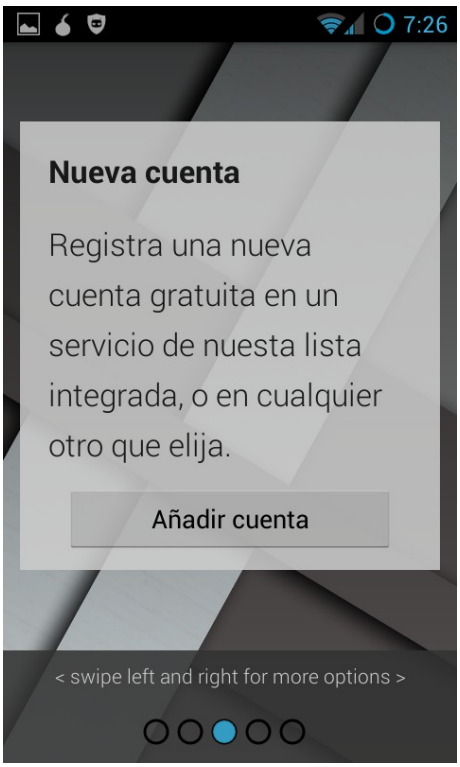
Una vez que la ejecutamos por primera vez, nos da la opción de ponerle password para bloquear el acceso a nuestros chats. Aunque es un poco petardo, mi consejo es que crees un password solo para la app y lo establecas



Lo primero que nos ofrece la app es ponerla a funcionar es mediante una cuenta de google / gmail, mi consejo es que NO uses nada relacionado con esa empresa

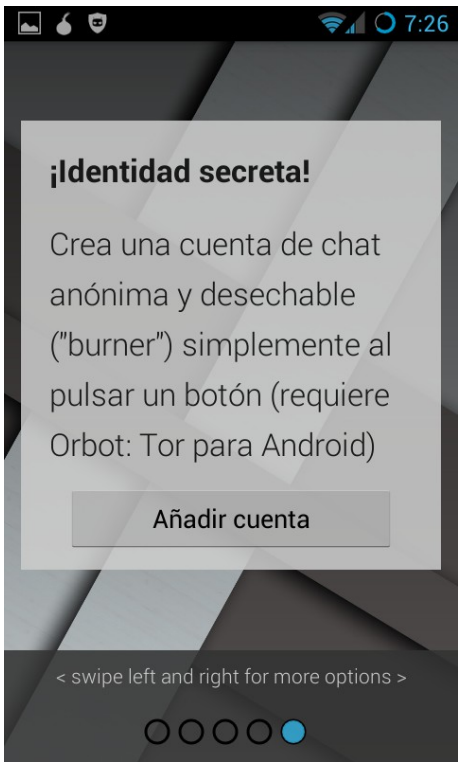


Si desplazas la pantalla hacia la derecha, te da la opción de poder añadir una cuenta de Algún proveedor ético de servicios que, ojo también te permitirá chatear con otra gente que use google/gmail

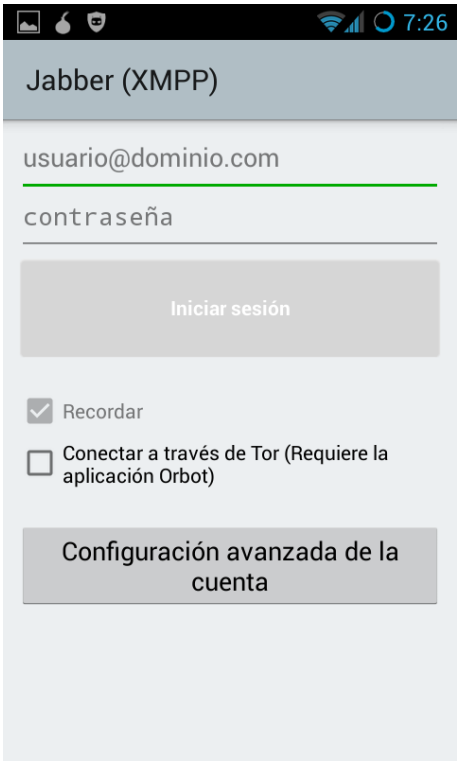


Si no tienes cuenta, puedes crear una en alguno de los proveedores éticos de servicios que luego listaré
Esta es la opción que yo te recomiendo

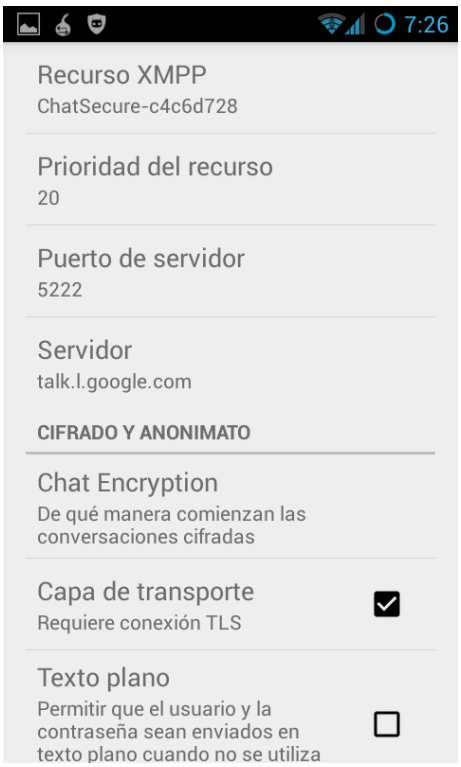
Si estás en alguna sala / pabellón / plaza con wifi
Y deseas hablar SIN conectarte a internet, nada como esta opción. No requiere tampoco de cuenta en ninguna parte



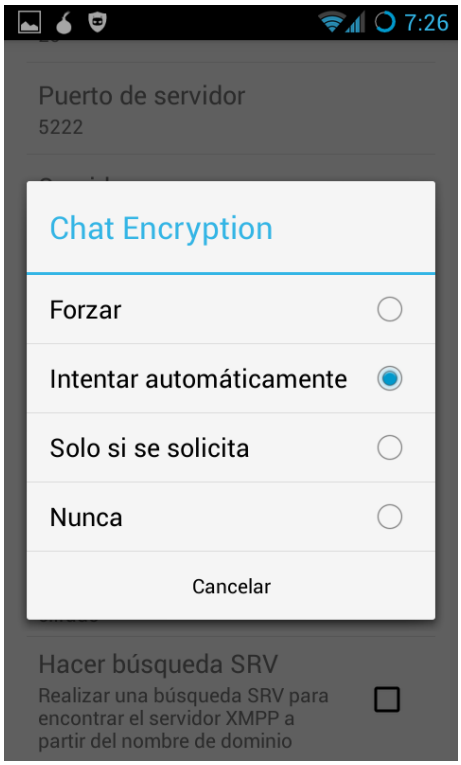
Cuentas deshechables: Al igual que las cuentas de email puedes recurrir a este tipo de tretas para chatear con total seguridad para tu privacidad y anonimato por internet
El programa se hace cargo de todo



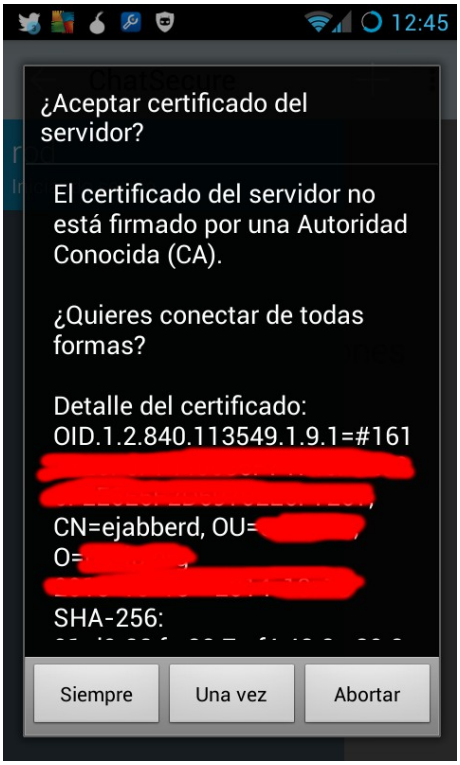
Vamos a la opción más esencial. Suponiendo que ya tienes una cuenta donde sea. Como verás hay varias opciones interesantes, como conectar a través de Tor. Mete los datos pero, en vez de darle a Iniciar sesión, selecciona configuración avanzada



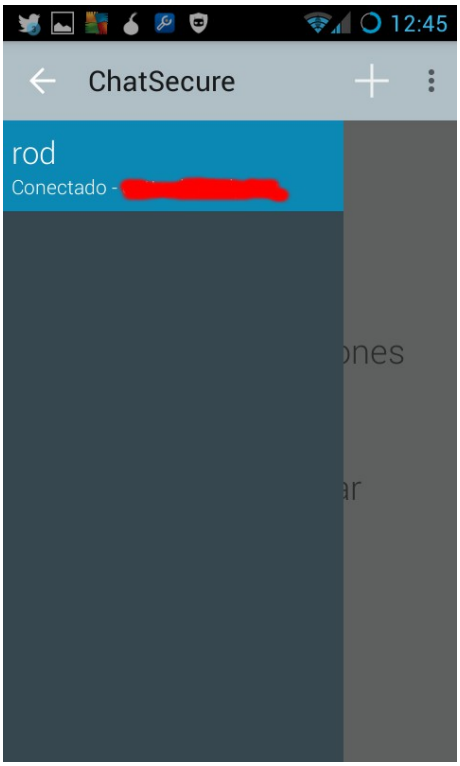
En esta pantalla te sale la configuración avanzada como por ejemplo la dirección del servidor o la forma en que se autentifica. Lo que nos interesa de este menú es la opción “chat encryption”



Al seleccionar Chat encryption se nos abrirá Esta pantalla con cuatro opciones, esto sirve para indicar como deseamos que se ejecute el cifrado OTR en nuestras conversaciones Mi consejo es que selecciones el automático Una vez hecho esto vuelve a la penultima pantalla que hemos visto. La de la cuenta e inicia la sesión

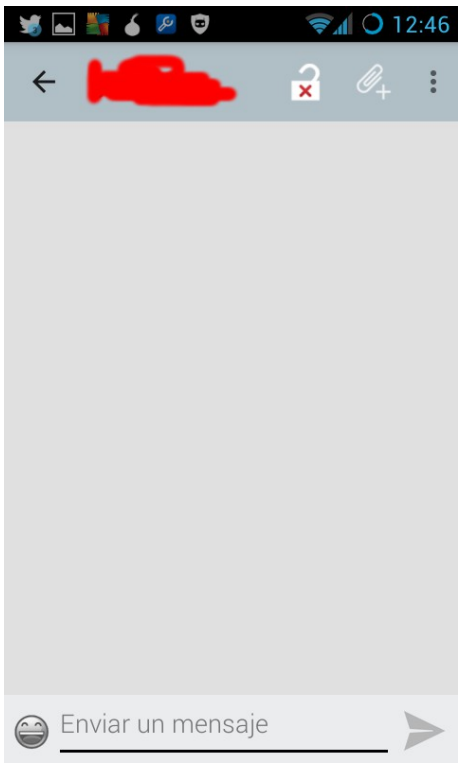


Al iniciar la conexión por primera vez, el servidor nos pregunta si deseamos aceptar su certificado, el que hará posible que nuestra conexión al servidor esté asegurada

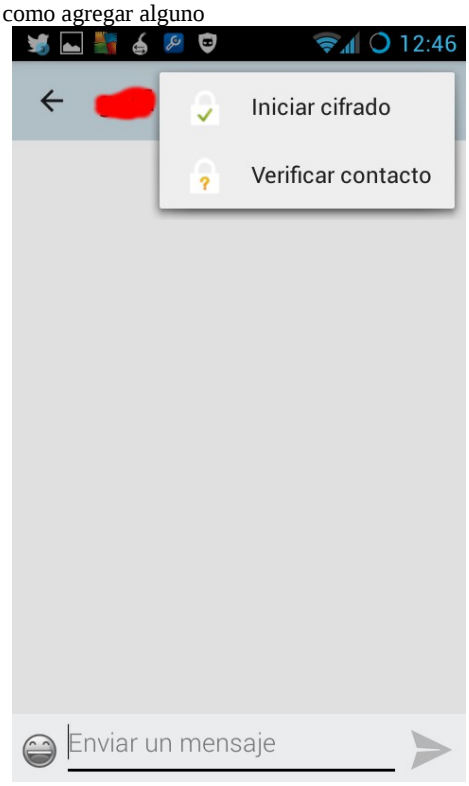


Una vez ya conectados, el programa mostrará el aviso Ya solo queda buscar un contacto

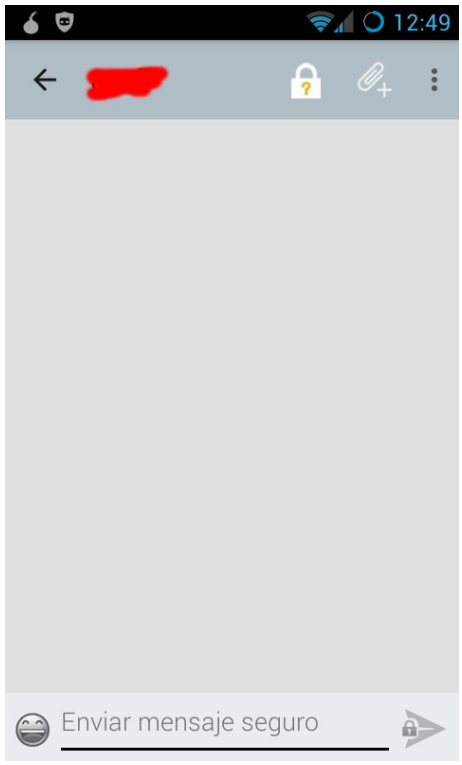
Esta es la pantalla principal de Chatsecure. Para ver o ñadir algún contacto, solo presiona en la “+” y podrás ver que contactos tienes agregados a tu agenda, o como agregar alguno



