INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

MÓDULO 7

Gestión de información y configuración de privacidad en dispositivos

ÍNDICE

1. Gestión de información almacenada en dispositivos

No cabe duda de que llevamos años inmersos en un proceso de digitalización en todos los aspectos de nuestro día a día, y todos y cada uno de nosotros somos parte de esta transformación que está dejando atrás cualquier rastro de información en formato físico.

Uno de los principales cambios para los usuarios es que cada vez almacenamos más información de todo tipo en nuestros dispositivos, siendo gran parte de ella privada, por lo que es muy importante conocer y aplicar ciertas medidas que nos ayuden a gestionar toda esa información y mantenerla a buen recaudo.

Es por todo ello que en este capítulo hablaremos sobre las principales recomendaciones que nos ayudarán a gestionar toda esa información de la mejor manera, asegurando que no llega a manos no autorizadas.

Configuraciones de seguridad y privacidad

Uno de los primeros pasos que hemos de llevar a cabo es preparar nuestro dispositivo

para almacenar la información de una forma segura. Dependiendo del dispositivo usado y su sistema operativo, deberemos aplicar ciertas configuraciones de seguridad y privacidad que nos ayudarán a mantener nuestra información a salvo. En los siguientes capítulos hablaremos en detalle de las configuraciones recomendadas para diferentes tipos de dispositivos, y los pasos para establecer correctamente la privacidad de estos. El bloqueo de pantalla, restringir y retirar permisos de aplicaciones o controlar la privacidad de nuestras notificaciones son algunas de las configuraciones que aumentarán la privacidad de nuestros dispositivos y nuestra información.

Cifrado de la información

El cifrado consiste en la codificación de información, alterando el contenido de ésta para hacerlo ilegible, y asegurando así su confidencialidad y privacidad. En los archivos digitales, esto se consigue mediante la alteración de *bits* de los datos (imágenes, documentos, emails, etc.). Esta alteración se realiza mediante una clave y un algoritmo matemático que transforma una información o mensaje en algo indescifrable para cualquier interlocutor que no conozca dicho algoritmo y clave.

En la actualidad, uno de los algoritmos de cifrado más usado es el algoritmo de cifrado simétrico *AES* (Advanced Encryption Standard), se usa para cifrar información confidencial. Como cualquier método de cifrado, convierte el texto en un código que sólo es descifrado por la persona que tenga la clave.

Fuente: Ver enlace

Si la información que contienen nuestros dispositivos está cifrada, y alguien intenta extraerla, ésta será totalmente ilegible y no se podrá hacer ningún uso de ella.

Para el cifrado de la información almacenada en nuestros dispositivos, existen numerosas herramientas disponibles que cumplirán esta función, aunque una opción interesante es usar la funcionalidad integrada que contienen los propios sistemas operativos. En el caso de Android o iOS, toda nuestra información ya está cifrada por defecto si usamos un método de bloqueo.

Copias de seguridad

Una copia de seguridad (*backup* en inglés) es un proceso en el que duplicamos o copiamos información existente de un dispositivo a otro lugar, para que podamos recuperarlos en el momento que lo necesitemos o lo consideremos oportuno. Estas copias de seguridad se guardan en un lugar seguro, el cual está protegido de incendios, robos, averías o actos que las pueda comprometer. También puede ser usada como medio para transferir información a un nuevo dispositivo.

Las copias se seguridad deben ser comprobadas de forma periódica para certificar que los datos pueden ser reparados en caso necesario.

Dentro de los sistemas operativos más usados, podemos encontrar funcionalidades integradas para realizar copias de seguridad en la nube como Google Drive (Google) e iCloud (Apple). El acceso a la información sólo es posible a través de las credenciales de las respectivas cuentas de Google o Apple.

Herramientas de seguridad

Además de las configuraciones y medidas de privacidad y seguridad propias de los sistemas operativos, siempre es recomendable usar herramientas de seguridad que nos ayuden a proporcionar un nivel extra de protección a nuestra información, ya sea para la prevención de accesos no autorizados o la detección de posibles amenazas. Entre muchas otras, cabe destacar algunos tipos de herramientas que nos ayudarán con la tarea de mantener la privacidad de nuestros datos:

- **Antivirus**: ya que nuestros sistemas están sujetos a vulnerabilidades y ataques de *malware*, un antivirus es siempre recomendable para mantener nuestros dispositivos alejados de amenazas, que, en la mayoría de las ocasiones, tienen como principal objetivo acceder a nuestra información privada.
- **Cortafuegos**: popularmente conocidos como *firewalls*, sirven para conocer y administrar la relación entre aplicaciones a través de Internet y los accesos que estas hacen, así como evitar potenciales conexiones peligrosas o indeseadas desde o hacia nuestros dispositivos, existen las aplicaciones cortafuegos.
- **Antirrobo**: como su propio nombre indica, las aplicaciones antirrobo son aquellas destinadas a evitar el robo de nuestros dispositivos y ayudarnos a localizarlos en caso de que se produzca. También permiten borrar su información de manera remota si creemos que ha caído en malas manos y evitar así que puedan acceder a tu información privada.

