NAVEGUE CON SEGURIDAD

INTERNET Y VIDA PRIVADA

ÍNDICE

6

DISPOSITIVOS MÓVILES

Gracias a los dispositivos móviles, es posible navegar en todas partes, siempre que se pueda acceder a una red Wi-Fi o se disponga de una conexión de datos móviles. Que Internet esté accesible por doquier y todo el tiempo facilita mucho la vida y, sin duda, la hace más interesante, pero hay que ser conscientes de que esta circunstancia no está exenta de riesgos.

USO DE LOS DISPOSITIVOS MÓVILES

Cada vez son más las personas que usan el teléfono móvil o su tablet como sustituto del ordenador, y los llevan a todas partes. Si también es su caso, es muy importante que proteja sus datos personales lo mejor posible: el simple hecho de dejar el aparato encima de la mesa para ir al lavabo les da a los indiscretos la posibilidad de curiosear en su vida privada o, poniéndonos en el peor de los casos, esos juguetitos tan caros son muy fáciles de sustraer.

En este capítulo, le diremos cómo proteger de forma óptima la confidencialidad de los principales sistemas operativos de teléfonos móviles y tablets, es decir, iOS de Apple y Android de Google. Tenga en cuenta que las opciones disponibles y el acceso a las mismas que se explican aquí pueden variar en función de la versión de Android o iOS instalada en su dispositivo, e incluso también en función del modelo de móvil o tablet, pero no suele haber grandes diferencias (hemos usado la última versión de ambos sistemas operativos disponibles en la fecha de edición de esta guía: Android 13 e iOS 17).

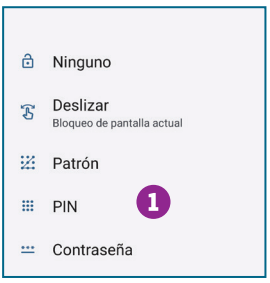
OCULTAR SUS DATOS SENSIBLES

Los consejos siguientes bloquearán el acceso a sus datos personales si, por desgracia, su teléfono o su tablet cae, aunque sea brevemente, en manos ajenas.

- Proteja el acceso a su teléfono con un código PIN o una contraseña. En la mayoría de los smartphones también puede optar por establecer un patrón (un recorrido creado deslizando un dedo sobre algunos de los elementos que se muestran en la pantalla) e incluso por reconocimiento facial. Estas variantes, no obstante, son menos seguras, la primera porque es fácil de copiar, la segunda porque el reconocimiento puede fallar dependien.do del dispositivo del que se trate. Los equipos más sofisticados disponen de la posibilidad de poder identificarse mediante la huella dactilar o un reconocimiento facial avanzado.

ESTABLECER EL PIN

- En **Android**: y toque **Seguridad y privacidad**. Toque en la opción **Bloqueo del dispositivo** y elija **Bloqueo de pantalla**. Seleccione una de las opciones de bloqueo: **Patrón**, **PIN** o **Contraseña** 1. La opción **Deslizar**, sin más, no es segura ya que cualquiera puede desbloquear el dispositivo.
- En **iOS**: acceda a **Ajustes** y, a continuación, **Touch ID y código** o **Face ID y código**. Por último, seleccione **Activar código**.



- Instale una app que lo ayude en caso de pérdida o robo. Esta función ya se encuentra integrada tanto en iOS como en Android, aunque también puede utilizar alguna app incluida por el propio fabricante del dispositivo, una app de seguridad tipo antivirus (muchas incluyen opciones de seguridad en caso de robo o pérdida) o programas como Prey (preyproject.com/es). Si utiliza alguna de las apps o funciones integradas en el móvil, no olvide verificar que el antirrobo está activado.
- Para proteger su aparato contra los últimos fallos en seguridad, instale siempre las actualizaciones más recientes de su sistema operativo. Cuando su teléfono le notifique que hay una nueva actualización, le recomendamos que espere un par de días y luego la instale. Si la actualización trae algún error, en ese período alguien lo habrá reportado y lo habrán corregido. Las actualizaciones no solo arreglan problemas de seguridad del teléfono, sino también características que no funcionaban correctamente o incluso introducen mejoras.
- Encripte los datos personales o delicados por si le piratean su código PIN. Esto es aún más importante para los datos almacenados en la tarjeta de memoria de su teléfono, pues alguien podría sacarlos y leerlos en cualquier otro dispositivo.