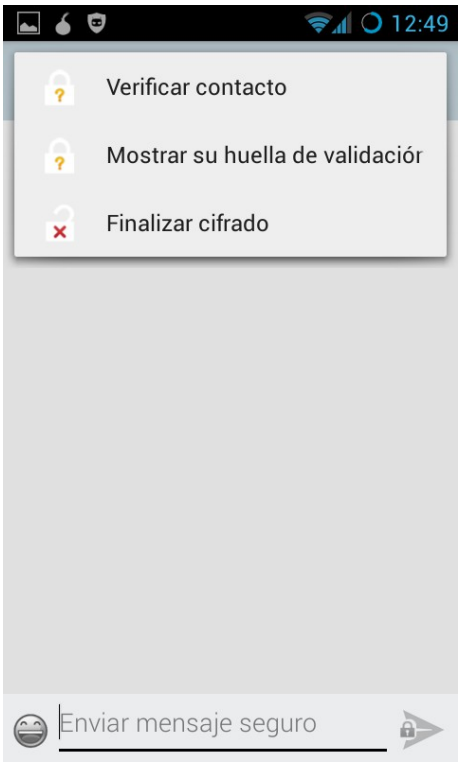
Una vez que hemos seleccionado un contacto esta será la ventana de conversación



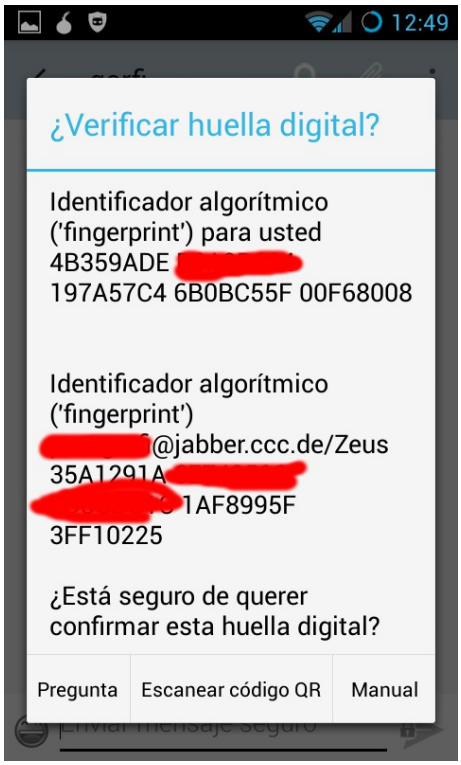
Si presionamos el candado de la parte superior, se nos abrirán las opciones para utilizar el cifrado OTR.
Es lo primero que debes hacer



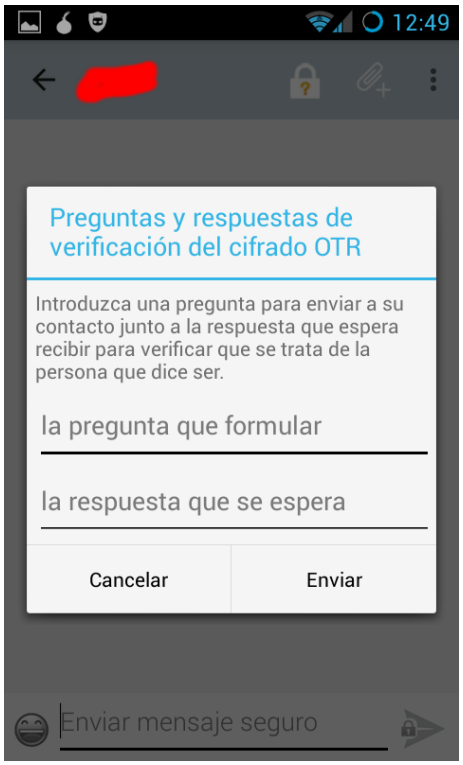
Una vez que nuestros clientes de XMPP se han puesto De acuerdo en la sincronización del cifrado, el icono del candado pasara a cerrarse pero con interrogante Eso indica que la conversación es segura pero que aun tenemos que verificar que la persona al otro lado es quien dice ser



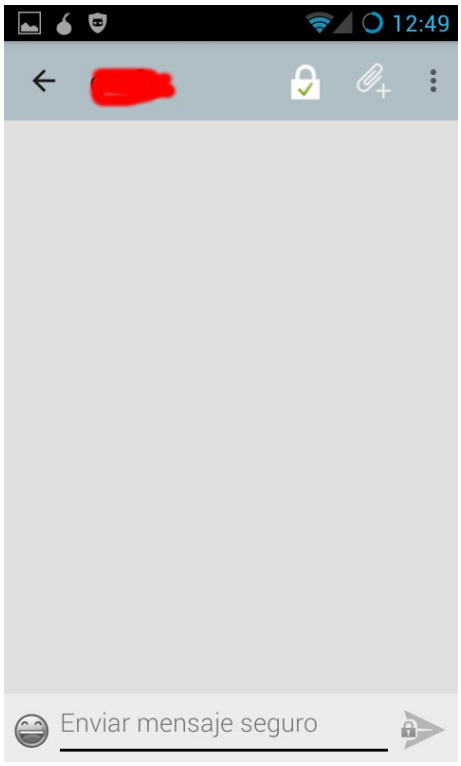
Al presionar de nuevo en el icono del candando se nos muestran estas tres opciones. Debemo verificar quien es la persona con la que vamos a chatear, asi que selecciona la primera



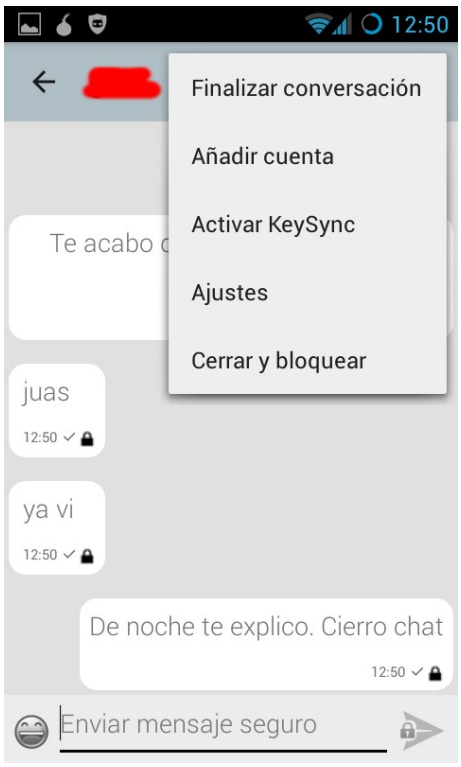
Al intentar verificar un contacto disponemos de tres opciones. De derecha a izquierda está “Manual” que verifica directamente, sin cuestionarnos nada más. “Escanear codigo QR” que sirve para aquella gente que previamente nos ha hecho llegar su huella digital en forma de código de barras, o finalmente hacerlo mediante una pregunta, especificando su respuesta. Tiene que ser una pregunta concisa, que solo la otra persona pueda conocer, y cuya respuesta sea una sola palabra, para minimizar posibles malinterpretaciones



Esta es la pantalla donde se especifica la pregunta y la respuesta que deseamos recibir. La gestión de este sistema la hace el programa automáticamente



Una vez y se ha verificado que la otra persona es quien dice, el candado se queda de color verde y con un “v” de aprobación. OJO: Aunque hay que prestar atención a que siempre esté verde solo lo hay que hacer una vez. La huella digital de esa persona quedará almacenada en el teléfono. No obstante asegurate bien, pues podrías ser víctima de una suplantación si el color del candado cambia al día siguiente.



Durante la conversación, junto al “v” que avisa que el mensaje ha llegado correctamente, también sale un pequeño icono de un candado que nos confirma que la conversación está siendo cifrada. Una vez hemos finalizado la conversación es IMPORTANTE usar el menú superior y darle a “Finalizar conversación”
De esa manera se detendrá el cifrado y borrará cualquier rastro de tu telefono acerca de esa conversación

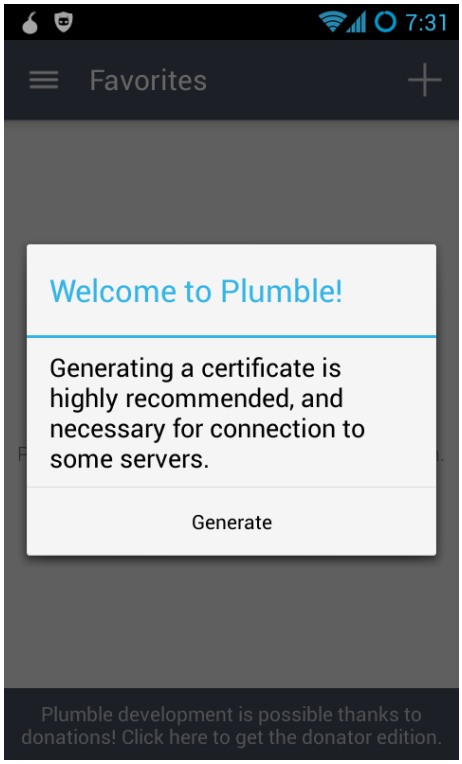
Así se ve un código QR de huella digital

VoIP: Mumble / Plumble

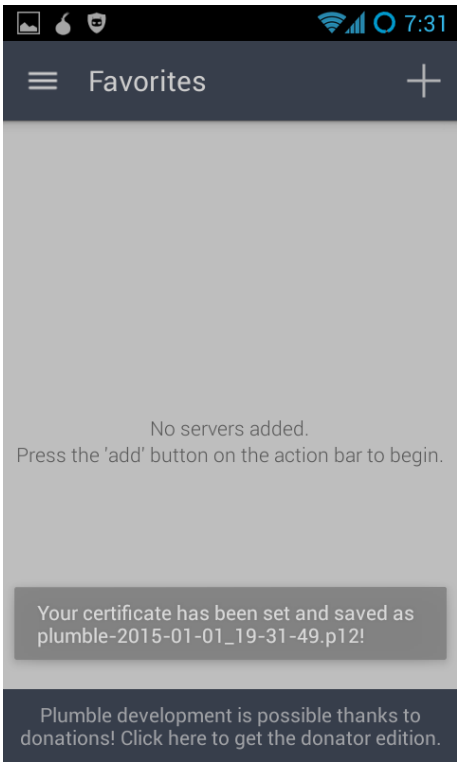
Como ya se ha comentado al principio de esta guía básica, utilizar los servicios GSM de tu teléfono movil para realizar conversaciones cuyo contenido no sería bueno que pudiera estar siendo monitorizado, no es buena idea porque, precisamente, a los cuerpos y fuerzas de seguridad del estado les resulta harto sencillo esta tarea gracias al sistema SITEL. Además, salvo que tengas alguna tarifa especial, su utilización ataca directamente al tamaño de tu factura. Por eso, afortunadamente para nosotros, disponemos de herramientas de VoIP (voz sobre internet) cuyo diseño nos permite añadirle capas y capas de protección en forma de cifrado para asegurar nuestra privacidad.

