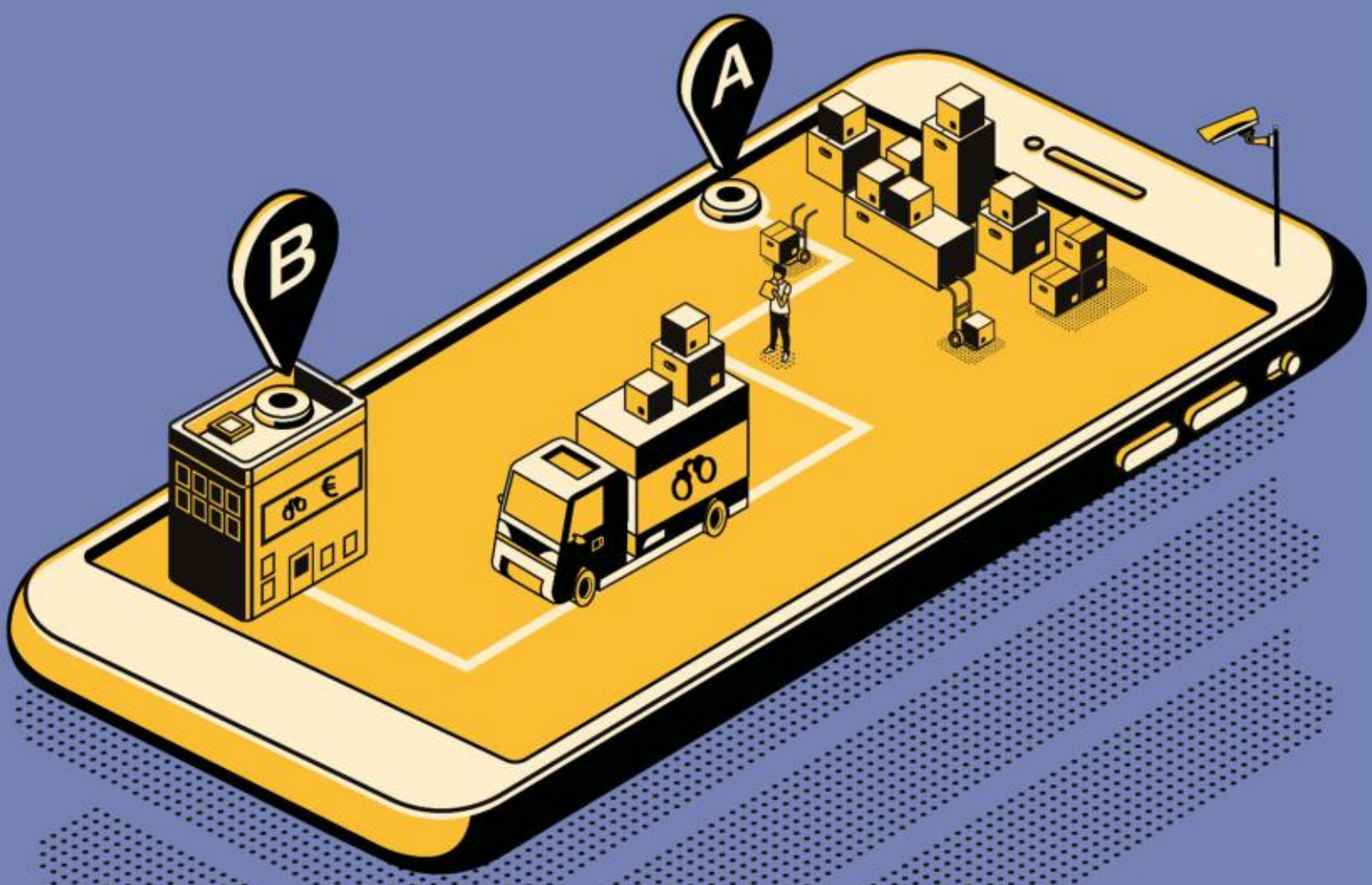
RESISTENCIA DIGITAL

Manual de seguridad operacional e instrumental para smartphones

Críptica

Prólogo de Enric Borràs



EDITORIAL DESCONTROL

Colabora con la CULTURA LIBRE

EDITORIAL & IMPREMTA SCCL

DESCONTROL

Desde el principio, **Editorial Descontrol** apuesta por las licencias de publicación libre, **Creative Commons,** por eso, podéis copiar, distribuir y descargar libremente nuestros libros. Algunos libros de nuestro catálogo se encuentran en libre descarga

Evidentemente, la cultura libre no quiere decir gratuita, el precio del libro incluye derechos de autor, de corrección, traducción editorial, imprenta...

Si estás a favor que la cultura siga siendo libre, p**uedes colaborar haciendo una aportación a nuestra editorial**, así ayudas a la cultura o, puedes hacerlo realizando un ingreso a la siguiente cuenta corriente:

ES52 3025 0011 7614 0012 4093
Concepto COLABORACIÓN CON DESCONTROL

Muchas gracias por el apoyo!

RESISTENCIA DIGITAL

Críptica

Título: *Resistencia Digital - Manual de seguridad operacional e instrumental para smartphones*

2a edición

Autoría: *Críptica*

Autoría prólogo: *Enric Borràs*

Depósito Legal B 10535-2019
ISBN 978-84-17190-68-2

PUBLICADO en Creative Commons CC-BY

EDICIÓN Y MAQUETACIÓN
Descontrol Editorial

CORRECCIÓN
Tym Hernández

IMPRESO EN LOS TALLERES DE DESCONTROL IMPREMTA
Impreso en Barcelona

-DESCONTROL EDITORIAL-

93 422 37 87 / 682 725 783
EDITORIAL@DESCONTROL.CAT
IMPREMTA@DESCONTROL.CAT
DISTRIBUCIO@DESCONTROL.CAT

WWW.DESCONTROL.CAT / @DESCONTROLED

C/CONSTITUCIÓ 19, RECINTE CAN BATLLÓ BLOC 11, NAU 83-90, 08014 BARCELONA
DE LUNES A JUEVES DE 10 A 14H Y DE 15H A 19H

RESISTENCIA DIGITAL

Manual de seguridad operacional e instrumental para smartphones

Críptica

Prólogo de Enric Borràs

EDITORIAL DESCONTROL

Índice

https://www.criptica.org
info@criptica.org | @CripticaOrg

Acerca de Críptica

Críptica es una asociación constituida a mediados del año 2015 con el objetivo de ofrecer formación en materia de privacidad. Desde su fundación, la asociación ha llevado a cabo charlas, talleres y ciclos tanto bajo demanda como por organización propia. Los receptores han sido de lo más variado: desde alumnos de instituto hasta colectivos activistas, festivales de arte, asociaciones de periodistas y estudiantes universitarios.

En sus ya cuatro años de vida, Críptica ha avanzado lenta pero segura, acercando las herramientas de protección de la privacidad a quienes las necesitaban, así como haciendo pedagogía de buenas prácticas de seguridad operacional.

Ante la perversión de la tecnología que debía servir para comunicar, informar y conectar a personas, Críptica se erige en defensa de la privacidad como barrera indispensable para proteger derechos fundamentales como la libertad de expresión, asociación y el derecho a la intimidad.

Ante el desafío de la vigilancia masiva, la asociación se ha mantenido firme en sus principios: criptografía, descentralización, código abierto y usabilidad como armas contra el espionaje global desvelado por las filtraciones de Edward Snowden en el 2013. Redes de anonimato, aplicaciones de mensajería segura, proveedores éticos de servicios, bloqueadores del rastreo, servicios en la nube descentralizados… Las herramientas evolucionan cada día, pero la maquinaria de vigilancia también. Es el objetivo principal de Críptica hacer de puente entre la innovación tecnológica en materia de privacidad y la sociedad, ofrecer herramientas seguras para proteger los derechos que se ven amenazados en la era en que vivimos.

Prólogo
Una decisión política

Si tienes este libro en tus manos significa que la seguridad de tu móvil –de las comunicaciones que mantienes y de los datos que almacenas en él– te preocupa; o crees que lo puede llegar a hacer. Si no, quizás son los que se preocupan quienes te intrigan, y lees estas líneas con una sonrisa burlona pensando que todo esto es inútil, una idiotez para gente que ha visto demasiadas películas. O quién sabe si eres un paranoico que está acostumbrado, antes de las reuniones, a guardar el teléfono con los otros móviles en una lata de galletas metálica; la clase de persona que sabría cómo hacerse una bolsa de Faraday con un poco de plástico y papel de aluminio y que guarda un par de tarjetas SIM a nombre de algún ciudadano extranjero, por si acaso. En cualquiera de los tres casos y de las infinitas opciones que hay entre ellos, yo de ti continuaría leyendo.

Este manual no es una lista de herramientas, aplicaciones y las instrucciones para usarlas. Todo esto está entre estas páginas —no te preocupes— bien hecho y actualizado. Eso sí, no esperes encontrarte una receta fácil con instrucciones cerradas. Los autores, los miembros de Críptica, te tratarán como a un adulto: explicándote los pros y los contras de cada opción y dejándote la elección a ti, en función de tu situación y condiciones, del contexto –una palabra que se olvida demasiado a menudo–. También, y sobre todo, el libro es una puerta a otra forma de ver las cosas, de pensar. Aunque esta guía se enfoca en el pequeño aparato que siempre llevas encima, te puede abrir el camino para entender cómo funciona el mundo hoy en día. Puede ser una vía para aprender un tipo de defensa personal que funciona sin armas ni golpes. Es posible que dudes que algo de esto te pueda llegar a ser útil alguna

vez, y es una buena pregunta, pero la respuesta ya la sabes tú mismo, o no lo leerías.

No recuerdo cuándo descubrí qué era la criptografía y me dio por investigarlo leyendo desordenadamente webs, blogs, libros, artículos, foros... Aún estudiaba, o sea que debía ser antes del 2004. Removiendo dentro y fuera de Internet descubrí el programa PGP (Pretty Good Privacy), de Phil Zimmermann, y el concepto de criptografía asimétrica o de clave pública. Todo aquello no tenía nada que ver con mi formación –había estudiado historia y acababa periodismo–, pero llamaba la atención y, en cierto modo, llegó a obsesionarme. Incluso me empeñé en intentar entender las operaciones matemáticas en las que se basaban diferentes técnicas criptográficas, incluyendo la de clave pública, y me pude hacer una idea aproximada. Lo probé, y resultó más fácil de lo que había pensado. Con la extensión Enigmail del cliente de correo electrónico Thunderbird me hice un juego de llaves. Ya podía enviar –¡y recibir!– correos electrónicos cifrados.

Pero ¿a quién? ¿Y por qué? No tenía ningún sentido. Los profesionales del oficio que empezaba a aprender y que me rodeaban no cifraban nunca nada, que yo supiera. Mis amigos aún menos, y si contaba a alguien algo de lo que iba descubriendo la respuesta más benévola que recibía era una mirada sarcástica que insinuaba que era un friki (cosa que, por otra parte, siempre ha sido un poco cierta). Todo lo que aprendía quedaba más o menos arrinconado en la memoria, como mucho servía para cansar los oídos de alguna chica y un par de amigos. Sin embargo, la curiosidad me asediaba, y continué leyendo sobre algunos conceptos básicos de funcionamiento de la red, anonimato en Internet y seguridad informática en general. Nunca he pasado de ser, como mucho, un usuario avanzado, pero insistí. Y durante años todo aquello parecía un conocimiento inútil. Una afición extraña. Hasta que Edward Snowden habló.

Los medios de comunicación, WikiLeaks y las redes sociales comenzaron a esparcir información sobre las técnicas de espionaje de Estados Unidos y sus aliados. Aquel goteo de filtraciones aún dura, hasta el punto de que casi se han nor-

malizado las noticias sobre la vigilancia masiva. Pero nadie ha ido a la cárcel y el espionaje continúa. Seguimos utilizando los servicios y los aparatos de las empresas tecnológicas que colaboraban en espiarnos. De hecho, nada ha cambiado. O eso parecía.

Sería bonito decir que una parte importante de la sociedad, de repente, tomó conciencia de hasta qué punto entregamos cantidades ingentes de información sobre nosotros mismos a empresas que, además de hacer negocio, la comparten con autoridades gubernamentales, agencias de espionaje y otras empresas. Sería bonito decirlo, pero falso. En parte, porque a la mayoría de ciudadanos la posibilidad de que los espíe la NSA, el GCHQ o el CNI les importa un bledo, y con razón. De entrada, porque difícilmente tendrán algo que temer. Pero también porque quien quiera evitar espionaje de este nivel lo que debería hacer, seguramente, es tirar el móvil al río y tomarse este libro como un pasatiempo.

Sin embargo, el mundo, después de Snowden, no es exactamente el mismo. Cierta ingenuidad general ha desaparecido y, aunque decidimos continuar como hasta ahora por comodidad, no podemos evitar sospechar hasta qué punto nuestros datos personales pueden ser valiosos, y volátiles. La verdad es que aquellos conocimientos que fui recopilando como por una afición extraña cada vez me han sido más útiles. Algunas –contadas– veces me han servido para acceder a alguna fuente especialmente prudente y comunicarme de forma segura, pero sobre todo me han permitido darme cuenta de cosas que pasan –y contarlas– y, además, me han ayudado a comprender mejor el mundo en que vivimos. Ahora no es raro ver periodistas que incluyen en su perfil de Twitter o en la firma del correo electrónico una secuencia de números y letras que sirve para que les puedan mandar correos electrónicos cifrados, o el enlace directo a su clave pública. Es más: hay herramientas que usan cifrado de extremo a extremo que son mucho más accesibles –y usables– que las de hace quince años. A muchos lectores os sonarán servicios como ProtonMail o aplicaciones como Signal, que no hace tanto habría parecido propia de una película de espías. Algunos incluso la habréis descargado.

¿Pero de qué sirve comunicarse con Signal, aunque sea con la opción de autodestrucción de los mensajes activada, si se muestra la pantalla del móvil con el brillo al máximo en un lugar público, lleno de periodistas, cámaras y fotógrafos armados con teleobjetivos inmensos? De lo mismo que puede servir comprar una puerta blindada y cerrar de golpe o dejarse la ventana de casa abierta. Pero ambas cosas pasan –pregunta a cualquier policía que se dedique a investigar robos, o al exconseller Toni Comín–. Descargarte una aplicación o aprender a cifrar un correo electrónico, por sí solo, no te blindará. De hecho, según cómo, no te protegerá nada y aún te hará la vida más complicada.

La principal aportación de este libro que tienes en tus manos es que expone los primeros pasos para entender la seguridad en los teléfonos móviles en función del contexto, y poder actuar en consecuencia. Por eso, aunque algunas de las aplicaciones que se detallan en la parte final pueden acabar desapareciendo, cambiando, o bien se puede descubrir que tienen agujeros de seguridad, el libro no caduca. Permite abordar la seguridad en el móvil de una manera holística, que no perderá el sentido pronto, a pesar de las actualizaciones constantes de un sector acelerado. Esto es así porque se entretiene en hablar de una parte olvidada en la mayoría de manuales y guías de este tipo, que suelen ser una lista más o menos conseguida de aplicaciones y de normas cerradas. Este libro habla de la seguridad operacional (OPSEC). No voy a entrar a definir qué es porque ya lo hacen las primeras páginas. Basta decir que tener el móvil cifrado y aplicaciones seguras, fiables y que respeten tu intimidad no garantiza nada si no se tienen en cuenta algunos conceptos básicos de seguridad operacional.

La información siempre ha sido la clave del poder. Esto no es nuevo, ya pasaba en tiempos de Sun Tzu, continuaba siendo así en la época de Raimondo Mazzarino y ahora se mantiene igual. La gran diferencia es la cantidad ingente de datos que se generan y se pueden procesar hoy en día, capaz de definir y radiografiar casi cualquier aspecto de la vida humana. Proyectos como este libro, y como el trabajo que hace

la entidad que lo ha escrito, Críptica, tan sólo pretenden que los ciudadanos podamos mantener un cierto control sobre nuestros propios datos, sobre nuestra propia vida. Que tengamos la opción de decidir.

Saber cómo funciona nuestro mundo no puede ser nunca un conocimiento inútil, es una base imprescindible para poder ser ciudadanos conscientes y actuar políticamente sobre aquello que no nos gusta del presente y lo que queremos para el futuro. En este sentido, este libro es una herramienta profundamente política. Porque el debate de la seguridad, aunque sea a nivel individual, es inseparable de la política, forma parte de ella. Optar por una aplicación u otra, para usar una contraseña resistente o el típico «1234», para cifrar el móvil o para compartir todo detalle de nosotros mismos en las redes sociales, son decisiones políticas. Aunque cuando las tomamos no seamos conscientes, no dejan de serlo. Incluso cuando renuncias a decidir, lo que haces en realidad es tomar una opción por omisión, de la peor manera posible.

Leer este manual, aunque sea por curiosidad, también es una decisión política. Es tomar la opción de empezar a ser consciente, de tragarte la píldora roja. Tu día a día no cambiará, pero tal vez, sólo tal vez, empezarás a pensar de una forma diferente. Y querrás más, como me pasó a mí.

Enric Borràs Abelló
Director ARA Balears

Introducción

> «En sus momentos de mayor intensidad, [el boxeo] parece contener una imagen de la vida tan completa y potente –belleza de la vida, vulnerabilidad, desesperación, coraje incalculable y a veces autodestructivo– que el boxeo *es* la vida, y difícilmente un simple juego. [...] El béisbol, el fútbol, el baloncesto: esos pasatiempos tan esencialmente norteamericanos son deportes de fácil reconocimiento porque implican juego: son juegos. *Se juega* al fútbol, no *se juega* al boxeo»[1].
>
> Joyce Carol Oates

Como no podría ser de otra forma, partimos de una *situación*. Situación que, fuera de toda duda, compartimos con la potencial comunidad de lectores: la era de la telefonía inteligente. «Esto lo cambia todo» era el eslogan del primer iPhone: como diagnóstico, no podía ser más acertado. El teléfono inteligente se ha convertido en el interlocutor central del diálogo que mantenemos con el mundo. No hace falta ser ingeniero para saber que los vínculos que se van estableciendo con la realidad exterior estarán dentro de poco determinados y dirigidos por el nuevo dispositivo fundamental, que se llama *smartphone*.

Aunque nuestro ámbito de trabajo sea el de la seguridad en las tecnologías de la información, esta guía es antes que nada el producto resultante de una apuesta visceral, fruto de nuestra experiencia sensible: detectamos una preponderancia absoluta del smartphone en nuestra vida cotidiana, lo que refuerza el interés que le asignamos como objeto de estudio, por delante de otros dispositivos informacionales como el or-

---

1 Joyce Carol Oates (2015): *Del boxeo*, Debolsillo, Barcelona, p. 39.

denador portátil, el reloj o la tableta –los cuales se han visto relegados a la condición de meros personajes secundarios, *periféricos*, respecto al objeto principal–. De este modo, la justificación del presente manual no es de índole tecnológica, sino *fenomenológica*.

Fenomenológica también en segunda instancia porque dejamos bajo criterio del lector la evaluación ética del smartphone. Este manual no formula juicios éticos «a favor» o «en contra» de dicho aparato o de la tecnología en general, sino que parte del análisis de una situación concreta (el papel central del smartphone en la vida diaria) para desarrollar el arte de saber moverse en ella, de hacerlo *a pesar de ella*. Lo que pretendemos con esta guía es comenzar a abordar el difícil periodo que la telefonía inteligente ha abierto para la seguridad, al margen de valoraciones éticas sobre su conveniencia o no en la vida social. «Mi escritura no es nada, mi boxeo lo es todo», solía decir Ernest Hemingway. Siguiendo su ejemplo, nuestras opiniones éticas o incluso políticas son aquí irrelevantes; nos contentaremos con ejercer bien nuestra labor técnica, con vistas a comunicar las mejores formas de afrontar el combate.

El primer consejo que daremos en este manual, respecto al cual todos los demás son secundarios, es el de dejar de tratar el teléfono inteligente como si fuera un contenedor masivo de todo tipo de informaciones[2]. El *alter ego* virtual que habita en nuestro smartphone se vuelve potencialmente más comprometedor para nuestra seguridad conforme lo alimentamos con fotografías, mensajes e interacciones de todo tipo, hasta generar un retrato robot perfectamente definido de quienes somos. Y dado que se trata de un dispositivo que tiende a centralizar la información perteneciente a una gran variedad de actividades diarias, lo más urgente será dejar de traducir

---

2 Información: nos referimos en todo momento a un concepto estrictamente computacional del término, en el sentido acuñado en la teoría matemática de la comunicación de Claude E. Shannon y Warren Weaver (no a conocimiento expuesto por medio de la lengua). Información entendida como unidades cuantificables de todo tipo de datos.

informacionalmente toda nuestra vida como primera medida de seguridad. No existe una información mejor protegida que aquélla que no se llega a generar, ya que no existe forma alguna, humana o técnica, de comprometerla. La función de la seguridad es la de ser una última barrera para garantizar la integridad de las informaciones que necesitamos, a pesar de todo, producir. No tener que depender de ella es la única manera posible de situar la confidencialidad de nuestra información en un plano superior, a salvo de todo tipo de artimañas por acceder a ella.

Asimismo, una excesiva dependencia del teléfono podría hacer que acabáramos depositando la mayor parte de los datos que generamos en un mismo aparato, inercia que se traduce en riesgo desde el momento en que un único ataque exitoso contra el terminal podría dejar integralmente expuesta nuestra vida digital. Sea como sea, tenemos que disminuir el peso de esta mochila de datos a la que llamamos smartphone: para que nuestra excursión no se acabe convirtiendo en un martirio, tendremos que aprender a cargar únicamente con lo fundamental de verdad.

El presente manual consta de dos dimensiones importantes por igual: seguridad operacional y seguridad instrumental. Únicamente con la sutil combinación de ambas disciplinas se pueden recrear las condiciones para desplegar cierto estado de seguridad (aunque en la mayoría de ocasiones no baste simplemente con eso). Bajo el paradigma cibernético actual, la seguridad operacional sin un conocimiento técnico estricto es mero parloteo existencial, mientras que la seguridad instrumental separada del pensamiento operacional es un abandono de la facultad estratégica que toda técnica contiene. Aprender las técnicas, sí, pero siempre atendiendo a las condiciones en las que su uso cobra sentido, de forma que sepamos a cuál de ellas recurrir en cada momento sin ceder un ápice de iniciativa. La situación que describimos exige algo más que *hackers* o estrategas en abstracto; requiere de su interacción forzosa para desarrollar conjuntamente una inteligencia de la situación, un análisis fenomenológico aplicado, capaz de captar al

detalle nuestra condición como seres atrapados en las redes de la cibernética. Y partir de ahí, para saber cómo hacer.

Seguridad operacional

La seguridad operacional (OPSEC, en sus siglas en inglés, *operational security*) es la gran olvidada de los manuales de seguridad. Llamamos OPSEC al tipo de seguridad que no se ocupa de desarrollar o aconsejar herramientas, sino pautas de uso y de comportamiento que nos sirven para adquirir ventaja estratégica en un hipotético choque de fuerzas con un determinado oponente. Hasta la fecha, el análisis operacional ha sido desatendido en pro del conocimiento estrictamente técnico o instrumental. La razón de este olvido puede encontrarse en la formación predominantemente técnica de la mayoría de formadores, los cuales pretenden transmitir en bloque los conocimientos técnicos más avanzados sin atender antes a los aspectos sociales de la seguridad y a su naturaleza táctica, cuando éstos de hecho los preceden. Contrariamente a lo que podría parecer desde fuera, el conocimiento técnico avanzado en absoluto garantiza un conocimiento notable en lo referente a la seguridad operacional, a no ser que evolucione a lo que llamamos *pensamiento adversarial*[3], el cual deja de ser «técnico» en gran medida.

La seguridad operacional es pensamiento adversarial aplicado a las exigencias de una empresa concreta, en un lugar y tiempo claramente delimitados, frente a antagonistas que pugnan por hacerse con la hegemonía. Le corresponde diseñar un marco táctico adecuado para desplegar exitosamente las propias operaciones, aun teniendo que hacer frente a situaciones no previstas, resultado de la interacción con fuerzas contrarias. Pensar en clave adversarial, teniendo en cuenta las capacidades de un rival dado en un espacio y momento

---

3 Denominamos *pensamiento adversarial* al arte de tener en cuenta las capacidades del adversario a la hora de desplegar una estrategia de seguridad.

concretos, impide que lo subestimemos, puesto que recrea el peor de los escenarios posibles para desplegar una defensa a la altura. O lo que es lo mismo: solamente habiendo valorado seriamente el talento del contrincante es cuando surge la posibilidad táctica de imponerse a él. «La invencibilidad es una cuestión de defensa», dice Sun Tzu[4].

Sea cual sea el instrumento, aplicación o herramienta utilizada, el punto de vista operacional nos recuerda que su uso se despliega siempre dentro de una situación concreta que no se limita a ser un mero telón de fondo, sino que recubre necesariamente cualquier actuación: un país autoritario con legislación hostil al derecho a la privacidad, una rueda de prensa con cámaras capaces de grabar nuestra pantalla, un autobús con un compañero de asiento pendiente de nuestras conversaciones... Corresponde a la vertiente operacional de la seguridad mostrarse escéptica ante la presunta infalibilidad de cualquier aplicación, precisamente porque asume que la riqueza de circunstancias que conforman el tejido de la realidad siempre acaba por superar todas las situaciones previstas de antemano por cualquier sistema de seguridad.

Operacionalmente hablando, se le llama *seguridad* al arte de saber levantar defensas que puedan imponerse (aunque sea de manera temporal, si cumplen con su función de protegernos durante el tiempo suficiente) a la realidad, con tal de proporcionar una relativa cobertura a las propias acciones, al tiempo que se intentan hacer infructuosas las posibles respuestas del adversario. «Los expertos en defensa se esconden en las profundidades de la tierra [...] en situaciones de defensa, acalláis las voces y borráis las huellas, escondidos como fantasmas y espíritus bajo tierra, invisibles para todo el mundo», se insiste en *El arte de la guerra*.

Desde Críptica consideramos fundamental la formación en cuestiones básicas de seguridad operacional, incluso como fase previa al uso de herramientas de seguridad en la vida diaria. Sin saber desarrollar una lectura detallada de cada si-

---

4 Sun Tzu (544-496 a. C.), autor de *El arte de la guerra*, libro clásico de estrategia.

tuación concreta, sin una vocación táctica que justifique el uso de cada herramienta utilizada, cualquier instrumento que incorporemos a nuestros protocolos de seguridad será siempre una apuesta a lo desconocido.

Seguridad instrumental

Aplicaciones de mensajería, alternativas de almacenamiento seguras, sistemas operativos libres... La seguridad instrumental es el tipo de conocimiento que uno espera encontrar tanto en los manuales como en los coloquios sobre seguridad informática. Las razones de su preponderancia son múltiples, pero seguramente se vinculen a una voluntad de facilitar el proceso de aprendizaje, reduciendo una disciplina sumamente compleja a la utilización de una serie de aplicaciones o herramientas alternativas a las hegemónicas. Corresponde a la seguridad instrumental la difícil pero fundamental tarea de democratizar el acceso a la seguridad, desarrollando y transmitiendo herramientas que no requieran de un conocimiento técnico avanzado para ser usadas.

Sin duda, el gran triunfo de este discurso reside en haber conseguido generalizar el uso de aplicaciones de seguridad entre la gente no experta. Una nueva hornada de aplicaciones pensadas para ser seguras por defecto ha logrado hacer por fin socialmente atractiva la seguridad. El crecimiento ha sido exponencial desde entonces: en Estados Unidos, las descargas de Signal se duplicaron en el primer trimestre del 2017, coincidiendo con el inicio del mandato de la administración Trump[5].

Como asociación, nuestros valores nos han ayudado a sintetizar una serie de criterios a la hora de recomendar herramientas, que naturalmente también aplicaremos a las

---

5 «Trump fears have helped double downloads for Signal, the private messaging app», *Recode* (4/4/2017): https://www.recode.net/2017/4/4/15124316/americans-privacy-signal-downloads-chart.

recomendaciones del presente manual. Intentaremos mantenernos fieles a ellos, siempre que esto no signifique para el usuario una pérdida notable en términos de usabilidad o que no existan opciones que los cumplan en su totalidad. El objetivo de expandir numéricamente el público potencial de las aplicaciones de seguridad pasa por recomendar herramientas con un diseño accesible e intuitivo, aunque como grupo no nos satisfagan enteramente a nivel de arquitectura, ideología o principios. La disposición a ser flexibles con los propios valores no implica claudicar, sino admitir la hipótesis de que es preferible una seguridad con impurezas a un concepto inmaculado de la misma pero inasumible por quienes no pertenezcan a una élite de expertos. Cuando la rigidez de criterios impone tan elevado umbral que la mayoría de aplicaciones de seguridad no llegan a cumplirlos es que unos valores que debieran orientar la acción la están, por el contrario, dificultando o incluso impidiendo.