ACTUALIZAR EL SISTEMA OPERATIVO

- En Android: entre en **Ajustes** y toque en **Actualizaciones del sistema**. Seguidamente, pulse sobre **Buscar actualizaciones**.
- En iOS: vaya a **Ajustes**, toque **General** y entre en **Actualización de software**. Puede seleccionar tanto la función **Actualizaciones automáticas** como **Actualizaciones beta** si desea probar las nuevas versiones de iOS antes de ser definitivas. Toque en **Descargar e instalar** **2** para actualizar de forma manual.

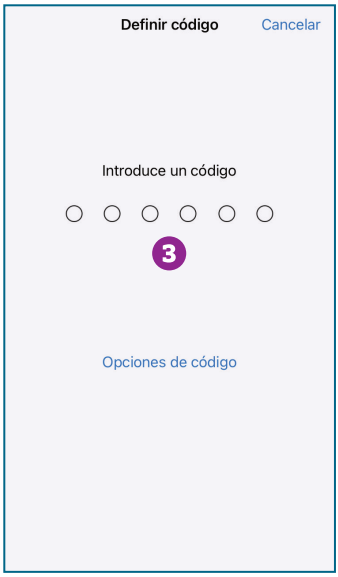
COMPARTIR LA TABLETA

Compartir tablets es algo bastante normal en el seno de la familia o entre amigos. Por desgracia, no todas están previstas para un modo multiusuario. Únicamente los modelos que trabajan con Android a partir de la versión 4.2 pueden funcionar con varias cuentas de usuario independientes. Los dispositivos iOS no permiten separar la información de distintos usuarios por lo que, si tiene un iPad y no es la única persona que lo usa, es aconsejable desconectarse de aplicaciones que se usan frecuentemente, como Facebook, cerrando sesión.

PROTEGER LOS DATOS

Esta posibilidad, además de poder configurarse en el dispositivo, puede encontrarse integrada en ciertos antivirus móviles y existen apps para ello, como Dual File Manager XT.

- En Android: entre en **Ajustes**. En el apartado **Seguridad y privacidad**, toque sobre **Más ajustes de seguridad** y, por último, **Cifrado y credenciales**. Asegúrese de que para el apartado **Cifrar teléfono** está habilitado el valor **Cifrado**.
- En iOS se puede activar la protección de datos configurando un código para el dispositivo: entre en **Ajustes** y, seguidamente, en **Touch ID y código** o **Face ID y código** dependiendo del modelo. Seguidamente, pulse en **Activar código**. Podrá elegir entre un código alfanumérico personalizado, un código numérico personalizado y un código numérico de 4 dígitos. Si no, por defecto le saldrá un PIN de 6 números **3**. En **Solicitar código**, no se olvide de seleccionar **De inmediato**.



PÉRDIDA O SUSTRACCIÓN DEL DISPOSITIVO

Pese a todas las precauciones que pueda tomar, es posible que pierda su móvil o tablet, o que sea víctima de un robo. Como ya hemos dicho en el punto anterior, si utiliza las últimas versiones iOS o Android, el dispositivo ya cuenta con una función antirrobo integrada que puede realizar acciones como localizar su móvil en el mapa, bloquearlo de forma remota o, en última instancia, eliminar todos sus datos si cree que no será posible recuperarlo. Eso sí, debe asegurarse de que dicha opción está configurada y ha sido activada.