De entre las multiples herramientas que hay por internet, yo recomiendo mumble que, aunque originariamente fue diseñada para videojuegos, ha terminado siendo una plataforma estupenda para, incluso, el desarrollo de asambleas online. Mumble es un proyecto de código abierto que, además usa cifrado de alto nivel para evitar “oidos ajenos” con una calidad en su sonido que no tiene nada que envidiar a otras herramientas nada seguras como puede ser Skype o Hangouts, cuyo uso desaconsejo encarecidamente. Por suerte para todos, cualquiera puede crear un servidor mumble desde un ordenador de sobremesa o, si no dispones de ninguno, conectarte a los multiples servidores públicos que ofrecen servicios y crear un canal para mantener una conversación más íntima. Veamos como se usa:

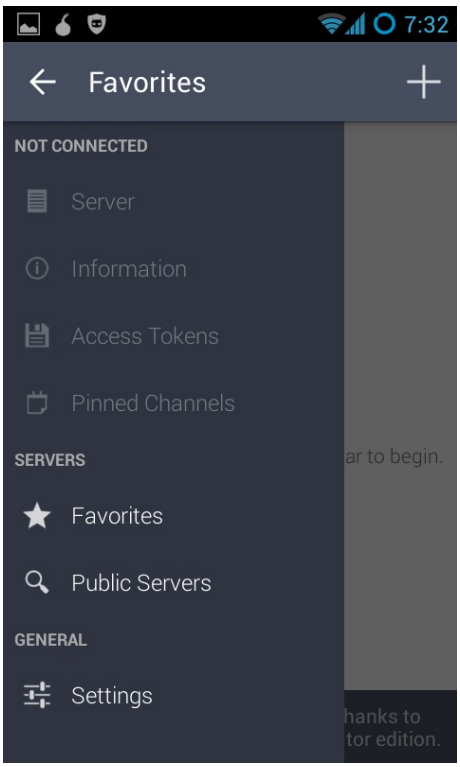
Esta es la aplicación que vamos a usar, disponible, como todas las de esta guía, en el google play



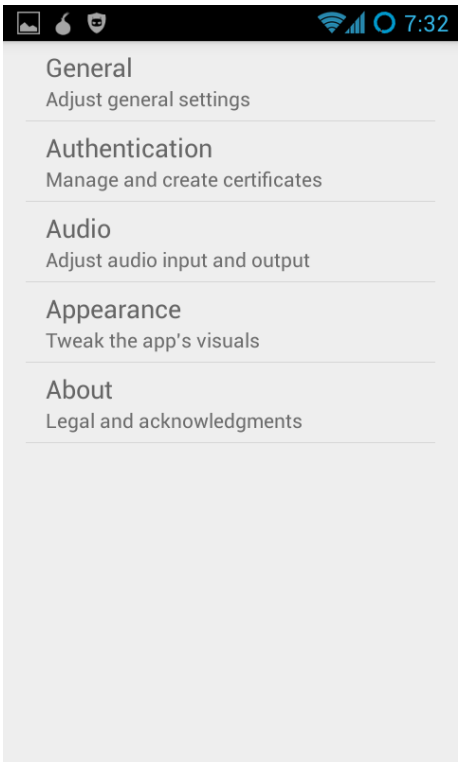
Al abrir la aplicación por primera vez nos dirá que es áltamente recomendable generar un certificado. Lo hace automáticamente. No requiere de ninguna acción salvo tocar el botón “Generate”



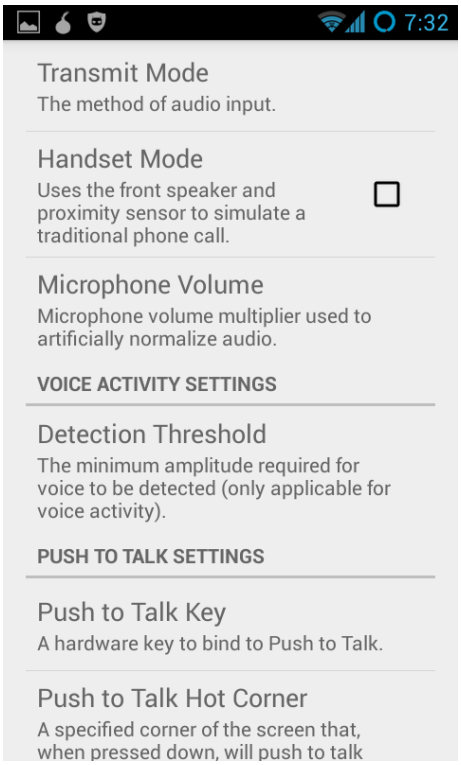
Cuando lo genere nos mostrará un aviso y pasará a esta pantalla, la principal de Plumble



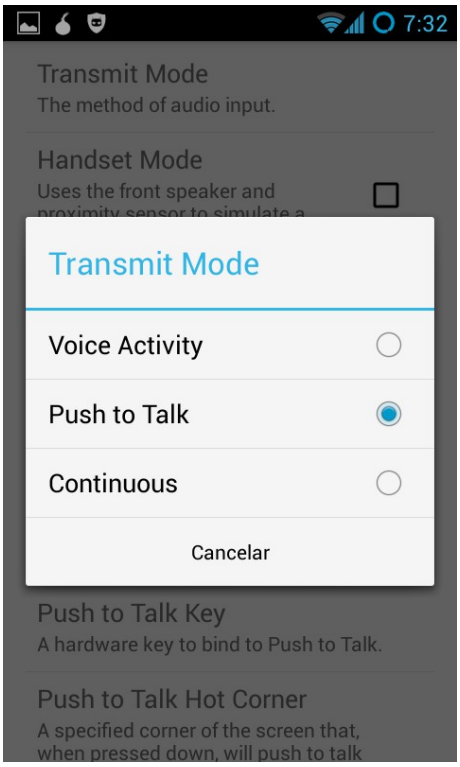
Tocando los guiones de la parte superior desplegamos el menú de la aplicación. Debemos tocar en “Settings”



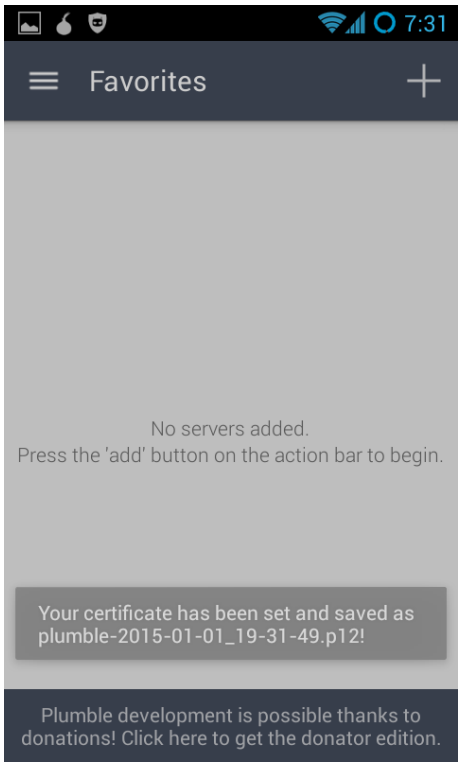
En la ventana de “Settings” nos ofrecen varias opciones la que nos interesa está dentro del menú “Audio”



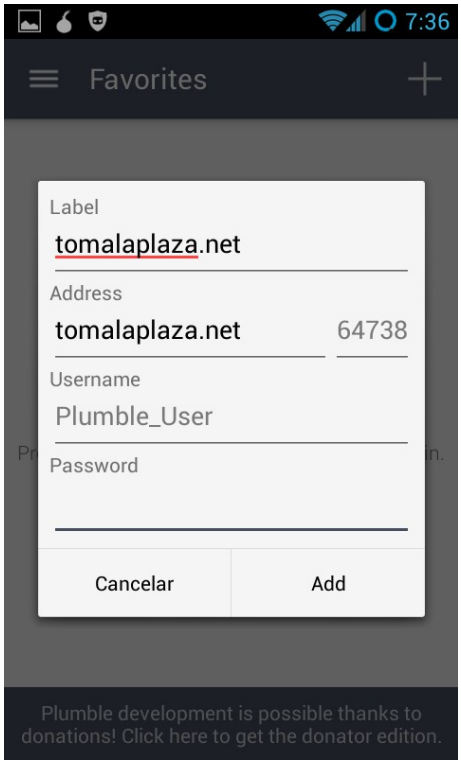
En este menú seleccionamos como deseamos operar a la hora de hablar. Por defecto utiliza el altavoz del teléfono, no obstante puedes hacer que funcione como un movil activando el “handset mode”, aunque para mi es mejor usar el accesorio de cascos + microfono que los teléfonos incluyen. Selecciona “Transmit mode”



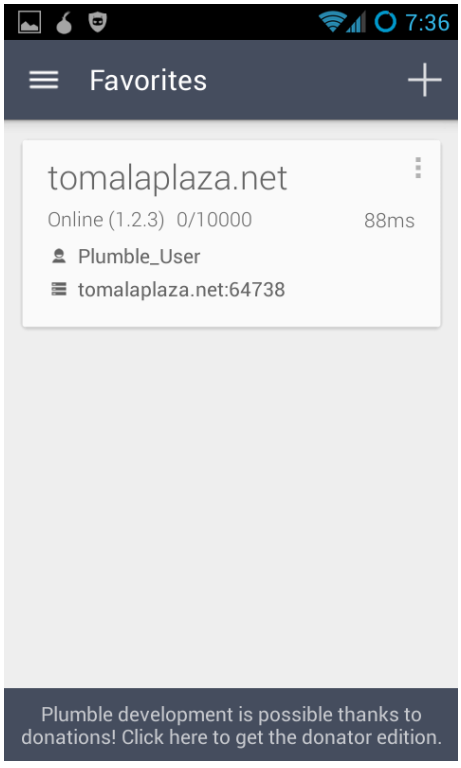
De entre las opciones mostradas, la mejor, la que más ancho de banda te va a hacer ahorrar es la “PTT” o Push To Talk, que, básicamente funciona como un walky talky. Salvo que presiones el accionamiento nadie podrá oir lo que dices



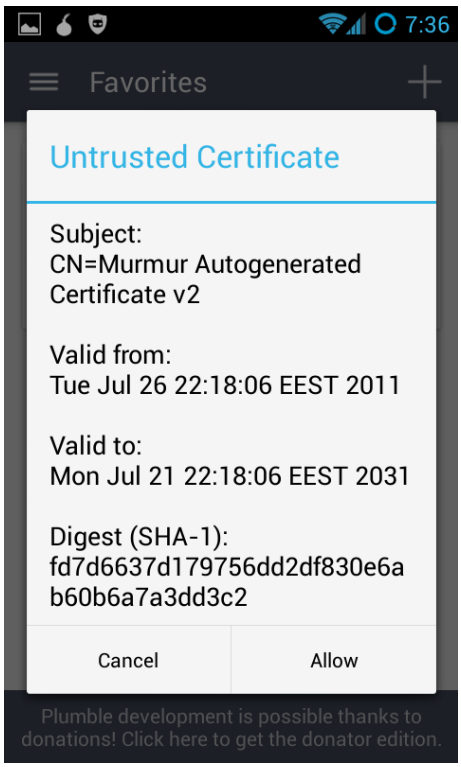
Una vez hecho esto, vuelve a la pantalla principal de la app y selecciona la “+” para añadir un servidor, o bien abre el menú de guiones y selecciona “Public servers” para ver un listado de servidores de todo el mundo



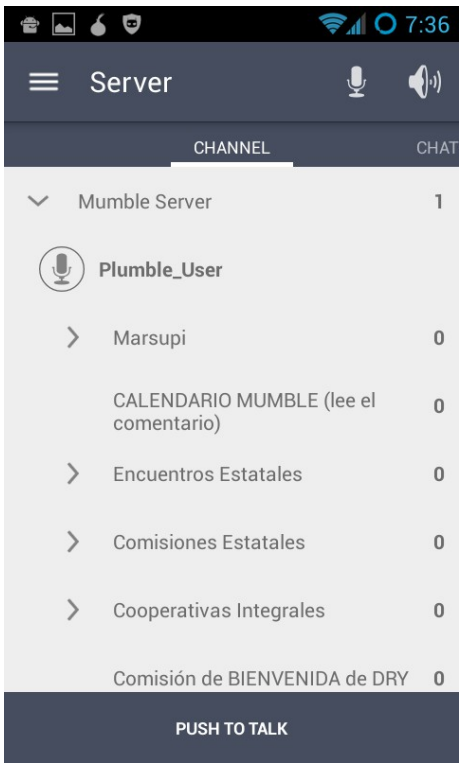
La pantalla para añadir un servidor solo requiere de estos datos: el nombre “label”, la direccion o “address” el puerto, un username que escojas y password si la sabes. Este servidor de ejemplo de “Tomalaplaza” es público y de acceso libre



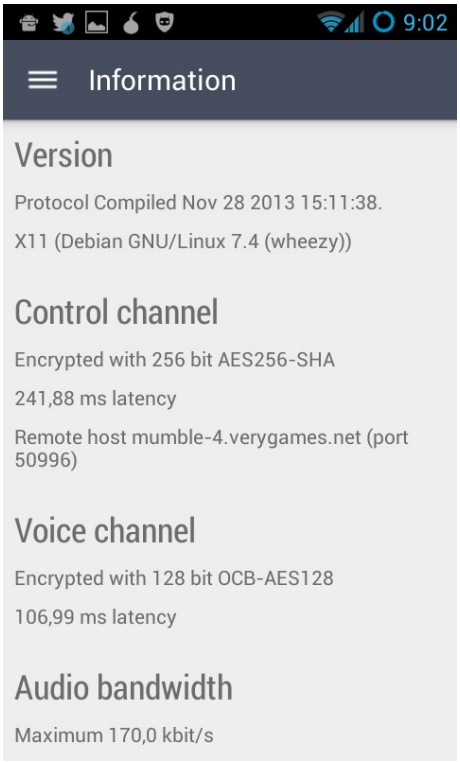
Una vez que lo hemos añadido correctamente nos lo mostrará de esta manera. Solo hay que hacer click en él para acceder



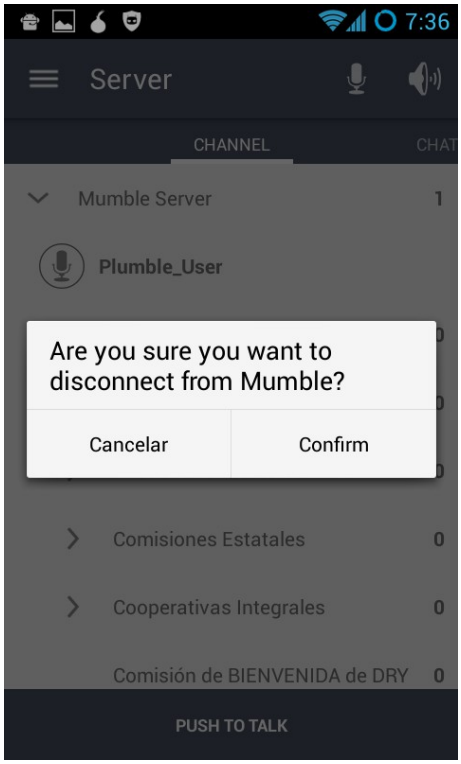
Durante la primera conexión nos preguntará si deseamos aceptar el certificado del servidor, que nos permitirá tener una conexión cifrada



Una vez dentro podemos hablar en el canal principal o entrar dentro de algunos de los canales creados dentro en cualquier caso, SIEMPRE que quieras hablar, debes mantener presionado la barra inferior “Push To Talk”



Si desplegamos el menú de los guiones, y seleccionamos la opción “Information” verás los cifrados que utilizas conectarse al servidor y para las conversaciones



Cuando termines de hablar tan solo tienes que darle a la tecla de atrás.