Una vez admitida la flexibilidad como base de todas nuestras prescripciones, exponemos los cuatro criterios que justifican la elección de las herramientas recomendadas a lo largo de esta guía (el orden de los mismos es puramente arbitrario):

- *Seguridad por defecto*. El mayor grado de seguridad debe ser el que la aplicación ofrece por defecto. La seguridad no puede delegarse en configuraciones concretas o procedimientos suplementarios a la instalación, tiene que estar garantizada de antemano con tal de que el error humano no pueda producirse.

- *Código abierto*. Para mayor seguridad, el código fuente de la aplicación debe estar públicamente disponible, permitiendo su revisión por parte de la comunidad. Las aplicaciones privativas impiden verificar si su funcionamiento real se corresponde de manera exacta con lo expuesto en su descripción.

- *Usabilidad.* Si el diseño de la aplicación no es fácilmente comprensible por el usuario final (disponga o no de conocimientos técnicos), su uso estará condenado a la marginalidad. Apostamos por herramientas intuitivas que faciliten la ya de por sí complicada tarea de la seguridad, no que la hagan todavía más difícil.

- *Descentralización.* Que no delegue en un único proveedor a la hora de ofrecer el servicio, puesto que esto sitúa a los usuarios en una posición de desequilibrio al depender de una infraestructura ajena, que puede cesar el servicio arbitrariamente.

Como venimos insistiendo, esta cadena de criterios no pasa de ser una mera declaración de intenciones que nos concede cierta inclinación a la hora de seleccionar determinadas herramientas, no unas reglas inamovibles que debieran prevalecer por encima de cualquier circunstancia. En la relación dialéctica que existe entre unos principios inquebrantables y la flexibilidad operativa derivada de su relativización en el plano de lo real, nosotros tenemos claro por cuál de las dos fuerzas tomamos partido, aun a riesgo de ver cuestionada nuestra fidelidad a unos principios supuestamente vehiculares de la comunidad hacker.

Que este manual, consagrado al dispositivo hostil por excelencia para este tipo de círculos, sea una prueba viva de ello.

A modo de advertencia

La absoluta mayoría de quienes lean este manual nunca tendrán entre sus adversarios a la NSA[6], el GCHQ[7] u otras agencias de inteligencia. Semejantes actores cuentan, además, con unos recursos y capacidades que sobrepasan ampliamente las prescripciones del presente manual. Por consiguiente, no queremos que se delegue en esta guía si lo que se espera de ella son enseñanzas para imponerse a los grandes organismos del espionaje internacional.

Creemos que, con tal de fomentar una cultura de la seguridad efectiva, es preciso comenzar por lo estrictamente básico, sin ofuscarse en organismos cuyas capacidades nos exceden hasta extremos que desconocemos.

He aquí, pues, nuestra humilde contribución.

---

6 NSA, National Security Agency: la Agencia de Seguridad de Estados Unidos.

7 GCHQ, Government Communications Headquarters: la Agencia de Seguridad del Reino Unido.

SEGURIDAD OPERACIONAL:

ADOPTAR UNA PERSPECTIVA ESTRATÉGICA

La mochila de datos

Aunque tiene una historia corta, el smartphone ha desarrollado rápidamente una relación centrípeta con el conjunto de nuestras actividades cotidianas. Nada o casi nada permanece al margen de su presencia: en el dormitorio, en el baño, en la sala de espera, en el gimnasio o incluso en el cine. Cualquier momento es adecuado para la intervención de dicho dispositivo, ya sea para tomar una fotografía, realizar una consulta, escribir una anotación o hacer una llamada. A finales del 2016, los teléfonos inteligentes superaron a los ordenadores tradicionales como principal medio de navegación[8], un hito inconcebible una sola década atrás.

A diferencia de los ordenadores de sobremesa, el smartphone nos acompaña en todo momento. Y por una razón bastante sencilla, en realidad: su reducido tamaño hace que toda la potencia del ordenador moderno quepa en nuestro bolsillo. Aun a riesgo de constatar lo que a todas luces parece una evidencia, desde nuestra perspectiva sigue siendo relevante reiterar que esto dificulta la desconexión. Y es que más allá de las consecuencias puramente sociales derivadas del uso intenso del smartphone (dependencia, distracciones, estrés...), existen también riesgos de tipo operacional que pueden comprometer seriamente nuestra seguridad, respecto a los cuales no se ha escrito todavía lo suficiente. El primero es estar cargando a cada instante un archivo digital que abarca la práctica totalidad de nuestras memorias recientes.

El teléfono inteligente tiende a concentrar cada vez más funciones que habitualmente pertenecían al mundo «real», no conectado. Allí donde la humanidad desarrollaba tradicionalmente una actividad, ahora existe una aplicación para llevarla

---

8 «Mobile web usage overtakes desktop for first time», *The Telegraph* (1/11/2016): http://www.telegraph.co.uk/technology/2016/11/01/mobile-web-usage-overtakes-desktop-for-first-time.

a cabo de manera «más eficiente», a través del smartphone: WhatsApp, Wallapop, Uber, BlaBlaCar, Deliveroo, o incluso Tinder. Asimismo, las necesidades que antes sufragaban objetos de uso corriente como el mapa, la agenda, el bloc de notas, la cámara fotográfica, el bolígrafo o el calendario (entre muchas otras) se delegan ahora en el terminal de bolsillo. Lo que se presenta como un solo objeto es en verdad el ensamblaje de muchos otros, de ahí el protagonismo del smartphone en cualquier circunstancia: ha asumido el rol de intermediario privilegiado entre nosotros y el mundo.

La omnipresencia de cualquier objeto en las interacciones que hacemos con el entorno (como ocurre con el smartphone en la actualidad) introduce un escenario sumamente adverso para pensar la seguridad. Mientras que antes era imperativo intervenir físicamente los seis objetos mencionados (necesariamente «no conectados» a ninguna red y situados en ubicaciones indeterminadas) para obtener una imagen completa del usuario, ahora basta con concentrar los ataques contra uno solo que reúne toda la información, lo que lo convierte en el blanco ideal.

El auge del teléfono inteligente ha conllevado centralizar muchas funciones en un solo aparato, de modo que se ha acondicionado el terreno para un fallo total en caso de que el terminal deje de funcionar[9]. Hemos pasado a ser seres que cargan consigo una pesada mochila de la cual sin embargo no perciben el peso, lo que dificulta que se den cuenta de la gravedad del problema: la mochila de datos. Conviene que aligeremos peso lo antes posible, so pena de arrastrarnos con ella cuando la aventura se complique.

Operacionalmente hablando, lo relevante del smartphone no es su dimensión tecnológica, sino su uso social: se trata de un aparato que llevamos a todas partes con nosotros, que suele integrar todas las facetas de la persona (trabajo, amistades, hábitos de consumo, actividad política), el cual sirve

---

9 La verdad de esto solamente se muestra cuando lo perdemos o se nos rompe: una buena parte de nuestras vivencias en forma de fotografía o texto pasa a ser inaccesible.

como archivo de sus vivencias y que concentra gran parte (si no la totalidad) de su historial relacional. A estas alturas, cualquier adversario que merezca tal nombre sabe que basta con hacerse con el control del teléfono del objetivo para acceder a un torrente de información relevante de modo inmediato. Irrumpir en un domicilio para colocar pequeños micrófonos o localizadores es una práctica que entraña riesgos innecesarios, sabiendo que el terminal de cada uno puede ser intervenido para que se comporte como un dispositivo espía. De lo que se tratará a partir de ahora es de hacerse con los instrumentos para ganar silenciosamente el control del dispositivo que almacena toda la información relevante, de ahí que la respuesta tenga que pasar necesariamente por disminuir de manera selectiva el uso que se hace del smartphone, reduciendo la cantidad total de datos que contiene. Calendarizar borrados de memoria o dejar de depositar en el terminal información que consideremos crítica son medidas orientadas a soportar esta pesada carga, sin llegar a suprimirla del todo.

Consejos:

- *Haz un inventario general de todas las cosas que llevas en tu mochila de datos* (mensajes, fotografías, correos, registros de actividad, etcétera). Valora cuáles de ellas te merecen la etiqueta de «sensible» (informaciones que de veras no quisieras ver comprometidas) para establecer prioridades a la hora de retirarlas del smartphone.

- *Aligera peso*. Probablemente delegues una cantidad excesiva de informaciones en un único aparato, lo que aumenta la probabilidad de ataques dirigidos. Realiza borrados periódicos, reduce el número de aplicaciones que tengas instaladas e intenta vincular lo menos posible tu identidad *online* a un mismo terminal (por ejemplo, cuentas en redes sociales), con vistas a dificultar la obtención de una imagen nítida de tu identidad real.

- *Ten en cuenta los riesgos.* A pesar de todo, el smartphone carga siempre con cierta cantidad de informaciones. Valora lo que podría obtener un adversario que consiguiese acceso físico o remoto a tu dispositivo, con tal de reducir el botín que espera obtener de una intrusión exitosa.

- *Identifica las situaciones en las que la mochila es un obstáculo.* Siguiendo la regla de oro, «no existe una información mejor protegida que aquélla que no se llega a generar», debes desarrollar un arte de saber cuándo *no* producir información alguna.

Elaborar una rutina de combate

El uso de las modernas tecnologías informacionales (teléfonos inteligentes, tabletas, relojes...) conlleva que cada una de las interacciones que hacemos con ellas se traduzca en términos de información, el único lenguaje apto para la comprensión computacional. Revisando estas grandes masas de datos, el ojo experto puede deducir patrones de uso, acción e interacción humanas, los cuales son únicos en cada persona.

El smartphone es el máximo exponente de una relación con el mundo basada en la informatización de cada vez más parcelas de la actividad humana, que ahora ha pasado a ser (aparentemente) compartimentalizable, cuantificable y administrable técnicamente, conducida por la ciencia de la estadística. Con la generalización de la informática, un duplicado virtual de nuestra existencia aspira a imponer su ley sobre nuestra presencia serena en el mundo, con toda su carga indomable. En tanto que sigamos preocupados por la seguridad, una desconfianza instintiva respecto a todas estas tecnologías debería prevenirnos de cualquier encaprichamiento de naturaleza cibernética, que con toda probabilidad sería al precio de renunciar a cualquier actividad desarrollada al margen de los sistemas informáticos de control –lo que antes se llamaba «esfera privada»–.

Cibernética: como seres que habitamos el primer cuarto del siglo XXI, vivimos bajo su sello. La cibernética, en calidad de disciplina que coloca la teoría de la información como modelo de organización social, equipara el funcionamiento de las sociedades humanas al del sistema nervioso; la cadencia de informaciones es constante dentro de una totalidad presupuesta de antemano, de forma que la acción de gobierno consiste en intervenir los flujos para pilotar sobre todas las situaciones que se puedan generar, anulando aquellos influ-

jos potencialmente destructivos para el organismo. A pesar de sus connotaciones *high tech*, la cibernética, –del griego *kubérnesis* («acción de pilotar un barco»)–, acaba remitiendo a la acción primera de todo gobierno: mantener el control sobre la nave contra todas aquellas fuerzas que pretenden hacerla naufragar.

Atrapados como estamos en este nuevo paradigma, irremediablemente tenemos que aprender a movernos en un medio que nos es hostil. Se nos ha arrojado al tatami cibernético sin recibir instrucción previa, lo cual nos hace sumamente vulnerables frente a adversarios que son más poderosos, más perseverantes y más experimentados de lo que somos nosotros. A menos que aprendamos a combatir en estas difíciles circunstancias, nuestra derrota es inminente. Pero nunca es tarde para conocer las reglas del juego: partir de las propias limitaciones en una situación concreta es el requisito fundamental para hacerse fuerte en ella.

La seguridad no debería considerarse una actividad especial, separada del resto de acciones humanas. Tanta es la confusión existente, que se la ha presentado como un momento aparte, cuando es justamente lo contrario: conforme la vayamos desdiferenciando e integrando en las facetas más cotidianas de nuestra existencia, más efectiva resultará. Un recurso típicamente marcial, la rutina de combate, guarda un potencial inesperado al ser aplicado en el contexto de la seguridad en las tecnologías de la información. La idea de la rutina consiste en reproducir condiciones similares a las de la lucha, pero sin riesgo de daños para la persona, en un espacio no hostil para ella. El resultado es la interiorización de estrategias de respuesta que solamente se ganan en circunstancias parecidas a las del combate –el desarrollo de una atención especial sobre los detalles, que es lo que caracteriza al guerrero experimentado–.

El objetivo de toda rutina es ganar una inteligencia de la situación, volverla legible a ojos del individuo familiarizado con ella, aunque sea por repetición, con tal de saber moverse en su seno (los simulacros de incendio o terremoto obedecen a esta misma lógica). Le da instrumentos para densificar su

presencia en ella, que le sirven para dejar de ser pasivamente conducido aun sin poder llegar a sustraerse del todo de sus circunstancias inmediatas. Una rutina de preparación para el combate, igual en el boxeo que en la cibernética, exige conocer cuáles son los golpes que podrían ser ejecutados contra el púgil en un momento dado, de forma que sepa resistirlos cada vez mejor.

La seguridad ha sido siempre un oficio sin brillo; solamente se percibe como ausencia cuando un golpe consigue atravesar una defensa que hasta entonces creíamos sólida. La estricta negatividad de la disciplina halla sin embargo su fundamento positivo al confrontarse con la estrategia del adversario: la seguridad nunca ha sido otra cosa que el penoso arte de saber encajar los golpes, con vistas a que ninguno de ellos pueda llegar a inducirnos un daño crítico. Es el pensamiento del repliegue *en tanto que repliegue*, un saber a la defensiva que puede ser determinante si nuestros movimientos consiguen volver ineficaces las arremetidas del contrincante.

Sabemos que ninguna rutina de combate es exactamente igual a otra: depende del tipo de arte marcial practicado (que delimita los golpes permitidos) y de las características del adversario (capacidades, psicología, instrumentos a su alcance, tamaño, peso, etcétera). Por ello, aunque pudiéramos circunscribir los saberes de este manual dentro del cajón de sastre de la «seguridad informática» (lo cual es dudoso), seguiríamos sin tener una imagen completa de cada uno de los posibles adversarios, los cuales varían enormemente según el país o la posición social, entre otros muchos factores. Como instructores en la materia, pretender sintetizar en una sola rutina la infinidad de variables ante las cuales la comunidad de lectores se pueda encontrar es irreal en la misma medida que irresponsable. Optaremos en su lugar por ofrecer seis pautas generales para la elaboración de una rutina informacional propia, que consideramos necesaria al margen del modelo de amenaza.

- *La rutina es un ejercicio diario*. Los saberes que derivan de ella son en gran medida fruto de la cotidianidad existencial, de manera que solamente llegaremos a desarrollar

cierta seguridad si la concebimos no como un momento separado del resto de nuestra actividad general, sino como un proceso incorporado a cada una de las interacciones que realizamos con las tecnologías de la información.

- *Toda rutina es gradual.* Empezar por lo mínimo para ir subiendo el nivel de exigencia gradualmente, conforme se dominen las técnicas básicas. No intentar incorporar herramientas o protocolos de seguridad que no se puedan integrar rápidamente en nuestra experiencia cotidiana, so pena de no saber usarlas o de perder usabilidad.

- *La rutina solamente es efectiva si cansa pero no extenúa.* Buscar constantemente el punto medio existente entre la comodidad derivada de la usabilidad total (que no supone esfuerzo alguno) y la perseverancia por mejorar nuestra seguridad de manera continuada (sin llegar al sobresfuerzo, que resulta perjudicial para un ejercicio prolongado).

- *Mantener la rutina al día.* El grado de efectividad real de cualquier rutina depende de las últimas tendencias en materia ofensiva. Estar al corriente de las prácticas en boga del adversario, incorporando constantemente nuevas técnicas de seguridad para contrarrestarlas en la medida de lo posible.

- *Dominar la rutina no significa ganar el combate.* Confiar en que un aprendizaje intensificado de todas las técnicas de seguridad te hace invulnerable en la lucha es un error que se remonta a los tiempos de Sun Tzu. El aprendizaje a nivel protocolario no garantiza que se sepa reaccionar a tiempo en un caso real, aunque contribuya a ello de manera crucial.

- *Convierte tu rutina personal en un ejercicio colectivo.* La vertiente social de las tecnologías de la información conlleva que fragmentos de nuestra identidad se transmitan a los dispositivos ajenos. Contribuir a que tu círculo tam-

bién implemente protocolos de seguridad para no quedar expuesto en caso de que un dispositivo de tu entorno sea comprometido.

Consejos:

La seguridad operacional es una rutina. Debes entrenarte…

- *Diariamente*: integra la rutina en tu día a día.
- *Gradualmente*: empieza por lo básico y hazla crecer.
- *Eficientemente*: no desdeñes la seguridad ni la comodidad, ambas son necesarias para una rutina eficaz.
- *De forma actualizada*: infórmate de las últimas tendencias de ataque que puedan afectarte, con tal de actualizar tu rutina para enfrentarte a ellas.
- *Consciente de los límites*: no hay garantías de que tu rutina te haga invulnerable, sea cual sea su grado de complejidad.
- *Colectivamente*: transmite tus prácticas a tus círculos, protegeos los unos a los otros.

El fin del anonimato

> «Cuando esta persona se desvanezca entre la multitud, si sé su nombre, seré capaz de encontrarla de nuevo. Inversamente, saber un nombre me permite consultar un registro central, en el que encontraré una descripción de la persona correspondiente [...]. Ser capaz de reconocer a alguien equivale a ser capaz de encontrarle de nuevo: una vez te haya reconocido, ya no te me podrás escapar»[10].

La telefonía inteligente introduce una paradoja singular desde la perspectiva de la seguridad: por un lado, tenemos que concederle a la industria el mérito que supone haber conseguido desarrollar dispositivos móviles notablemente seguros; por otro, observamos que en este proceso nos hemos ido desprendiendo gradualmente de la posibilidad de un uso anónimo, hasta casi desaparecer.

La relación que *se* desarrolla habitualmente con el smartphone parece refractaria al anonimato: la condición «personal» de un dispositivo se obtiene a cambio de que todos los datos que contiene correspondan a la vida de una única persona, de forma que acceder a la información almacenada en el teléfono también significa obtener una imagen integral de la vida de su poseedor[11]. Haber dejado de utilizar dispositivos compartidos probablemente favorezca la seguridad al ganar un control total sobre aplicaciones y procesos,

---

10 Grégoire Chamayou y Kieran Aarons (2013): «Fichte's Passport - A Philosophy of the Police», *Theory & Event*, núm. 16 [2].

11 Tanto es así, que el censo español del 2021 prevé utilizar la información de las antenas de telefonía para saber cuáles son los desplazamientos habituales del conjunto de la población, suprimiendo la necesidad de cuestionarios. «Las operadoras seguirán el rastro de tu móvil para alimentar el censo del 2021», *El Diario* (10/3/2016).

pero anula la posibilidad de un acceso anónimo, lo cual puede abrir nuevos vectores de ataque que se derivan, precisamente, del carácter «personal» de los aparatos.

El anonimato, como necesidad distinta de la seguridad o la privacidad, ha sido un recurso necesario en un buen número de ocasiones históricas, actuando como medida de prevención para limitar la superficie de ataque del adversario: sabido es que no puedes golpear aquello que no puedes ver. Lo ilustran a la perfección las filtraciones de Edward Snowden, que tuvo que mantener su identidad real en secreto para establecer contacto con la prensa sin llamar la atención de la NSA americana. La estrategia del anonimato pasa por confundir el propio rastro en un conjunto más amplio de personas o informaciones, lo que obliga a multiplicar los esfuerzos necesarios para localizar al objetivo. Más que «seguridad», el anonimato ofrece una protección similar a la del camuflaje, puesto que sirve para alargar la fase de identificación previa al ataque –lo que ralentiza las operaciones de un adversario que apuntara a un objetivo concreto–. Por contra, el aparentemente inocuo «ser visible» facilita las acciones que se quieran emprender contra la persona o su entorno, porque revela los posibles puntos donde es vulnerable.

Si bien existen un buen número de iniciativas que aspiran, en términos generales, a mejorar la seguridad y la privacidad del usuario (esta misma guía, por ejemplo), también es cierto que en la mayor parte de ellas el anonimato ha dejado de jugar un papel importante. Como *se* entiende que nuestro acceso a la información se practica siempre desde los mismos dispositivos, el desafío se limitaría a protegerlos contra las intrusiones de terceros. Dicho esquema descarta de antemano el tipo de protección concedido por el anonimato, un error fatal que deja desatendidos los modelos de amenaza en los que la identificación es ya una derrota, como es el caso de los *whistleblowers*[12].

---

12 *Whistleblower*: filtrador de información, habitualmente para llamar la atención acerca de una irregularidad.

La función de la seguridad, dijimos en la introducción, es la de ser una última barrera cuando nuestro adversario ya ha descubierto nuestra identidad. Es decir, que idealmente deberíamos recurrir a ella como último recurso, cuando todo lo demás falla. Conocer nuestro nombre, los dispositivos o sistemas operativos que utilizamos son informaciones fundamentales para que el adversario pueda no solamente elegir sus ataques, sino llevar a cabo la selección según la probabilidad de que sean exitosos. «Nunca hables de tu configuración de seguridad» es de ese tipo de reglas que nunca debemos dejar de lado, precisamente porque al hacerla pública comprometes cada una de las piezas que la conforman. Dejar ver las sutilezas de un sistema de seguridad, o dejarnos ver a nosotros mismos como parte integrante del conjunto, precipita una situación de desequilibrio que un adversario experimentado puede aprovechar para imponerse.

Cuando rehuimos la confrontación en vez de asumirla como algo inevitable, es cuando nos damos cuenta tanto de la necesidad del anonimato como de su escasez en el modelo de sociedad instaurado por la cibernética. «El guerrero sabio evita el combate», dice Sun Tzu. Pero para hacerlo necesita dominar el fino arte del camuflaje, de la confusión, los cuales son valores que cotizan a la baja en un contexto saturado por dispositivos «personales», asociados a la vida de una persona en singular.

Consejos:

- *Toda la información almacenada en tu smartphone es información personal.* Tu situación particular es única, lo que comporta que las informaciones depositadas en tu smartphone lo sean también. Si quieres desvincular una determinada actividad de tu identidad real, lo más aconsejable es que mantengas bien al margen tu teléfono.

- *Dificulta la labor de identificación.* Aun a riesgo de no ser suficiente, la única precaria forma que tenemos de proporcionar cierto grado de anonimato a las actividades del

teléfono personal es usando redes anonimizadoras como Tor o una VPN, o en su defecto aplicaciones expresamente pensadas para proteger este aspecto de la privacidad.

Seguridad en grupos

Cuando pensamos en medidas concretas para proteger nuestro dispositivo de intromisiones no deseadas, lo hacemos orientados a minimizar el total de ataques al alcance de nuestro adversario, así como restarle eficacia a aquéllos que no podamos evitar. Toda mejora real en materia de seguridad pasa por limitar la superficie de ataque del rival, por hacer infructuosa su estrategia anulando la ventaja que espera obtener de los golpes dirigidos en contra nuestra.

El uso de dispositivos conectados a una red mundial implica que, en términos adversariales, nos veamos repentinamente arrojados a un combate asimétrico contra organismos de fuerza sumamente dispar, que van del ciberdelincuente de poca monta a la misma NSA, sin que podamos determinar cuando nos situarán bajo su radar. «Presa» no es un predicado que se asuma libremente por el sujeto perseguido. Por el contrario, es un atributo impuesto a la fuerza por el poder que busca darle caza.

Un criptógrafo honesto afirmaba recientemente que «en la actualidad, la seguridad informática consiste fundamentalmente en *resistir* ataques. Todavía no sabemos cómo prevenirlos en su totalidad»[13]. Como no podremos decidir sobre las acciones del rival, solamente nos queda saber anticiparlas, perfeccionando nuestra guardia hasta dominar el penoso arte de saber recibir los golpes, con tal de que ninguno de ellos sea capaz de inducirnos un daño crítico. «Para poder anticipar las reacciones de sus perseguidores, el hombre capturado debe aprender a leer sus propias acciones a través de la mirada de su depredador»[14]. Y es que, aunque los

---

13 Matthew Green: «Secure computing for journalists», *A Few Thoughts on Cryptographic Engineering* (5/3/2017): https://blog.cryptographyengineering.com/2017/03/05/secure-computing-for-journalists.

14 Grégoire Chamayou (2012): *Las cazas del hombre*, Errata

esfuerzos que dediquemos a defendernos puedan llegar a no ser suficientes como para aguantar frente a adversarios perseverantes, habremos dificultado su tarea de manera notable. Incluso acorralados, no tenemos que renunciar nunca a pensar estratégicamente.

Mejorar la resiliencia[15] de nuestro smartphone contra dichos ataques es el horizonte genérico al cual debemos apuntar, aunque esto sea solamente un primer paso todavía insuficiente para afrontar seriamente la cuestión. El teléfono inteligente cumple en primer lugar una función social de intercambio permanente de informaciones con nuestros contactos, lo cual supone un riesgo operacional añadido: al comunicarnos, transmitimos una parte de nuestra información personal al dispositivo de nuestro interlocutor, sobre el cual es poco probable que tengamos el mismo grado de control que sobre el nuestro propio.

Aunque la analogía del combate introduzca algunas buenas intuiciones del pensamiento adversarial, la imagen de dos únicos combatientes en un espacio cerrado pertenece por completo a otro tiempo. Un adversario mínimamente experimentado se aprovecha de la vertiente social de todo ser humano para conseguir sus objetivos. Fragmentos de nuestra identidad, como fotografías y mensajes de voz o de texto, permanecen dispersos en terminales ajenos, algunos incluso en manos de completos desconocidos (por no hablar de las copias de seguridad en la nube –entendiendo por «nube» los servidores de Google u otro proveedor–). Seleccionando los fragmentos apropiados, es probable que un adversario con capacidades notables pueda obtener la misma información que buscaba en un principio sin tener siquiera que ir al encuentro del objetivo original, en el caso de que éste se revelara demasiado resiliente. Así, nuestra meticulosa guardia puede romperse en mil pedazos en caso de que el adversario sepa

---

Naturae, Madrid.

15 La resiliencia, definida por la Real Academia Española, es la capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos.

buscar objetivos alternativos para imponerse, usando nuestro mapa de relaciones como medio para acceder a nosotros.

La información, «el 'recurso' más manipulable y almacenable que ha formulado el ser humano»[16], arrastra consigo un doble filo sumamente peligroso: que, si bien es fácil de transmitir a todo tipo de dispositivos adaptados, es igualmente un recurso sumamente difícil de eliminar del todo. Desde el momento en que transmitimos (nosotros o un intruso) alguna clase de información a otro dispositivo o directamente la subimos a Internet, su distribución queda fuera de nuestro control, independientemente de nuestra voluntad o de que borremos la copia guardada localmente en nuestro terminal. Si algo demuestran incontables efectos Streisand[17] es la imposibilidad material de acallar todo el ruido informacional en un contexto completamente saturado por dispositivos conectados.

Como seres humanos, tendemos a formar grupos de toda clase (formales o informales, permanentes o temporales, cerrados o abiertos, estrictamente «políticos» o no...). Cada tipo de asociación cuenta evidentemente con unos riesgos intrínsecos que, por cuestiones de espacio, no entraremos a detallar. Optaremos mejor por señalar una serie de características generales de la sociología de grupos, que apuntan a riesgos que se repiten necesariamente en todos ellos.

La accesibilidad a la información suele ser una condición indispensable para el correcto funcionamiento de una organización (mensajería instantánea, correos, credenciales de acceso a determinadas cuentas, etc.). No obstante, si la información facilita la coordinación, solamente lo hace a cambio

---

16 G. R. Alonso (2016): *Heidegger ante el PC: La filosofía de la técnica de Heidegger y las nuevas tecnologías*, p. 62.

17 «El efecto Streisand es el fenómeno por el cual un intento de remover o censurar un contenido determinado tiene como consecuencia la difusión mucho más amplia de esa información», en «El efecto Streisand, o por qué es tan difícil censurar contenido en Internet», *Hipertextual* (5/2/2016): https://hipertextual.com/2016/02/efecto-streisand-censura.

de poder replicarse de igual forma en todos los dispositivos integrados, lo que significa que basta con intervenir uno solo[18] para tener acceso a todo. Cada nuevo terminal que se incorpora al ecosistema informacional del grupo le proporciona al adversario un frente de ataque adicional. Pensemos en un grupo de Signal o en una lista de correo: cada uno de los miembros tiene acceso constante a la totalidad de las interacciones publicadas, indistintamente de ser o no el autor del mensaje. Si lo que interesa es hacerse con el contenido que se publica dentro del grupo, el repertorio de ataques es tan variado como dispositivos conectados al ecosistema existan. Y confiar en los dispositivos (atribuirles el calificativo de «seguros») no deja de ser una quimera si no es posible confiar antes en sus dueños: la criptografía no protege de los ataques de ingeniería social, contra los que nadie (mucho menos un grupo) es invulnerable del todo. La falta de compromiso con la integridad del ecosistema de informaciones (sea por simple dejadez, sea por tener al enemigo en casa) amenaza con hacer soluble hasta la mejor arquitectura de seguridad.