A pesar de la cantidad de datos privados que albergan nuestros dispositivos, un gran número de usuarios no realizan una gestión apropiada de la información, manteniendo sus dispositivos con configuraciones inseguras y dejando sus datos al alcance de cualquiera, incluidos los ciberdelincuentes.

Esta infografía resume brevemente los cuatro pilares fundamentales que te ayudarán a mantener tu información en privado.

2. Configuración con Android

Android es actualmente el sistema operativo más usado del mundo. Podemos encontrarlo en un volumen muy alto de los teléfonos inteligentes o tabletas que utilizan los usuarios. Dada la importancia y la cantidad de datos que se almacenan en nuestros dispositivos, es importante conocer cómo configurar el dispositivo correctamente para asegurar la seguridad y la privacidad de nuestra información.

1. Bloqueo de pantalla

Una de las configuraciones más recomendables y a la vez extendidas por su facilidad de configuración es el bloqueo de pantalla que, como su propio nombre indica, bloquea el dispositivo de tal forma que nadie puede usarlo si no conoce el método que se utilizó para este fin. Por tanto, no podremos acceder a ninguna función o información de nuestro teléfono si no lo desbloqueamos con anterioridad. Función muy útil para que a tu información solo accedas tú y nadie más.

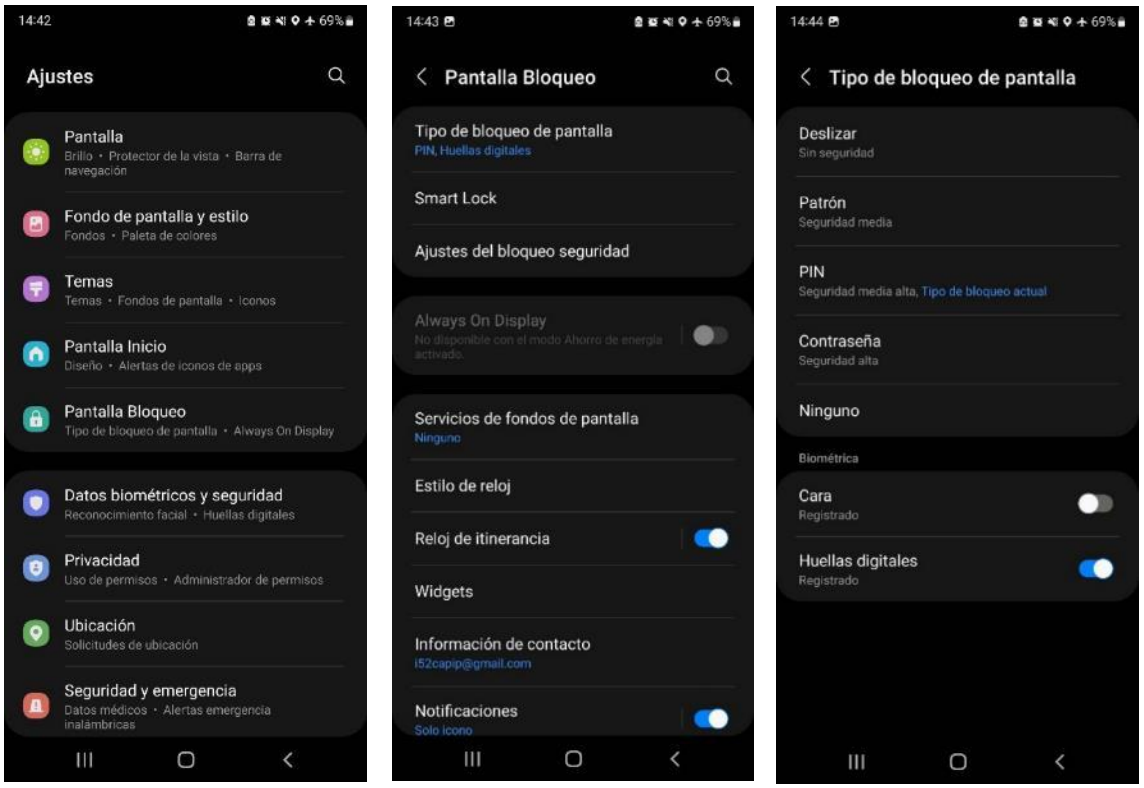
Pero para que esto sea aplicable, hemos de configurar alguno de los métodos de bloqueo disponibles en Android, lo que hará que el acceso a nuestra pantalla de inicio o *home screen* solo se produzca una vez demos la respuesta correcta al bloqueo establecido.