Email cifrado: K9Mail con APG (OpenPGP)

De antemano, y antes de comenzar con este capítulo, que sin duda será el mas árduo y complejo de explicar, nos gustaría afirmar que el email es, hoy por hoy, una de las formas más inseguras de comunicarse que existen. Y es que depositar temporalmente nuestra intimidad en una bandeja de entrada alojada en algún remoto servidor nos expone a que, durante el tiempo que transcurre entre que se recibe un email, y se borra del servidor (si es que, realmente se borra, tal y como NO sucede en Gmail, por ejemplo) cualquier persona con permisos (un administrador, un agente de la ley con orden judicial) podría curiosear en el contenido de los mensajes allí almacenados. Aunque estémos utilizando proveedores éticos de servicios -de los que hablaremos más adelante- siempre existe la posibilidad de que alguien vulnere el servidor y lea el contenido. Como mandar emails es, también, una de las formas más sencillas de comunicarse en el mundo moderno, vamos a proceder a añadirle una capa de seguridad más para que, mientras están almacenados en nuestras bandejas de entrada a la espera de que nos los descarguemos, nadie pueda leerlos: Usando OpenPGP

OpenPGP es un estandar abierto de criptografía que usa cifrado asimetrico, o de llave pública -tranquilos, lo explicaremos más adelante- desarrollado a finales de los 90 y que aún a día de hoy ofrece mucha seguridad, pero tiene algunos inconvenientes o incomodidades que, a continuación empezaremos a narrar.

Que un cifrado sea asimetrico indica que, cuando generamos una contraseña para nuestro email se generan dos archivos, uno de llave secreto y otro público -también se le llama claves, es lo mismo-:

El archivo de llave secreto deberá permanecer en nuestro poder, pues es el que nos permitirá descifrar todo lo que nos envíen encriptado. Este archivo nunca debe dejar de estar bajo nuestro control. En el momento en que perdamos el control de ese archivo, bien porque nos requisen el teléfono, bien por las razones que sea, deberémos considerarlo como comprometido, y notificar inmediatamente a nuestros contactos que dejen de usarlo. Tendremos que generar uno nuevo y, por desgracia, todo lo que no hayamos podido descifrar hasta entonces, lo perderemos pero, mejor perder un par de emails que la libertad ¿no?

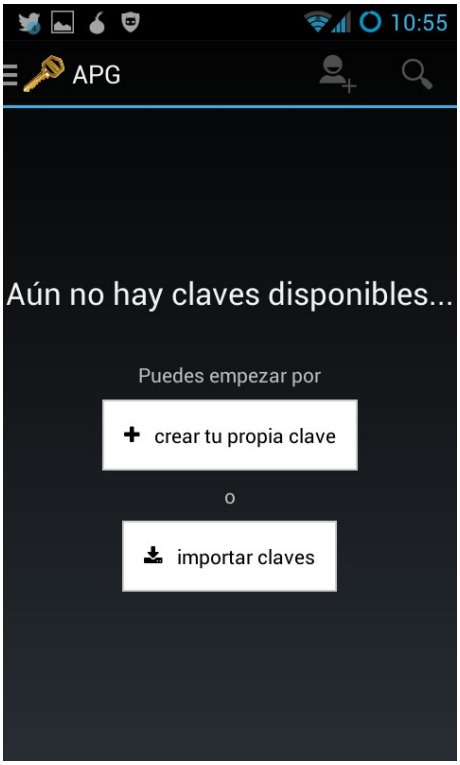
El archivo de llave pública por contra, podemos distribuirlo sin miedo alguno, de hecho es obligatorio hacerselo llegar a todas aquellas personas con las que deseemos mantener correspondencia, pues es el que hará posible que recibas información encriptada, de manera que, cuando dos personas quieren comunicarse entre sí por email, cada uno deberá tener su propia clave privada y, además, la clave publica del otro.

Este sistema, además de proteger el contenido de nuestros mensajes tiene otra ventaja, y es que nos permite verificar que la persona que nos ha enviado el correo es quien dice ser, pues cada vez que nos envía un correo cifrado con nuestra llave pública, además lo está firmando con su llave privada. Le está imponiendo su huella digital, lo que garantiza que la comunicación es segura en ambas direcciones. De otro modo, cualquier persona podría escribirte un email desde una cuenta sin que pudieras verificar si, en efecto, es quien dice ser.

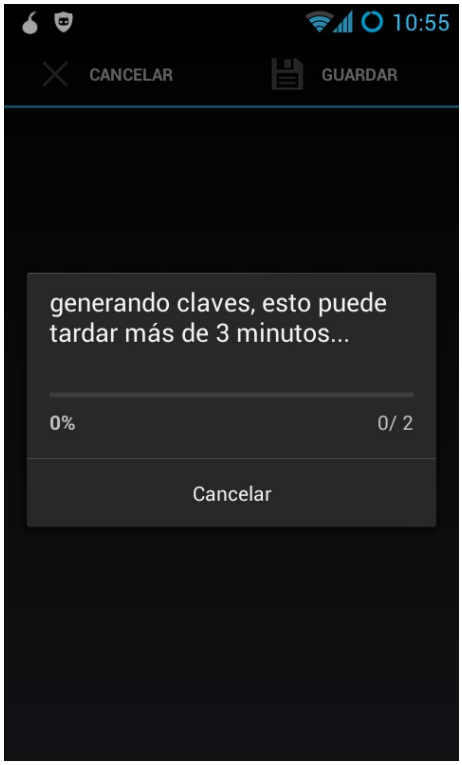
Por eso, insisto, es muy importante asegurar que las personas disponen de nuestra llave pública, bien enviándosela por email, bien haciendosela llegar por otros médotos más locales (¿bluetooth?) Que permitan verificar in situ que es quien dice ser. Así mismo, es importante que ellos nos hagan llegar sus llaves públicas.

Para Android gozamos de dos aplicaciones que, si bien son independientes, se integran perfectamente una con la otra: K9Mail como cliente de correo, y APG como app de gestión del estandar OpenPGP

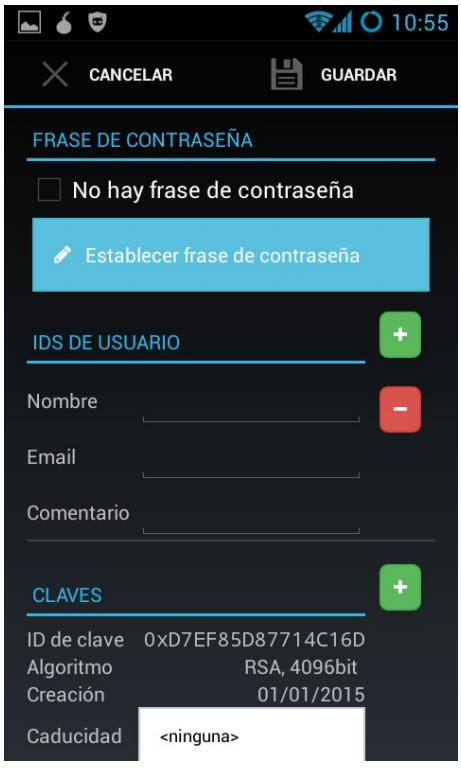
Así se ve la app de APG en el Google Play, descargala



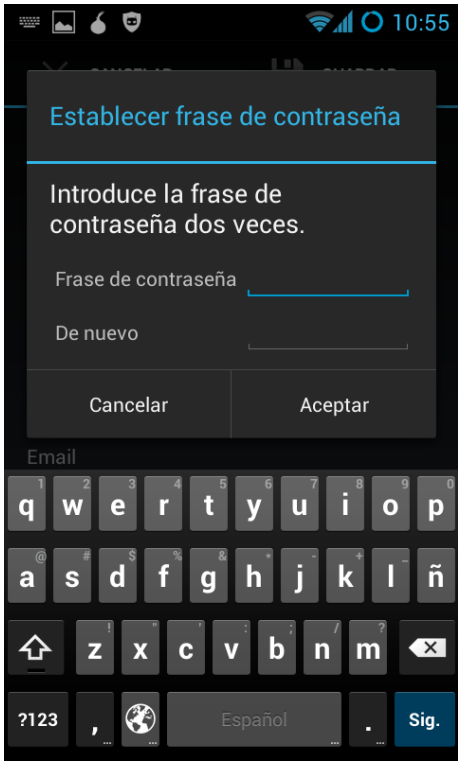
Al ejecutarla por primera vez nos dice que no hay claves / llaves disponibles. Si ya tienes claves porque usas OpenPGP en ordenador dale a importar, de lo contrario, deberás crear tu propia clave



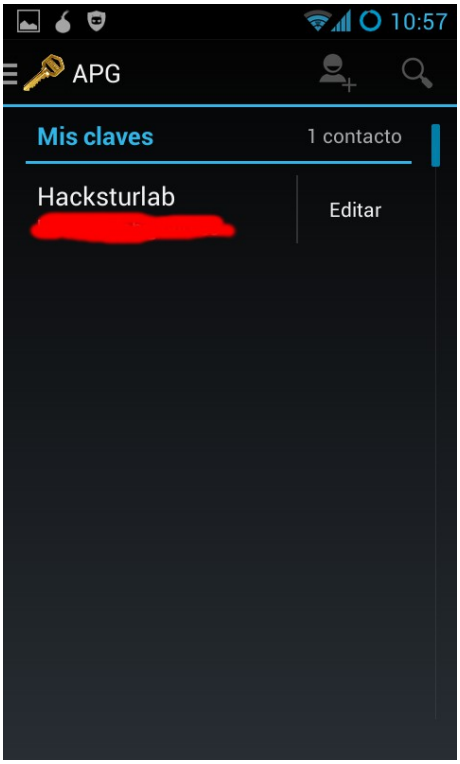
Al generar una clave el programa empieza a hacer cálculos matemáticos que pueden tardar un poco aunque no suele tardar más de 10 – 20 segs



Estamos listos para crear nuestras llaves privada y publica. Lo primero establece una contraseña lo más robusta posible. A continuación especifica tu nombre y email, lo demás puedes dejarlo por defecto, como esta. Es seguro. Y dale a guardar



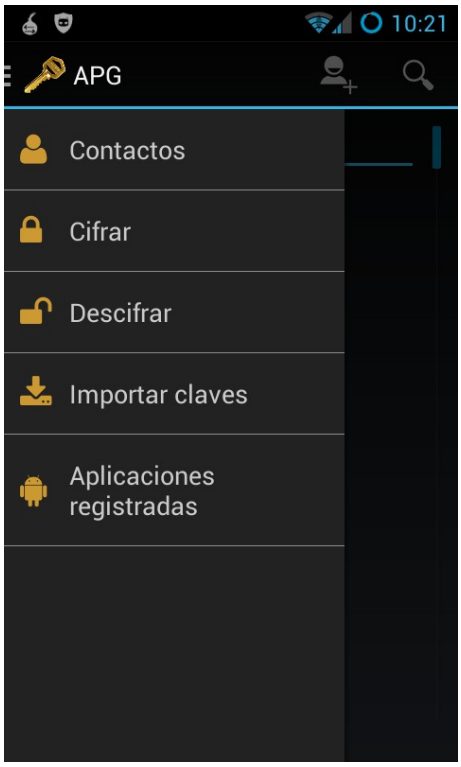
Para evitar posibles meteduras de pata, cuando generes la contraseña te pedirá que la escribas dos veces



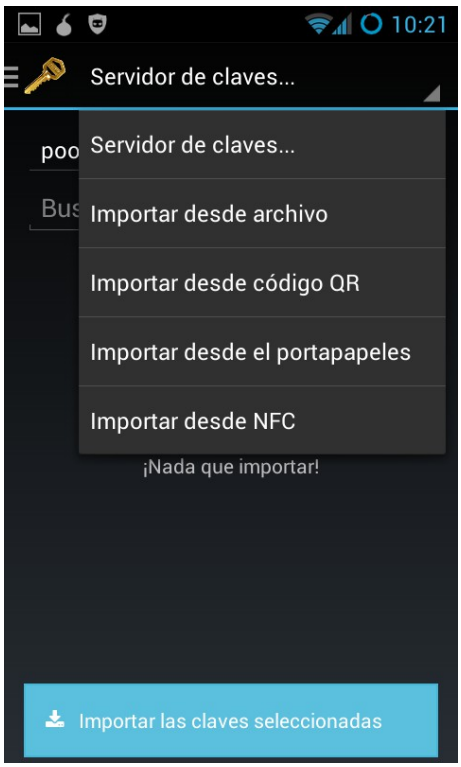
Ya está, hemos generado un llavero público y privado para nuestra dirección de correo