Afrontar el desafío planteado por la seguridad en los grupos implica necesariamente establecer una especie de «acuerdo de mínimos» al respecto, que garantice cierto nivel de seguridad en el ecosistema informacional de la organización. «Un sistema de seguridad es tan seguro como el menos seguro de sus elementos» sigue siendo en este caso una regla de oro[19]. Decidir cuál es el umbral mínimo queda en manos de cada grupo, siempre teniendo en cuenta que cuanto más exigente sea éste, mayores serán los problemas relacionados con la exclusión, tanto de personas como de aparatos (dispositivos obsoletos incapaces de asumir el mínimo, dificultad

---

18 Presumiblemente, el «eslabón más débil», un terminal con el sistema operativo desactualizado o con vulnerabilidades conocidas, por ejemplo.

19 La respuesta individual al problema no deja de ser una huida hacia delante cuando los otros miembros no disponen de un nivel de protección similar o no tienen el mismo cuidado transmitiendo información.

de cumplir con todos los compromisos, desconocimiento técnico…). Medidas altamente efectivas, como son habilitar el cifrado de dispositivo o tener el sistema operativo actualizado, son directamente incompatibles con terminales viejos, lo cual alimenta por otro lado el preocupante ciclo de la obsolescencia tecnológica.

Hasta ahora, los grupos han priorizado el acceso general por encima de la seguridad, lo cual ha ido lógicamente en detrimento de la segunda. Por contra, pasar a centrarse en la seguridad no es sin embargo una solución realista para la mayoría de organizaciones, vistos no solamente los problemas de exclusión, sino también la presumible ralentización de los procesos de coordinación. Pero deberíamos poder establecer un umbral mínimo más allá de los grupos de WhatsApp o del almacenamiento en la nube de Dropbox. Urge dar con este punto medio en el que la accesibilidad no sea a costa de renunciar a toda seguridad, si es que eso es posible.

Consejos:

- *No dejes ninguna puerta abierta*. Por cada aparato conectado al ecosistema del grupo que no tenga una contraseña de acceso (pero que tiene acceso a la mensajería o a otro tipo de informaciones), se genera el mismo número de «agujeros negros» de seguridad que bien podrían hacer inútiles todos los demás esfuerzos por mantener cierto nivel de protección.

- *No seas el eslabón más débil*. Cuando tu dispositivo no es seguro, ensanchas la superficie de los ataques dirigidos no solamente contra tu persona, sino también contra tu entorno social. Protege tu smartphone adecuadamente frente a accesos no deseados, actualiza el sistema operativo siempre que se te ofrezca la opción, ten una contraseña de acceso segura y, en caso de usar Android, cifra tanto la tarjeta SD como la memoria interna del teléfono (si fueras usuario de iOS, este último procedimiento no es necesario,

ya que todos los iPhones a partir del 5S tienen habilitado el cifrado por defecto).

- *Nunca dejes de lado la seguridad*. Sabido es que no toda la información que genera un grupo es de dominio público. Indiferentemente del punto en el que se sitúe el umbral de acceso a la información por parte de terceros (sea alto o sea bajo), asegúrate de que exista un compromiso colectivo por mantener a salvo la información calificada como «privada».

- *Aunque incluso un paranoico tenga enemigos reales, no caigas en la paranoia*. Pretender estar a salvo de la NSA o del GCHQ es incompatible con llevar una vida «corriente», usando a diario dispositivos conectados a Internet. Mejor desplegar una defensa eficaz a la hora de anular las capacidades de adversarios reales, que de verdad ambicionan hacerse con la información interna del grupo.

- *Incrementar injustificadamente el umbral de la seguridad exigida no hace a una organización más segura; por el contrario, hace que el error humano sea más probable*. Conforme los protocolos de seguridad del grupo ganan en complejidad, su cumplimiento estricto se hace menos probable, especialmente en círculos no experimentados.

- *No seas un bocazas*. La seguridad en los grupos es el resultado de la suma de compromisos individuales por no exponer la privacidad de los demás miembros. Mantente alerta contra posibles ataques de ingeniería social, los cuales podrían comprometer parcelas de seguridad del colectivo. Nunca hables más de la cuenta en lo que respecta a los asuntos del grupo –una boca demasiado grande bien podría estar allanando el camino al adversario–.

El olvido del mundo

Los formadores en materia de seguridad solemos adoptar una postura en buena parte instrumental («utiliza tal herramienta en vez de tal otra») porque resulta sencilla de hacer entender a la gente de a pie. La experiencia nos dice que lo mejor es empezar presentando una imagen no demasiado compleja de la seguridad, reduciendo deliberadamente el espectro al uso de herramientas alternativas o proveedores seguros. Signal en vez de WhatsApp, ProtonMail en lugar de Gmail. Con el discurso instrumental pretendemos transmitir la idea de que cualquiera que utilice las herramientas apropiadas puede ver mejorada notablemente su seguridad, lo cual es en general correcto. Cuidar las aplicaciones que se instalan, actualizarlas a menudo, administrar bien los permisos. En eso consiste la seguridad móvil, a fin de cuentas.

El discurso instrumental es popular porque es accesible a todos. Su triunfo consiste en dejar de demandar un conocimiento experto para disponer de una buena seguridad; basta con estar usando las herramientas adecuadas, las cuales nos inmunizan contra sucesos inesperados: los peligros existentes pueden atajarse en gran medida cuando tomamos el control sobre nuestro dispositivo, tomando decisiones sobre la configuración de privacidad, instalando solamente aplicaciones de confianza o formulando un complicado código de desbloqueo. Sin embargo, algo fundamental queda suprimido en esta forma de afrontar la cuestión, condenando al discurso instrumental a ser siempre limitado, insuficiente, parcial: que el mundo exterior, el entorno circundante que nos acompaña siempre al utilizar cualquier tipo de dispositivo, queda fuera de nuestro ámbito de actuación, de forma que deja de pensarse en clave adversarial.

Cometemos un error estratégico cuando no prestamos la suficiente atención a la materialidad que nos rodea, sobre la cual es evidente que no gozamos del mismo grado de in-

tervención que sobre nuestros aparatos. Interaccionar con el mundo desplaza al usuario de su posición hegemónica en lo que se refiere al diseño de su sistema de seguridad, puesto que él deja de ser el factor determinante capaz de conducir todas las situaciones. Cada situación se encuentra atravesada por infinitas variables que no pueden decidirse de antemano, de modo que deja de ser presumible que el usuario pueda preverlas con vistas a obtener siempre el mejor beneficio para su seguridad. Es cuando lo imprevisto entra en escena que las cosas pasan a un nuevo plano de complejidad: independientemente de nuestros conocimientos en materia de seguridad, nunca podremos seleccionar el tipo de ataque que queremos que nuestro adversario ejecute contra nosotros, ni tampoco el momento (probablemente porque eso lo anularía como adversario). El mundo exterior hace imposible el estado de seguridad absoluta, que solamente puede recrearse artificialmente en el laboratorio de lo instrumental.

Por complejo que pueda llegar a ser, todo sistema de seguridad es una precaria estructura flotante en el mar de la incertidumbre, navegando sin rumbo en una realidad que siempre lo acaba superando. Ya sea por el contexto político o legal, por las personas encargadas de administrarlo o por las capacidades ofensivas del adversario, nunca dejaremos de enfrentarnos a torsiones no esperadas del movimiento original, el cual se corresponde con nuestro estado ideal de seguridad. Un simple descuido al escribir el código de desbloqueo es capaz de echar por tierra toda nuestra sofisticada arquitectura de seguridad, mientras que la mala suerte puede convertirnos en candidatos a un serio interrogatorio en el que acabemos entregando nuestras claves e información.

Con esto venimos a decir que, como formadores, el discurso instrumental no es suficiente. Que la recreación de parcelas virtuales aparentemente «seguras», desprendidas por completo de nuestra realidad material, es un proyecto abocado al fracaso. La crítica que se le suele dirigir a los sistemas de seguridad basados en la biometría[20] es en realidad igualmen-

---

20 La biometría es la disciplina encargada del estudio de las

te aplicable a la mirada instrumental: que solamente pueden atribuirse el calificativo de «seguros» a cambio de pecar del olvido de su realidad física. Que tu huella dactilar sea la única llave para desbloquear tu teléfono es en efecto la medida de protección más segura… únicamente en un mundo en el cual nadie pueda forzarte físicamente a introducirla, aun sin tu consentimiento. Es decir, una situación ideal que *no puede existir*, puesto que sólo se puede dar en caso de suprimir físicamente cualquier contacto humano. Lo mismo sucede con la perspectiva instrumental: solamente podríamos llegar a convencernos de su efectividad real a cambio de asumir el ideal cibernético de un espacio en el cual tenemos el lujo de decidir *in vitro* sobre cada uno de los procesos, es decir, eliminando de nuestro esquema la persistente irreductibilidad del mundo exterior, que no se deja dominar.

Consejos:

- *Aspira a desarrollar una inteligencia de la situación*. El grado de efectividad real de cualquier sistema de seguridad depende de tu propia capacidad de hacer frente a situaciones no previstas de antemano. Ten una cautela adicional cuando utilices el teléfono en espacios públicos o lugares con una gran afluencia de personas, especialmente cuando vayas a desbloquearlo, intercambies mensajería o introduzcas contraseñas. Disminuir el brillo en este tipo de situaciones es una buena medida de prevención.

- *Relativiza tu propia arquitectura de seguridad*. La seguridad de un smartphone es sumamente volátil, dado que en nuestro día a día existen situaciones inesperadas en las que todas las medidas preventivas pueden acabar siendo inútiles (sustracción del dispositivo desbloqueado, pérdida, ingeniería social, que tu adversario descubra el patrón de desbloqueo o te fuerce físicamente a introducirlo…). Conviene alejarse de un optimismo excesivo en lo que

---

propiedades corporales únicas de los seres biológicos.

respecta a la supuesta condición de impenetrabilidad de cualquier aparato que llevemos con nosotros de manera diaria. Y la mejor forma de prevenirse de ello es delegando la menor información posible en el teléfono.

- *Desconfía del discurso instrumental puro.* A menudo, el discurso instrumental tiende a minusvalorar los aspectos sociales de la seguridad, lo que conlleva un serio riesgo añadido cuando se trata de dispositivos móviles (más proclives a situaciones imprevistas por su condición portátil). Las mejores herramientas son necesarias para una buena seguridad, pero por sí solas nunca han bastado para conseguirla.

DE LA SEGURIDAD OPERACIONAL A LA SEGURIDAD INSTRUMENTAL:

CONSEJOS GENERALES

Una vez introducidos los principios de seguridad operacional, es hora de adentrarse en la parte instrumental, entendiendo las distintas amenazas que se ciernen sobre nuestro dispositivo y la información que contiene. En este capítulo hablaremos brevemente sobre la tecnología de telefonía móvil y lo que implica, trataremos medidas de mitigación de adversarios que pueden acceder física o remotamente a nuestro terminal e introduciremos conceptos básicos de privacidad en nuestros smartphones, desde el control de permisos de aplicaciones hasta las redes sociales.

Breve introducción a la red telefónica

El uso de un smartphone conlleva, consecuentemente, el uso de la red de telefonía móvil. Esta red es la que nos permite realizar y recibir llamadas, enviar y recibir SMS, y más recientemente, acceder a Internet.

Para poder entender las amenazas y los riesgos que supone el uso de un smartphone, es imprescindible conocer algunos conceptos básicos de esta tecnología, y las consecuencias inherentes a su uso.

Una de las primeras cosas que debemos saber es que el uso de las funciones de telefonía de nuestro teléfono (llamadas, SMS y «datos») implica que un teléfono móvil, y por ende la persona que va con él, debe estar *permanentemente* localizado por su proveedor de telefonía (Movistar, Vodafone, etc.).

Esto se debe al diseño de la propia tecnología de telefonía móvil, que se compone de antenas (o «torres») repartidas por toda la geografía a las que nuestros móviles se conectan para comunicarse los unos con los otros.

No será algo nuevo para la persona que lea este libro el hecho de que para poder realizar una llamada de calidad, por ejemplo, es necesario «tener buena cobertura». Dicha cobertura es precisamente la calidad de la conexión del móvil con una antena de telefonía.

Para poder enrutar[21] las llamadas, mensajes y paquetes de datos hacia los móviles, la compañía telefónica debe saber en todo momento a qué antena está conectado el teléfono, o no sabría cómo hacer llegar esta información a los terminales.

Por este sencillo motivo, el uso de un terminal móvil, *independientemente de si es smartphone o no*, conlleva la monitorización de la localización física aproximada por parte del proveedor y de aquellos terceros a los que dicho proveedor proporcione acceso.

Esta circunstancia debe evaluarse también desde un punto de vista colectivo. Se puede deducir que dos o más personas se desplazan juntas si sus teléfonos se van conectando a las mismas antenas al mismo tiempo a medida que se mueven.

Además de tenerte permanentemente geolocalizado, tu compañía telefónica tiene acceso al contenido y metadatos de tus SMS y llamadas, así como a algunas partes de tu navegación web, como qué sitios visitas, cuándo y desde dónde.

Existen algunas publicaciones muy representativas de esta intromisión en nuestra vida privada, intrínseca al diseño de la tecnología móvil. Una de ellas, realizada por Malte Spitz, eurodiputado del partido verde europeo, publicó los datos recopilados por su operador de telefonía durante seis meses del 2009. La representación visual del trabajo de Spitz es un muy buen ejemplo de cómo estos datos son recopilados de todos los usuarios de forma silenciosa[22].

Llevar un teléfono móvil en el bolsillo, sea cual sea el modelo, conlleva una situación de rastreo permanente, que todo el que se preocupe por su privacidad debería tener en cuenta.

---

21 Enrutar: calcular el camino que debe realizar la información que viaja de un terminal a otro.

22 La publicación puede ser consultada en: https://www.zeit.de/datenschutz/malte-spitz-data-retention.

Protección frente al acceso físico

Esta parte comprende un conjunto de medidas que tienen un único objetivo: garantizar en la mayor medida posible que la información y las funcionalidades de tu smartphone no sean accesibles a terceros, en el caso de que se hallara físicamente en su poder.

Para ello deberemos entender cuáles son los ataques que se pueden realizar sobre nuestro terminal cuando está en las manos de otra persona y qué configuraciones podemos aplicar para mitigar dichos accesos ilegítimos.

Desbloqueo seguro

Existen diversas maneras de proteger el desbloqueo de nuestro teléfono: patrones, pines, contraseñas y, en los últimos años, incluso medidas biométricas.

Es muy importante proteger el desbloqueo con alguna de estas medidas. La carencia de esta protección ante el desbloqueo hace que el acceso a la información de nuestro dispositivo sea extremadamente fácil.

Una vez establecido esto, la siguiente cuestión a resolver es: ¿cuál es el método más seguro? Como en muchas otras cuestiones de seguridad, la respuesta es «depende». Vamos a revisar los pros y los contras de los métodos más habituales.

- **Patrón de desbloqueo**. El patrón de desbloqueo, muy popular entre los usuarios de Android, tiene varias características que disminuyen su eficacia como sistema de protección, en concreto:
    - *Trazas en la pantalla*. La grasa presente en nuestros dedos deja trazas en la pantalla, que pueden servir para reconstruir fácilmente el patrón de desbloqueo utilizado.
    - *Fácilmente visibles y recordables*. Es relativamente sencillo para un tercero malintencionado averiguar

cuál es el patrón de desbloqueo del terminal simplemente mirando por encima del hombro.

- *Alfabeto reducido e imposibilidad de repetición.* Los patrones normalmente están compuestos por nueve puntos que no se pueden repetir, ofreciendo un número más reducido de combinaciones que el que posibilitan los demás métodos.

- **PIN numérico**. Otra opción muy utilizada, especialmente por los usuarios de iPhone. Tiene la desventaja de tener un alfabeto muy reducido (0123456789), que podemos compensar usando pines largos, de diez cifras o más.

- **Contraseña**. Tiene la ventaja de tener un alfabeto amplio (mayúsculas, minúsculas, números y símbolos), pero es menos usable que un PIN o un patrón, ya que normalmente tardaremos más y cometeremos más errores al introducirla.

- **Desbloqueo biométrico**. Este tipo de desbloqueo se diferencia de los demás en un concepto fundamental: los patrones, pines y contraseñas son algo que *sabes*. La biometría, en cambio, es algo que *eres*. Por tanto, mantener la biometría bajo control es más complicado que mantener una buena contraseña bajo control. Pongamos por ejemplo el desbloqueo por huella dactilar. Dejamos nuestras huellas literalmente en todo lo que tocamos, y además nuestro adversario podría desbloquear nuestro dispositivo sin nuestro consentimiento mediante el uso de la fuerza, obligándonos a poner el dedo sobre el sensor.

El mejor método de desbloqueo dependerá de nuestro modelo de amenaza: una contraseña o PIN es un sistema robusto si es lo bastante complejo y si nuestro adversario no es capaz de obtenerlo por otras vías. Un desbloqueo biométrico es un sistema robusto si nuestro adversario no es capaz de capturar y reproducir nuestra biometría, o de forzarnos a utilizarla. A

la hora de escoger un sistema, es importante pararse a pensar: ¿de qué o de quién me estoy defendiendo?

Cifrado de memoria

Hoy en día es imprescindible proteger criptográficamente la memoria de nuestros dispositivos. De este modo, garantizamos que la información contenida en dichos dispositivos no puede ser accedida sin el conocimiento de la contraseña que permite el descifrado de dicha información.

Esto es diferente a utilizar un PIN de desbloqueo de pantalla. Al cifrar la memoria del teléfono, estamos protegiendo la información de un tipo de ataque más sofisticado: incluso si la memoria es copiada mediante equipo especializado, no se podrá leer la información que contiene si no se dispone de la clave de cifrado.

Los dispositivos iPhone incorporan cifrado de memoria por defecto, pero en el caso de los dispositivos Android, ésta debe ser activada manualmente, para lo que es necesario tener la batería cargada al 100 % y tener el teléfono conectado a un cargador. Además, no todos los modelos de Android soportan cifrado de memoria.

Normalmente encontraremos la opción para cifrar nuestro teléfono Android en la aplicación de *Ajustes*, bajo la opción *Seguridad*. Una vez en este menú, sencillamente pulsaremos *Cifrar teléfono* y seguiremos los pasos indicados. Es altamente recomendable realizar un respaldo de seguridad de nuestros datos antes de habilitar el cifrado de memoria.

Filtración de información a través de la pantalla o altavoces

En ocasiones, determinadas configuraciones pueden ceder a nuestro atacante información confidencial. Es el caso de la previsualización de notificaciones, que permite al usuario ver el contenido de los mensajes desde la pantalla de bloqueo, sin necesidad de desbloquearlo.

Esto podría suponer no sólo el compromiso del contenido de una conversación confidencial, sino que podría permitir a un atacante sortear la autenticación de dos factores de algunos servicios o aplicaciones, viendo por ejemplo el código de seguridad recibido en un SMS, lo que le podría dar acceso a cuentas o permitir realizar otras acciones maliciosas.

Es importante asegurarnos de que el contenido de las notificaciones generadas en nuestros terminales sólo es visible si el terminal está desbloqueado.

Otro aspecto que tenemos que tener en cuenta en relación a la pantalla del móvil es la presencia de mirones cuando introducimos nuestras contraseñas, PIN o patrón de desbloqueo. Medidas como disminuir el brillo de la pantalla o utilizar pantallas de privacidad pueden ayudar a mitigar esta amenaza.

Una pantalla de privacidad es una pequeña pieza de plástico polarizado que se sitúa sobre la pantalla del móvil, permitiendo ver el contenido de la misma solamente a quien se halla justo en frente del terminal, y no a las personas que hay a su alrededor. Es una buena contramedida frente al acceso físico no autorizado, ya que dificulta mucho a nuestro adversario averiguar cuál es la contraseña de desbloqueo.

También es importante desactivar asistentes de voz como Siri (iPhone), que permiten interactuar con el teléfono incluso estando bloqueado, pudiendo acceder a mensajes o últimas llamadas y mostrarlas en pantalla.

Rooteo y jailbreak

A aquellas personas que quieren liberar todo el potencial de sus dispositivos les será familiar la práctica del *rooteo* (Android) o del *jailbreak* (iPhone). Estas prácticas permiten acceder a funcionalidades que están bloqueadas por defecto en nuestros terminales, como la posibilidad de acceder como usuarios administrativos.

Pese a las ventajas que tiene disponer de un dispositivo en estas condiciones, desde el punto de vista de la seguridad debemos plantearnos cuáles son las consecuencias de tener el acceso administrativo habilitado en nuestro teléfono.

Está claro que desde un punto de vista de soberanía tecnológica, ganar nivel administrativo en nuestro terminal, ejecutar cualquier tipo de *software* sin restricciones, eliminar programas privativos no deseados e incluso instalar sistemas operativos personalizados es algo que empodera al usuario. Sin embargo, ¿qué pasa cuando nuestro terminal modificado ha caído en manos de un tercero?

El nivel administrativo en un terminal móvil permite hacer una copia bit a bit de toda la memoria del teléfono. Esto significa que quien tenga acceso al teléfono móvil, si consigue desbloquearlo podrá acceder a muchísima más información que si no se hubiera modificado, incluso a datos que hayan sido borrados. Información como historiales de localización, navegación, datos privados de aplicaciones y del sistema operativo que de otra manera serían inaccesibles. Esto es especialmente cierto en el caso de Android, no tanto en el caso de iOS.

En iOS, se puede realizar un *backup* completo del teléfono si se tiene la capacidad de desbloquearlo. Mensajería, datos sensibles, contactos… Todo puede ser extraído y copiado por un adversario que pueda desbloquear el terminal. El nivel administrativo no permitiría acceder a archivos eliminados en iOS, porque el cifrado se realiza a nivel de archivo. El *jailbreak* sólo le daría una ventaja a nuestro oponente, que es la de poder instalar *malware* en el teléfono de forma más sencilla.

Debemos sopesar bien las ventajas y desventajas de *cacharrear* con nuestro smartphone, ya que puede suponer un gran descenso en la seguridad de nuestra información. Nuestro consejo es sólo realizar estas prácticas cuando se conoce bien lo que se está haciendo, lo que se pone en riesgo y se extreman las medidas de seguridad para protegerlo.

Definiendo nuestro sistema de protección frente a acceso físico

A la hora de protegernos es imprescindible preguntarse: ¿de qué me estoy protegiendo? En otras palabras, debemos definir a nuestro adversario, de acuerdo con sus capacidades. Como en tantas otras ocasiones, la respuesta correcta pasa por hacerse la pregunta adecuada:

- ¿Puede mi adversario observarme desbloquear el teléfono antes de ganar acceso físico a él?
- ¿Puede mi adversario obligarme o coaccionarme para desbloquear el dispositivo?
- ¿Mi adversario puede recoger muestras biométricas (huellas, iris, fotografías) para desbloquear el dispositivo con ellas?
- ¿Mi adversario cuenta con conocimientos o medios especializados para el desbloqueo por fuerza bruta[23] de mi dispositivo?

Si la respuesta a estas preguntas es afirmativa, seguramente la mejor opción es la de utilizar una buena contraseña, en combinación con un polarizador de pantalla, cifrado de me-

---

23 Desbloqueo por fuerza bruta: ataque consistente en ir probando contraseñas automáticamente hasta dar con la correcta.

moria y previsualización de notificaciones desactivada, en un dispositivo actualizado y sin acceso administrativo habilitado.

Además, en el caso de utilizar una contraseña, es altamente recomendable cambiarla regularmente, ya que cuanto más tiempo se lleve usando, más probable es que haya sido comprometida.

Protección frente al acceso remoto

Otro de los aspectos que nos debe preocupar respecto a la seguridad de nuestro smartphone es el de si un atacante puede acceder a nuestros datos de forma remota. Es decir, sin acceder físicamente al terminal.

Al igual que con el acceso físico, conocer las diferentes posibilidades y defensas nos permitirá escoger la mejor estrategia para proteger nuestra información y comunicaciones.

Origen y estado de las aplicaciones

Uno de los puntos más importantes para evitar que nuestro teléfono acabe siendo controlado remotamente por terceros malintencionados, es instalar aplicaciones de proveedores y canales de comunicación fiables y mantenerlas siempre actualizadas.

Imagina por un momento el terrorífico escenario de una aplicación usando tu cámara y micrófono para verte y escucharte en directo cuando piensas que el teléfono está bloqueado o incluso apagado. Desgraciadamente, es un escenario perfectamente viable si no vigilamos qué tipo de aplicaciones nos instalamos, desde dónde, y si no mantenemos nuestros dispositivos actualizados.

Hablemos primero de los canales de distribución de aplicaciones: Google Play y F-Droid en el caso de Android, y App Store en el caso de Apple.

Android

En Android, por defecto, sólo podemos descargarnos aplicaciones que provengan de Google Play, la tienda oficial de Google de aplicaciones para Android. No obstante, este sistema operativo brinda al usuario la posibilidad de instalar aplicaciones de terceros o de *fuentes desconocidas*, habilitando esta opción desde el panel de ajustes. Esto ha posibilitado la proliferación de mercados alternativos a Google Play y también de versiones troyanizadas[24] de aplicaciones oficiales, fácilmente instalables desde fuentes poco fiables.

En este sentido, los usuarios de Android cuentan con más libertad que los de iPhone a la hora de escoger sus aplicaciones y su canal de distribución de *apps*, pero esto les obliga a estar alerta cuando descargan aplicaciones desde fuera de Google Play.

Incluso cuando descargamos aplicaciones desde Google Play no podemos tener la seguridad de estar cien por cien a salvo. Dentro de esta tienda han aparecido en muchísimas ocasiones aplicaciones maliciosas en forma de juegos y otros elementos atractivos que invitan a su descarga por parte de los usuarios.

Críptica defiende desde sus orígenes el software libre y de código abierto como mejor solución a las aplicaciones malintencionadas y recomienda su uso en la medida de lo posible. Existe una tienda alternativa a Google Play, llamada F-Droid, que sólo distribuye aplicaciones de código abierto para Android. Puedes leer más información sobre este repositorio en el capítulo de reseñas de aplicaciones en la página 118.

En la línea de todo lo que se ha dicho, debemos extremar la precaución con los enlaces de descarga de aplicaciones que recibamos vía SMS, correo electrónico o similar. *Nunca debemos instalar aplicaciones de fuentes desconocidas.*

---

24 Un troyano es un programa o aplicación que permite el control remoto no autorizado del dispositivo de manera oculta.

iPhone

Los usuarios de iPhone, a diferencia de los de Android, no tienen opción a la hora de escoger el origen de sus aplicaciones: deben ser obligatoriamente de la App Store. La única manera de instalar aplicaciones desde otros orígenes es mediante el ya mencionado *jailbreak* u obteniendo una licencia de desarrollador para tu dispositivo, que cuesta 99 dólares al año.

Esta filosofía cerrada resta libertad a los usuarios a la hora de escoger qué es lo que quieren ejecutar en sus terminales, pero limita también la cantidad de opciones disponibles para que los atacantes consigan colocar su *malware* en estos dispositivos.

Esto no significa que no haya *malware* en la App Store. Debemos escoger siempre con cuidado qué es lo que instalamos y decidir si confiamos en los desarrolladores de la aplicación.

En este sentido, al igual que en Android recomendamos encarecidamente el uso de aplicaciones de software libre y código abierto, como las que aparecen en la sección de reseñas.

Actualizaciones

No sólo debe preocuparnos de quién y de dónde descargamos las aplicaciones que ejecutamos en nuestros móviles, también debemos preocuparnos por mantenerlas actualizadas. Las actualizaciones no sólo incluyen funcionalidades nuevas en las *apps*, sino que también solucionan aquellos problemas de seguridad que se van descubriendo con el tiempo. La única manera de minimizar los agujeros de seguridad de nuestras aplicaciones es mantenerlas siempre actualizadas.