INSTALE LA APP DE RECUPERACIÓN DE SU TELÉFONO

1. En Android**:** descargue del Play Store la app **Encontrar mi dispositivo** de Google (dependiendo de la versión, puede que ya venga instalada con el nombre de **Buscar**). Puede configurar la app para, por ejemplo, reproducir un sonido y bloquear remotamente el dispositivo
2. En iPhone**,** utilice la app **Buscar**, instalada por defecto en las versiones más recientes de iOS.

También puede descargar una app específica, como Prey, mencionada anteriormente. Este tipo de aplicaciones puede contar con otras funciones adicionales, como sacar una foto del potencial ladrón, recibir avisos si se retira la SIM de su móvil o un listado con las llamadas entrantes y salientes realizadas con su dispositivo.

Si ha perdido su teléfono es el momento de tratar de recuperarlo, es muy importante darse prisa en hacer lo siguiente:

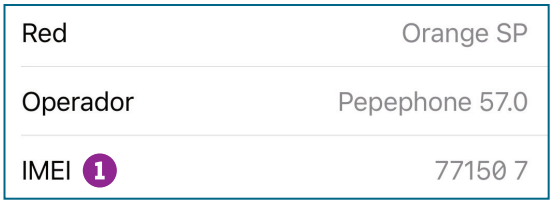
1. Sitúelo en el mapa. Entre en google.com/android/find si tenía un teléfono Android o acceda a icloud.com y ejecute la aplicación **Buscar** si tenía un iPhone. La aplicación de rescate le indicará en un mapa la última posición registrada de su terminal, quizá se lo dejó en la oficina o en el restaurante.
2. Trate de contactar con la persona que pueda tenerlo. Para ello pruebe a llamar a su propio teléfono. Si instaló alguna app de recuperación más avanzada como **Prey**, podrá mandar mensajes a su propio teléfono, que se mostrarán en pantalla, e incluso le avisarán del nuevo número de teléfono en caso de que cambiaran la SIM.
3. Borre sus datos. Si cree que no va a recuperar su móvil, elimine rápidamente todos los datos y archivos que no quiera que nadie vea. Con las apps de rescate puede hacer un reseteo remoto. Eso sí, al hacerlo, las aplicaciones ya no podrán localizar ni rastrear su teléfono.
4. En cualquier caso, es de vital importancia que denuncie a la Policía inmediatamente la pérdida de su móvil o tablet, para estar protegido ante las consecuencias de un posible mal uso de sus datos confidenciales. Es importante que incluya en la denuncia el IMEI del dispositivo (en el recuadro siguiente le enseñamos a localizarlo).
5. Por supuesto, comunique la circunstancia a su operador de telefonía y siga sus instrucciones para evitar que hagan un uso fraudulento de su línea.
6. Recuerde asimismo cambiar todas las contraseñas de las apps enlazadas a su móvil o tablet y avise a las personas de su entorno por si detectasen una actividad sospechosa vinculada a su dispositivo o a sus cuentas. Algunas redes sociales permiten por ejemplo cerrar la sesión en remoto para evitar tener que cambiar la contraseña.
7. Si el dispositivo está asegurado en caso de robo, puede reclamar al seguro una compensación.

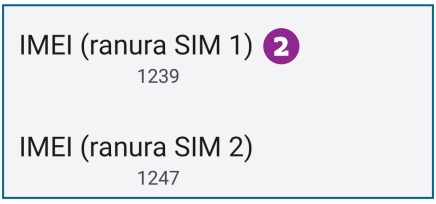
LOCALICE SU IMEI

El IMEI (*International Mobile System Equipment Identity*) es un identificador único a nivel mundial de su dispositivo móvil. Es muy importante que tenga localizado su IMEI para bloquear su dispositivo en caso de pérdida o robo.