Una vez generada la llave tenemos que exporar la parte pública, que es la que mandaremos a nuestros contactos. Para ello presiona unos segundos la llave

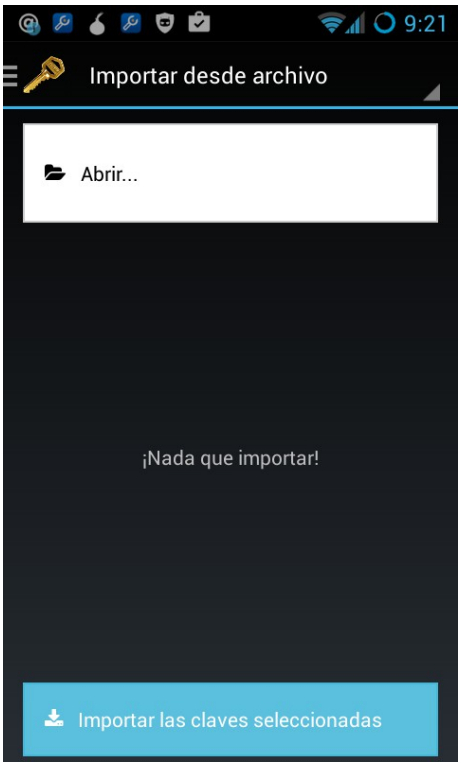
Nos preguntará donde deseamos guardarla, y con que nombre, además nos preguntará si deseamos tambien exportar las claves secretas. NO SELECCIONES ESA OPCIÓN SALVO QUE SEA PARA HACER, MÁS TARDE UNA COPIA DE SEGURIDAD. Nunca debe enviarse a otra persona nuestra llave secreta. Al darle a aceptar nos saldrá tras unos segundos, un aviso de que se ha realizado con éxito. ESE archivo es el que has de hacer llegar a tus contactos. ESA es tu llave pública



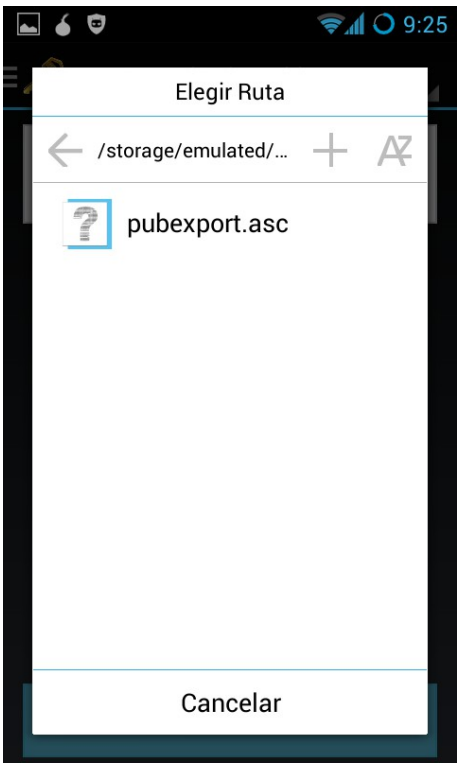
Ahora vamos a ver como se importan las claves públicas de nuestros contactos. Como ya he dicho, previamente nos habrán hecho llegar un archivo ".asc" que habrán obtenido de la misma forma que nosotros en el paso anterior
Así pues tocamos arriba a tu izquierda para desplegar el menú de la app, donde nos ofrecen varias opciones. Seleccionamos importar



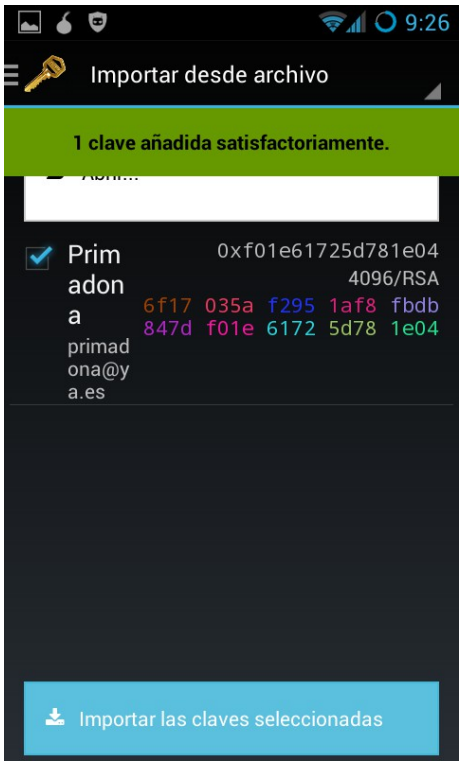
Nos ofrece varias opciones para importar claves, por defecto nos pregunta si queremos usar un servidor de claves, pero ya que no hemos visto esa parte, haremos el importado desde archivo desplegando el menú de arriba a tu derecha



Esta es la pantalla para seleccionar el archivo que nos ha hecho llegar nuestro contacto. Selecciona abrir para buscarlo dentro de la memoria de tu teléfono

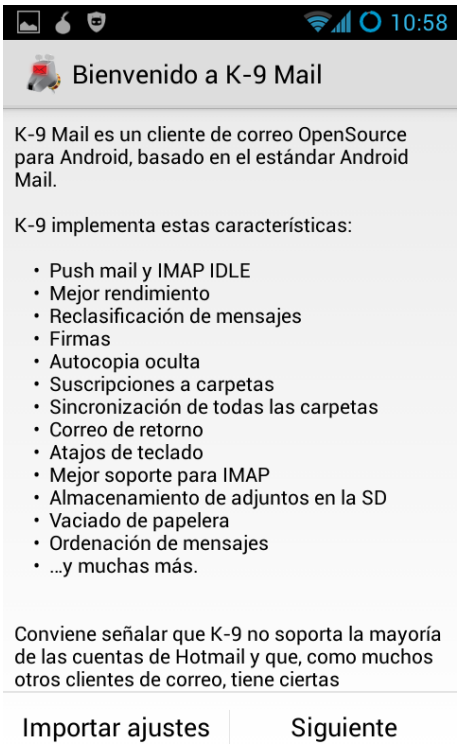


Seleccionando el archivo que nos importará la llave pública de nuestro contacto. Normalmente siempre se trata de un archivo que termina en .asc

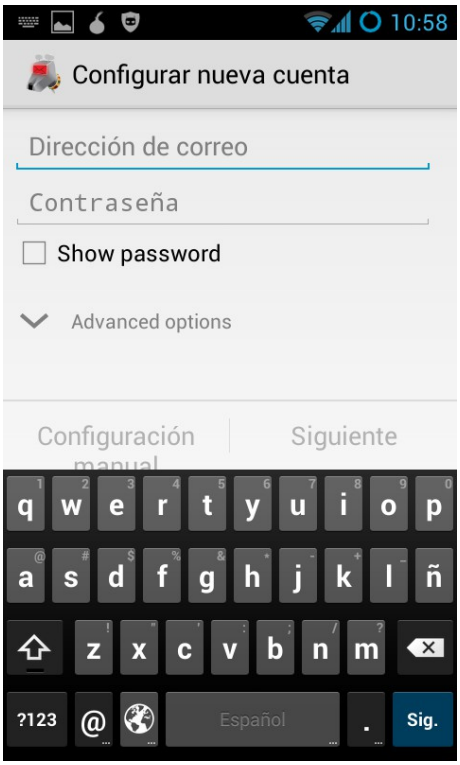


Una vez seleccionado el archivo debemos importar las llaves seleccionadas. Si ha tenido éxito nos saldrá un mensaje como este. Este procedimiento de importado hay que repetirlo con cada contacto que nos haga llegar su llave pública.

Esta es la app de cliente de correo que nos permitirá gestionar nuestro correos mediante OpenPGP, tal y como se ve a través de Google Play

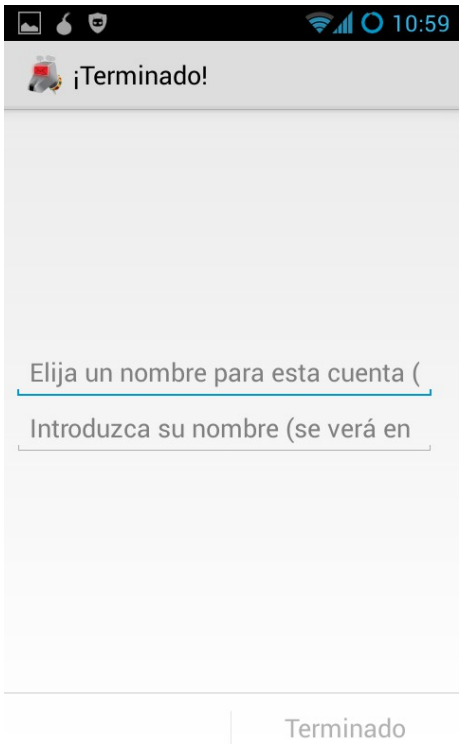


Al ejecutarla por primera vez nos pregunta si tenemos alguna cuenta ya creada proveniente de otro Android Como no va a ser el caso, presionamos en Siguiente

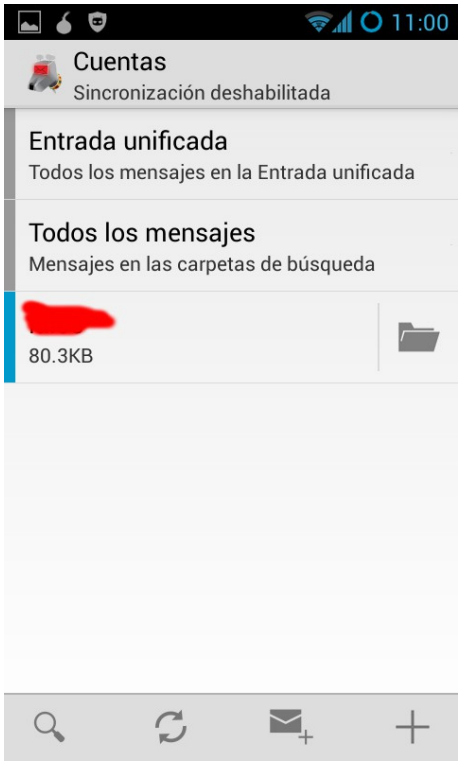


Normalmente basta con introducir el nombre de tu email y su contraseña para que el cliente se autoconfigure. Por desgracia no todos los proveedores de correo son así así que, en caso de que falle, deberás contactar con el administrador de dicho servidor para que te facilite los datos para el acceso pop3 o imap

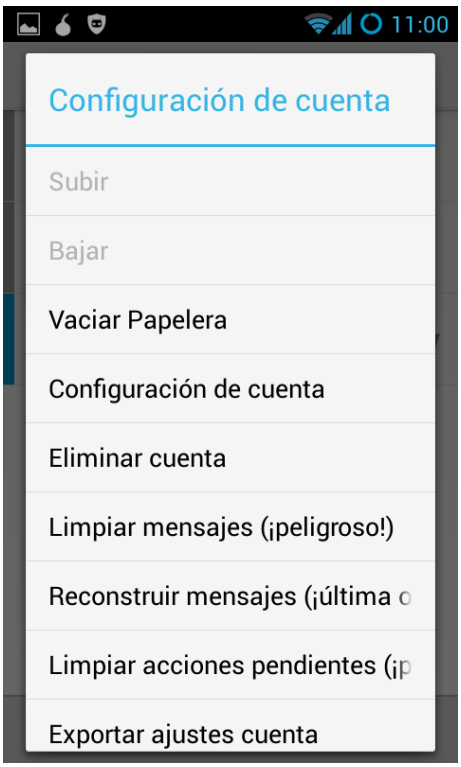
La mayoría de los servidores de correo corrientes se Autoconfiguran sin necesidad de intervención por nuestra parte. Puede que aquí te salgan avisos sobre certificados. Aceptalos siempre



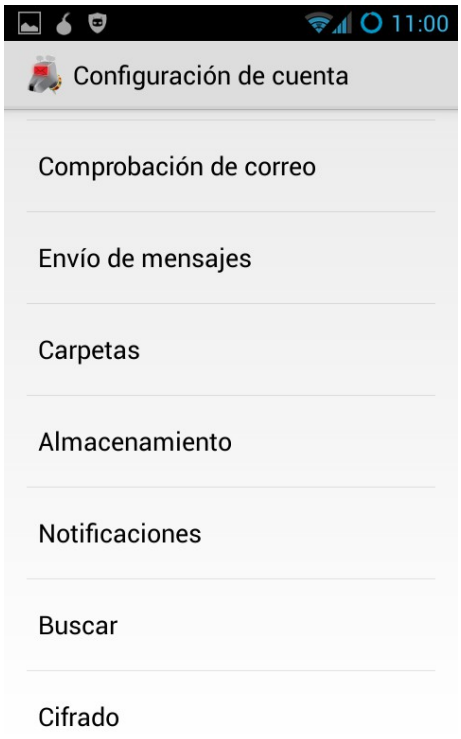
El paso final es escoger un nombre para esta cuenta para identificarla entre las diversas que deberíamos tener, así como el nombre que deseas salga como autor de los correos (tu pseudonimo, por ejemplo)