Asimismo, es igualmente importante mantener actualizado nuestro sistema operativo, ya que de esta manera se solucionan también aquellos problemas de seguridad que pueda tener, una vez han sido descubiertos. Prácticamente cada semana se publican nuevas vulnerabilidades que podrían comprometer seriamente la seguridad del terminal (acceso re-

moto e ilegítimo), de ahí que sea fundamental estar al día de cada actualización publicada, en vez de posponerla indefinidamente.

Esto es especialmente problemático en el ecosistema de Android, ya que normalmente dispondremos de actualizaciones durante entre uno y tres años desde la salida del dispositivo al mercado, dependiendo de la marca. Apple, por otro lado, ofrece entre cuatro y cinco años de soporte para los dispositivos iPhone.

Comunicaciones seguras: cifrado de comunicaciones

Nuestros smartphones son, en esencia, dispositivos de comunicación. Y por tanto, otro aspecto a tener en cuenta a la hora de protegernos de accesos remotos es el de si nuestras comunicaciones están protegidas adecuadamente. ¿Puede un atacante ver el contenido de mis mensajes? ¿Puede escuchar mis llamadas? ¿Puede modificar el contenido de los paquetes que viajan por Internet cuando visito una web?

Todas estas acciones son posibles para un atacante que cuente con las condiciones adecuadas. Debemos, por tanto, asegurarnos de utilizar las herramientas adecuadas para proteger la información que viaja desde y hacia nuestro smartphone, para que nadie pueda acceder a ella o modificarla con fines maliciosos.

Navegación web: HTTPS y el candado verde

A la hora de navegar, debemos saber que existen dos protocolos para visitar una página web: HTTP y HTTPS. Los protocolos no son más que el «lenguaje» que habla nuestro navegador con el servidor web para poder descargar una página determinada.

La diferencia entre usar HTTP y HTTPS es simple: cuando utilizamos HTTP, los mensajes que envía nuestro navegador al servidor web y viceversa viajan «en claro». Es decir, toda información que enviemos y recibamos del servidor viaja como

si de una postal se tratase, pudiendo ser vista (y modificada) por todos aquellos lugares por donde pasa. El navegador no tiene manera de garantizar que la información enviada o recibida no haya sido registrada o alterada por terceras partes. Tampoco puede verificar la identidad del servidor web, con lo que no hay ninguna garantía de que se esté visitando el lugar que el usuario cree que está visitando.

HTTPS pretende solucionar estos problemas, haciendo que la comunicación entre navegador y servidor sea cifrada, garantizando la confidencialidad de la información durante su viaje. Además, este protocolo también garantiza que la información no ha sido alterada y permite al navegador verificar que realmente se está visitando la página que el usuario cree que está visitando. En estas ocasiones, el navegador nos mostrará un candado verde junto a la dirección.

Asimismo, siempre que vayamos a introducir información sensible en una página (contraseñas, mensajes privados, números de cuenta...), debemos asegurarnos de que se muestra el candado verde junto a la dirección de la página y de que el nombre del dominio que visitamos es correcto. Pongamos por ejemplo que un atacante ha registrado el dominio «mibacno.com» con la intención de conseguir contraseñas de usuarios de «mibanco.com». Al controlar el atacante el dominio, puede configurar un servidor web adecuadamente para que cuando un usuario despistado lo visite y vea el candado verde piense que esté visitando «mibanco.com», cuando en realidad la dirección es «mibacno.com». Por eso es importante asegurarse de que la dirección está bien escrita, especialmente cuando hemos visitado un enlace que nos ha proporcionado un tercero. Este tipo de ataques donde el atacante suplanta la identidad de un sitio legítimo se conoce como *phishing*.

Redes no confiadas: VPN

En ocasiones nos conectamos a redes wifi en cafeterías, hoteles u otros lugares donde no sabemos si hay atacantes al acecho. Incluso la propia red wifi podría haber sido desple-

gada con intenciones maliciosas. Con el fin de dotar de una capa de seguridad a nuestras comunicaciones en estos entornos desconocidos, podemos utilizar una VPN[25].

En el capítulo de reseñas de aplicaciones del libro, en la página 130, encontrarás cómo utilizar una aplicación que permita a tu smartphone conectarse a una de estas redes y darte una capa extra de seguridad y privacidad.

Comunicación instantánea: cifrado de extremo a extremo.

Los SMS y las llamadas tampoco están exentos de peligros. Nuestro proveedor de telefonía tiene la capacidad (a nivel técnico) de escuchar nuestras llamadas y leer nuestros SMS, los cuales quedan almacenados por ley durante doce meses[26]. Por tanto, si queremos proteger la confidencialidad de nuestras comunicaciones frente a un adversario con dichas capacidades, deberemos utilizar alternativas de comunicación instantánea que utilicen cifrado de extremo a extremo (*end-to-end encryption*).

El cifrado de extremo a extremo es una medida de protección que consiste en que sólo los extremos de la comunicación (es decir, los smartphones u ordenadores que se comunican) disponen de las claves necesarias para descifrar la información que están intercambiando. Ningún elemento intermedio (proveedores de telefonía, Internet, mensajería, VoIP, NSA…) puede descifrar esta información, ya que no dispone de la clave. Es un grandísimo ejemplo de la llamada *privacidad por diseño*, que garantiza a nivel técnico que nuestra información sólo puede ser accedida por quien se supone que debe acceder a ella.

---

25 VPN, Virtual Private Network: una red VPN cifra todo el tráfico entrante y saliente de nuestro dispositivo y lo enruta a través de una localización de confianza, de manera que aunque estemos en una red no confiada, ningún atacante será capaz de ver o alterar el contenido de los mensajes.

26 Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

En la página 108 encontrarás una comparativa entre distintas alternativas de comunicación instantánea, con sus respectivos pros y contras.

Contraseñas y 2FA

Otra manera en la que un atacante podría obtener acceso remoto a nuestra información es accediendo de forma ilegítima a una de nuestras cuentas (correo electrónico, redes sociales, etc.). Es por eso por lo que es muy importante conocer qué medidas de protección podemos utilizar para evitar este escenario.

La medida de protección básica que protege el control de cualquiera de nuestras cuentas es la contraseña. Escoger nuestra contraseña adecuadamente es por tanto algo importante. Una frase recurrente en nuestras charlas es que una contraseña es como la ropa interior: no la reutilices, no la compartas y no la dejes a la vista.

Una contraseña debe ser única para cada cuenta, debe ser secreta y robusta: no utilices elementos públicos de tu vida, como fechas, nombres o lugares. Escoge frases o palabras al azar, e intenta hacerlas largas e impredecibles.

Una vez has generado y aplicado una contraseña segura, hay varios aspectos a tener en cuenta a nivel de usabilidad y seguridad. El primero y que seguramente te estás preguntado es: ¿cómo recuerdo todas esas contraseñas?

El mejor modo es no tener que recordarlas: utiliza un gestor de contraseñas como KeepassDroid (o KeePassX, en tu PC). Encontrarás una reseña de KeepassDroid en nuestro capítulo de aplicaciones. Estos gestores permiten proteger todas tus contraseñas de forma ordenada y segura, con una única clave maestra, de manera que puedes desbloquearlas y consultarlas siempre que lo necesites.

Otro aspecto a tener en cuenta en la gestión de nuestras contraseñas es el referente a las medidas de protección que puedan tener las bases de datos de nuestros proveedores de servicios. Cada año somos testigos de como varios proveedores sufren ataques y brechas de seguridad en las que se ven comprometidas cientos de miles de contraseñas: Adobe, LinkedIn,

PlayStation... El hecho de no reutilizar claves te protege de que incluso si un atacante llega a descubrir cuál es la tuya en un servicio, no pueda utilizarla para acceder a tus otras cuentas. Si, por el contrario, tienes una misma contraseña que usas para todo, en caso de que alguien se hiciera con ella ganaría un acceso integral a tu identidad *online* (solamente tendría que introducirla en los distintos servicios).

Dicho esto, hay dos medidas que se pueden aplicar para protegernos de estas brechas de seguridad:

- Cambiar las contraseñas frecuentemente. Esta medida mitiga el riesgo de que accedan a nuestras cuentas al cabo de un determinado tiempo de haberse producido la brecha, ya que la contraseña ya no será válida. Tiene un elevado coste de usabilidad, sobre todo si tenemos muchas contraseñas.

- Utilizar autenticación de dos factores o 2FA. A la hora de proteger el acceso a una cuenta, existen tres factores que se pueden utilizar para verificar tu identidad: algo que sólo tú sabes (contraseña, PIN), algo que sólo tú tienes (tarjeta, móvil) o algo que sólo tú eres (biometría). La autenticación 2FA implica utilizar dos de estos factores para proporcionarte acceso a tus cuentas. El caso más habitual es el de usar una contraseña más un código recibido vía SMS o aplicación en nuestro smartphone. Este tipo de medida es efectiva frente a un adversario que controla nuestra contraseña pero no nuestro teléfono, aunque tiene el coste de revelar nuestra identidad real (vinculada a nuestro teléfono) al proveedor del servicio que queremos proteger. Debemos escoger en cada caso si preferimos gozar de más anonimato o de una capa adicional de seguridad en el acceso a nuestras cuentas.

Un servicio muy útil a la hora de descubrir si nuestras contraseñas han sido comprometidas es https://haveibeenpwned.com. En esta página podrás consultar si tu cuenta de correo

ha aparecido en una filtración de alguna base de datos, y por tanto si tu contraseña puede haber sido comprometida o no.

Protección de la privacidad

Desde el punto de vista de la privacidad, el ecosistema de los smartphones es una auténtica pesadilla. Contactos, SMS, llamadas, localización... Gran parte de la información que acumula nuestro terminal puede ser accedida y recopilada por una infinidad de aplicaciones. Por eso es especialmente importante examinar detenidamente las capacidades de las *apps* que vayamos a instalar.

La fiebre de las apps

Hay una *app* para todo. Cualquier servicio que puedas pensar, desde el más útil hasta el más estúpido, hay una aplicación para ello. Es una clara tendencia: todo lo que antes se hacía vía web, ahora se hace vía *app*.

Y esta aparentemente pequeña diferencia entre una web y una aplicación es en realidad muy grande. Cuando visitamos una página web, la información que ésta puede recopilar sobre nosotros es sustancial pero limitada. Además de los datos que introduzcamos en la web, puede recopilar información como nuestra dirección IP, navegador, sistema operativo, idioma, *cookies* que permitan correlacionar con actividad previa o futura... Pero todos estos aspectos son fácilmente protegibles mediante el uso de Tor o VPN (encontrarás aplicaciones para usar estos servicios en el capítulo de reseñas) o complementos de navegación. Las *apps*, en cambio, están hechas de otra pasta.

Una aplicación puede llegar a acceder a prácticamente toda la información y sensores de nuestro teléfono si tiene los permisos adecuados: identidad, contactos, información del wifi, localización GPS, SMS, llamadas e incluso micrófono o cámara.

La información que recopila una aplicación es por tanto mucho mayor, y como usuarios debemos decidir con cuidado qué aplicaciones tienen acceso a qué datos en nuestro teléfono.

Aplicaciones: recuperando la privacidad

Desde el punto de vista de las aplicaciones, hay dos cosas que como usuarios podemos hacer para mejorar la privacidad en nuestro smartphone:

- Control de permisos de nuestras aplicaciones.
- Utilizar aplicaciones respetuosas con nuestra privacidad.

Control de permisos

Tanto Android como iPhone ofrecen la posibilidad de autorizar o denegar permisos a las aplicaciones, de manera que se puede controlar el acceso a diferentes aspectos de nuestro smartphone de forma más o menos granular.

En ocasiones encontraremos aplicaciones que son extremadamente invasivas en cuanto a los permisos que solicitan. Hay aplicaciones que incluso dejarán de funcionar correctamente cuando desactivemos ciertos permisos. A veces se debe a que necesitan dicho permiso para hacer su función, pero en otras es un mero chantaje para acceder a tus datos.

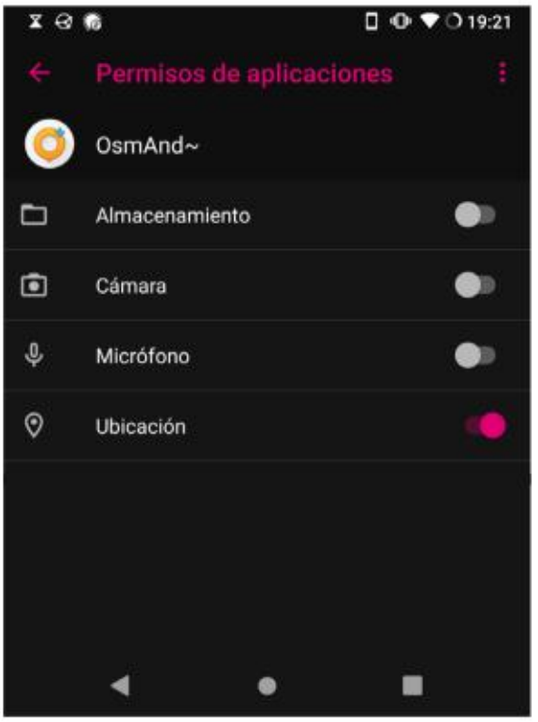
En estas ocasiones, está en la mano del usuario decidir si cede o si busca una aplicación alternativa, respetuosa con su privacidad.

En Android podemos controlar los permisos aplicación por aplicación a partir de la versión 6.0, desde el menú de aplicaciones[27]. Si nos dirigimos a *Ajustes* > *Aplicaciones*,

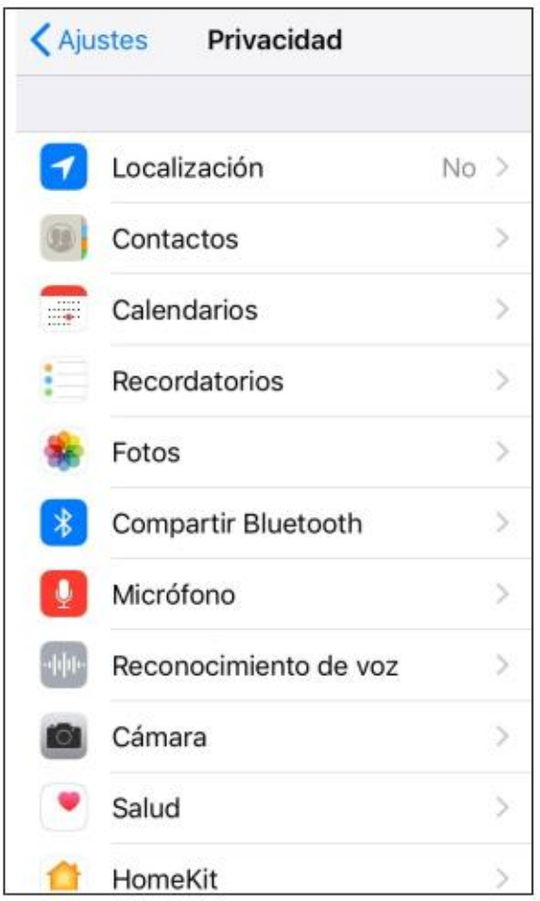
---

27 Esto podría cambiar en un futuro: algunas versiones de Android ya permiten controlar los permisos a nivel general, a la manera de iOS.

podemos ver todas las aplicaciones instaladas. Para gestionar los permisos de cada aplicación, pulsaremos sobre ella y luego sobre *Permisos*. En este panel podremos consultar qué permisos están activos y denegar o permitir aquéllos que queramos.



En iOS, por otro lado, el control de permisos se realiza a nivel general, en vez de a nivel de aplicación. Para gestionar los permisos, debemos dirigirnos a *Ajustes* > *Privacidad*. En este menú encontraremos cada uno de los permisos que se pueden conceder a las aplicaciones, y pulsando sobre ellos podremos gestionar qué aplicaciones pueden gozar de cada uno.



Aplicaciones respetuosas con la privacidad

Existen multitud de alternativas para muchos de los servicios y aplicaciones invasivas que usamos cada día, aunque en este sentido, en Android encontraremos muchas más que en iOS.

Al principio de este libro explicamos cuáles son nuestros criterios para proponer estas alternativas, y al final del mismo encontrarás un apartado de reseñas de aplicaciones que si-

guen dichas directrices. Descubrirás alternativas a Google Maps, Calendar, WhatsApp…

Cabe mencionar que, igual que iOS ofrece un cifrado de memoria a nivel de archivo y por defecto, en Android encontraremos un ecosistema de aplicaciones respetuosas con la privacidad considerablemente más grande.

Navegación y privacidad

Una vez abordado el tema de las *apps*, pasemos a cómo podemos mejorar nuestra privacidad cuando navegamos desde nuestro smartphone.

Para navegar, recomendamos utilizar un explorador con licencia libre y una filosofía respetuosa con la privacidad, como Firefox. Además, Firefox cuenta con multitud de complementos que dificultan la monitorización a la que estamos sometidos cuando navegamos[28]. Estos complementos son:

- **uBlock Origin**. Bloquea los anuncios y por tanto los *trackers*[29] que llevan incorporados para monitorizar nuestra actividad.

- **Privacy Badger.** Bloquea *trackers* presentes en las páginas que visitemos. Nos otorga un control granular de qué programas de terceros queremos permitir o bloquear.

- **Cookie AutoDelete**. Destruye las *cookies* descargadas por una página en cuanto cerramos la pestaña.

- **HTTPS Everywhere**. fuerza la conexión por HTTPS siempre que sea posible.

---

28 Podemos descargar e instalar todos los complementos mencionados desde https://addons.mozilla.org.

29 Se denomina *tracker* a la técnica que utilizan algunos sitios web para hacer un seguimiento de la actividad del usuario a través de múltiples páginas sin que éste sea consciente de ello.

Si queremos una capa extra de privacidad, podemos también anonimizar nuestra IP de origen usando una VPN o Tor, a costa de perder velocidad de navegación. Habrá ocasiones en las que queramos tener una navegación lo más anónima posible, y es en estos escenarios donde podemos usar estos servicios.

Puedes encontrar reseñas de OpenVPN y Tor Browser en el capítulo de reseñas.

Protección de la accesibilidad

Un aspecto nada desdeñable de la seguridad de nuestros datos es la accesibilidad a nuestra información. Dicho en otras palabras, la capacidad de seguir accediendo a nuestros datos cuando lo necesitemos.

Los smartphones son elementos propensos a ser perdidos, robados o rotos. Por esta razón debemos tener en cuenta que los datos que tenemos guardados en ellos hoy, pueden quedar inaccesibles mañana. Por ello, realizar copias de seguridad regulares de nuestra información es importante.

En la nube versus *offline*

Cuando realizamos una copia de seguridad, podemos guardarla «en la nube» o en un dispositivo externo bajo nuestro control (PC, disco duro, NAS[30]...). Cada una de estas localizaciones tiene sus ventajas y sus desventajas.

Subir las copias de seguridad a la nube tiene una clara ventaja de usabilidad. Generalmente, estos respaldos son automáticos, transparentes al usuario y, al estar la información disponible *online*, podemos acceder a ella siempre que tengamos conexión a Internet.

La desventaja de este enfoque es que perdemos parcialmente el control de nuestra información cuando la subimos

30 NAS, Network Attached Storage: dispositivo que permite almacenar archivos en una red local.

a los servidores de la empresa que nos ofrece el servicio de almacenamiento. Tener la información en la nube implica ceder esta información a una empresa para que la guarde, y también a quien ésta se la quiera ceder. Podemos escoger en qué proveedor realizar nuestros respaldos, buscando aquéllos que nos ofrezcan una mayor confianza en cuanto al respeto de nuestra privacidad.

También existe el riesgo de que la cuenta de almacenamiento en la nube sea accedida de forma ilegítima debido a algún fallo de seguridad. Un ejemplo es la filtración producida en octubre del 2014 de cientos de fotografías de celebridades, muchas de ellas de desnudos, que habían sido extraídas ilegítimamente de iCloud.

Por otro lado, los respaldos *offline* o «en local», son aquéllos que realizamos de manera manual a otro dispositivo que poseamos, como un PC o un disco duro externo. Generalmente deberemos tomarnos el tiempo de hacer estos respaldos a mano y puede que no los tengamos disponibles desde cualquier lugar cuando los necesitemos. La ventaja es que la información respaldada está bajo nuestro control y nadie podrá acceder a ella sin acceder físicamente al dispositivo que la guarda o mediante el uso de *malware*.

En función del nivel de privacidad, accesibilidad y modelo de amenaza, deberemos escoger cuál es el método que más nos conviene. En cualquier caso, es importante realizar estos respaldos para garantizar que conservamos al menos parte de nuestra información tras un robo, pérdida o accidente.

Redes sociales

Introducción

Las redes sociales actualmente cuentan con un impacto bastante grande en nuestra sociedad. Hoy en día, no pertenecer a ninguna red social puede ser considerado motivo de marginación, aunque hayas decidido no hacerlo por principios. El mundo de las redes sociales cada vez crece más y nos expone de distintas maneras, no solamente a través de nuestros datos personales (número de teléfono, correo electrónico, nombre y apellidos, etc.), sino también a través de nuestra manera de usarlos. En muchos casos, el propietario de una cuenta expone más sobre sí mismo de lo que parece.

Pensar que por tener un *nickname* o nombre en clave, e inventarse los datos asociados a tu cuenta ya estás protegido, es obviar el gran poder que tienen las redes sociales sobre nosotros. La necesidad de compartir nuestra ubicación, nuestros gustos, aficiones o ideología política consigue que en muchos casos seamos fáciles de asociar con otros usuarios e incluso con grupos afines a nuestra manera de pensar.

Es posible que después de haberlo considerado no puedas desconectar tu vida de las redes sociales, y por eso vamos a darte unos consejos para que puedas protegerte, pero sin caer en la obviedad de que la mejor protección para tu intimidad y privacidad es el sentido común. Evitar compartir detalles personales que expongan tu intimidad en el día a día es la prevención más importante sobre el control de las redes sociales. A día de hoy no existe ninguna herramienta que nos proteja íntegramente de personas de personas que quieran herirnos o controlar nuestra actividad.

Existen diversas herramientas que relacionan tus «me gusta» o retuiteos con movimientos sociales o ideologías políticas afines, y esto le concede un mayor poder a tu adversario. Cuanto más información generas, más fácil es ubicarte en una base de datos ideológica sumamente detallada, atendiendo a tu rango de edad, ciudad y círculo social. O peor aún, también existen herramientas *online* que se dedican a clasificar toda la

información que hayas generado en tus perfiles para que con un solo clic quede expuesta por categorías.

En este apartado te exponemos ciertas características que se pueden desactivar de las redes sociales más usadas, permitiendo un mayor control sobre los datos que se publican. Es importante remarcar que este manual está actualizado en la fecha de publicación del mismo, pero que con la velocidad a la que las aplicaciones son mejoradas, quedará desactualizado pronto. Sin embargo, suelen tener patrones parecidos en cada actualización, es cuestión de buscar intensamente apartados similares a los aquí citados para conseguir el mismo resultado. Puede que incluso hayan incluido nuevas opciones para limitar o desactivar la recopilación de algunos datos.

No evitaremos en ningún caso que la empresa tenga el control sobre nuestros datos, la única manera de que eso suceda es no haciendo uso de estas redes sociales.

Críptica no recomienda en ningún caso el uso de Facebook, Twitter o Instagram como redes sociales respetuosas con la privacidad. Estas empresas recogen datos y metadatos de las imágenes o vídeos publicados, de interacciones entre usuarios, de navegación, ubicaciones, IP, etcétera, para analizarlos y almacenarlos con fines comerciales y publicitarios.

Si no pagas por el producto, el producto eres tú

Facebook

Facebook. Uno de los gigantes entre las redes sociales. Una empresa que crece exponencialmente a un ritmo frenético comprando otras redes sociales o aplicaciones de mensajería (Instagram, WhatsApp) para relacionar aún más a los usuarios entre ellos y conseguir un mayor número de datos para comercializarlos posteriormente.

Facebook actualmente recopila y almacena una vertiginosa cantidad de datos de sus usuarios. Sin olvidar el aviso de la propia corporación: «Las categorías de datos que recibimos, recopilamos y guardamos pueden cambiar con el tiempo», para dejar claro que aún pueden guardar más información en un futuro o que pueden estar recopilando información que no están obligados a mostrarte.

Dentro de la red social, tienes un apartado donde puedes descargarte un archivo con todos los datos que Facebook tiene almacenados sobre ti. Desde la pestaña *Configuración* dentro de tu perfil, tienes el apartado *Tu información de Facebook*, donde dispones de un enlace en la parte de abajo que dice: *Descargar tu información*. Facebook tardará un tiempo en proporcionarte el enlace, pero dentro de esta copia verás todas las IP desde donde te has conectado, los horarios, las ubicaciones, todos los comentarios hechos y recibidos, las fotos etiquetadas, intereses, eventos a los que has sido invitado y un largo etcétera de información personal.

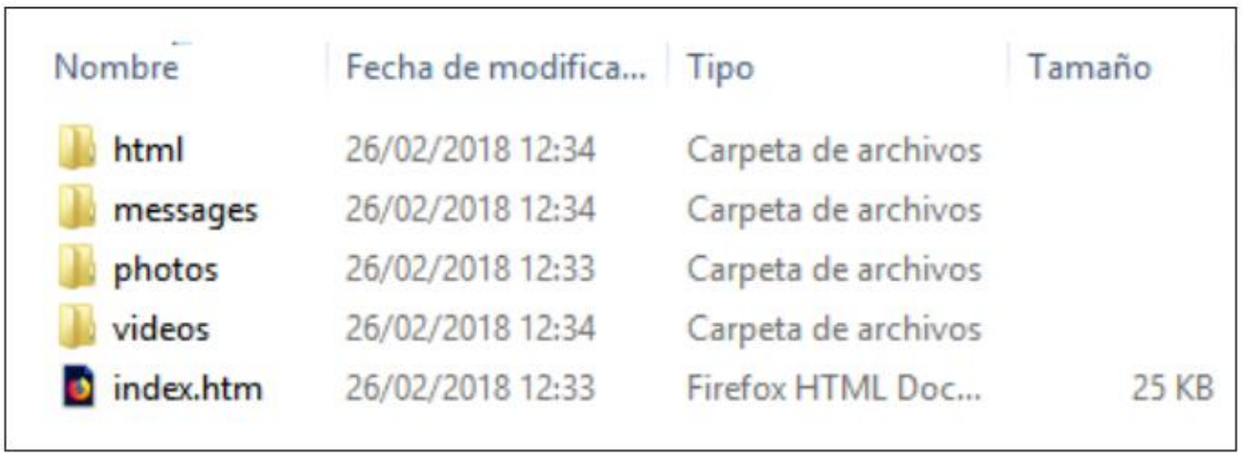
Tras la aplicación del GDPR[31] y el escándalo de Cambridge Analytica[32], si procedías a descargarte el fichero con tus datos podías observar un incremento bastante reseñable en los datos que tenían guardados sobre ti. ¿Significa esto que

---

31 GDPR, General Data Protection Regulation: nuevo reglamento de protección de datos a escala europea, que significa un avance en materia de privacidad.

32 Véanse https://www.lavanguardia.com/internacional/20180323/441820476947/como-utilizo-cambridge-analytica-datos-facebook-manipular-votantes.html, y https://www.bbc.com/mundo/noticias-43472797.

Facebook ha comenzado a recopilarlos ahora? No. Significa que la empresa poseía muchísima más información de ti de la que decía tener antes de verse obligada a revelártela una vez entrado en vigor el GDPR.



Nombre	Fecha de modifica...	Tipo	Tamaño
html	26/02/2018 12:34	Carpeta de archivos	
messages	26/02/2018 12:34	Carpeta de archivos	
photos	26/02/2018 12:33	Carpeta de archivos	
videos	26/02/2018 12:34	Carpeta de archivos	
index.htm	26/02/2018 12:33	Firefox HTML Doc...	25 KB

La imagen de arriba es la descarga del archivo de datos de un usuario medio en Facebook en febrero del 2018; la imagen de la derecha es la descarga del mismo archivo del mismo usuario en septiembre del 2018.