Disponemos de diferentes métodos de bloqueo para configurar en nuestros dispositivos Android: **PIN, patrón, contraseña y biometría (huella dactilar o reconocimiento facial)**. Esto último dependerá del modelo de teléfono que tengamos. Los modelos más antiguos puede que no incorporen lectura de huella digital o reconocimiento facial.

Para establecer un bloqueo de pantalla, accederemos al menú Ajustes > Pantalla > Bloqueo > Tipo de Bloqueo de Pantalla. Desde aquí, seleccionaremos la opción que deseamos configurar en el teléfono. Es posible establecer más de un mecanismo, entre los que se incluyen:

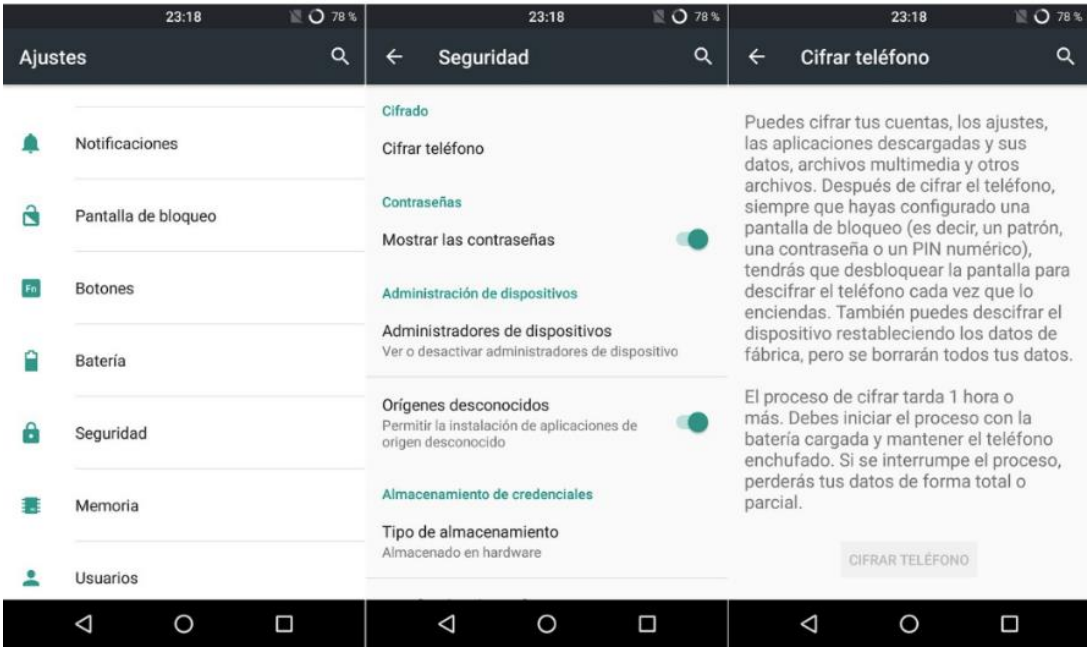
- **Pin**. Número pin para acceder a la pantalla.
- **Contraseña**. Uso de una contraseña alfanumérica.
- **Patrón**. Se dibuja/traza un patrón en una cuadrícula de puntos para acceder a la pantalla.
- **Huella digital**. Uso de sensor dactilar.
- **Reconocimiento facial**. Identifica rostros.

Debemos evitar hacer uso del patrón, por ser el mecanismo menos seguro, es el más sencillo de adivinar. Por el contrario, la contraseña y reconocimiento biométrico, son los más recomendables.



Además, es importante destacar que en las últimas versiones del sistema operativo Android, cuando configuramos un método de bloqueo en nuestros dispositivos, este es usado para cifrar la información almacenada en ellos, dando un gran valor añadido a esta funcionalidad.

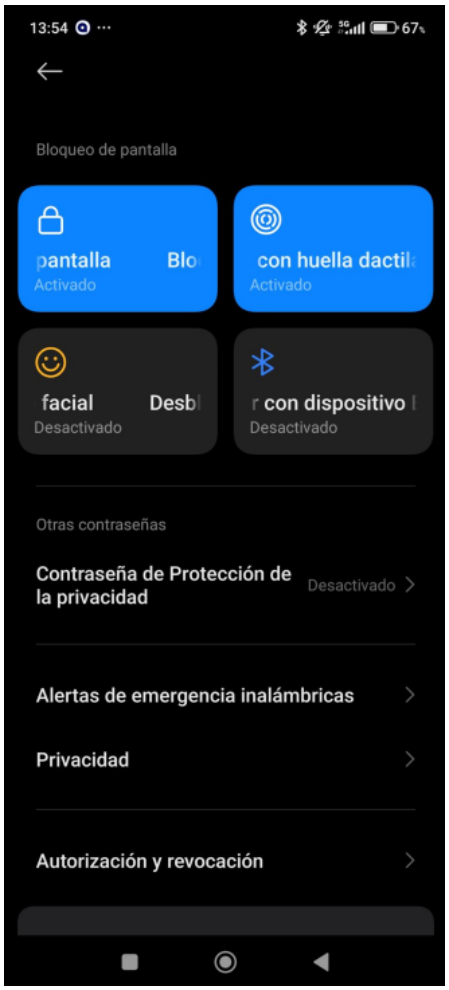
Desafortunadamente esto no ocurre en versiones más antiguas, en las que habrá que activar el cifrado de la información manualmente, haciendo uso de nuestro método de bloqueo para ello. Para activar esta opción, deberemos entrar en el menú Ajustes > Seguridad > Cifrar teléfono.