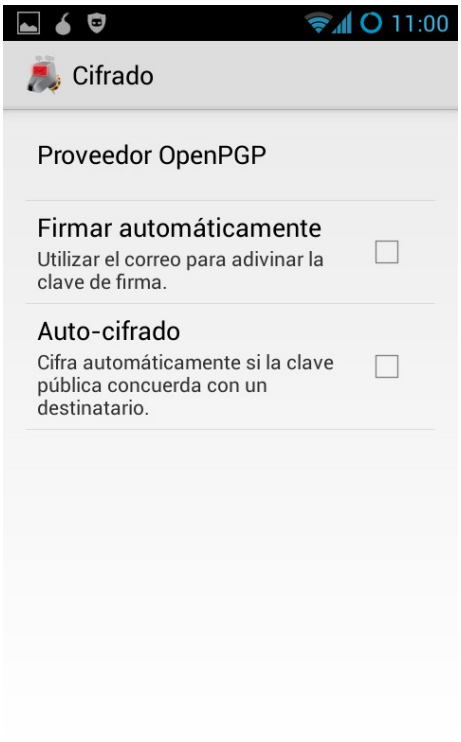
Así se verá la pantalla principal de la aplicación al terminar de configurar tus cuentas de correo y durante su uso habitual. Presiona continuado sobre la cuenta de correo para desplegar un menú

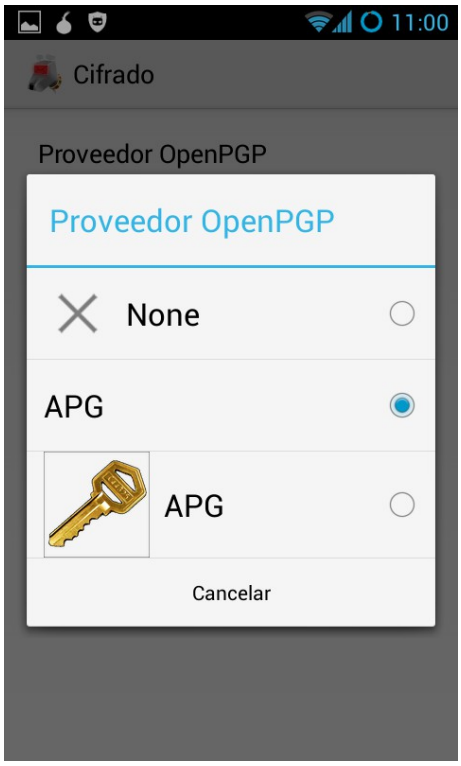


Este es el menú que saldrá al presionar de forma continuada sobre la cuenta de correo. Selecciona la opcion “configuración de cuenta”

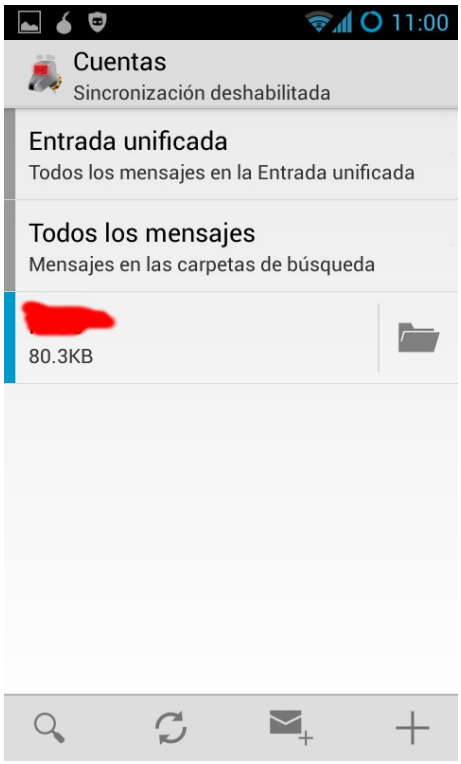


Aunque dentro de este menú se pueden seleccionar las opciones en las que deseamos recibir los emails, y más cosas, la opción que nos interesa está en cifrado. Las demás, que cada uno sea libre de ponerlas como quiera

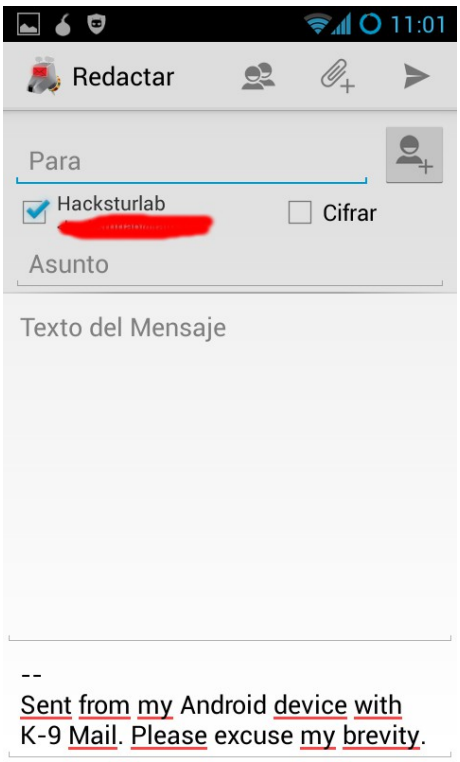




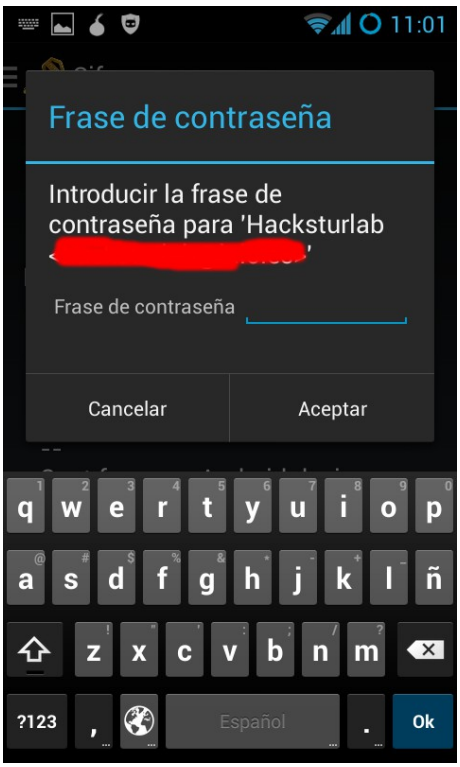
En proveedor de OpenPGP seleccionaremos “APG”, si es que no está ya seleccionado por defecto. Así mismo, activaremos las otras dos opciones: Firmar automáticamente, para que quien reciba el correo pueda verificar que somos realmente nosotros quienes le escribimos (requiere que esa persona tenga tu llave pública) y la otra opción, “AutoCifrado” para enviarle el correo que, además hemos firmado, de forma cifrada para que solo esa persona pueda leerlo (requiere que tu tengas la llave pública de esa persona)



Para enviar un correo, desde la pantalla principal de la app, seleccionamos el sobre que hay en la parte inferior de la misma y se nos abrirá esta ventana



Aquí redactaremos nuestro correo y especificaremos el destinatario del mismo. Una vez hemos terminado asegurate que la opcion firmar (la que pone tu nombre) está seleccionada. Y que también la opción cifrar está activada. Debería estarlo automáticamente si tenemos la llave pública de esa persona importada. Cuando terminemos, solo hay que presionar el triángulo de la esquina superior para enviar

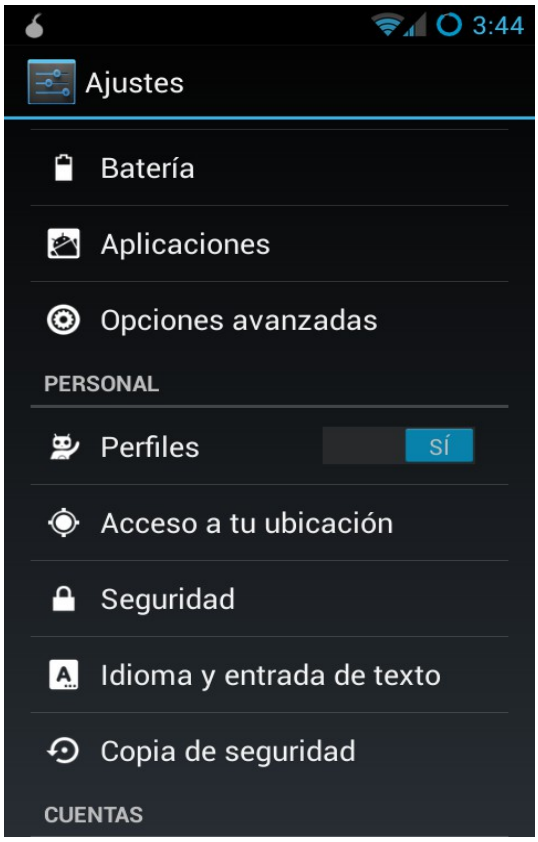


Antes de enviar nos pedirá que introduzcamos nuestra propia contraseña para proceder al firmado digital del correo y estar seguros de que somos, efectivamente, nosotros quienes enviamos También nos pedirá la contraseña cada vez que recibamos nosotros un email cifrado con nuestra llave, para leerlo.

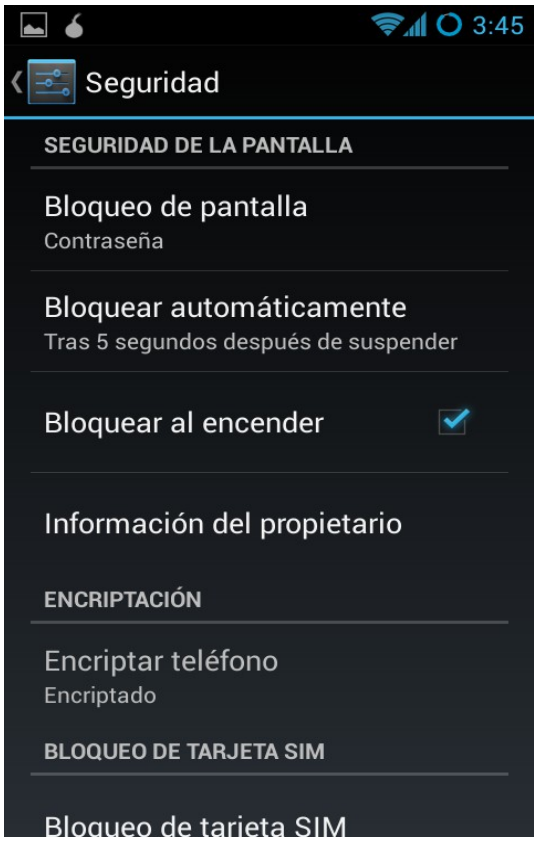
Cifrado del sistema Android

Desde su versión 3.0, el sistema operativo Android, que es en el que, mayormente, se encuentra basada esta guía básica, se incluye la opción de cifrar el contenido del sistema, o al menos la parte referente a los datos del usuario. Con lo que, en caso de pérdida, robo o, peor aún, confiscado por parte de las fuerzas de seguridad del estado, contamos con una última barrera excepcional en caso de que, por una razón u otra, nuestra seguridad se haya visto comprometida. Y digo que es una barrera excepcional pues porque no solo te servirá para que un ladrón no pueda acceder a tus fotos, tus emails o, incluso, la app desde la que controlas tus cuentas bancarias, sino que además, te "están buscando las cosquillas" judicialmente, este es el único escudo que nos quedará para que la negación plausible siga protegiendonos. Para que no sean capaces de verificar que, en efecto, según que archivos o actividades han quedado registradas desde nuestro teléfono. Así, con este cifrado, cada vez que enciendas el teléfono, o cada vez que quieras desbloquearlo tras un tiempo sin usarlo, tendrás que introducir la susodicha contraseña.

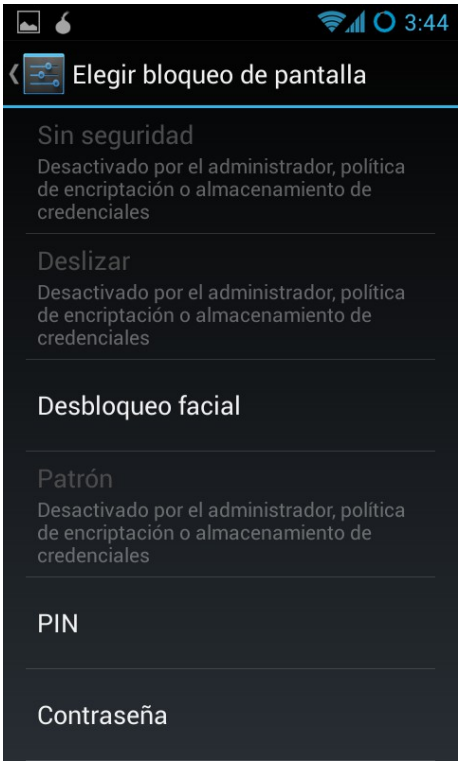
Antes de realizar el cifrado, asegúrate de dos cosas: Ten la batería del teléfono cargada al 100 % y con el cargador a mano, y además, piensa en la mejor contraseña que puedas crear nunca siguiendo el método expuesto en esta misma guía básica pues, aunque luego sea incómodo tener que introducir la contraseña -Sí, llega a hacerse incómodo- pero mejor repetir un proceso de introducir una contraseña cada vez que quieras conectarte a internet, que luego sufrir de angustia por miedo a ver tu vida expuesta. Vamos a ver como se hace:



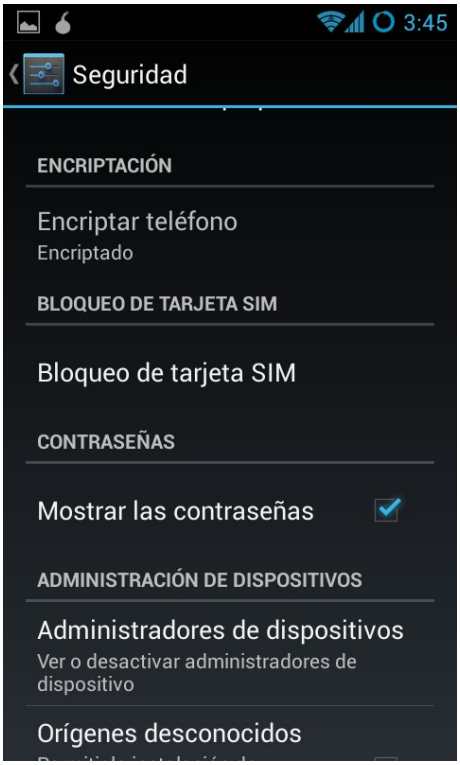
Entrando en el menú "Ajustes" debemos buscar la opción "Seguridad" y entrar en ella.