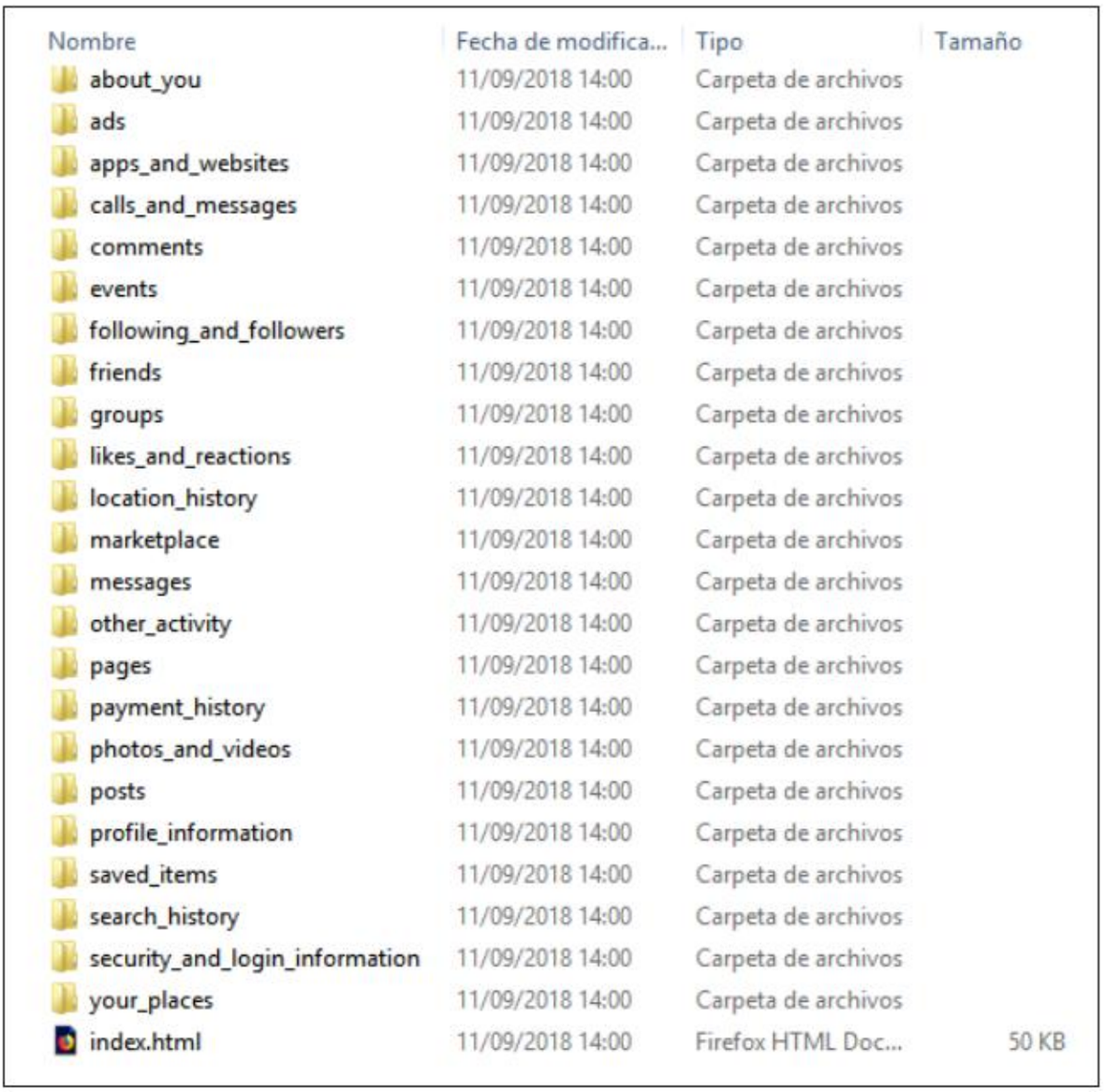
¿Podemos hacer algo con toda esta información que ya tiene sobre nosotros? La respuesta es ambigua. Hay información que Facebook se compromete a borrar de sus servidores cuando eliminas tu cuenta, y por otro lado, hay información que por desgracia ya ha sido cedida a terceras empresas y ya no podremos volver a tener el control sobre ella, no con las leyes actuales, al menos[33].

A continuación, explicaremos cómo limitar o desactivar algunas opciones de recopilación de datos desde la aplicación para móvil de Facebook. Si accedemos desde un navegador, las opciones son más amplias, e investigando un poco más a fondo podemos limitar aún más el acceso (eliminando las *cookies* del navegador, por ejemplo[34]).

---

33 Sobre esta cuestión, véase https://www.elmundo.es/tecnologia/2018/03/15/5aaa4546468aeb196f8b45f0.html.

34 Véase la sección «Navegación y privacidad» para más información al respecto.



Nombre	Fecha de modifica...	Tipo	Tamaño
about_you	11/09/2018 14:00	Carpeta de archivos	
ads	11/09/2018 14:00	Carpeta de archivos	
apps_and_websites	11/09/2018 14:00	Carpeta de archivos	
calls_and_messages	11/09/2018 14:00	Carpeta de archivos	
comments	11/09/2018 14:00	Carpeta de archivos	
events	11/09/2018 14:00	Carpeta de archivos	
following_and_followers	11/09/2018 14:00	Carpeta de archivos	
friends	11/09/2018 14:00	Carpeta de archivos	
groups	11/09/2018 14:00	Carpeta de archivos	
likes_and_reactions	11/09/2018 14:00	Carpeta de archivos	
location_history	11/09/2018 14:00	Carpeta de archivos	
marketplace	11/09/2018 14:00	Carpeta de archivos	
messages	11/09/2018 14:00	Carpeta de archivos	
other_activity	11/09/2018 14:00	Carpeta de archivos	
pages	11/09/2018 14:00	Carpeta de archivos	
payment_history	11/09/2018 14:00	Carpeta de archivos	
photos_and_videos	11/09/2018 14:00	Carpeta de archivos	
posts	11/09/2018 14:00	Carpeta de archivos	
profile_information	11/09/2018 14:00	Carpeta de archivos	
saved_items	11/09/2018 14:00	Carpeta de archivos	
search_history	11/09/2018 14:00	Carpeta de archivos	
security_and_login_information	11/09/2018 14:00	Carpeta de archivos	
your_places	11/09/2018 14:00	Carpeta de archivos	
index.html	11/09/2018 14:00	Firefox HTML Doc...	50 KB

Para empezar a configurar nuestro Facebook, accederemos al apartado *Configuración y privacidad* en la lista de opciones dentro de la propia aplicación. Aprovechamos para recordar que, si queremos ocultar el origen de nuestra conexión, podemos utilizar Orbot o una VPN.

Configuración

· Dentro del apartado *Seguridad* podemos ver las aplicaciones a las que hemos dado permiso desde Facebook para acceder a nuestros datos.

  En el primer punto, *Sesión iniciada con Facebook*, podremos ver qué aplicaciones tienen acceso a nuestros datos en este instante y desactivarlas al momento.

  En *Preferencias* desactivaremos la opción *Aplicaciones, sitios web y juegos*. Esto limitará el acceso a nuestros datos por parte de aplicaciones de terceros dentro de la plataforma de Facebook.

· Continuamos con el siguiente apartado: *Privacidad*. Aquí podremos configurar nuestro perfil para que las publicaciones sean privadas e incluso limitar quién puede ver publicaciones antiguas. Un punto importante es el de poner al máximo la privacidad de tu lista de amigos, escogiendo la opción para que nadie pueda ver esta lista, ni siquiera tus propios amigos. Otro punto importante son los motores de búsqueda que enlacen a tu perfil, tenemos que escoger la opción *No* para un mayor grado de privacidad. Los buscadores registran constantemente palabras clave en todo tipo de páginas, de forma que algunas de las acciones o mensajes vinculados a nuestra cuenta podrían quedar reflejados en los resultados de Google u otro

motor de búsqueda, en caso de no seleccionar este parámetro.

Tenemos que desactivar el reconocimiento facial de las fotografías y vídeos, y escoger privacidad máxima en el etiquetado de fotos o publicaciones que otras personas hagan sobre ti.

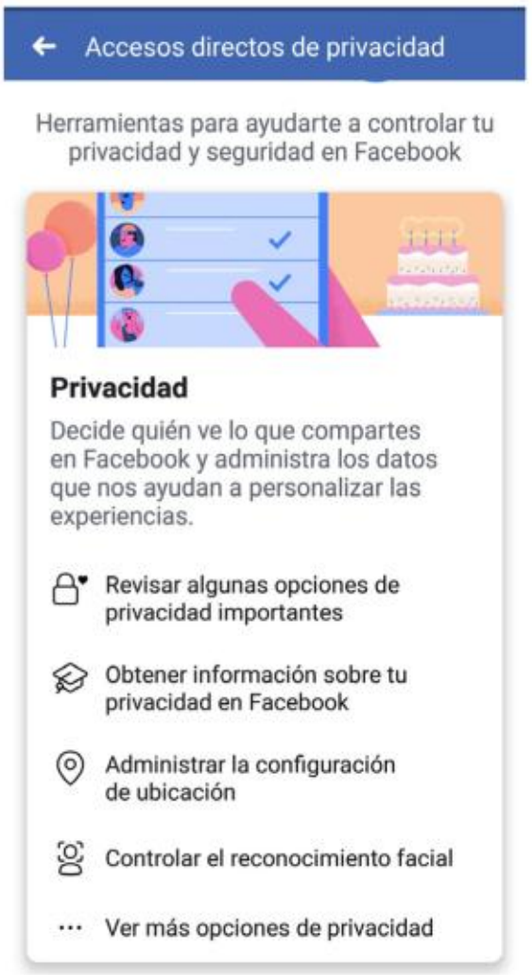
Desactivaremos la opción *Estado activo* para evitar que desde el Messenger de Facebook se pueda ver si actualmente estás frente a la aplicación o cuándo fue la última vez que lo estuviste.

- En *Tu información de Facebook* podrás consultar la información generada en la red social clasificada por categorías, el registro de tu actividad reciente y descargar una copia de toda la información que poseen sobre ti. Aquí podrás desactivar temporalmente tu cuenta y volver cuando te apetezca o eliminarla definitivamente. Esto último no significa necesariamente que toda la información que hay en Facebook sobre ti desaparezca, pero es un punto de partida para desvincularte lo máximo posible de la corporación.

- Seguidamente nos encontramos con el apartado *Anuncios*, donde podrás ver con qué anuncios has interactuado y cuáles son las preferencias que ellos tienen sobre ti a la hora de mostrarte publicidad. Aconsejamos tener estas opciones desactivadas para evitar que hagan un perfilado aún mayor de tus gustos e interacciones.

Accesos directos de privacidad

Dentro de esta categoría tenemos varias opciones para, con un vistazo sencillo y rápido, controlar el acceso que otras personas tienen a nuestro contenido.



- *Privacidad*. Facebook te proporciona el apartado *Revisar algunas opciones de privacidad importantes*, donde podrás, en tres sencillos pasos y de una manera muy visual, limitar el acceso a terceras personas a tu perfil y a tus publicaciones. Debemos limitar la información que mostramos a los demás al máximo, y evitar tener apartados públicos. Más abajo desactivaremos los servicios de ubicación y el reconocimiento facial en fotografías o vídeos.

- *Protección de la cuenta*. Aquí podrás actualizar tu información personal y cambiar tu contraseña. Recomendamos cambiar la contraseña de manera regular, al igual que todas las que utilices en otras cuentas.

- *Preferencias de anuncios*. Es importante que deniegues el permiso a Facebook a usar tus datos de usuario para mostrarte los anuncios que consideren más relevantes. Dentro de estas opciones marcaremos todas como *No permitido*, y más abajo elegiremos que nadie de nuestros contactos pueda ver nuestros me gusta a páginas publicitarias.

Por último, aconsejamos que si utilizas Facebook desde un navegador, no olvides instalarte *plugins* totalmente necesarios para evitar que nos rastree allá por donde naveguemos: Cookie AutoDelete (elimina las *cookies*), uBlock Origin (bloquea publicidad) o Facebook Container (contiene las *cookies* de Facebook en una pestaña). Estos *plugins* evitarán que

Facebook monitorice tu actividad por la web para ofrecerte posteriormente publicidad orientada dentro de la red social.

Es importante puntualizar que hay información que nosotros controlamos si publicar o no en esta red social; sin embargo, existen muchos otros datos que Facebook recopila de nosotros a través de sus *trackers* y que no podemos controlar.

Twitter

Twitter es una red social que nos ofrece un grado de anonimato superior a Facebook, pero en ningún caso un anonimato absoluto. Por ejemplo, a la hora de crearte la cuenta, Twitter registra la ubicación desde donde fue creada y ésta se queda guardada para siempre. Crearla a través de Tor o de una VPN no garantiza un anonimato total, ya que la política de Twitter contempla exigir sistemáticamente al usuario un número de teléfono. Para solventar este inconveniente disponemos de pocas opciones, por lo que si al final lo que deseas es tener una cuenta totalmente anónima, tendrás que ingeniártelas.

Una vez creada la cuenta de Twitter, puedes anonimizar el origen de tu conexión mediante el uso de Orbot o de una VPN.

Desde el menú de la aplicación podremos configurar algunas opciones importantes para mejorar nuestra privacidad, pero, como siempre, es más limitado que la versión del navegador.

Configuración y privacidad

- En *Cuenta* podrás descargarte el fichero de datos que Twitter tiene sobre ti en *Tus datos de Twitter*. Recomendamos revisar el apartado *Aplicaciones y sesiones* para ver qué aplicaciones externas a Twitter tienen permisos para acceder a tu cuenta (como por ejemplo Twidere o TweetDeck), y en el caso de no utilizarlas, revocar estos permisos. Además, podrás controlar en qué dispositivos tienes la sesión activa en ese momento, pudiendo cerrarlas instantáneamente.

Al final de este apartado encontraremos cómo desactivar nuestra cuenta.

- Seguidamente continuaremos con *Privacidad y seguridad*, en donde podremos: proteger nuestro perfil, seguidos y seguidores, además de los tuits (hacer nuestra cuenta candado); desactivar el etiquetado de fotos para evitar que nos relacionen con personas o eventos determinados, y desactivar la confirmación de lectura de los mensajes privados.
  Si escogemos que la cuenta sea privada, las personas que quieran ver nuestra actividad, tuits, "me gusta", seguidos o seguidores necesitarán nuestra aprobación. Correspondería al nivel máximo de privacidad de cara a otros usuarios de la red social o público general de Internet.

- En el apartado *Visibilidad y contactos*, recomendamos deshabilitar que otras personas te encuentren por tu correo electrónico o tu número de teléfono, además de no sincronizar los contactos de tu libreta de direcciones. No olvidemos que toda la información que proporcionemos quedará grabada en los servidores de Twitter, aunque posteriormente la deshabilitemos. Twitter te da la opción de eliminar todos los contactos que algún día sincronizaste, pero no deja claro en ninguna parte que también lo haga de sus servidores.

- En *Ubicación* desactivaremos la ubicación exacta. Más abajo Twitter explica que si activas esta opción, se dedicará a recopilar, almacenar y utilizar la ubicación exacta de tu dispositivo para mejorar tu experiencia (mostrarte anuncios de recomendaciones locales). Es por esto que *nunca* debemos activar esta opción.

- Más abajo podemos encontrar *Personalización y datos*, donde podremos desactivar todas las opciones de publicidad orientada que ofrece Twitter. Puedes desactivar todas las opciones una por una o directamente en un botón en la parte superior, que sirve para deshabilitarlo todo. De nuevo, en *Consulta tus datos de Twitter* podrás descargarte un fichero con tus datos o bien consultarlos según categorías.

- Desde *Pantalla y sonido* en las opciones generales podremos desactivar el uso del navegador web interno de Twitter; esto es importante para evitar que recopile información de los enlaces externos a los que hagamos clic en la aplicación.

Instagram

Instagram es una red social que en los últimos años se ha ido expandiendo, aumentando su número de usuarios considerablemente. Desde que pertenece a Facebook, la red social ha experimentado cambios para asemejarse a ésta y viceversa. Debido al gran número de personas que la utilizan hoy en día, hemos considerado necesario mencionarla.

Para ocultar el origen de tu conexión, puedes hacerlo a través de Orbot o de una VPN, y además configurar el cliente del móvil con las opciones que te detallamos a continuación para aumentar un poco más el control de tus datos.

Desde nuestro perfil, entraremos dentro de la opción *Configuración* situada arriba a la derecha, donde nos encontraremos con:

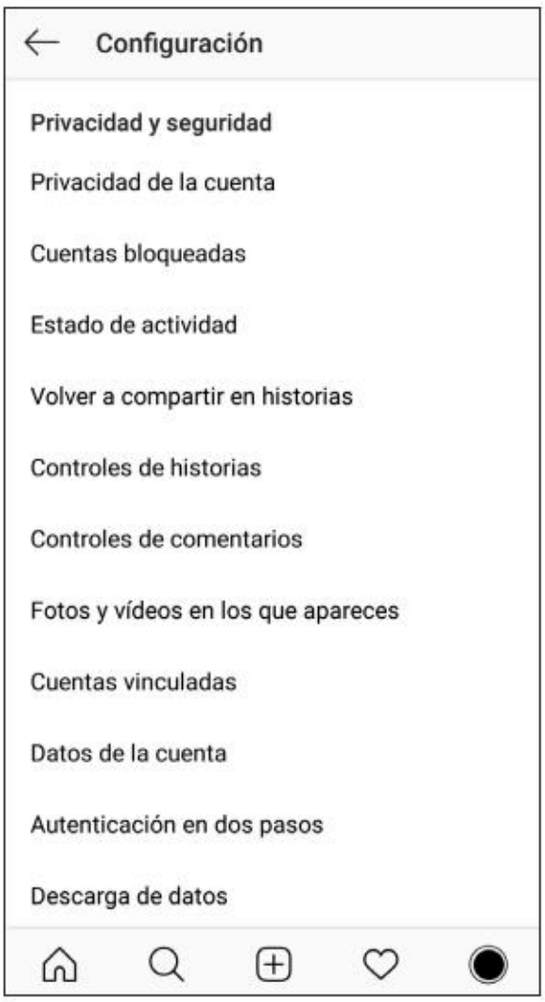
Cuenta

En este apartado podremos elegir que nuestra cuenta sea privada, es la manera más sencilla y rápida de proteger tu contenido hacia otros usuarios. Así puedes asegurarte de que sólo quien aceptes podrá ver tus fotos, vídeos, seguidos/seguidores o actividad.

En Instagram no existe otra manera de poder ocultar tus seguidos/seguidores, los *hashtags* que sigues o la actividad que generas. Ten en cuenta que desde la pestaña ♥ puedes observar la actividad de quienes sigues; esto incluye los comentarios y *likes* a los contenidos de otros usuarios o a quién comienzan a seguir.

Privacidad y seguridad

- *Privacidad de la cuenta*. De nuevo nos deja escoger que nuestra cuenta sea privada. Recomendamos marcar esta opción para ocultar por defecto tu actividad a cualquier usuario que no desees aceptar.



- *Estado de actividad*. Desmarcando esta opción nos aseguramos de que nadie pueda controlar si estamos actualmente interactuando en la red social o cuándo fue la última vez que estuvimos conectados.

- *Volver a compartir en historias*. Esta opción permite que otros usuarios decidan compartir nuestra historia asociada a nuestro usuario desde su propia cuenta, sin necesidad de pedirnos permiso. Para un mayor control de tus historias publicadas es recomendable desactivar esta opción.

- *Controles de historias*. En este apartado podremos decidir a qué usuario queremos ocultar las historias que publicamos. También podremos decidir quién puede enviarnos un mensaje a través de la historia publicada. Recomendamos de nuevo desactivar la opción *Permitir compartir* las historias destacadas, esto servirá para que las historias fijadas a nuestro perfil principal no puedan ser compartidas en perfiles ajenos sin nuestro permiso.

- Seguidamente denegaremos el permiso a compartir nuestras publicaciones e historias en Facebook para disminuir la correlación de información entre nuestras cuentas.

- *Fotos y vídeos en los que apareces*. Aquí podremos desactivar la opción de que las imágenes o vídeos donde seamos etiquetados por otras personas se añadan directamente a

nuestro perfil, e incluso ocultarlos. De esta manera no podrán relacionarte tan fácilmente con otras personas o con determinados eventos y situaciones que puedan dar mayor información de ti.

- En *Cuentas vinculadas* vigilaremos que no tengamos ninguna otra red social asociada a nuestra cuenta. Es importante recordar que si utilizas el mismo correo electrónico en todas ellas, compartes tu número de teléfono, o simplemente conectándote desde el mismo dispositivo a Facebook e Instagram, automáticamente se estará compartiendo cierta información entre ellas sin que tú puedas elegir no hacerlo, como por ejemplo contactos o intereses para poder recomendarte en cada red social lo que sea más afín a ti.

- Podrás descargarte una copia de tu actividad en Instagram en la opción *Descarga tus datos* para hacerte una idea de la información que has ido generando. Recuerda que al igual que en las otras redes sociales, existe mucha información que no están obligados a proporcionarte actualmente, pero que recopilan de ti y sobre la que has perdido todo el control.

- Mantén la opción *Sincronización de contactos* desactivada para que no pueda apropiarse de tu agenda y guardar una copia en sus servidores. Siempre es más recomendable buscar a la persona directamente antes que ceder estos datos a la empresa.

WhatsApp

Aunque WhatsApp no sea una red social como tal, sino una aplicación de mensajería instantánea, hemos considerado oportuno mencionar cuatro consejos básicos para mejorar tu privacidad a la hora de usarla.

- Si vamos a las opciones de *Ajustes*, desde el apartado *Cuenta* encontramos un subapartado llamado *Privacidad* donde podremos restringir quién puede ver nuestra información personal (horario de conexión, las fotos de perfil, el estado, la información y la ubicación en tiempo real). Es aconsejable restringir al máximo estas opciones, y especialmente desactivar la ubicación en tiempo real.

- WhatsApp pertenece a Facebook, esto quiere decir que ambas plataformas intercambian información personal. Si bien es cierto que los chats de WhatsApp están cifrados, hemos de ser conscientes de que haciendo uso de esta aplicación generamos ciertos metadatos que proporcionan bastante información sobre patrones de conducta. Por ejemplo, con qué personas hablamos más, con qué grupos de gente solemos tener mayor intercambio de mensajes, nuestros horarios de uso habitual de la aplicación, etc. Esta información ya ha sido utilizada por Facebook sin nuestro consentimiento en el pasado[35], por lo que nadie nos dice que no puedan volver a hacer uso de ella.

- Las copias de seguridad que WhatsApp hace de nuestros chats son archivos cifrados que solamente la aplicación puede descifrar. Sin embargo, el resto de archivos (mensajes de voz, fotos de perfil, imágenes enviadas o recibidas) se guardan en claro, sin cifrar. Esto quiere decir que si hacemos copias de seguridad y las subimos a Google Drive o iCloud (en el caso de iPhone), desde Google o Apple no

35 Véase https://www.elmundo.es/tecnologia/2018/03/15/5aaa4546468aeb196f8b45f0.html.

podrían descifrar los mensajes de texto sin que la empresa WhatsApp les diese la clave para ello, pero el resto de archivos estará en la nube en claro. Por tanto, desde Críptica no recomendamos que las copias de seguridad del servicio se suban a Google Drive o iCloud, sino que se guarden en el teléfono y posteriormente se haga una copia en otro dispositivo de manera cifrada, por ejemplo un *pendrive*.
Si alguna vez activaste la opción de guardar en Google Drive o iCloud, podrás desactivarla rápidamente desde el apartado *Copia de seguridad*, en la opción *Chats* dentro de *Ajustes*.

Alternativas

Actualmente existen redes sociales alternativas, libres, descentralizadas y que son respetuosas con tu privacidad. Este número va *in crescendo* año tras año, y si bien aún tienen cosas a mejorar en lo que a la seguridad respecta, son una buena alternativa si no quieres renunciar a ella.

- Mastodon (https://mastodon.social), al igual que Quitter, es una red social con cierto parecido a Twitter. Está distribuida en distintos servidores independientes, llamadas "instancias", unificados, permitiendo interactuar entre ellos. Puedes crearte una cuenta en cualquier servidor e interactuar con usuarios que pertenezcan a otros.

- Quitter / GNU Social (https://quitter.es) es una red social distribuida en distintos servidores independientes que pueden comunicarse entre sí. Independientemente del servidor donde te hayas creado la cuenta, podrás interaccionar con los usuarios de los otros servidores. Tiene cierto parecido a una versión antigua de Twitter, con la diferencia de que cada servidor pone sus reglas, con lo que en algunos el texto está limitado a 140 caracteres y en otros a 240 o incluso 1000.

- Diaspora* (https://diasporafoundation.org/) consiste en un grupo de servidores independientes (los llamados *pods*) que interactúan entre ellos para formar la red social. Estos servidores son mantenidos por muchos individuos e instituciones diferentes. Cada uno de ellos actúa como un servidor web personal con una copia del software de Diaspora. Al igual que Mastodon, puedes interactuar con usuarios de otros servidores.

SEGURIDAD INSTRUMENTAL:

APLICACIONES PARA MEJORAR TU SEGURIDAD

¡Atención!
Peligro de obsolescencia

Estas herramientas fueron analizadas en el último trimestre del año 2018. Cuanto más se aleje la lectura a nivel temporal, más probable es que alguna de ellas haya quedado obsoleta, se hayan descubierto nuevas vulnerabilidades o que nuevas aplicaciones hayan tomado el relevo de las que aquí recomendamos. Por ello, aconsejamos que las reseñas se lean de acuerdo con la necesidad humana que cada una de las aplicaciones busca satisfacer, y no como herramientas imperecederas, imperturbables al paso del tiempo.

Comparativa de mensajería instantánea

Pensar en clave adversarial: contexto y modelo de amenaza

Como hemos ido viendo a lo largo de este libro, la seguridad absoluta no existe como tal, y las medidas que debemos tomar para proteger nuestra privacidad varían en función del contexto y del modelo de amenaza al que nos enfrentemos. Sabido es que no es lo mismo enfrentarse a un adversario de tipo estatal que empresarial, o a alguien con conocimientos de nuestro entorno social cercano. Además, para el caso de la mensajería instantánea, entran en juego unos cuantos factores más que debemos tener en cuenta a la hora de decidir qué plataforma usar en cada caso: tampoco existe en esto una regla de oro, aplicable a todos los contextos por igual.

Nuestra actuación en este sentido debe ir orientada de acuerdo con las capacidades del adversario del cual nos queremos proteger: cada uno tiene distintas formas de acceder a nuestra información, de manera que las medidas de protección que utilizaremos deberían ser sustancialmente distintas unas de otras[36].

Por consiguiente, el objetivo de este capítulo no puede ser el de recomendar una aplicación de mensajería en términos

---

36 Si nuestro adversario fuera la empresa de mensajería instantánea que gestiona los servidores, debemos tener en cuenta que, a pesar de no tener acceso físico a nuestro dispositivo, sí que tiene acceso a nuestros mensajes en caso de no estar utilizando una herramienta que cifre de dispositivo a dispositivo (E2E, explicado en la siguiente sección). Si, por el contrario, se trata de una persona de nuestro entorno cercano, debemos cuidar de que no gane acceso físico al dispositivo, ya sea para instalar aplicaciones maliciosas o para leer nuestros mensajes.

generales, haciendo abstracción de las circunstancias particulares de cada persona, sino más bien desglosar algunos de los factores ya mencionados, los cuales tendremos que valorar pausadamente antes de tomar la decisión de utilizar o no determinada plataforma de comunicación. Asimismo, en la parte final entraremos a considerar qué características cumplen las aplicaciones de mensajería instantánea para smartphone más conocidas.

Cifrado E2E

Uno de los factores a tener más en cuenta siempre que establezcamos comunicaciones digitales con otras personas, es el de tener acceso a mecanismos de cifrado, con tal de que una tercera persona que estuviera escuchando el tráfico del canal[37] no pueda obtener el contenido de los mensajes. Y más concretamente, el tipo de cifrado que nos interesa en este caso es que sea de dispositivo a dispositivo (en términos técnicos, cifrado *end-to-end* o simplemente E2E), puesto que proporciona las mejores condiciones para una comunicación segura, por encima de alternativas como el cifrado de cliente a servidor. En este último caso, el contenido de la comunicación queda expuesta a los ojos de quien controla el servidor u otros actores que consiguieran acceso al mismo.

El cifrado de dispositivo a dispositivo significa que el mensaje que Alice le manda a Bob se cifra en el mismo dispositivo de Alice, y solamente se descifra al llegar al de Bob. Con lo que si alguien estuviera tratando de monitorizar el canal (ya sea el propio servidor en el que se establece la comunicación o un atacante externo), no tendría acceso al contenido de los mensajes como tal. Concluimos, por lo tanto, que una de las principales características en la que nos fijamos como asociación es que la aplicación tenga habilitado por defecto este tipo

37 Escuchar el tráfico es analizar las comunicaciones que mantienen diferentes dispositivos en un mismo canal.

de cifrado, sin depender de que el usuario tenga que activar ninguna configuración especial.