- Si utiliza iOS, acuda a **Ajustes**, entre en **General** y luego en **Información**, desplácese hacia abajo para encontrar el apartado IMEI **1**.
- En el caso de Android, para consultarlo, entre en **Ajustes** y toque en **Acerca del teléfono**. A continuación, localice **IMEI 2**. En caso de disponer de dos tarjetas, se mostrarán los dos identificativos IMEI

Otra alternativa consiste en entrar en la función de llamada y teclear el siguiente código: *#06#, y el IMEI de su teléfono se mostrará en su pantalla. Si no cuenta con su dispositivo pero conserva la caja en la que venía cuando lo compró, tenga en cuenta que el IMEI también aparece en ella.





APPS

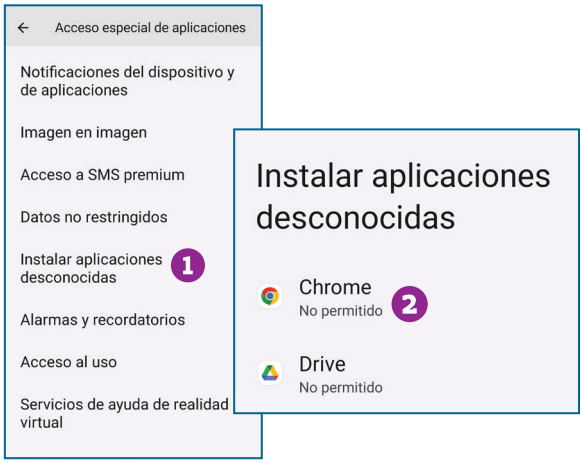
Existen, literalmente, millones de apps para smartphones, y no solo son jueguecitos divertidos, también hay muchas aplicaciones prácticas. Por desgracia, al igual que sucede con los programas clásicos, hay ovejas negras entre ellas; algunas son malintencionadas y su finalidad es robar datos o enviar SMS a números de tarificación elevada.. y las hay que incluso pueden interceptar los SMS que contienen los códigos que autorizan operaciones bancarias en Internet. Apple analiza cada app antes de admitirla en la App Store, lo que le proporciona una ventaja mayor en cuestión de seguridad. Por su parte, el Play Store de Google también cuenta con la función Play Protect, que comprueba regularmente si hay comportamientos dañinos en las aplicaciones instaladas y verifica la seguridad de las aplicaciones del Play Store antes de que se descarguen.

Las aplicaciones realmente nocivas son, afortunadamente, poco frecuentes, pero existe una zona poco clara donde operan gran cantidad de apps maliciosas. Hay muchas que explotan con destreza el margen de maniobra que les deja el sistema operativo para recoger datos de usuario. Los juegos gratuitos, en concreto, consiguen mucho dinero revendiéndolos a los anunciantes.

Algunas son poco conocidas, pero otras son muy populares. Son muchas las apps que intentan conocer su ubicación o tener acceso a su lista de contactos. Las hay, incluso, que examinan su historial de navegación. En principio, no hay nada de malo en ello, siempre que el permiso solicitado sea necesario para que la app pueda proporcionar el servicio que se espera de ella. Este sería el caso, por ejemplo, de una app de navegación que quiera acceder a su GPS, o el de WhatsApp que necesita acceder a su lista de contactos. Sin embargo, para un juego como Trivial, su ubicación no es pertinente si no es para personalizar los anuncios que se le envíen.

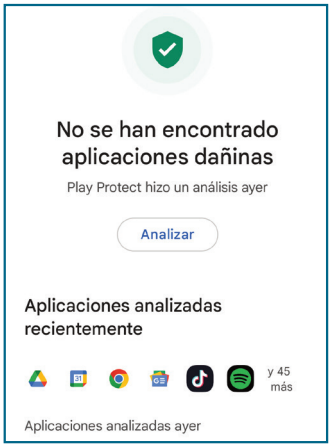
BLOQUEAR DESCARGAS NO OFICIALES EN ANDROID

1. Vaya a **Ajustes** y, a continuación, pinche **Aplicaciones** y toque en **Acceso especial de aplicaciones**.
2. A continuación, pulse sobre **Instalar aplicaciones desconocidas** **1**. Aparecerá un listado de apps y debajo de las mismas debería aparecer **No permitido** **2**. Si figura **Permitido**, pulse sobre la app y deslice el conmutador para desactivar las descargas de esa fuente.