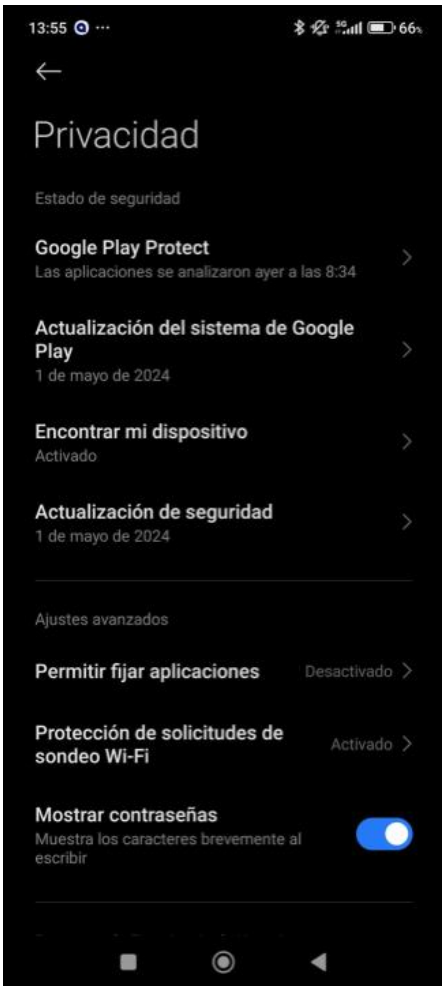


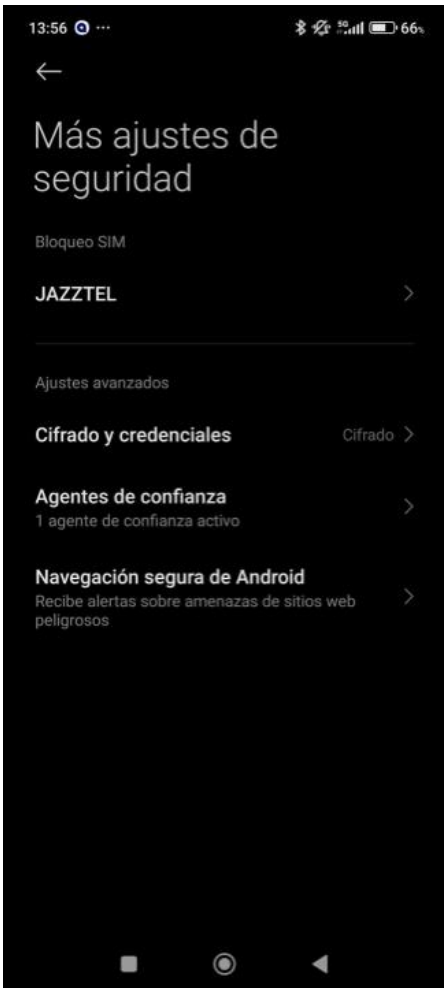
2. Bloqueo de la tarjeta SIM

Para evitar que nuestro teléfono pueda ser encendido y utilizado sin nuestro consentimiento, es importante que, además de la pantalla de bloqueo, activemos la opción que nos hará introducir el PIN de la SIM siempre que encendamos el dispositivo.

Comprobar si lo tenemos así configurado es fácil, nuevamente iremos a los Ajustes, accederemos a Seguridad y privacidad > Más ajustes de seguridad > Seguridad de tarjeta SIM y nos aseguramos de que se encuentre activado, que por defecto suele ser así.