Borrado automático de los mensajes

El acto de cifrar es fundamental cuando se trata de comunicarnos de manera segura con otras personas. Imaginemos, no obstante, que Alice recibe los mensajes de Bob a través del cifrado anteriormente descrito, el E2E (el mejor de todos los que podemos elegir). Una vez llegan a su dispositivo, la aplicación los descifra automáticamente para que Alice pueda leerlos en la pantalla de su smartphone. Por consiguiente, si alguien accediera al teléfono de Alice podría exponer tanto a Bob como a ella, puesto que tendría acceso a la totalidad de los mensajes descifrados. Es fundamental recordar que la seguridad proporcionada por el cifrado de las aplicaciones se limita únicamente a la fase de transmisión de los mensajes, pero no otorga ninguna protección especial a los mensajes ya almacenados en el teléfono.

Una vez los mensajes llegan a nuestro dispositivo, su confidencialidad deja de depender de la arquitectura de seguridad de la aplicación, haciendo que tengamos que contemplar medidas adicionales. Una forma de asegurarnos de que nuestras conversaciones no queden comprometidas es, naturalmente, borrar los mensajes una vez los hemos leído. De esta forma, si una tercera parte interviniese el dispositivo, no podría leer el contenido de los mismos. Entra pues dentro de nuestros intereses buscar aplicaciones que dispongan de opciones para que los mensajes se borren del dispositivo pasado cierto tiempo de su recepción.

Los riesgos de revelar tu número de teléfono

Cuando usamos una aplicación de mensajería instantánea, necesitamos algún tipo de identificador para que las

demás personas puedan encontrarnos, con vistas a iniciar una conversación.

Una buena cantidad de servicios utilizan el número de teléfono como identificador público. Así, para establecer una comunicación con otra persona o grupo, tenemos que darles nuestro número personal, que en muchos países (caso de España) se encuentra forzosamente vinculado a una identidad legal (habitualmente, la del usuario que utiliza el dispositivo o de alguien de su entorno más cercano). Cuando se trata de contactos de confianza, esto no suele entrañar riesgos para la privacidad, a pesar de que les estemos dando la posibilidad técnica de averiguar la identidad real que se esconde tras un número de teléfono: confiar en alguien significa tener la seguridad de que hará todo lo posible porque las informaciones que le entreguemos no acaben comprometidas o en manos de un adversario.

Sin embargo, cuando se trata de contactos de menor confianza, el acto de dar a conocer nuestro número puede ser *demasiada* información. Es el caso de muchos grupos de chat, habitualmente creados por afinidad política o al calor de determinados acontecimientos, que al recurrir a plataformas que dependen del mencionado número están creando a su vez una jugosa base de datos ideológica, vinculada a identidades reales. Esto supone un riesgo para la privacidad desde el momento en que cualquier componente del grupo puede conocer los números asociados al resto de participantes, adquiriendo la posibilidad de vincular personas reales a determinadas opiniones o posicionamientos de carácter político. Naturalmente, esto no sería un riesgo estructural si todos los miembros fueran de nuestra plena confianza, pero es frecuente encontrarnos en la situación de no poder poner la mano en el fuego por cada uno de los participantes, especialmente cuando se trata de grupos de mucha gente y creados a toda prisa.

Por ello, es posible que una de las características que acabemos buscando en el proceso de decidir una aplicación antes que otra, es no tener que darle nuestro número de teléfono para ser empleada. O en el caso de que esto no fuera posible,

al menos elegir un servicio que no le revelara al resto de personas nuestro número personal.

La ausencia de actividad también revela información

Igual que de cada proceso comunicacional pueden extraerse informaciones que ayudan a contextualizar la interacción (interlocutores, duración, tamaño de los mensajes), también la «no comunicación» o la ausencia de interlocuciones en determinados momentos del día es reveladora de algún tipo de información. Pongamos, por ejemplo, una conversación de chat entre dos personas, Alice y Bob. Un tercer individuo, Chuck, anda analizando el tráfico de los mensajes, a pesar de no poder leer el contenido de los mismos (si se tratara de un chat cifrado). Cuando Alice y Bob dejan de intercambiarse mensajes, Chuck tiene constancia de esta interrupción, porque la actividad del canal cesa. Analizando esta carencia de interlocuciones en ciertas horas del día, Chuck puede especular con los motivos por los cuales el proceso comunicacional ha parado (ya sea porque uno de los dos ha empezado su jornada laboral, por ser temprano por la mañana, o porque se ha ido a dormir, en caso de que sea a altas horas de la noche).

Siguiendo con el ejemplo, pongamos que Chuck no solamente analiza los intercambios de mensajes entre Alice y Bob, sino de todas las conversaciones de Alice. Teniendo esta información, el individuo a la escucha bien podría acabar dibujando un mapa horario general de las comunicaciones de Alice, con vistas a obtener los hábitos de conexión de ella, así como sus pautas frecuentes de interacción[38]. Además, si la

---

38 ¿Por qué Alice responde muy tarde a los mensajes de Bob, mientras que contesta prácticamente al instante los de Grace? La rapidez dando una respuesta suele ser un indicador de cercanía, personal o laboral, con la otra persona. ¿Por qué Alice empieza a contestar sus mensajes a las siete de la mañana? Probablemente porque ésa sea la hora exacta a la que se despierta.

aplicación de chat que usa Alice revelara detalles de cuándo está conectada o «en línea» (caso de WhatsApp), Chuck podría complementar su investigación con información de las horas en que tiene esa plataforma abierta en su dispositivo (aunque no intercambie mensajes), obteniendo un patrón horario todavía más preciso.

Consecuentemente, uno de los factores que debemos tener en cuenta a la hora de comunicarnos a través de este tipo de aplicaciones será el de proteger adecuadamente nuestros patrones horarios reales, ya sea utilizando herramientas que no revelen cuándo estamos en línea o leemos los mensajes, que no tengan un interés comercial o político en monitorizar nuestra actividad o que contemplen maneras de dificultar esta clase de seguimientos por parte de terceros.

Descentralización

La seguridad en un sistema de mensajería no depende en exclusiva del tipo de cifrado implementado para asegurar la confidencialidad de los mensajes, sino también de la topología de la red, es decir, del grado de centralización de su estructura. Si hacemos uso de un sistema centralizado en un único servidor, estamos otorgando al proveedor del servicio un poder inusitado, puesto que puede bloquear arbitrariamente nuestras comunicaciones y monitorizar nuestra actividad en caso de caer bajo su interés.

Para evitar situaciones como la descrita, precisamos de sistemas descentralizados, los cuales no dependen de un servidor central para llevar a cabo el proceso comunicacional. Así, estaremos disminuyendo las cuotas de poder que recaen en manos de los proveedores de los distintos servicios, con tal de prevenir un potencial abuso. No obstante, es preciso tener en cuenta que, en caso de utilizar tecnología descentralizada pero con una gran cantidad de gente usando el mismo nodo para acceder a la red, estaremos recentralizando la red en ese nodo: un sistema descentralizado no asegura nada por él

mismo, precisamos también de una arquitectura distribuida, que evite la concentración del poder en pocos nodos.

Disponibilidad del código

La búsqueda de una seguridad efectiva genera la necesidad de una transparencia por parte del servicio que estamos utilizando. Cuando no se tiene acceso al código de programación de la aplicación (su mecanismo interno, la necesaria sala de máquinas de la que precisa cualquier herramienta para funcionar), lo que el desarrollador nos pide es un acto de fe: confiar en la integridad del servicio gracias a su sola palabra. Desde la perspectiva que nos ocupa, ésta es una exigencia inasumible, puesto que, idealmente, un buen sistema de seguridad debería permanecer abierto para su meticulosa revisión y mejora, con tal de verificar no solamente su efectividad más allá del discurso, sino para asegurarnos también de que no contiene funciones ocultas, que pudieran menoscabar la integridad de la herramienta. Sin un acceso transparente al código, toda seguridad acaba siendo siempre relativa.

Nuestra experiencia particular nos ha llevado a desarrollar una desconfianza instintiva frente a la mera palabra, que bajo ningún concepto puede ser sustitutiva de un acceso integral al código. Su condición de disponibilidad suele garantizar que una mayor cantidad de personas hayan podido revisarlo (no solamente unas pocas), de manera que el número de vulnerabilidades ocultas sea (potencialmente) menor. Las exigencias de una seguridad robusta nos llevan, por lo tanto, a delegarla en aplicaciones con el código de programación públicamente disponible, en oposición a los modelos cerrados que no permiten verificar nada. Y dentro de esta condición, tendremos preferencia por el software libre, que permite la mejora de la herramienta gracias a la participación activa de la comunidad.

Modelo de financiación

Cada día más, el modelo de financiación de la aplicación (o, en su defecto, del organismo que la administra) tiene una importancia mayor, dado que puede condicionar todos los anteriores criterios que hemos ido exponiendo. El fructífero negocio de los datos se ha convertido, en la era digital, en una de las principales fuentes de ingresos de las empresas desarrolladoras, que han pasado a tener un interés comercial directo por registrar, almacenar y analizar la información que generamos con nuestros dispositivos móviles. Por lo tanto, al utilizar herramientas que recopilan este tipo de datos con el objetivo de crear perfiles de cliente, estaremos cediendo a la empresa parcelas considerables de nuestra privacidad.

Existen distintos tipos de datos a partir de los cuales hacer negocio: desde los horarios de conexión, hasta la explotación de determinadas funcionalidades del teléfono (ya no es ningún secreto que Instagram registra, gracias a su acceso al micrófono, el ruido de ambiente para ofrecer publicidad personalizada)[39]. En lo que respecta a las aplicaciones de mensajería, el negocio suele residir en los metadatos, esto es, en el análisis tanto del gráfico social (personas con las que uno se comunica de entre todas las de su agenda, para sondear su grado de cercanía gracias a la frecuencia de las interacciones), como de los patrones temporales de conexión (de los que se puede extraer un esquema de nuestra vida diaria: tipo de régimen laboral u horas de sueño). Y es que, por mucho que usemos una aplicación que proteja el contenido de los mensajes con el mejor cifrado posible, si existe un interés corporativo por recabar los mencionados metadatos, una buena parte de nuestra información personal permanecerá susceptible de explotación comercial.

---

39 Una de las primeras denuncias en este sentido fue la de Damián Le Nouaille-Diez, en septiembre del 2017: https://medium.com/@damln/instagram-is-listening-to-you-97e8f2c53023.

El modelo de negocio condiciona seriamente la seguridad y privacidad de una herramienta. Como respuesta, entra dentro de nuestros intereses directos recurrir a aplicaciones cuyo modelo de negocio (y, por ende, de sostenibilidad) no dependa en modo alguno de sacar provecho económico de la información que generamos al utilizarlas. Apostamos por servicios que no basen su sostenibilidad financiera en el lucrativo negocio de los datos, un mercado en pleno apogeo que compromete notablemente nuestros esfuerzos por hallar privacidad.

Protegerte como forma de proteger a las personas de tu alrededor

La faceta social del smartphone conlleva que fragmentos de nuestra identidad se transmitan de manera constante a dispositivos que no son el nuestro: notas de voz, mensajes íntimos, opiniones políticas o fotografías, entre muchos otros, quedan dispersos y en manos de nuestro entorno desde el momento en que decidimos transmitirlos. Es por eso que todos los criterios anteriormente expuestos pueden ser completamente superfluos si el dispositivo de alguien de nuestro entorno llega a quedar comprometido. Por más que nuestro teléfono tenga las últimas actualizaciones de seguridad, si el que se sitúa al otro extremo de la comunicación no tiene el mismo grado de cautela, una buena parte de nuestra identidad será fácilmente accesible para nuestros adversarios.

Si alguien toma la decisión personal de no protegerse, su decisión individual repercute *ipso facto* en la seguridad y privacidad del conjunto de comunidades de las que forma parte. *La seguridad es un deporte de equipo*: intentemos que la totalidad de nuestro entorno habilite un código de desbloqueo y cifre el aparato para evitar que terceras personas puedan acceder a su contenido, que en buena medida será contenido que puede exponer también a su red de contactos.

Análisis de aplicaciones

Una vez expuestos los distintos criterios de privacidad, corresponde al lector la laboriosa tarea de evaluar cuáles son sus exigencias particulares de seguridad, con tal de elegir una aplicación de mensajería capaz de sufragarlas. Asimismo, es probable que nuestras necesidades cambien según el escenario en el que nos encontremos, de modo que es casi inevitable tener que recurrir a distintas plataformas para obtener el tipo de protección que deseamos en cada momento. *Como asociación, no podíamos caer en la tentación de recomendar un servicio en concreto, que tuviera que ser usado incondicionalmente y al margen de las circunstancias de la comunicación* (nada más opuesto a nuestra cultura que las soluciones permanentes). Consecuentemente, si queremos crear una cultura de la privacidad, resultará indispensable que como usuarios hagamos un esfuerzo por hacer transparentes nuestras demandas de seguridad en la mensajería, con el objetivo de escoger la aplicación correcta para cada caso[40].

Añadimos a continuación un esquema que repasa algunas de las características mencionadas anteriormente, aplicadas a las aplicaciones de mensajería más populares. Sobra decir que ni es la tabla definitiva, ni contiene todas las características existentes: es sólo un pequeño apoyo a tener en cuenta, que puede ayudar a elegir la aplicación adecuada en cada momento, sin olvidar su condición temporal. La tabla no deja de representar una imagen congelada del panorama en el momento de escribir este libro (último trimestre del año 2018, insistimos), conque será preciso atender a posibles cambios en el funcionamiento de cada servicio conforme el tiempo pase,

---

40 Por ejemplo: cuando se trate de comunicaciones con personas próximas y de confianza, primará disponer de cifrado E2E, y probablemente no será un problema que la otra parte conozca nuestro número de teléfono. Sin embargo, habrá otro tipo de comunicaciones (grupos abiertos o con individuos en los que no podamos confiar) donde resultará jerárquicamente más importante no revelar nuestro número de teléfono, por encima incluso del cifrado E2E.

de manera que nuestra seguridad no quede comprometida por confiar demasiado en la palabra de un manual que, tarde o temprano, pasará a la condición de reliquia.

SMS . El sistema de identificación requiere un número de teléfono, que se muestra a los contactos con los que interactuamos. No existe la posibilidad de acceder al cifrado E2E, de modo que la totalidad de los mensajes que intercambiamos son completamente legibles a ojos del operador de telefonía.

WhatsApp. El sistema de identificación requiere un número de teléfono, que se muestra a los contactos con los que interactuamos. Usa siempre cifrado E2E, tanto en chats individuales como grupales. El modelo de negocio de la empresa (Facebook) consiste de manera exclusiva en la compraventa de datos con fines comerciales, además de cruzar (potencialmente) la información obtenida con las redes sociales Facebook e Instagram para tener unos perfiles de cliente más detallados. Su arquitectura es centralizada y su código es completamente privativo.

Telegram. El sistema de identificación requiere un número de teléfono, aunque no lo expone al resto de usuarios del servicio. El cifrado E2E se limita a los chats secretos, que se tienen que habilitar manualmente. Ni las conversaciones predefinidas ni los grupos tienen disponible este tipo de cifrado, siendo su contenido legible para Telegram. El modelo de negocio de la empresa (Telegram) sigue siendo un misterio, con la única certeza de que delega en buena medida en la figura de Pável Dúrov[41]. Ofrece la opción de autoborrado, aunque sólo en los ya

41 Pável Dúrov es un multimillonario ruso del sector de las nuevas tecnologías, creador entre otros de la red social VK y Telegram.

mencionados «chats secretos», en los cuales tiene que ser activada de forma manual. Su arquitectura es centralizada y solamente el cliente es de código abierto.

Signal. El sistema de identificación requiere un número de teléfono, que se muestra a los contactos con los que interactuamos. Usa siempre cifrado E2E, tanto en chats individuales como grupales. Ofrece la opción de autoborrado para ambos tipos de chats. Lo administra una fundación sin ánimo de lucro (Signal Foundation) fuertemente comprometida con la privacidad. Su arquitectura es centralizada y tanto las aplicaciones de cliente como el servidor son de código abierto.

Wire. El sistema de identificación no requiere necesariamente un número de teléfono, siempre y cuando registremos la cuenta a través del sitio web oficial. Usa siempre cifrado E2E, tanto en chats individuales como grupales. El modelo de negocio de la empresa (Wire Swiss), pese a no ser un completo enigma (dado que tienen una versión de pago para empresas), podría ser más transparente. Su arquitectura es centralizada y tanto las aplicaciones de cliente como el servidor son de código abierto.

Matrix (**Riot**). El sistema de identificación no requiere un número de teléfono. Existe la posibilidad de acceder al cifrado E2E tanto en las salas de chat individuales como grupales, pero se tiene que habilitar de forma manual (hasta entonces, permanecen legibles a ojos de quien gestiona el servidor). Lo administra una fundación sin ánimo de lucro (Matrix.org Foundation). Su arquitectura es federada y tanto las aplicaciones de cliente como el servidor son de código abierto.

APLICACIÓN	CIFRADO E2E	AUTOBORRADO DE MENSAJES	IDENTIFICACIÓN CON NÚMERO DE TELÉFONO
SMS	NO	NO	SÍ
WHATSAPP	SÍ	NO	SÍ
TELEGRAM	Sólo en los chats secretos (no aplicable en grupos)	Sólo en los chats secretos habilitado manualmente	SÍ
SIGNAL	SÍ	SÍ, aunque debe ser habilitado manualmente	SÍ
WIRE	SÍ	NO	No necesaria en caso de activar la cuenta a través de la web
MATRIX (RIOT)	SÍ, aunque debe ser habilitado manualmente	NO	No necesaria

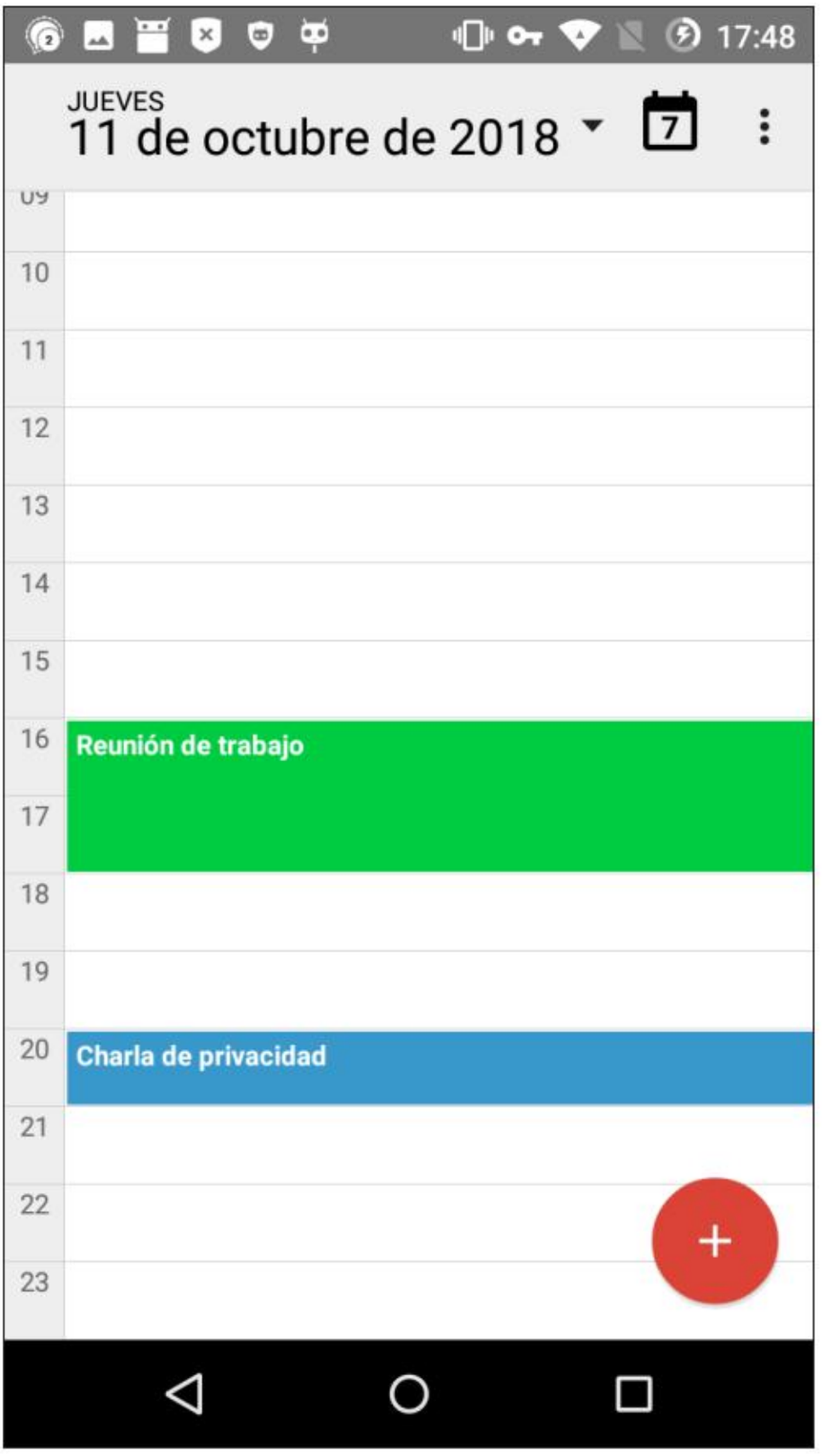
NÚMERO DE TELÉFONO EXPUESTO	ARQUITECTURA	DISPONIBILIDAD DEL CÓDIGO	MODELO DE NEGOCIO
SÍ	CENTRALIZADA	-	EMPRESA
SÍ	CENTRALIZADA	NO	EMPRESA PROPIEDAD DE FACEBOOK INC.
APLICACIÓN	CENTRALIZADA	SÍ	EMPRESA
SÍ	CENTRALIZADA	SÍ	FUNDACIÓN SIN ÁNIMO DE LUCRO
NO	CENTRALIZADA	SÍ	EMPRESA
NO	SISTEMA FEDERADO	SÍ	FUNDACIÓN SIN ÁNIMO DE LUCRO

Aplicaciones respetuosas con tu privacidad

A continuación, el lector encontrará un pequeño listado de reseñas de aplicaciones que se adecúan a los criterios de privacidad y seguridad mencionados en la introducción del libro. Dicha lista no abarca la totalidad de aplicaciones existentes y no se rige por un orden de tipo jerárquico: únicamente quiere ser una referencia para ilustrar algunas alternativas seguras a las aplicaciones y servicios mayoritarios.

DAVx5 (anteriormente DAVdroid)

Alternativa al calendario de Google en Android
(disponible nativamente en iOS)



Descripción:

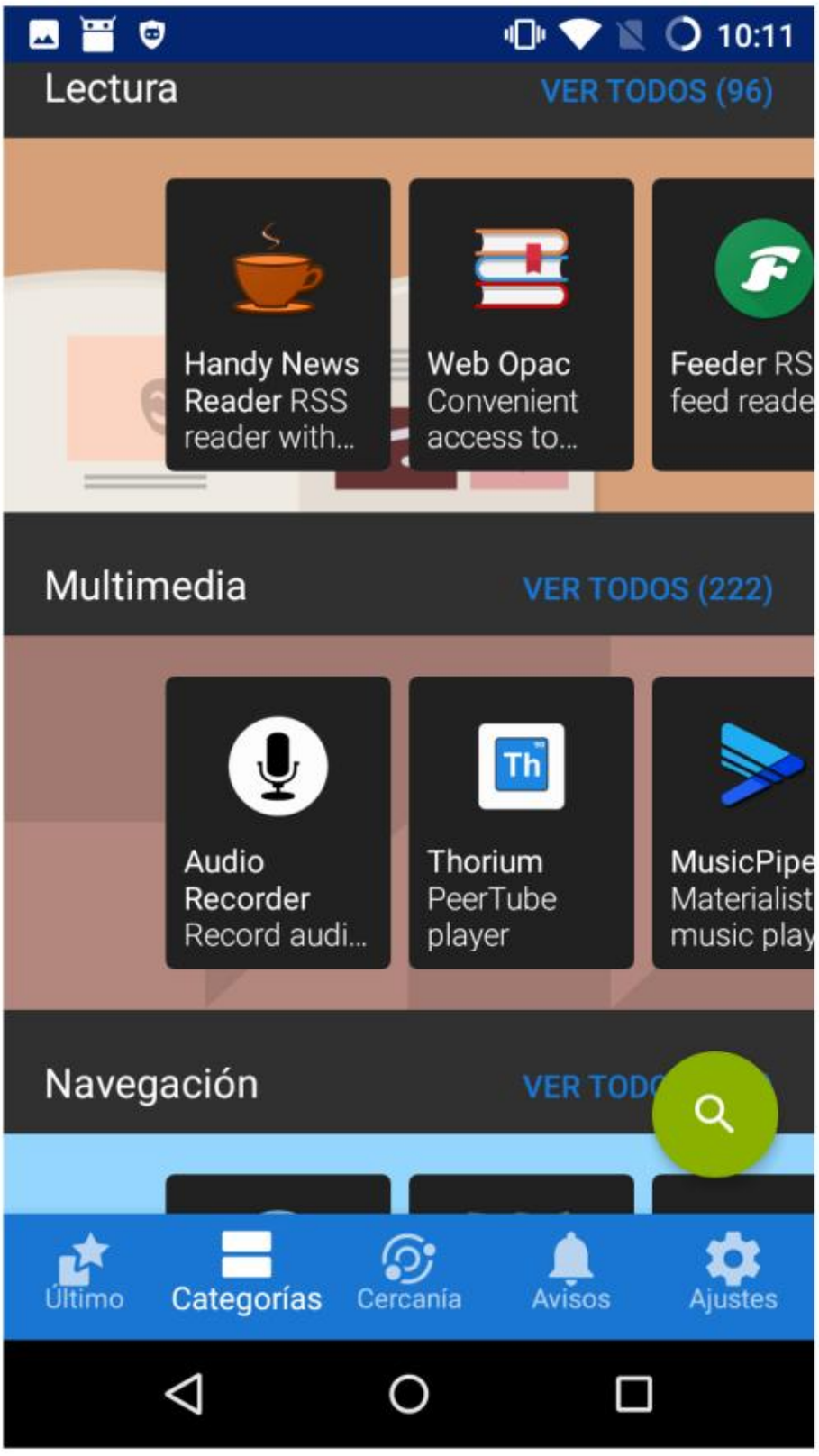
Esta aplicación permite sincronizar el calendario de Android y otras aplicaciones de calendario como Etar mediante el protocolo CalDAV, ofrecido por muchos proveedores de correo electrónico alternativos. Es la alternativa ideal al calendario de la cuenta de Google.

Características de privacidad:

Si sincronizamos nuestro calendario con un proveedor de correo que respete nuestra privacidad, tendremos mayor confianza en que no haya nadie que espíe los detalles de nuestra agenda personal.

F-Droid

Alternativa a Google Play Store en Android



Descripción:

Repositorio de aplicaciones con una funcionalidad similar a Google Play Store, ofreciendo tan sólo aplicaciones cuya licencia es libre.

Algunas de las características son:

- Permite añadir nuevos repositorios (por ejemplo, The Guardian Project).
- Notificaciones cuando las aplicaciones instaladas tienen actualizaciones.
- Descripción de la aplicación (en algunos casos con capturas de pantalla), así como valoración de características que puedan no ser respetuosas con la privacidad.
- Listado de aplicaciones recientemente actualizadas (ideal para descubrir nuevas aplicaciones).
- Permite compartir aplicaciones instaladas en un teléfono con otro terminal sin necesidad de conexión a Internet.

Características de privacidad:

F-Droid sólo ofrece aplicaciones cuya licencia es libre y que tienen su código disponible públicamente. Este hecho ayuda a establecer confianza en que la aplicación no tendrá funcionalidades ocultas que espíen al usuario. Además, las descripciones de las aplicaciones indican en qué casos éstas usan servidores de terceros que podrían obtener datos del usuario.