Los siguientes consejos permitirán frenar la curiosidad malsana de las aplicaciones hacia su smartphone o su tablet.

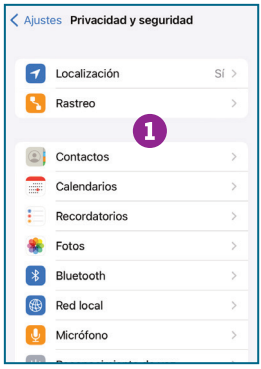
- No haga clic de forma mecánica en los enlaces de los mensajes SMS o de las apps sospechosas: el *malware* suele propagarse de este modo
- Puede suceder que se envíen SMS desde un teléfono sin que su dueño se dé cuenta. Si detecta envíos espontáneos en su aparato, puede ser indicativo de la existencia de una aplicación malintencionada.
- Para mayor protección, también puede instalar un antivirus móvil o app de seguridad para su dispositivo móvil como, por ejemplo, los desarrollados por AVG o ESET.



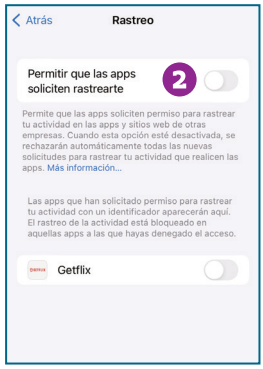
- Si duda de la autenticidad de una app, entre en el sitio web de su desarrollador e investigue sobre ella.
- Redoble la prudencia con las apps que vengan de sitios que no sean Europa, pues en ellos la legislación sobre protección de datos personales es bastante menos estricta.
- Acepte una app solo si está convencido de su utilidad. Siempre puede rehusar el acceso si resulta que una función no le convence.
- Elimine las apps que no use.
- Las versiones más nuevas de iOS y de Android permiten un mayor control sobre los permisos que se dan a las apps y a los anunciantes.

CONFIGURAR LA PRIVACIDAD EN iOS

Para controlar a qué pueden tener acceso sus apps, vaya a **Ajustes** y entre en **Privacidad y seguridad**. Seleccione qué apps pueden acceder a los permisos que se muestran en esa sección **1**.



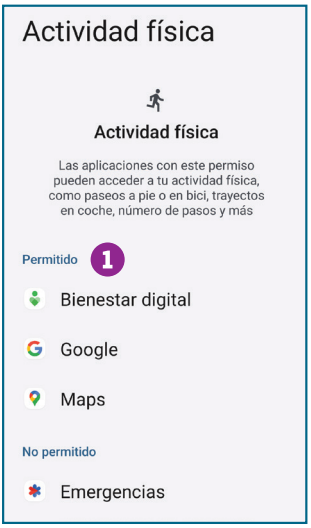
Para ajustar la configuración que impide el uso de su ID para fines publicitarios, acceda a **Ajustes**, y toque **Privacidad y seguridad**. Pulse sobre **Rastreo** y asegúrese de que el conmutador de la opción **Permitir que las apps soliciten rastrearte** está apagado **2**.



- Busque previamente qué derechos tiene la app. Si un juego gratuito reivindica el derecho a enviar SMS, eso tiene que despertar su desconfianza. Tanto en la Play Store de Android como la App Store de Apple detallan qué funcionalidades y datos solicita la app.
- Los usuarios de X pueden ir a x.com/settings/sessions para saber qué dispositivos tienen acceso activo a su cuenta y para eliminar los derechos de acceso. Por otro lado, las apps son inofensivas, porque lo más habitual es que solo quieran publicar un post pero no está de más que vigile su comportamiento.
- Vea si la app incluye una declaración de confidencialidad. Unas veces, se encuentra en la propia app; otras, en el sitio web del desarrollador (indicado en play.google.com o en la aplicación **App Store** de iOS).