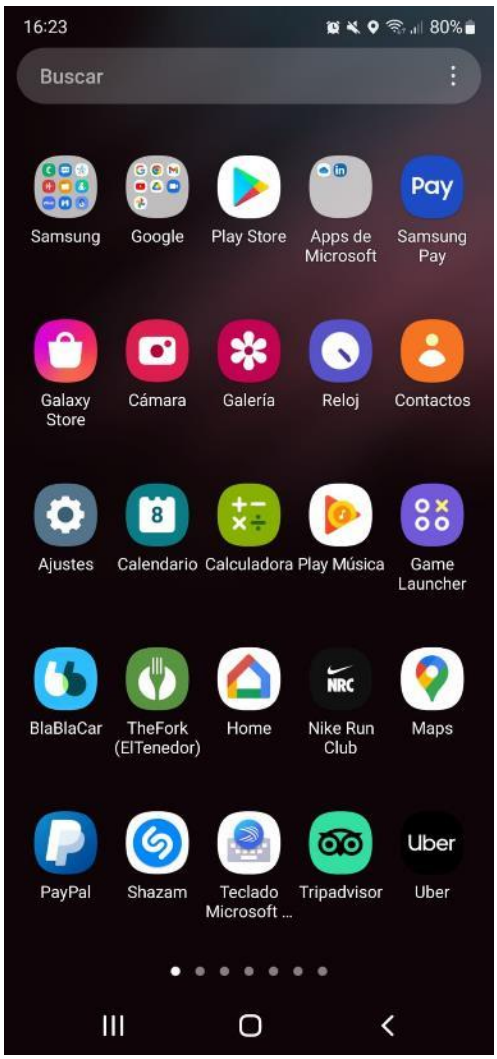
3. Encuentra mi dispositivo (*Find my device*)

'Encontrar mi dispositivo' es una función integrada en Android, que nos permitirá saber dónde se encuentra nuestro dispositivo de forma remota a través de un ordenador u otro dispositivo Android, conectándonos a nuestra cuenta de Google.

Además, ofrece algunas funciones de manera remota, las cuales, podemos ver en la siguiente imagen:

Aunque esta funcionalidad integral está activa por defecto en las últimas versiones de Android, es importante asegurarnos de que la tenemos activada, ya que será nuestro principal método de localizar y borrar datos confidenciales remotamente en caso de robo o pérdida del dispositivo.

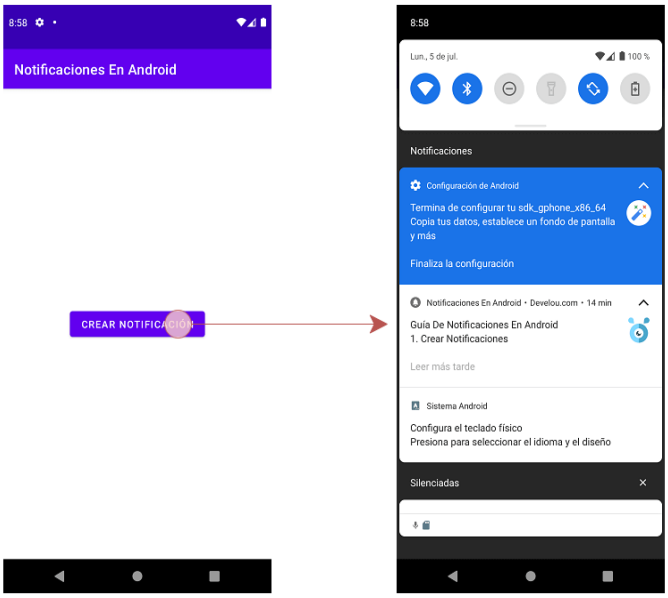
Normalmente, Google nos sugiere su activación cuando realizamos la configuración inicial de un terminal, pero si lo hemos pasado por alto o no nos pareció buena idea en aquel momento, tan solo tendremos que acceder a nuestra cuenta de Google dentro de Ajustes.



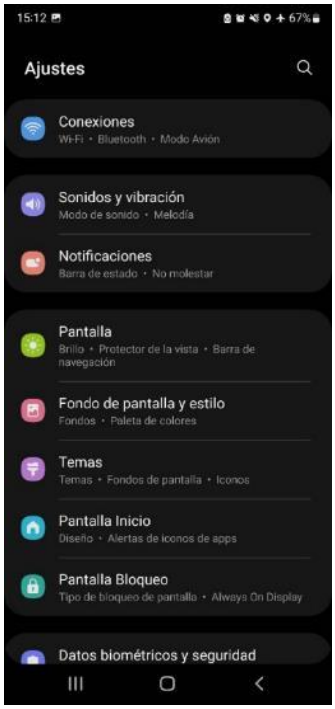
Una vez dentro de Google, buscaremos la opción de 'Encontrar mi dispositivo' y pulsaremos sobre ella para acceder al menú de la función y poder activarla:

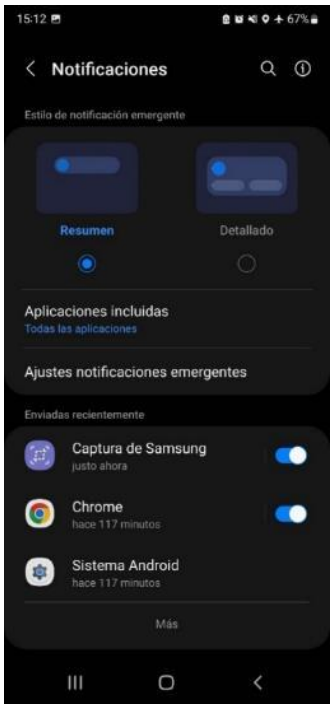
4. Notificaciones

Estas notificaciones aparecen como mensajes o alertas en la pantalla del dispositivo móvil, advirtiendo al usuario sobre las novedades y posibles actualizaciones del contenido que puedan ir apareciendo en las aplicaciones instaladas en el dispositivo móvil.