Firefox

Navegador web para Android e iOS

Descripción:

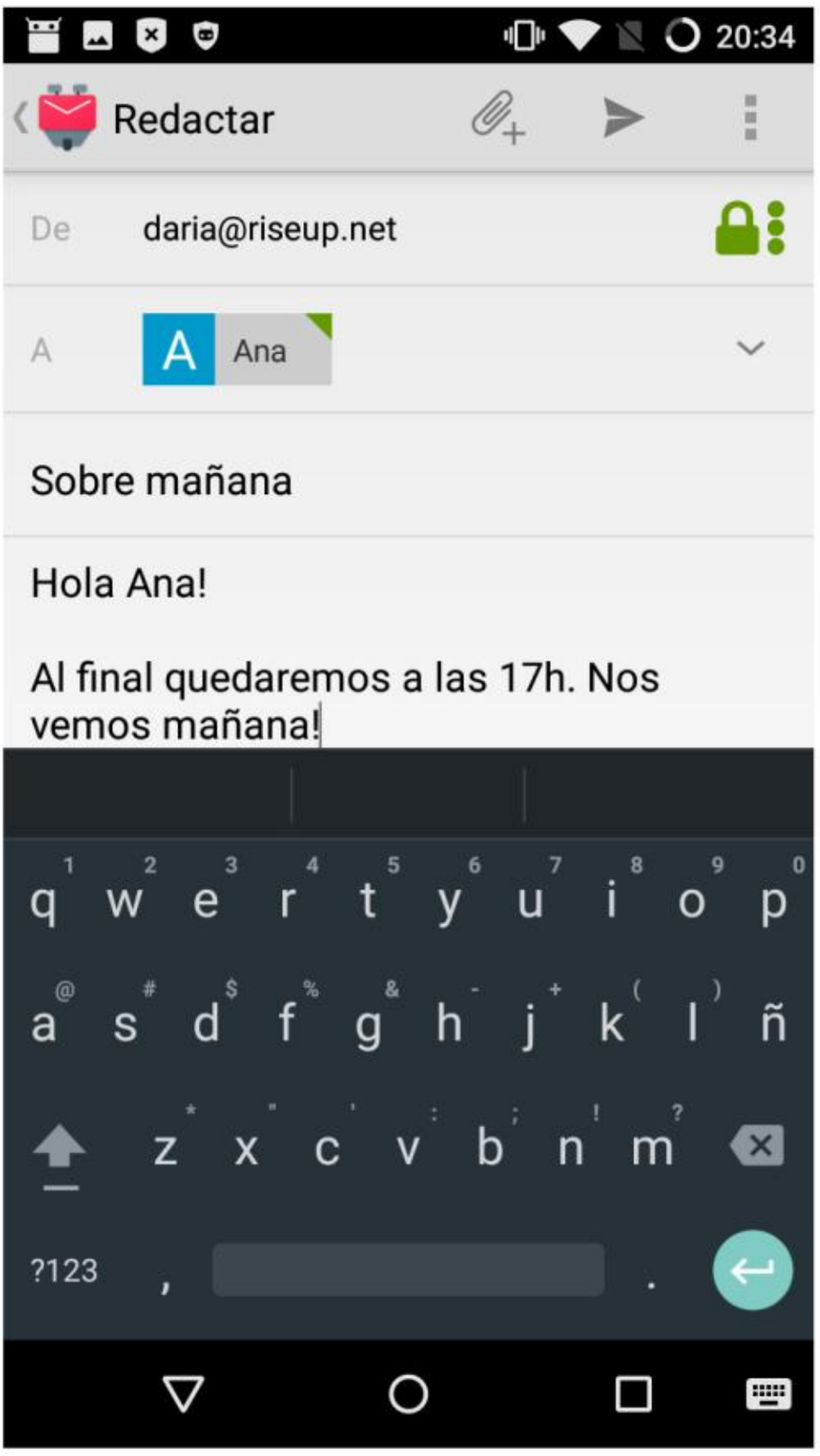
Navegador web desarrollado por Mozilla, una fundación sin ánimo de lucro comprometida con la privacidad y la cultura libre. Firefox dispone de complementos que permiten mejorar nuestra privacidad al navegar por la web.

Características de privacidad:

Firefox permite habilitar complementos de privacidad desde su página de descargas, accesible desde el menú. Consulta la sección «Navegación y privacidad» para saber más al respecto.

K-9 Mail

Gestor de correo para Android



Descripción:

Cliente de correo electrónico (equivalente a Thunderbird en PC) que nos permite acceder, leer y enviar correos electrónicos desde nuestro dispositivo Android.

Características de privacidad:

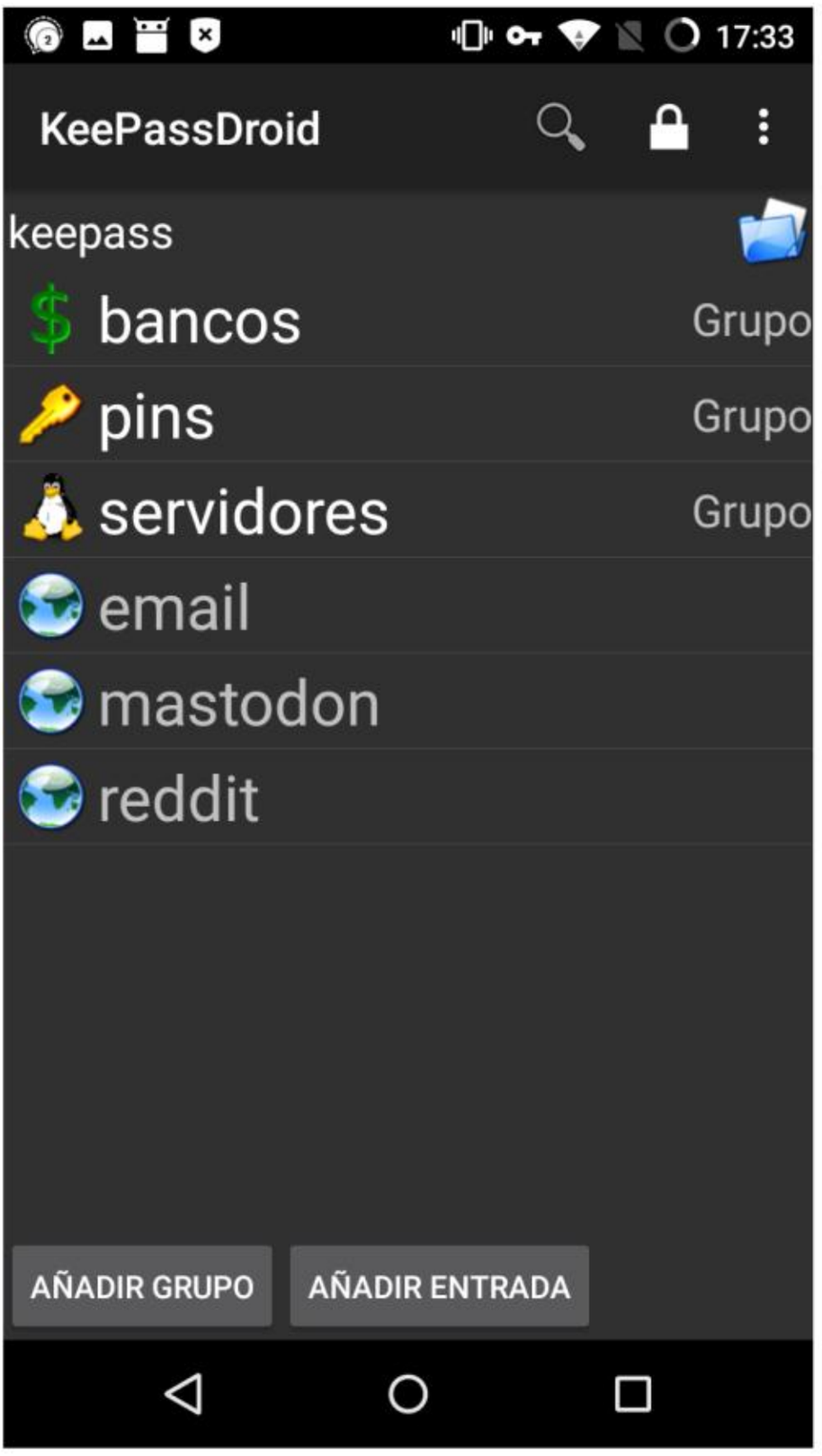
K-9 Mail es un cliente de correo de código abierto en el que podemos configurar una cuenta de correo de cualquier proveedor que soporte los protocolos de correo estándar (POP3, IMAP, SMTP).

Esta aplicación, junto con el uso de un proveedor de correo electrónico ético, supone una mejora considerable de nuestra privacidad respecto a aquellos proveedores cuyo modelo de negocio son nuestros datos.

Además, se puede integrar con OpenKeyChain para enviar correos cifrados. Si usamos PGP para proteger nuestros correos y queremos poder seguir haciéndolo desde nuestro smartphone, ésta es una buena opción.

KeePassDroid

Gestor de contraseñas para Android (en iOS: MiniKeePass)



Descripción:

Aplicación que permite consultar y añadir contraseñas a una base de datos cifrada, y que además es compatible con KeePass, su equivalente de escritorio.

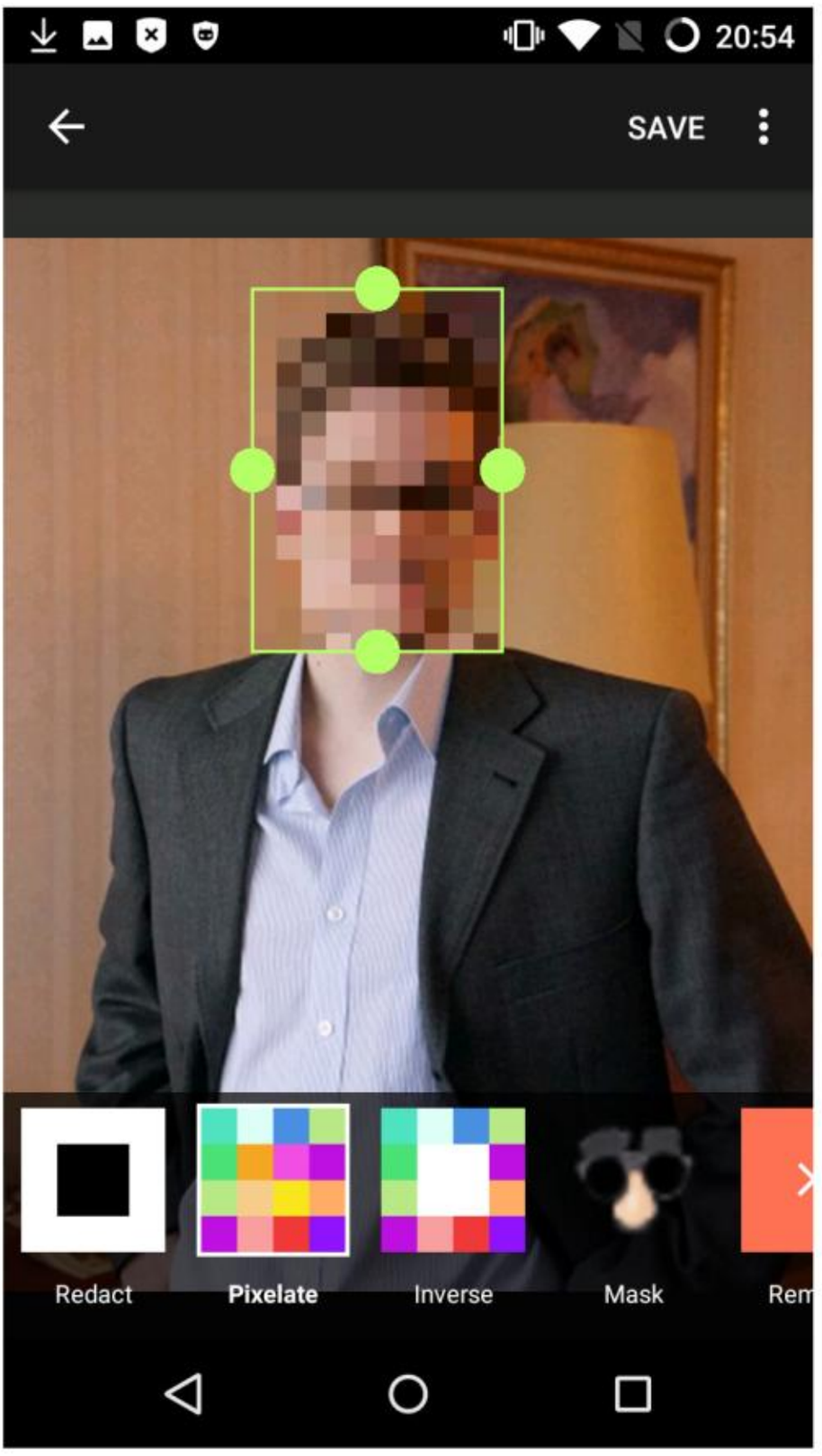
Útil para llevar claves encima de forma segura. Accede a tu base de datos cifrada para copiar tus contraseñas cuando lo necesites y no tener que recordarlas.

Características de privacidad:

El uso de contraseñas cortas e inseguras puede ser catastrófico para nuestra privacidad. Usar un gestor de contraseñas es una forma muy práctica de poder tener una contraseña diferente y segura para cada servicio sin necesidad de memorizarlas todas.

ObscuraCam

Aplicación de fotografías para Android



Descripción:

Aplicación que ofrece al usuario la posibilidad de realizar o editar fotografías protegiendo la información contenida en ellas. Desde el pixelado de caras hasta la eliminación de metadatos que puedan asociar la fotografía con la persona que la ha realizado. Es una pequeña navaja suiza para la privacidad en las instantáneas de nuestro smartphone.

Características de privacidad:

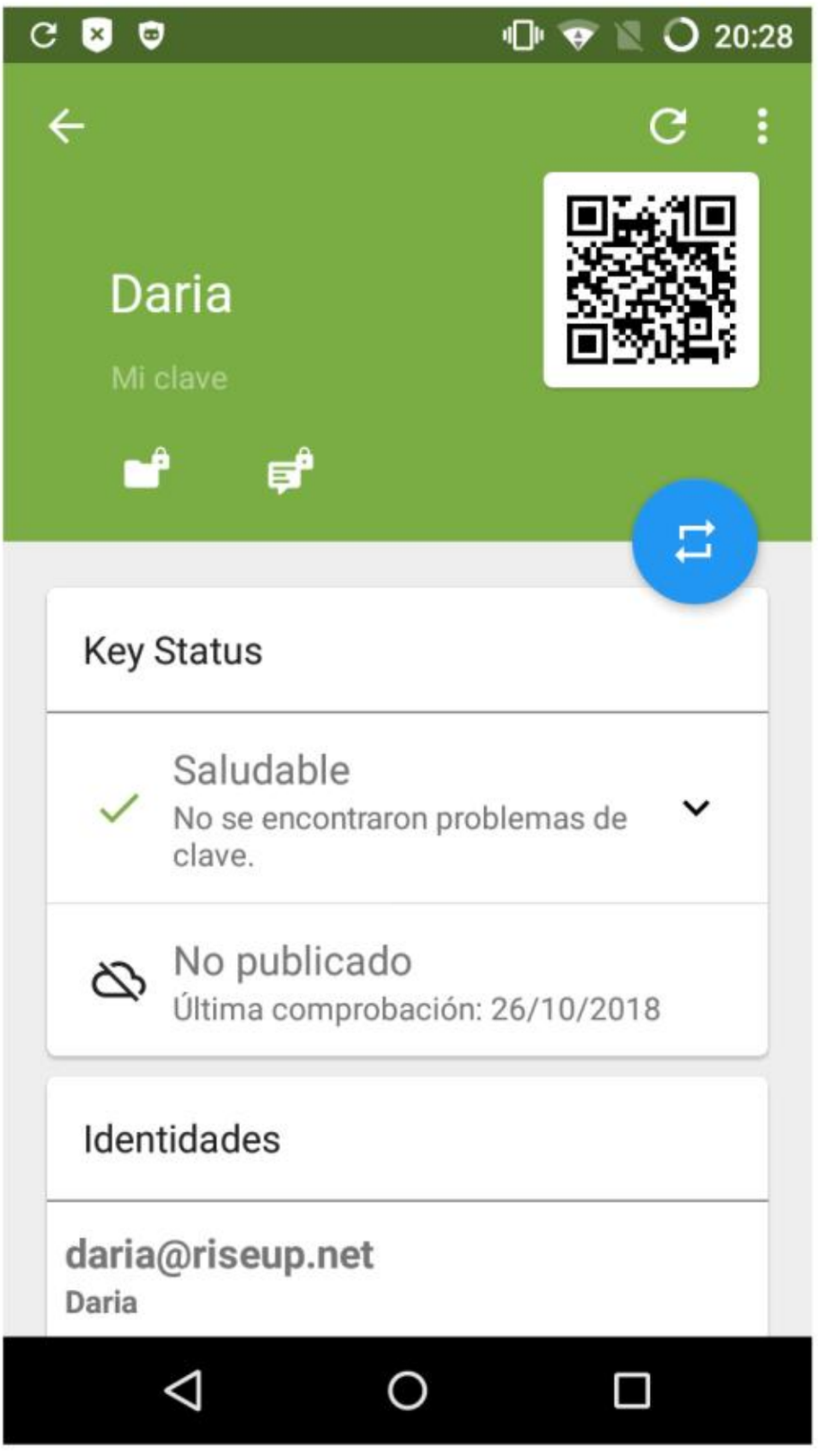
- Obtención de fotografías con detección y pixelado automático de caras.

- Eliminación automática de metadatos de las imágenes obtenidas con la aplicación.

- Posibilidad de editar imágenes y limpiarlas de metadatos e información personal antes de compartirlas o publicarlas.

OpenKeyChain

Gestor de claves PGP para Android



Descripción:

Aplicación que permite gestionar claves PGP para enviar y recibir correos cifrados.

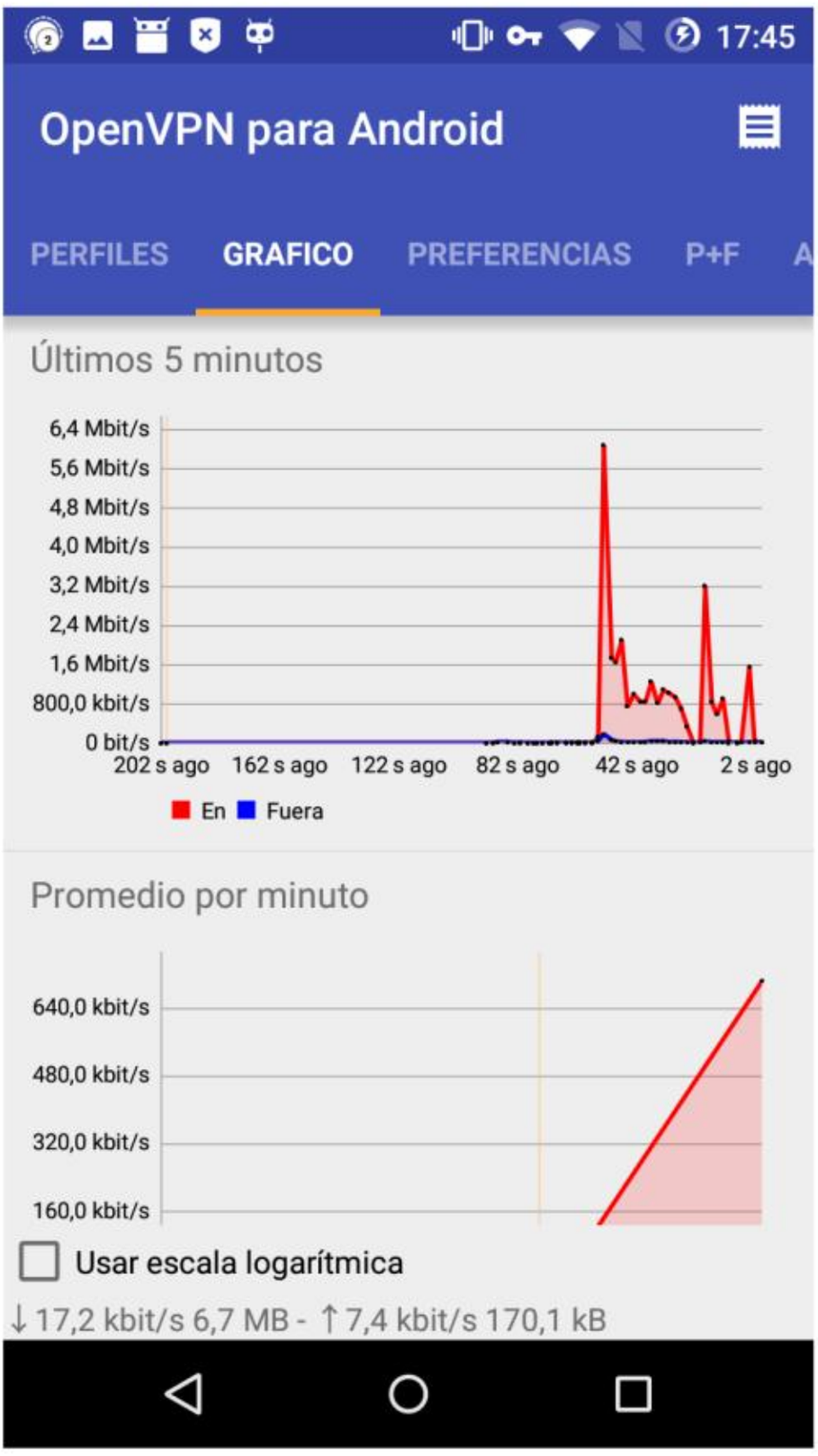
OpenPGP es un protocolo estándar para enviar correos usando cifrado de extremo a extremo (E2E). Para utilizar este sistema de protección de correo correctamente, es necesario comprender algunos conceptos básicos de criptografía asimétrica. Explicar PGP está más allá de los objetivos de este libro, por lo que nos limitamos a explicar que si sabes utilizarlo, puedes hacerlo desde tu Android con esta aplicación.

Características de privacidad:

- Permite gestionar claves PGP desde nuestro smartphone.
- Es integrable con K-9 Mail.

OpenVPN

Gestor de VPN para Android e iOS



Descripción:

Aplicación para cifrar el tráfico de red del teléfono a través de una VPN con el protocolo abierto OpenVPN (ofrecido por multitud de proveedores). La aplicación es sencilla de usar: tan sólo hay que importar la configuración de OpenVPN (normalmente ofrecida por el proveedor) y activar la conexión a la VPN. Además, la aplicación se puede configurar para conectarse automáticamente al encender el teléfono.

Características de privacidad:

Al usar una VPN conseguimos que el proveedor de red (compañía telefónica, generalmente) no sepa qué páginas ni qué servicios usamos en Internet. Además, ayuda a dificultar que las páginas que visitemos nos identifiquen (ya que estamos enmascarando nuestra IP real).

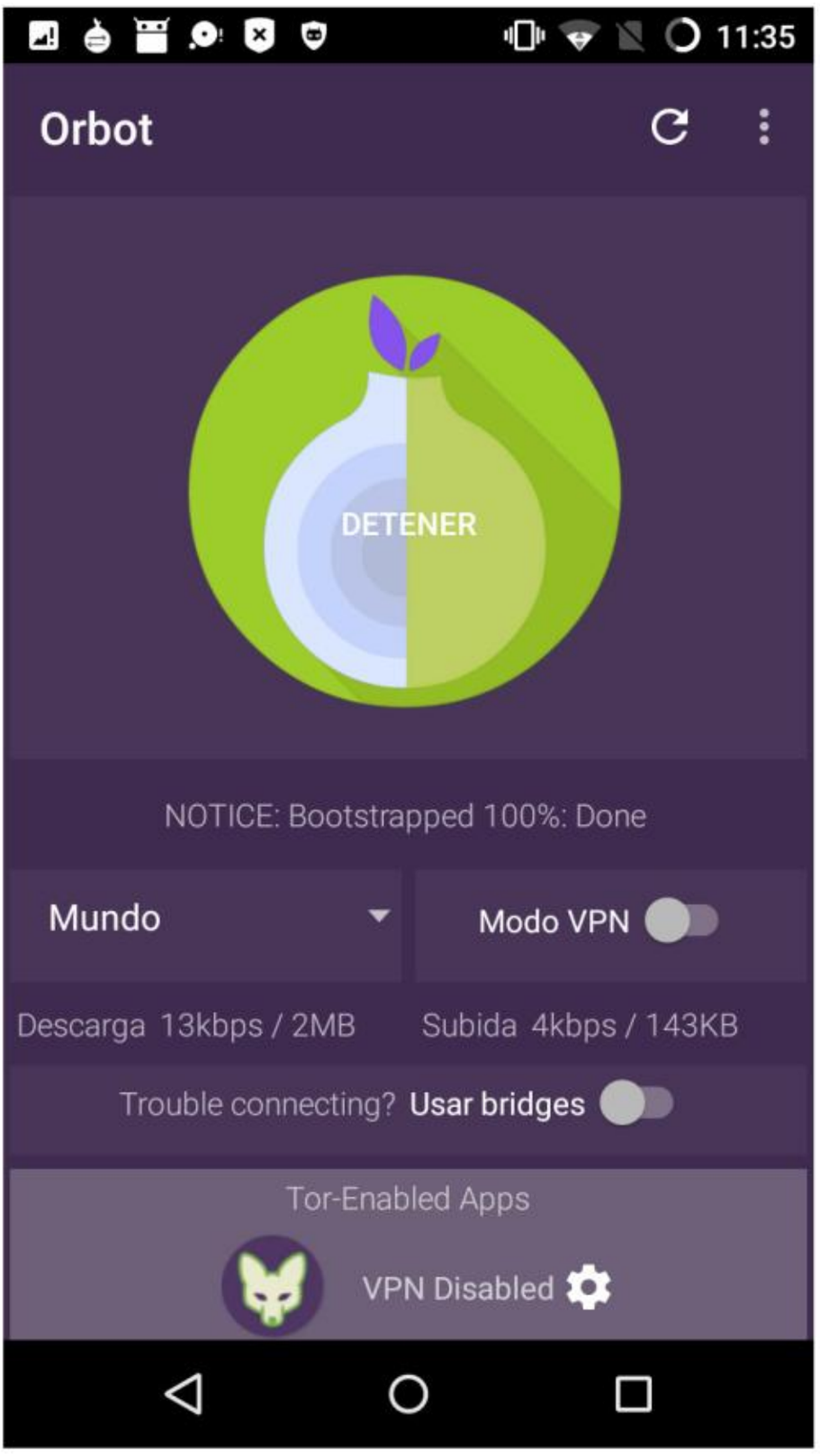
Es muy útil para conexiones en redes wifi sin confianza (aeropuerto, biblioteca, etc.)[42].

---

42 En caso de que la conexión wifi requiera *login* mediante portal cautivo (ventana que solicita credenciales del usuario para acceder a Internet), habrá que desactivar OpenVPN for Android temporalmente para hacer el *login*. Naturalmente, esto conlleva que durante este intervalo un atacante que esté en la misma red wifi pueda observar e incluso modificar el tráfico que de otra manera estaría protegido por el protocolo OpenVPN.

Orbot

Red de anonimización Tor en Android



Descripción:

Aplicación que permite conectar otras aplicaciones de tu teléfono con la red Tor. Es el equivalente al programa Tor en PC[43].

Características de privacidad:

- Cualquier aplicación que permita acceder a Internet vía *proxy* (SOCKS) puede conectarse con Orbot para anonimizar el tráfico.

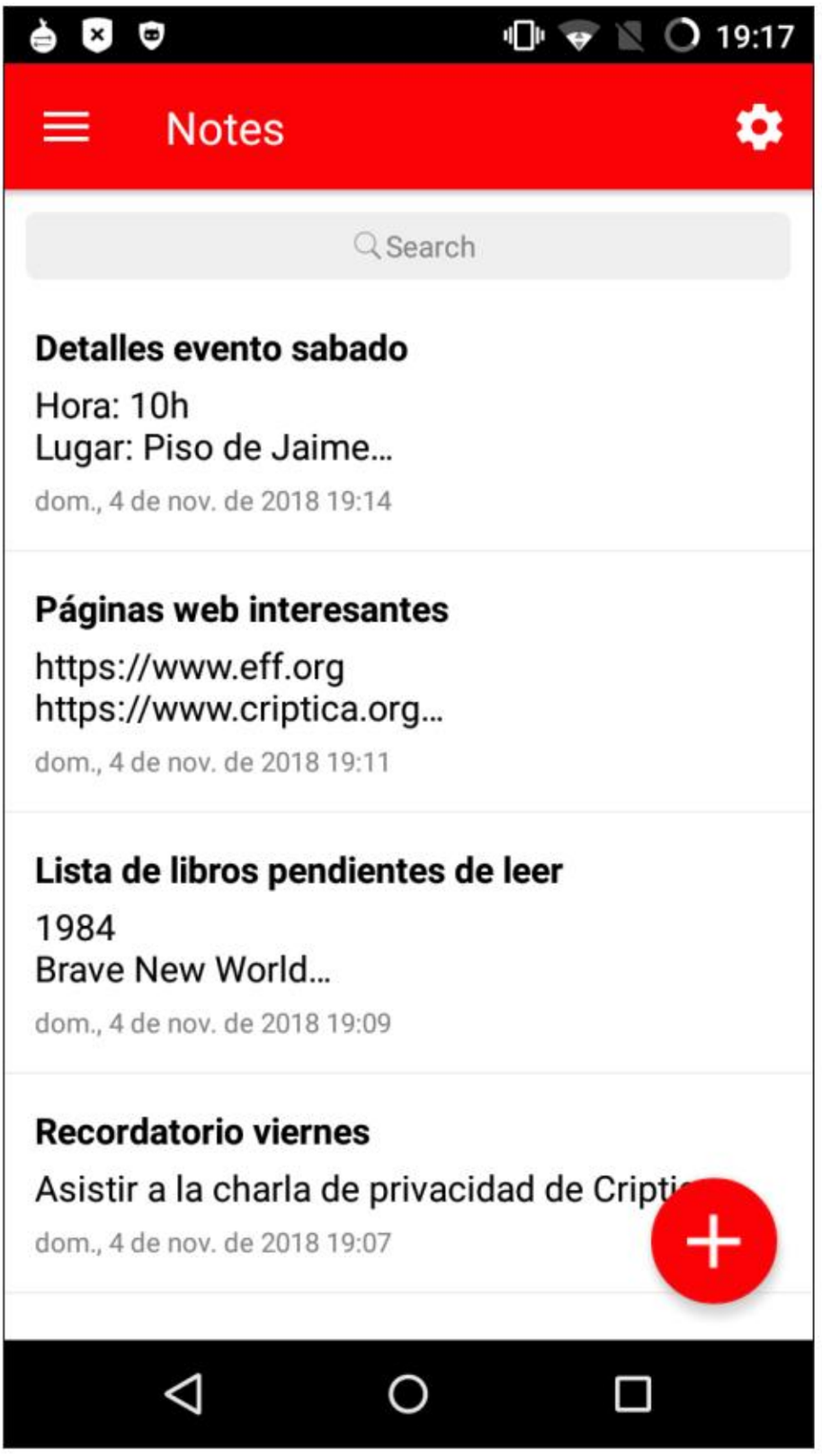
- El Modo VPN permite enrutar el tráfico de nuestras aplicaciones a través de Tor, ofreciéndonos la posibilidad de escoger qué aplicaciones queremos conectar a Tor y cuáles no.