CONFIGURAR LA PRIVACIDAD EN ANDROID

Para controlar a qué pueden tener acceso sus apps, vaya a **Ajustes** y entre en **Seguridad y privacidad**. A continuación, pulse en **Privacidad** y pinche en **Gestor de permisos**. Verá un listado de los permisos a los que acceden las apps y, pulsando en cada uno de ellos, podrá habilitar o deshabilitar dicho permiso para cada aplicación **1**.
También permite impedir el uso de su ID para mostrar publicidad personalizada. Para ello vaya a **Ajustes** y pinche en **Google**. A continuación, en el apartado **Servicios en este dispositivo**, pulse en **Anuncios** y, seguidamente, seleccione **Cambiar ID de publicidad**. También puede optar por utilizar la opción **Eliminar ID de publicidad** para evitar por completo que el dispositivo muestre anuncios personalizados.



EL CAZADOR FLURRY

El nombre de Flurry (flurry.com) ha aparecido con frecuencia en los estudios sobre el uso que hacen las apps de los datos personales. Esta empresa de marketing ha sido identificada como una de las mayores cazadoras de perfiles de usuario del mundo móvil. Muchas apps le venden datos de usuarios y la empresa se jacta de haber creado el perfil de millones de usuarios de smartphones. Si lo desea, puede borrarse en developer.yahoo.com/flurry/end-user-opt-out/

GEOLOCALIZACIÓN

No hace mucho, tener GPS era casi un lujo, pero en la actualidad, todos los smartphones lo llevan. De él se derivan una gran cantidad de servicios útiles que le facilitan la vida: piense en las apps que utilizan su ubicación para calcular el trayecto más rápido para volver a casa, para encontrar un restaurante en las proximidades, una farmacia abierta por la noche o la gasolinera más barata de los alrededores.

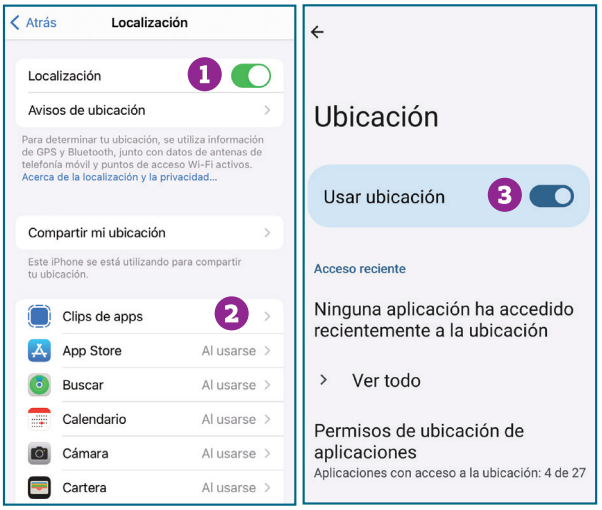
Por otra parte, existe también en la actualidad todo un abanico de aplicaciones que sirven, exclusivamente, para estar al tanto de la ubicación de sus amigos o para que estos lo sigan a usted, como Google Maps o la app Mapas de Apple. Lo malo es que no son sus amigos los únicos que pueden comprobar sus idas y venidas. Los ladrones también pueden llegar a saber dónde está o no está usted gracias a la información de las apps que publican la localización de sus usuarios.

Piénselo dos veces antes de comunicar su ubicación, aunque la trampa consiste en que dicha ubicación suele transmitirse sin que usted lo sepa, por ejemplo, a apps o a sitios web que la solicitan para proporcionar publicidad personalizada (vea *Localización y dirección*, capítulo 2).