Lo primero que hay que hacer es definir el bloqueo De pantalla mediante contraseña (NO VALE OTRO)



Como ya he dicho, hay que seleccionar el bloqueo por contraseña, de otro modo el sistema no nos dejará hacer el cifrado del sistema. No sirve de nada intentar otros métodos porque, además, son más inseguros



Una vez hemos activado el bloqueo por contraseña se vuelve a atrás, al menú seguridad y buscamos la parte que nos permite encriptar el teléfono. Llegados a este punto, nos saldrá un asistente que nos pedirá introducir la contraseña que hemos especificado y, acto seguido se iniciará el procedimiento

Generación de contraseñas seguras

A lo largo de la guía, nos hemos visto en la necesidad de generar contraseñas. Existen muchos métodos de generación: Los hay de lo más variopinto: Desde programas para generarlas aleatoriamente, cuyos resultados son del estilo de “4f7fiuh/HUI7#*f4” que es totalmente imposible de memorizar, sistemas manuales que consisten en crear palabras con números (s0yElm3j0R) hasta la utilización de programas “baúl” o carteras, para guardarlas protegidas en un único archivo, protegido por una única contraseña (la única que hay que memorizar) .

A continuación te explico uno que considero efectivo y que se basa en la combinación de frases que solo tengan sentido para nosotros, muy potentes y dificiles de romper, y que a su vez sean relativamente sencillas de recordar

La contraseña ideal es aquella que es larga (como muy muy muy mínimo 9 caracteres), que incluye números, mayúsculas y minúsculas, e incluso algún carácter ASCI (!”·$%&/ł*:¡) . Cuanto más variedad de tipos de caracteres, y más larga sea, mejor . No obstante, con los tiempos que corren, más que una contraseña, o password, hoy en día, con la evolución de la velocidad de computación, se hace más seguro una frase de paso, o passphrase. Una frase que represente algo para nosotros, que sea larga, que incluya números, caracteres especiales y tanto mayúsculas como minúsculas
.
Ejemplos: Mi cuenta en twitter es @Manolito, una forma de generar una contraseña sencilla de recordar y, aun así larga sería algo por el estilo: “MiCuentaDe_Twitter_SeCreoEn2011”. Otra posibilidad es recurrir a algo mas familiar “MiPrimerMovilFu€UnNokia3310”. o“ElPisoEnElQueVivoEsUn3ero!”

La forma más habitual de atacar un cifrado, que aún no ha sido comprometido mediante criptoanálisis, es mediante fuerza bruta: De todas las combinaciones posibles solo una es la correcta, y solo mediante ensayo-error se llega a ella. La fórmula que determina cuantas combinaciones posibles hay para una contraseña, vista en notación científica, es la siguiente: X^Y donde “X” es la longitud de tu contraseña en, números, e “Y” es el número de caracteres posibles de que dispongas para generarlas. Por ejemplo, si para tu contraseña has usados números, letras mayúsculas y minúsculas, y caracteres especiales ASCII, “Y” equivaldrá a 256 .

Julian Assange, uno de los principales miembros de Wikileaks, publicó hace tiempo, a través de internet, varios archivos en los que afirmaba, se contenían secretos de estado muy oscuros sobre los estados unidos. Se refirió a él como su póliza de seguros y también reveló que solo 3 personas, inconexas entre sí, en todo el mundo, disponían de la contraseña y que, si le pasaba algo, estas personas liberarían la contraseña a través de Internet para que todo el mundo pudiera descifrar el archivo. Dichos archivos tuvieron millones de descargas, e incitaron todo tipo de conjeturas sobre que podrían ir incluido en ellos, pues eran archivos muy grandes. Si no conoces la historia de Julian Assange, podrás investigar porIinternet que, a día de hoy se encuentra refugiado en una embajada ecuatoriana en Londres, intentando evitar que lo extraditen a Suecia y, posteriormente, a Estados Unidos.

Con el tiempo, se reveló que uno de esos archivos, que contenía los, para entonces ya conocidos y publicados, cables diplomáticos estadounidenses, (Cablegate) tenía esta contraseña:
“AcolllectionofDiplomaticHistorySince_1966_ToThe_PresentDay#” Como puedes ver, se trata de una exquisita forma de aplicar el sistema del que estamos hablando aquí.

Hay que tener en cuenta que no se debe repetir NUNCA una contraseña para diferentes sitios o servicios de internet. Siempre es recomendable tener una contraseña diferente para cada cosa.
Usando este método de frases es algo realmente sencillo, con un poco de imaginación.

Ejemplo:

“MiUsuarioEnFacebookTiene666amigos#” o algo como “EscriboEnTwitter_20_MensajesAlDia” y por supuesto “EsteEm@ailEsSoloParaMis2Ojos”.

Hazlo sencillo, piénsalo MUY bien antes de buscar tu propio camino y asegúrate de que podrás recordarlo.En todo sistema criptográfico, la debilidad mas grande SIEMPRE viene por la contraseña

2º Principio de Kerckhoff: Todo criptosistema será seguro, en tanto en cuanto, aunque todo su funcionamiento, sea de dominio público, la contraseña siga siendo secreta

Proveedores de servicios éticos

Un proveedor de servicios ético se trata de una entidad, grupo, asociación, plataforma o, incluso, una sola persona, que pone a disposición del mundo algún servicio de internet de forma gratuita, abierta y con el compromiso de no retener dato ninguno, y menos aún, de comercializar de forma alguna, con tu actividad online dentro de "sus dominios". Como ya ha quedado de sobra probado, google, twitter, facebook, microsoft... no tienen mayor interés en que puedas comunicarte con los tuyos de forma rápida y gratuita. No se trata de empresas altruistas que, por el bienestar de la humanidad, se dedican a ofrecer esta clase de servicios. Su único fin es lucrarse y, además, está el asunto de que tienen que responder ante los gobiernos de los paises donde tributan. Tanto economicamente, como a la hora de colaborar en una investigación.

Por eso hoy en día se están abriendo más y más proveedores de servicios éticos, y por eso es importante utilizarlos y promover su uso, así como, si es necesario, colaborar en los crowdfundings que algunos suelen organizar para poder seguir operando en internet de forma independiente. Existen muchos proveedores, aquí solo citamos algunos. Sientete libre de buscar por internet más información

En el capítulo de redes sociales mencionamos, someramente,la existencia de redes sociales distribuidas / federadas, basadas en plataformas de software de código abierto que hacen posible que cualquiera pueda montarse su propio "twitter", con la ventaja añadida que muchas de esas redes sociales, además de ser independientes y no comerciales, permiten la interconexión con lugares como twitter o facebook de manera que, si así lo deseas, toda información que compartas será automáticamente reenviada a esas otras redes sociales comerciales. Así pues, a continuación enlazo algunos sitios web sobre redes sociales interesantes de conocer donde, además de explicarte como funcionan, te dan la posibilidad de conectarte a su red para que te registres y pruebes, si así lo deseas :

GnuSocial : http://gnu.io/social/

Diaspora : https://joindiaspora.com/

Pump.io : http://pump.io/

Con respecto a mensajería instantanea, hemos mencionado en el capítulo al efecto que, aunque es posible utilizar una cuenta de gmail, donde tendrás todos tus contactos de gtalk ya agregados, para conectarte con chatsecure, siempre habrá datos que queden registrados en los servidores de google que, ellos acabarán utilizando. Por eso, si deséas disponer de una cuenta en un servidor amigable, te enlazamos estos dos servidores que tienen una larga tradición de solidez, así como un compromiso de no comercialidad muy claro

Servidor de Jabber / XMPP del Chaos Computer Club : http://web.jabber.ccc.de/

Servidor de XMPP de DuckDuckGo : https://duck.co/blog/using-pidgin-with-xmpp-jabber

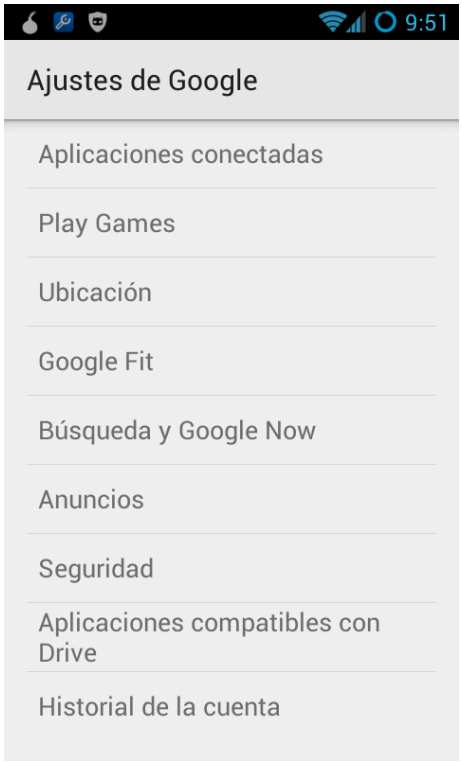
Respecto del email, hemos dicho que es inseguro per se, pero con el uso de OpenPGP se puede lograr una seguridad más que aceptable, y si además la combinas con algún proveedor de correo ético, mejor que mejor, por eso recomendamos el uso de alguno de estos:

OpenMailbox : https://www.openmailbox.org/

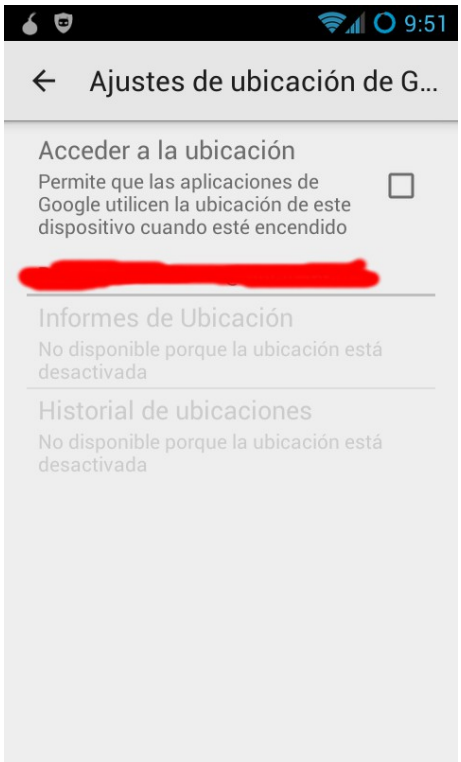
RiseUp : https://help.riseup.net/

Consideraciones sobre el uso de Android para usuarios un poco más avanzados

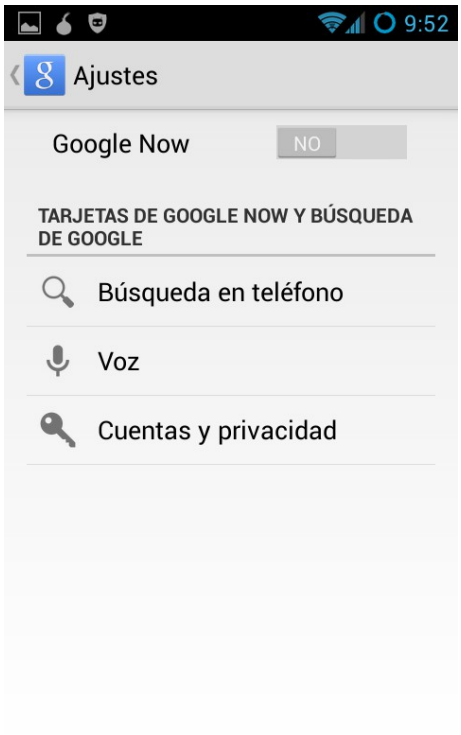
A lo largo de toda la guía, hemos utilizado siempre programas provenientes de Google Play, la plataforma de software de google, porque consideramos que, para un usuario novato, es la mejor vía de hacerse con aplicaciones que han pasado un filtro para verificar que, en efecto, no son maliciosas. Además, aunque todas las aplicaciones aquí mencionadas no requieren de disponer de un smartphone "rooteado" (es decir, con privilegios avanzados para modificar el sistema) para poder hacerlas funcionar en su forma más básica, muchas de ellas ofrecen características más avanzadas si así lo deseas. No obstante, y dado que todo el mundo, en mayor o menor medida conoce a "el amigo informático" que, en un momento dado, nos podría instalar una rom de Android modificada, o mejor aún, una version de cyanogenmod para nuestro téfono. Así pues, vamos a ver algunas de las características de los teléfonos android que conviene tener desactivadas para no ser víctimas del tan mencionado "bigdata" con fines comerciales