En ocasiones, queremos impedir que otras personas puedan ver las notificaciones que aparecen en nuestra pantalla, ya que pueden contener información privada, por ejemplo, un nuevo mensaje de chat o SMS. Para ello, dentro de Ajustes > Notificaciones > Estilo de notificación emergente, podremos configurar si queremos recibir solo un resumen, por ejemplo, "Tienes un nuevo mensaje de WhatsApp" o detallado, que mostrará el contenido del mensaje recibido parcial o totalmente.



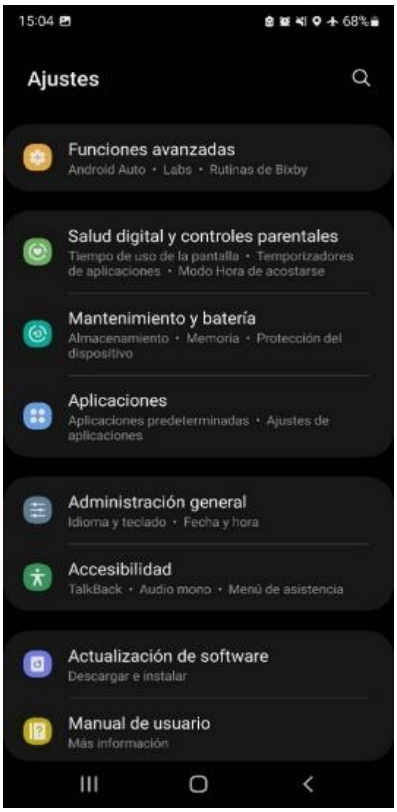


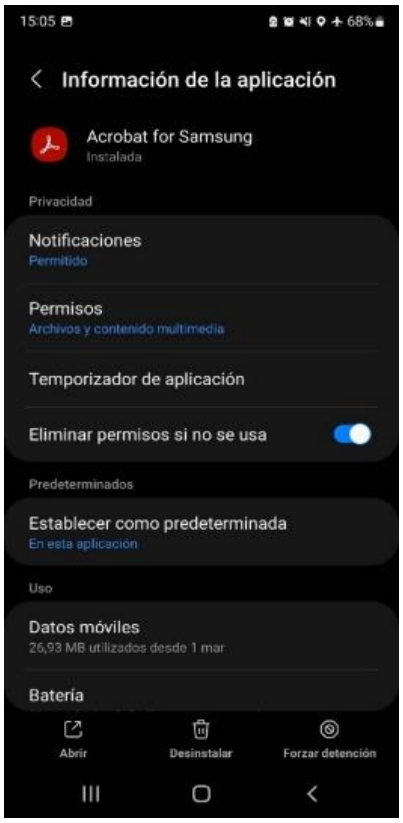
5. Permisos de aplicaciones

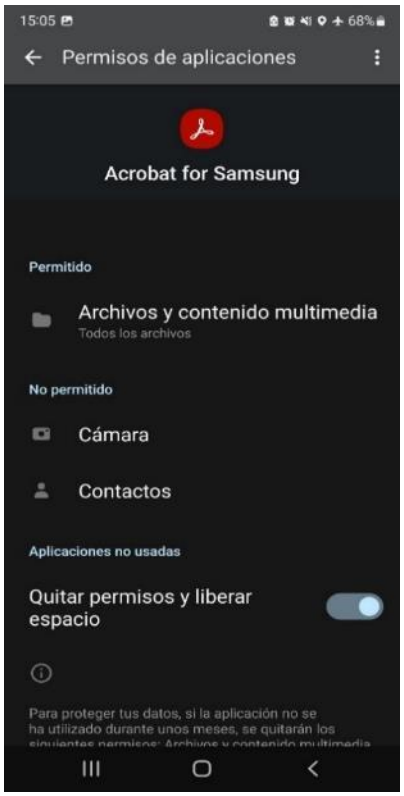
También es altamente aconsejable revisar los permisos que solicitan las aplicaciones cuando las instalamos, pero no solo en ese momento, también de manera regular, ya que, con las actualizaciones de las aplicaciones, estos pueden cambiar.