- En el momento de escribir estas líneas, TorBrowser for Android necesita Orbot para poder funcionar correctamente.

43 Puedes informarte más sobre el funcionamiento de Tor en su página oficial: https://torproject.org.

Standard Notes

Aplicación de notas segura para Android e iOS



Descripción:

Aplicación para sincronizar notas de manera segura entre todos tus dispositivos. Tiene un diseño minimalista para favorecer una escritura fluida, con un apartado de configuraciones reducido. Además, puedes asignar etiquetas a cada nota para encontrarlas con rapidez.

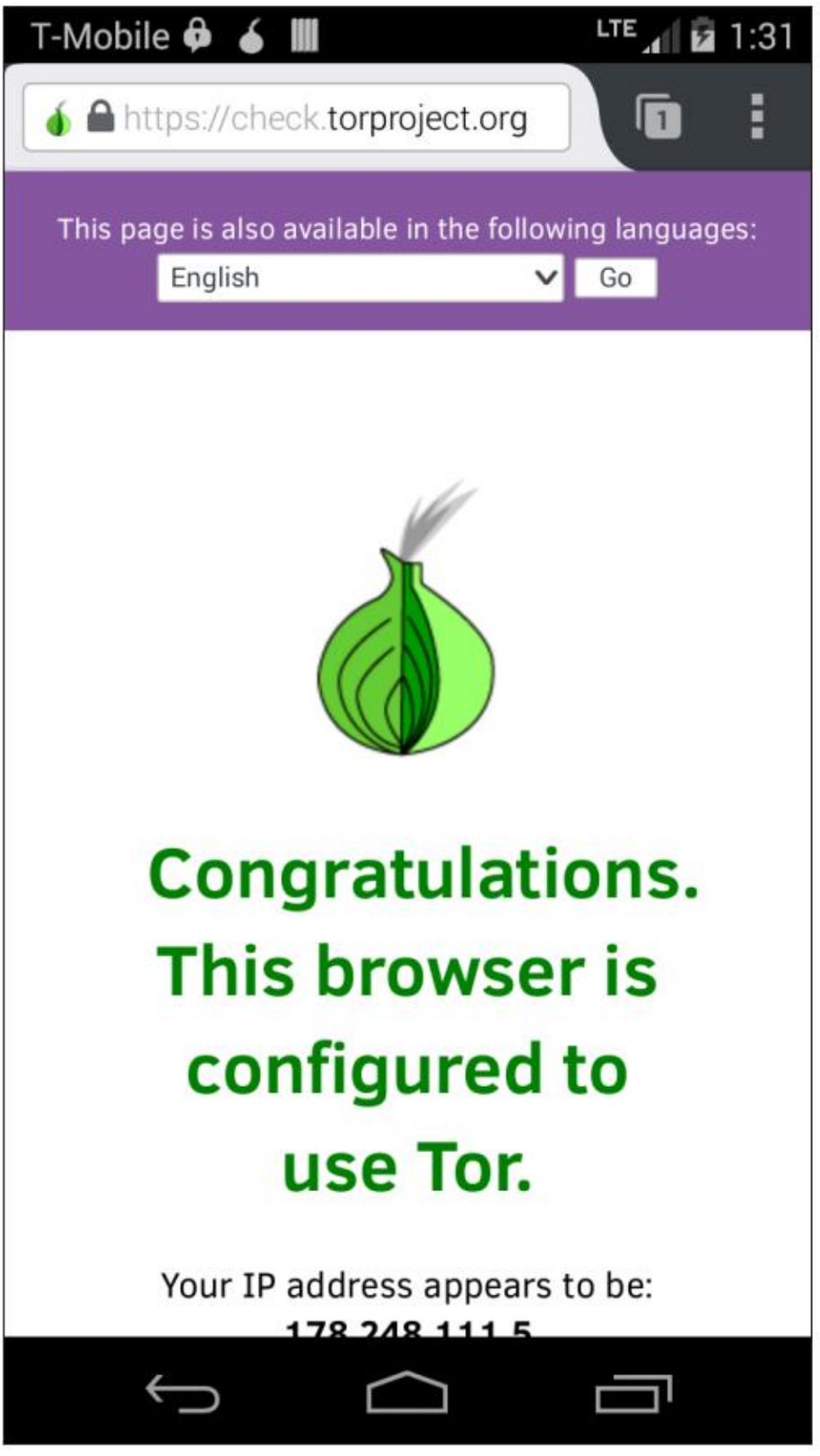
Características de privacidad:

- Todas las notas almacenadas en Standard Notes se cifran por defecto, de manera que ni el propio proveedor puede tener acceso a nuestra información.

- La empresa que gestiona la aplicación tiene un compromiso férreo con la privacidad, renunciando (en la fecha en la que escribimos esto) al uso de herramientas de análisis comercial en sus aplicaciones.

Tor Browser

Navegador web Tor para Android
(en iOS: OnionBrowser)



Descripción:

Navegador basado en Firefox que te permite navegar por la web de manera anónima. Esta aplicación utiliza la red de Tor para acceder a las páginas que quieres visitar, enmascarando tu IP y reduciendo la probabilidad de que la página visitada identifique quién eres o desde dónde te conectas. Es una aplicación oficial de Tor Project.

En iOS encontramos OnionBrowser, mantenido por Mike Tigas, desarrollador y periodista de investigación en ProPublica.

Características de privacidad:

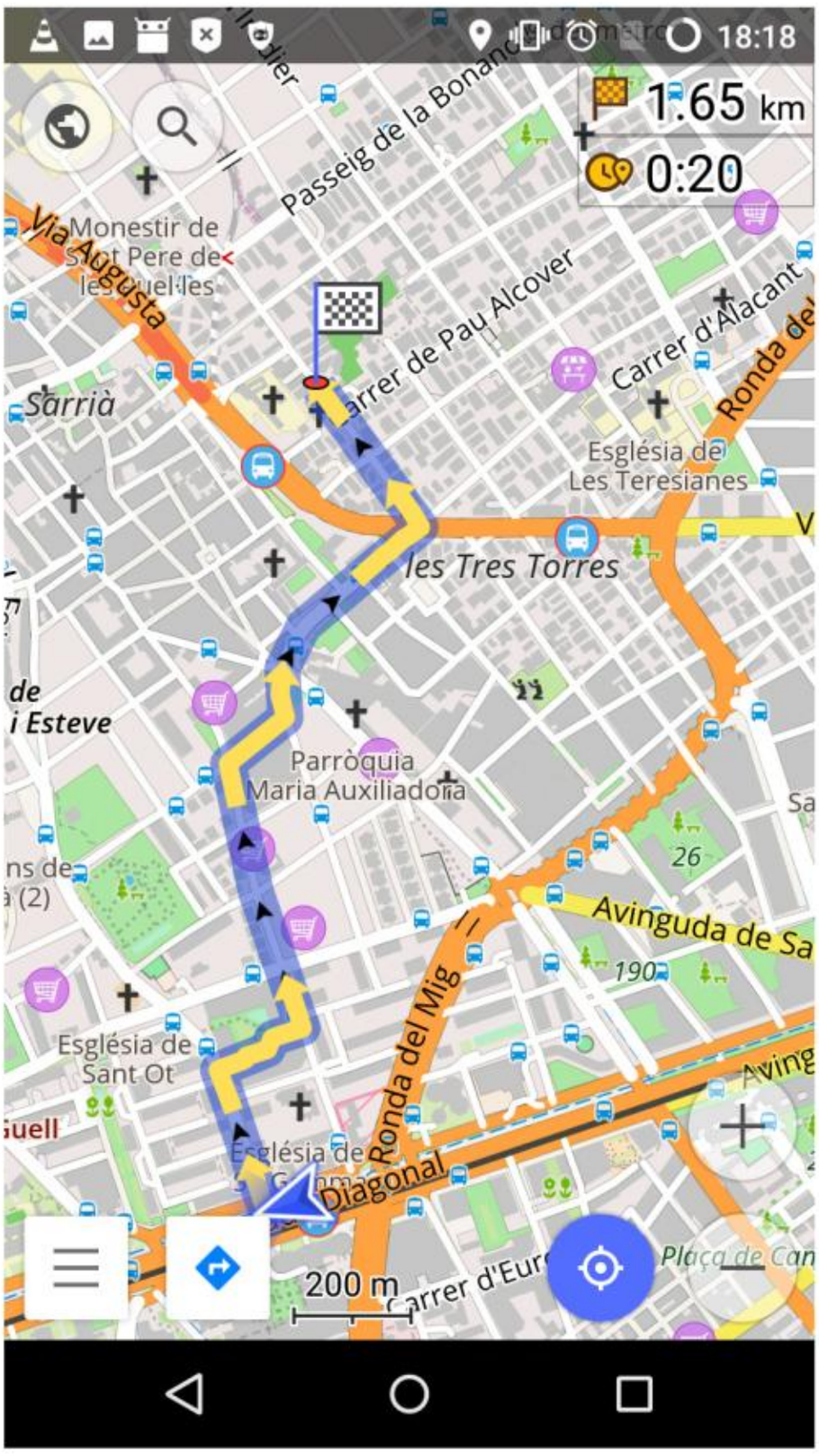
- Acceso anónimo a páginas web: las páginas que visitas no podrán saber tu IP real ni relacionar tu conexión con actividad anterior o posterior mediante las técnicas habituales.

- Acceso a servicios ocultos de Tor: podrás acceder a direcciones acabadas en *.onion*, llamados servicios ocultos o *onion services*. Estas páginas se caracterizan por ser sólo accesibles desde Tor y no se puede determinar su IP o localización de forma sencilla. Tampoco se puede determinar la localización de sus visitantes.

- La aplicación no permite hacer capturas de pantalla.

OsmAnd

Alternativa a Google Maps para Android



Descripción:

Aplicación ideal para reemplazar a Google Maps. Utiliza los mapas abiertos del proyecto OpenStreetMap, una colección de mapas de todo el mundo colaborativa, llevada a cabo en parte por voluntarios y de libre distribución y uso. Esta aplicación ofrece muchas características interesantes, como por ejemplo:

- Los mapas de cualquier territorio (por ejemplo toda España) se pueden descargar para consulta *offline*.

- Permite añadir localizaciones favoritas, organizarlas y compartirlas con otros usuarios.

- Puede mostrar sitios como restaurantes, tiendas, gasolineras, puntos de interés con descripciones extraídas de Wikipedia, así como paradas de transporte público (y en algunos casos sus rutas), todo ello sin necesidad de conexión.

- Ofrece navegación para coche, bici y a pie (usando los caminos indicados para cada caso, incluyendo carriles bici y rutas de senderismo) con instrucciones de voz en castellano. La ruta en coche muestra lo que se espera de un navegador GPS para vehículos: velocidad actual, velocidad máxima de la vía, tiempo estimado hasta llegar al destino o recálculo de ruta al desviarse.

- Permite registrar rutas, exportarlas e importarlas.

A diferencia de Google Maps, OsmAnd no ofrece navegación para usar transporte público (aunque sí se pueden consultar las rutas y paradas) ni recomendación de rutas según el tráfico en tiempo real.

Características de privacidad:

Dado que la aplicación puede trabajar con mapas descargados, no necesita enviar nuestra posición a ningún servidor, por

lo tanto, nuestra localización no será compartida con ningún servicio externo[44]. También es posible utilizar los mapas en línea de OpenStreetMap, pero en ese caso sí que se revelaría nuestra posición a los servidores del proyecto.

44 La tecnología GPS permite que los dispositivos conozcan su ubicación geográfica tan sólo recibiendo la señal de los satélites, sin la necesidad de enviar ningún dato, conque nuestra posición real seguirá protegida.

ANEXOS

Seguridad y libertad en condiciones no ideales: una polémica final

> «La 'razón pura' no es el entendimiento, sino una manera extremada de funcionar de éste. Cuando Robinsón aplica su inteligencia a resolver los urgentes problemas que la isla desierta le plantea, no usa de la razón pura. Impone a su intelecto la tarea de amoldarse a la realidad circundante, y su funcionamiento se reduce a combinar trozos de esa realidad. La razón pura es, por el contrario, el entendimiento abandonado a sí mismo, que construye de su propio fondo armazones prodigiosas, de una exactitud y de un rigor sublimes. En vez de buscar contacto con las cosas, se desentiende de ellas y procura la más exclusiva fidelidad a sus propias leyes internas»[45].
>
> José Ortega y Gasset

Como sucede en cualquier otra disciplina, la historia de la seguridad está repleta de polémicas, puntos de inflexión, impresiones radicalmente opuestas y hasta rupturas. Lejos de existir una unidad compartida entre la pluralidad de voces que participan de la discusión, cada sector acaba por proyectar un camino propio a partir de sus circunstancias particulares, de su singular experiencia.

«De la unidad no queda más que la nostalgia»[46]. Y por el bien de la disciplina, creemos que es bueno que así sea: nada

---

45 José Ortega y Gasset (1939): *El tema de nuestro tiempo*, Espasa-Calpe, Buenos Aires, p. 110.

46 Comité Invisible (2017): *Ahora*, Pepitas de Calabaza, Logroño, p. 30.

más ajeno a la buena marcha de un debate que las burbujas de opinión, versiones informatizadas de las asfixiantes pautas de socialización vigentes en ciertos círculos militantes desde hace décadas, encomendadas a simular exteriormente una unidad de opiniones que nunca han tenido.

La unidad de opiniones es todo lo contrario a lo que, como disciplina, se nos exige. Asumirla como ideal significa vagar entre las hojas de una tijera, que limita o directamente suprime los diagnósticos alternativos de una misma situación. Equivale a dejar congelada la tarea de la reflexión, paralizar el debate sin llegar a unas conclusiones satisfactorias para todo el mundo, además de desaprovechar el potencial de exámenes distintos que pueden enriquecer el propio punto de vista.

Entendemos que la seguridad, para ser efectiva, necesita alimentarse del mayor número de impresiones y de la mayor cantidad de experiencias posibles. A nuestro pesar, practicamos este arte sin tener una hoja de respuestas, es decir, soluciones permanentes para todos los problemas que se nos puedan aparecer. A lo sumo, disponemos de distintos manuales de instrucciones de tipo general (como éste), que nunca van a ser capaces de estar a la altura de nuestras demandas de seguridad concretas en cada situación. Y tampoco se les debería exigir tanto.

Igual que sucede con los manuales, un código de ideales o valores fomenta el rápido aprendizaje al familiarizarnos con un determinado tipo de respuesta, pero en ambos casos ésta suele ser una mera indicación de tipo abstracto, que no nos sirve para resolver situaciones cotidianas. Crítico con las abstracciones de este cuño, Michael Oakeshott[47] habla de la «política del libro»[48] para referirse al tipo de política que, asimilándose con la ingeniería, la reduce a «un conjunto de reglas que, idealmente, conforman un método infalible cuya

---

47 Michael Oakeshott fue un filósofo del escepticismo inglés del siglo XX, afín al conservadurismo político.

48 Michael Oakeshott (2017): *Ser conservador y otros ensayos escépticos*, Alianza Editorial, Madrid, p. 47.

aplicación es mecánica y universal»[49]. Y dada la formación técnica de una buena parte de los expertos en seguridad, parece casi inevitable la tentación (tan en boga en los distintos manuales) de querer explicarlo todo mediante su formulación en «reglas, principios, directrices, máximas» que son siempre abstractas, perdiendo el conocimiento sobre el terreno, su faceta eminentemente práctica, *operativa*.

Como resultado de esta percepción de la seguridad no como una laboriosa tarea pedagógica, sino como algo parecido al despliegue ordenado de una operación de ingeniería, la manera de afrontarla a nivel de posicionamientos o valores se ve reducida a un repertorio de hermosas recetas en abstracto, aplicables por encima de cualquier circunstancia, «que deberá[n] adquirirse por instrucción en una ideología más que por una educación en el comportamiento»[50]. Así, valores que desde Críptica compartimos, como son el software libre o los proyectos comunitarios, dejan con ciertas posturas morales de ser meros principios orientativos de las acciones para convertirse en auténticas barreras ideológicas, que no se pueden sortear en modo alguno.

Situar un principio como condicionante de toda prescripción posterior, por bienintencionado y loable que pueda ser, limita inmediatamente la flexibilidad estratégica de los formadores, puesto que disminuye la cantidad de instrumentos que podemos poner al servicio del usuario. Ciertamente, una aplicación que reuniera el conjunto de características que deseamos como asociación (segura por defecto, usable, software libre y estar enmarcada en un proyecto sin ánimo de lucro) tendría todos los números para que la acabáramos recomendando..., pero los servicios que cumplen esas condiciones en su totalidad conforman una (honrosísima) excepción, claramente minoritaria en un ecosistema móvil en el que no existen tantas alternativas como nos gustaría.

Hasta ahora, la usabilidad ha pagado los platos rotos del proceso de autolimitación que resulta de la rigidez de princi-

---

49 *Ibid.*, p. 57.

50 *Ibid.*, p. 131.

pios, siendo el usuario final (naturalmente, no el experto en seguridad, ni tampoco el ingeniero) el gran perjudicado. La mente del técnico, que se abstrae de sus propias circunstancias (formación específica, experiencia profesional, facilidad para interaccionar con las tecnologías de la información, entorno personal proclive a probar las últimas herramientas), ha dejado de considerar la usabilidad como un requisito indispensable, porque en sus condiciones particulares (favorables a la experimentación constante) no se la contempla como necesaria, sino más bien como un lujo prescindible. Así, el usuario debiera verse forzado a *aprender*, a dominar la técnica igual que lo hace el ingeniero desde su rectitud moral, dejando de lado el hecho de que no comparta su misma situación.

Queremos, con esta parte final, llamar a la polémica. Por el bien de la disciplina de la seguridad, a pesar de que ello nos pueda conllevar posibles críticas por nuestra falta de pureza ideológica. Afirmamos:

Aunque creamos que se necesita pedagogía en materia de seguridad, creemos que son nuestros principios los que deben terminar por adaptarse a las circunstancias de cada persona, no al revés. No estamos en la situación de exigir al usuario final aprender más allá de un umbral mínimo, ni de justificar su pérdida de usabilidad por tratarse de una herramienta que se amolda mejor a los valores que predicamos.

Esta decisión entra dentro de nuestra responsabilidad desde el momento en que sabemos que no todo nuestro público es experto en la materia ni tampoco desea llegar a serlo algún día, pero siente una franca inquietud ante las constantes intromisiones a su privacidad.

Vayamos ahora a algunas de las consecuencias prácticas de este posicionamiento, que nos ha llevado meses de debate a nivel interno. Durante el largo proceso de elaboración de este manual, la búsqueda de una seguridad móvil robusta para el usuario medio nos ha conducido a tener que plantearnos seriamente las ventajas e inconvenientes tanto de Android como de iOS, sin dar nada por sentado y pese a que este examen pueda acarrear ver menoscabados (en parte) algunos de nuestros principios. Aunque en algunos sectores puedan considerar ex-

tremadamente superfluo este dilema (dado que el iOS de Apple representa todo lo contrario a los valores del software libre), un factor diferencial ha complicado mucho nuestra elección: el hecho de que, a diferencia de los dispositivos Android, el iPhone opte por la seguridad por defecto en su configuración. Cualquiera que haya interaccionado mínimamente con terminales Android, sabe que son poco afines a tener configurados de serie los parámetros de seguridad o a hacerlos intuitivos para el usuario, además de no poseer tampoco la sencillez derivada de la uniformidad de interfaces, pues cambian según modelo, versión y fabricante[51].

Nuestro periplo de los últimos años nos ha llevado a concluir que, para ser efectiva, la seguridad tiene que ser intuitiva, accesible y fácil de conseguir. Y la mejor manera de hacerlo es pidiéndole lo menos posible al usuario, proporcionándole de antemano la configuración adecuada para que su dispositivo disponga de un considerable nivel de seguridad tan pronto como empiece a usarlo. Cuantos más procesos se dejan en manos del usuario final, mayor es el umbral de exclusión, más difícil le es aprenderlos todos y más probable que se equivoque al configurarlos u olvide algún parámetro importante. Ahí radica el mérito de herramientas como Signal o Wire: han hecho que la seguridad no sea opcional, sino que venga incrustada por defecto en la aplicación, de forma que el menos hábil tiene acceso al mismo nivel de protección que el experto que lleva años en la disciplina.

El iPhone, a pesar de pertenecer a un ecosistema cerrado y tutelado por Apple, también mantiene una férrea política de seguridad por defecto, dado que se trata de un dispositivo cuya memoria se encuentra cifrada de serie y las opciones de

---

51 Aprovechamos para mencionar que la existencia de más de un actor en el ecosistema de Android (Google y el fabricante, como mínimo) perjudica potencialmente el ritmo de adopción de las actualizaciones de seguridad: hasta que el fabricante (Huawei, Samsung, Xiaomi…) no las incorpora a su versión personalizada de Android, los dispositivos de la marca siguen desprotegidos independientemente de que Google sí haya publicado la actualización.

seguridad y privacidad son eminentemente simples, además de compartir todos los modelos una misma interfaz. Asimismo, Apple mantiene una política de actualizaciones de seguridad sumamente regulares, hasta el punto de que un 75 % de sus dispositivos en uso son compatibles con la última versión de iOS en el momento de escribir estas líneas[52].

Por el contrario, la mayoría de marcas de Android no cifran por defecto la memoria de sus productos, no los actualizan con la regularidad que deberían (solamente un 21,5 % del total de teléfonos Android disfrutaban en octubre del 2018 de la última versión del momento, Oreo, lanzada un año atrás[53]) y la configuración de privacidad se encuentra dispersa entre múltiples aplicaciones. El peor escenario posible, en definitiva, para pensar la seguridad, por mucho que Android aventaje claramente a iOS en su condición de proyecto de software libre (aunque administrado por Google, lo cual no es poco relevante teniendo en cuenta que se trata de una empresa cuyo modelo de negocio son los datos que generamos).

Con esto no estamos prescribiendo un tipo concreto de teléfono ni tomando partido por ninguna de las dos partes. Nada más lejos de nuestra intención. Tampoco significa confiar ciegamente en Apple: perdimos la ingenuidad al entrar en este juego, de forma que somos conscientes de que agencias como la NSA americana bien podrían tener una llave maestra para entrar en la memoria del iPhone (de hecho, es altamente probable que la tenga). Pero la realidad de la gran mayoría de nuestro público es la siguiente: nunca van a tener un adversario del tamaño de la NSA. Y en el remoto caso de que alguien lo acabara teniendo, el tipo de móvil que usara sería la menor de sus preocupaciones, si es que llegara a tener uno (probablemente no).

Queríamos, con este anexo, poner en circulación un malestar que no estamos plenamente seguros de que sea compartido,

---

52 Las estadísticas de Apple pueden consultarse en: https://developer.apple.com/support/app-store.

53 Las estadísticas de Android pueden consultarse en: https://developer.android.com/about/dashboards.

pero con el que nuestra experiencia singular se ha encontrado al buscar la mejor protección para el usuario medio, sin que ello le tuviera que comportar una pérdida notable de usabilidad. Cuando decimos que la seguridad debería ajustarse a las circunstancias reales de cada uno, nos referimos a estructurar para cada persona una defensa que tenga en cuenta sus conocimientos en la misma medida que las amenazas que pesan sobre ella (las realmente existentes, no las hipotéticas). Afrontar esta laboriosa tarea implica someter nuestros valores a las capacidades y exigencias concretas de cada individuo o grupo sin querer imponerles un esquema abstracto y, por ello, «ideal», válido por encima de cualquier situación circunstancial pero imposible de asumir para la aplastante mayoría de gente no técnica.

Nuestros principios, de querer mantenerlos inquebrantables, los guardaríamos en una urna de cristal, a salvo de los caprichos del tiempo. Pero hemos preferido asumir el reto, no para distanciarnos de los valores generales de la comunidad, sino precisamente para hacerlos operativos en el plano de lo real. Una cultura de la seguridad no se conseguirá formulándola en reglas derivadas de firmes e insalvables barreras ideológicas. Sea cual sea la situación de la que se parta, nuestra experiencia cotidiana nos ha llevado a concluir que todas ellas son distintas e irreductibles a las plantillas diseñadas de antemano por una minoría de expertos en la técnica. El imperativo categórico nunca pudo ser una fórmula social, sino una moral de élites.

Instruir es, ante todo, saber adaptarse al contexto, que no siempre tendrá las mismas necesidades, formación ni voluntad de aprendizaje. Por eso es imprescindible que, como formadores, hagamos un esfuerzo por ser flexibles en lo que intentamos transmitir, una cultura de la seguridad factible de asumir por el mayor número de gente que sea posible, independientemente de su conocimiento técnico. Este horizonte que perseguimos es un cambio tan radical respecto a la actual situación de vulnerabilidad, que la interpretación táctica de nuestros valores habrá merecido la pena. Digan lo que digan los portavoces de unos principios cualitativamente más puros que los nuestros.

Otros sitios de referencia

- Autoprotección digital contra la vigilancia: consejos, herramientas y guías para tener comunicaciones más seguras: https://ssd.eff.org/es

- Guía de indicaciones para preservar los derechos fundamentales en Internet: https://xnet-x.net/manual-tecnico-derechos-fundamentales-internet/

- Guía de Seguridad Digital para Feministas Autogestivas: https://es.hackblossom.org/cybersecurity/

- Los Defensores Digitales, manual de privacidad para niños y niñas: https://edri.org/files/defenders_v_intruders_es-la_web.pdf

- PRISM Break: https://prism-break.org/es/

- PrivacyTools: https://victorhck.gitlab.io/privacytools-es/

- Security in a Box, herramientas y tácticas de seguridad digital: https://securityinabox.org/es/

- Seguridad en Internet, recursos para padres y docentes: https://www.ecuaderno.com/seguridad/

- Seguridad y privacidad digital para los defensores de los Derechos Humanos: https://www.frontlinedefenders.org/es/file/2477/download?token=6LHgPoPY

- Yo y mi sombra, toma control sobre tus datos: https://myshadow.org/es

Existe tal cantidad de manuales y guías sobre seguridad digital, que es altamente probable que nos hayamos dejado alguna en el tintero. Las razones de este olvido (de haberse producido) son exclusivamente por nuestro propio desconocimiento, y en ningún caso por una voluntad deliberada de minusvalorar la labor de quienes trabajan en los mismos campos que nuestra asociación.

Agradecimientos

A Descontrol Editorial, por la confianza y, especialmente, la paciencia con los plazos de entrega.

A HacksturLab, por su guía de seguridad, que fue el punto de partida de este manual.

A Xnet, por tantos años de trabajo en materia de seguridad para activistas.

A Hacking Lliure, por ser un ejemplo de compromiso con la privacidad y la seguridad.

A la comunidad del software libre, que durante años ha diseñado, desarrollado y mantenido incontables herramientas de seguridad cada vez más robustas.

Este libro se acabó de imprimir en 1984
en los talleres de la antigua Editorial Descontrol
ahora llamada Editorial Control Total