GEOLOCALIZACIÓN

Es posible configurar el dispositivo para que las aplicaciones no utilicen sus datos de localización.

- En iOS: acceda a **Ajustes**, entre en **Privacidad y seguridad**. A continuación, acceda a **Localización**. Aquí, puede desactivar el servicio **1** o elegir qué aplicaciones pueden tener acceso **2**
- En Android: puede desactivarlo en **Ajustes**. Entre en **Ubicación** y deshabilite la opción **Usar ubicación 3**.



Le ofrecemos, seguidamente, algunos trucos para ocultar su ubicación.

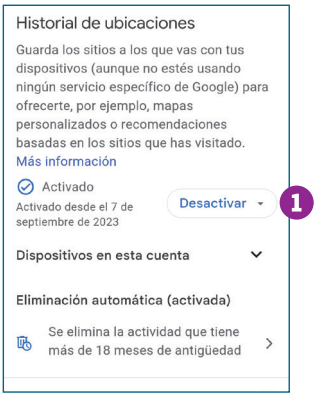
- No divulgue su ubicación a la ligera; los ladrones también navegan y están a la caza de gente confiada.
- Mire qué apps tienen acceso a su ubicación y desactívelas si lo cree más seguro.
- Tanto en iOS como en Android, las apps deben solicitar permiso para usar la información de ubicación, y es posible activar o desactivar este ajuste en cada app.
- Las fotos entrañan un riesgo oculto, porque las cámaras de los smartphones pueden incluir en ellas la ubicación del GPS. Si usted envía una a un amigo, otra persona podrá extraer de ahí ese dato, aun cuando usted no lo haya añadido manualmente. Facebook, WhatsApp, X, Linkedin o Instagram eliminan los

metadatos, por lo que solo quedará registrada la ubicación de dónde se tomó la fotografía si, posteriormente, dentro de la app se especifica la ubicación.

- En X, redoble la prudencia cuando transmita su ubicación, tanto en un mensaje como en una etiqueta, porque estará disponible para todo el planeta.
- Existe la posibilidad de limitar los anuncios ligados a su ubicación, en el caso de iPhone, provenientes de la plataforma publicitaria móvil creada por Apple.

LIMITAR LOS ANUNCIOS

- En iOS: entre en **Ajustes** y toque sobre la opción **Publicidad de Apple** ubicada en el apartado **Privacidad y seguridad**. A continuación, deshabilite la función **Anuncios personalizados**.
- En Android: para consultar y desactivar el historial de ubicaciones de Google, entre en **Ajustes** y, seguidamente, en **Ubicación**. Toque en **Servicios de ubicación** y a continuación en **Historial de ubicaciones de Google**. Seguidamente, podrá activar o desactivar **1** el historial de sus dispositivos.



LA RED WI-FI DELATA SU UBICACIÓN

Google es capaz de localizar con bastante precisión los dispositivos sin necesidad de utilizar el GPS. Lo hace, entre otras cosas, ayudado por las direcciones IP, pero esto no es todo. Su truco son las redes Wi-Fi. Por exigencias de su servicio Street View, Google ha dado la vuelta al mundo en una furgoneta y ha fotografiado multitud de calles. Al mismo tiempo, ha grabado la ubicación de todas las redes Wi-Fi que ha encontrado en su camino. Así, desde entonces, puede llegar a saber dónde se encuentra de forma aproximada, por ejemplo, un ordenador portátil cuando accede a una red de este tipo.

Este proyecto ha suscitado no pocas controversias, pues no se había puesto al corriente a la gente. Si no quiere que Google recabe información de su *router* inalámbrico, modifique su nombre de red (SSID o *Service Set Identifier*) añadiendo la extensión "nomap". Por ejemplo, si su SSID actual es "Vicente", entonces renómbrelo como "Vicente_nomap".