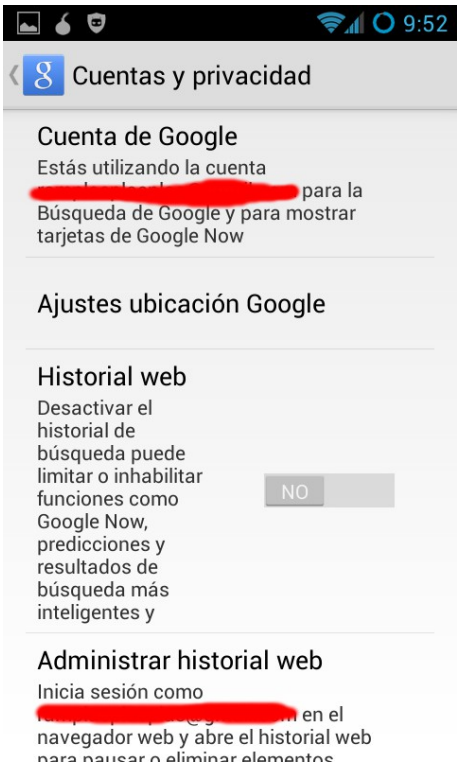
En el menú de aplicaciones de Android, existe una, "Ajustes de Google" donde se especifica como funciona nuestro teléfono de cara a los servidores de Google que hacen posible que funcione su plataforma Google Play



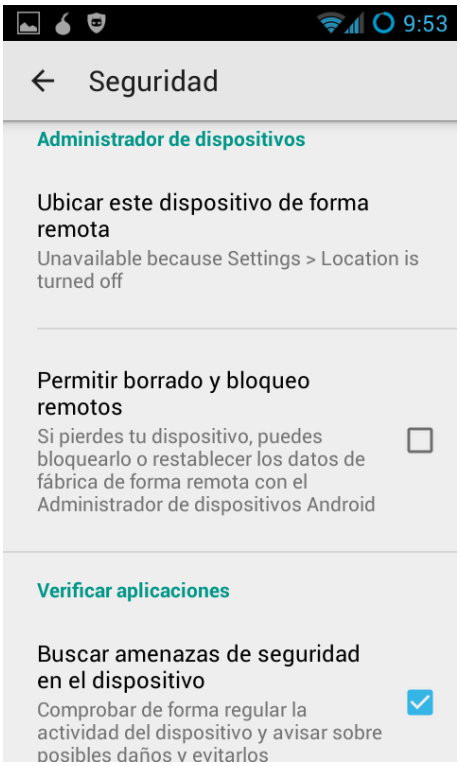
Seleccionado ubicación se nos abre esta pantalla donde debemos DEseleccionar que las apps de Google puedan acceder a nuestra localización



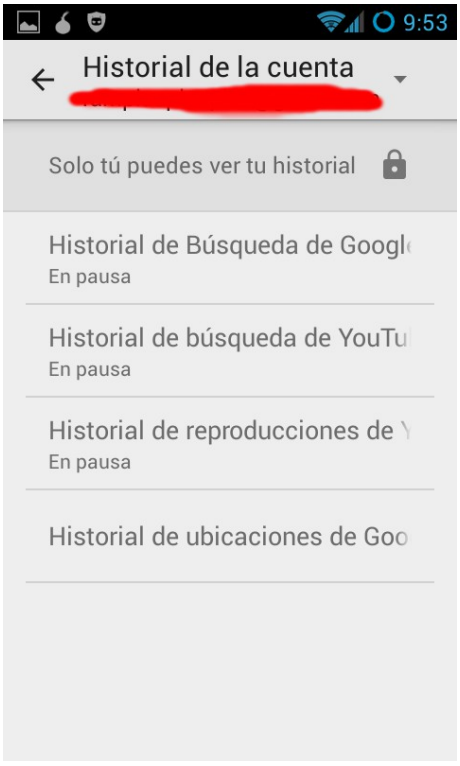
En el menú “búsqueda y google now” debemos quitar el servicio, para que quede tal que así



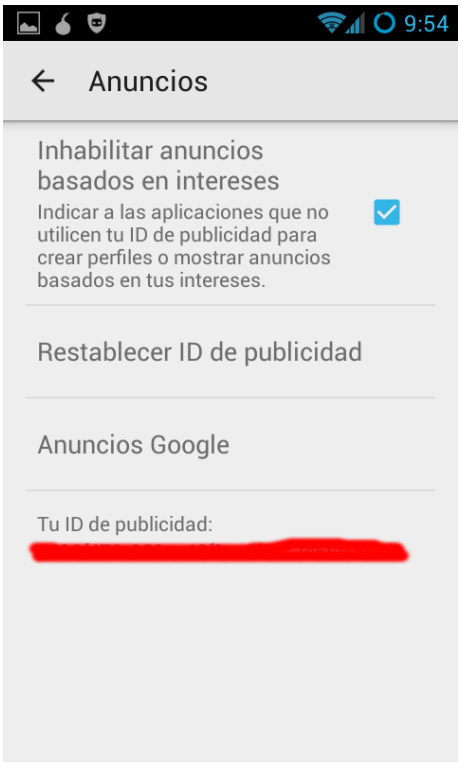
Ahí mismo menú, entra en “Cuentas y Privacidad” y verifica que TODO está desactivado en esa sección



Volviendo al menú principal de ajustes, entramos ahora en “Seguridad y desactivamos las dos primeras opciones



Volviendo de nuevo atrás, entramos en “historial de la cuenta” y ponemos en pausa todo, tal y como se ve en la imagen de justo arriba



El último menú que debemos comprobar es el referente a Anuncios, donde desactivaremos que se nos muestren anuncios basados en nuestros intereses (perfiles fantasma)

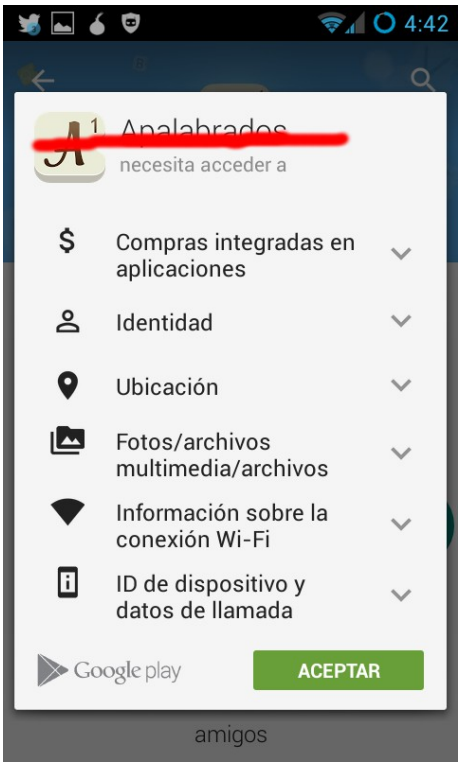
Permisos de aplicaciones

Cuando instalamos una aplicación cualquiera, antes de proceder a su descarga, Google Play nos muestra los permisos necesarios para que esa aplicación funcione en nuestro sistema. Muchas veces las necesidades de permisos son excesivas en comparación con lo que esa aplicación va a permitirnos hacer en nuestro sistema.

Esto es porque, si nos plantearamos leer la letra pequeña de las condiciones de uso de dicha aplicación, comprenderíamos que, no por negarle el acceso a esos datos la aplicación no va a funcionar, sino que en realidad lo estamos autorizando es a que la aplicación actue de enlace entre nosotros y el creador de la misma, para que este recolecte datos sobre nuestra identidad, sobre nuestras actividades y, por ejemplo -solo por mencionar muchas de tantas aplicaciones del “bigdata” comercial-, nos muestre publicidad personalizada con la que obtener un rédito económico.

Esto explica la existencia de muchas aplicaciones gratuitas en Google Play: Al final nadie trabaja gratuitamente. Así pues, antes de instalar ningún tipo de aplicación adicional a tu teléfono, revisa que permisos requiere dicha aplicación, y considera si realmente te compensa autorizarla a que acceda a tu identidad, a tu privacidad. En especial si hay otras alternativas más libres en cuanto a necesidades de permisos o, incluso, de pago. Despues de todo, si no eres el cliente, eres el producto

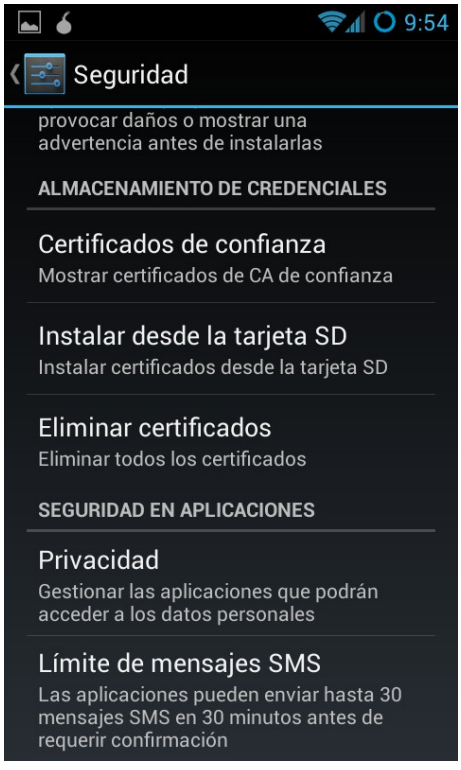
A continuación vamos a ver un ejemplo de una aplicación cualquiera, en este caso una de ocio, a la que hemos censurado el nombre para no perjudiciar a nadie y que, previamente a comenzar su descarga, nos muestra estos requerimientos. ¿por que un juego online desea acceder a nuestras fotos y videos, o a la identidad de nuestro teléfono?

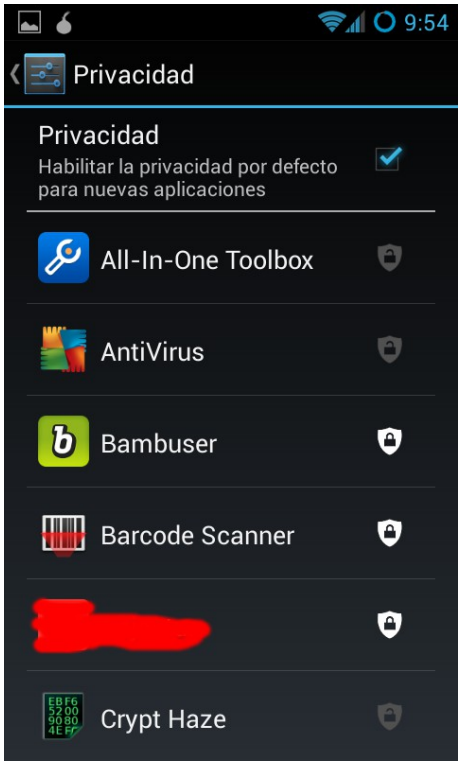


Ejemplo de requerimientos de una aplicación de ocio cualquiera

Cyanogenmod:

Esta versión de Android trae incorporada una polémica función que permite, de serie, bloquear el acceso a las aplicaciones que nosotros deseemos, a nuestros datos más personales, tales como la agenda de contactos, los SMS o los registros de llamada. Algo que es una defensa maravillosa en contra de la recolección de datos contra nuestra voluntad. Veamos como se activa

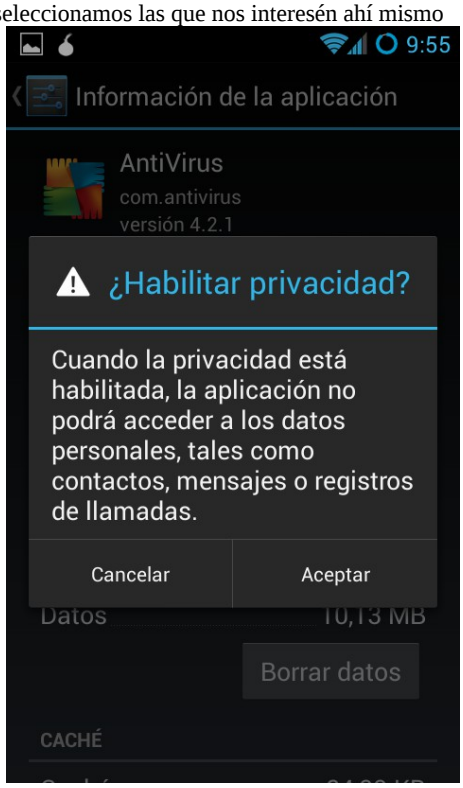




En el menú “Ajustes” buscamos seguridad y luego bajamos en busca de “Privacidad”

Desde el propio menú de aplicaciones, en ajustes podemos entrar dentro de una aplicación cualquiera si no deseamos que esta opción funcione por defecto, seleccionando la casilla de “habilitar privacidad”

Activamos la opción “por defecto para nuevas apps” y seleccionamos las que nos interesén ahí mismo



El sistema nos advierte de las consecuencias de usar la opción de privacidad. Aceptamos sin duda.