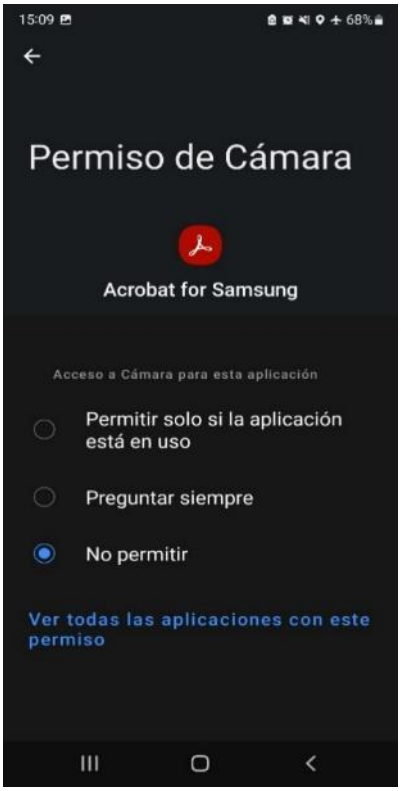
Con esta acción, descubriremos que la gran mayoría de aplicaciones tienen concedidos por defecto muchos más permisos de los que necesita para cumplir con sus funciones básicas.

¿Cómo revisar los permisos que tiene cada aplicación instalada? Accederemos a los Ajustes y después al menú Aplicaciones. Una vez ahí, podremos ver aplicación por aplicación qué permisos tiene concedidos y eliminar aquellos que no consideremos necesarios. En la siguiente imagen, hemos puesto como ejemplo la aplicación *Acrobat for Samsung* y sus permisos.


15:04
68%
Ajustes
Funciones avanzadas
Android Auto • Labs • Rutinas de Bixby
Salud digital y controles parentales
Tiempo de uso de la pantalla • Temporizadores de aplicaciones • Modo Hora de acostarse
Mantenimiento y batería
Almacenamiento • Memoria • Protección del dispositivo
Aplicaciones
Aplicaciones predeterminadas • Ajustes de aplicaciones
Administración general
Idioma y teclado • Fecha y hora
Accesibilidad
TalkBack • Audio mono • Menú de asistencia
Actualización de software
Descargar e instalar
Manual de usuario
Más información


15:05
68%
Información de la aplicación
Acrobat for Samsung
Instalada
Privacidad
Notificaciones
Permitido
Permisos
Archivos y contenido multimedia
Temporizador de aplicación
Eliminar permisos si no se usa
Predeterminados
Establecer como predeterminada
En esta aplicación
Uso
Datos móviles
26,93 MB utilizados desde 1 mar
Batería
Abrir
Desinstalar
Forzar detención

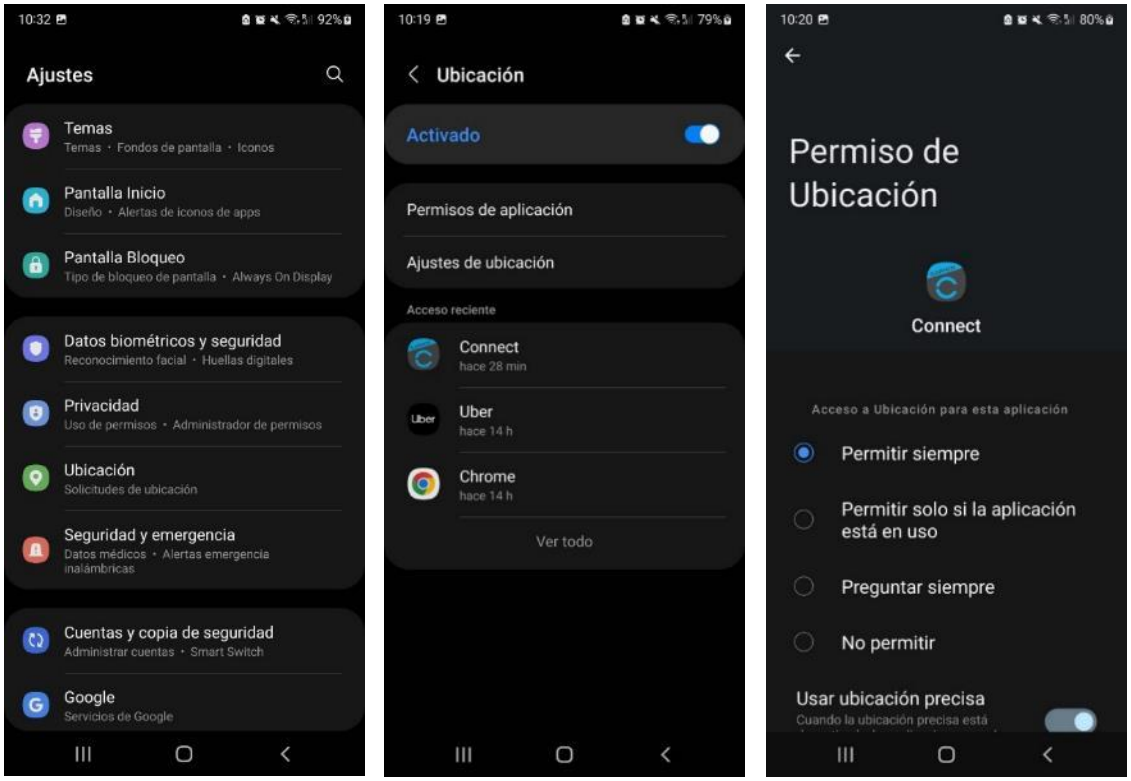

15:05
68%
Permisos de aplicaciones
Acrobat for Samsung
Permitido
Archivos y contenido multimedia
Todos los archivos
No permitido
Cámara
Contactos
Aplicaciones no usadas
Quitar permisos y liberar espacio
Para proteger tus datos, si la aplicación no se ha utilizado durante unos meses, se quitarán los


15:09
68%
Permiso de Cámara
Acrobat for Samsung
Acceso a Cámara para esta aplicación
Permitir solo si la aplicación está en uso
Preguntar siempre
No permitir
Ver todas las aplicaciones con este permiso

6. Ubicación

Es recomendable no compartir nuestra ubicación, o al menos, restringir qué aplicaciones y cuándo tienen acceso a dicha información. Para configurarla, entraremos en Ajustes > Ubicación. Desde este menú, podremos tanto desactivar la ubicación por completo, como configurar cuando cada aplicación puede hacer uso de la ubicación, dentro de Permisos de Aplicación y accediendo a cada una de las aplicaciones que queramos revisar.

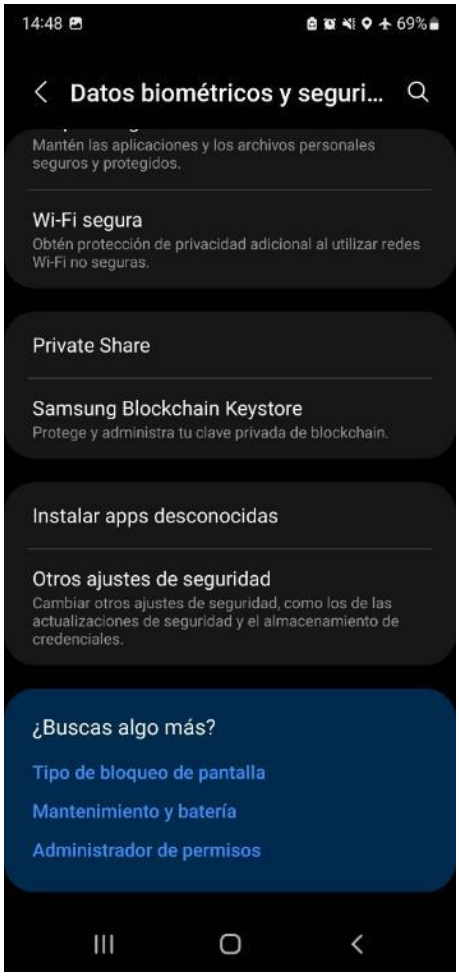
Las versiones de Android más recientes permiten ajustar de una manera más precisa cuando una aplicación puede hacer uso de la ubicación: permitir siempre, permitir solo mientras se usa la aplicación, preguntar siempre o no permitir.

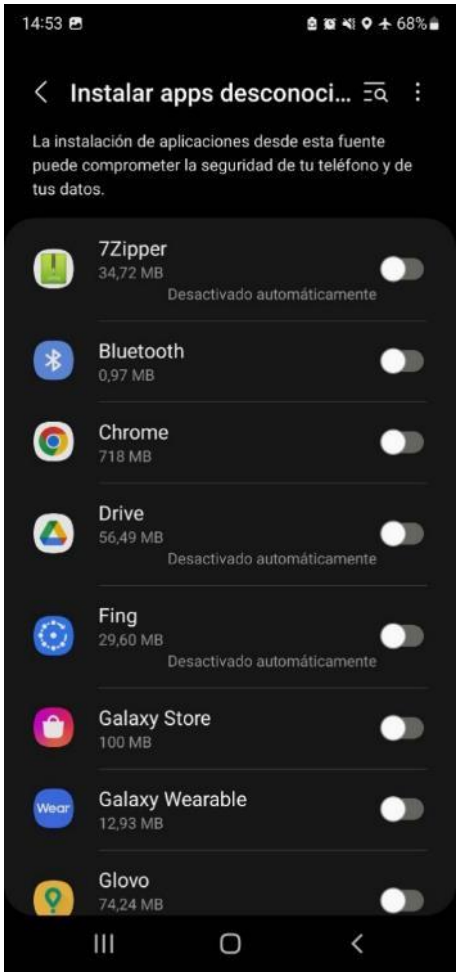


Desde la Ubicación, también podremos activar o desactivar algunas funciones específicas que Google pone a nuestra disposición. Concretamente a través de 'Ajustes de ubicación', entre las que destacan el aviso de terremotos basado el nuestra ubicación o la localización en caso de emergencia. También podremos desactivar el historial de localizaciones para incrementar nuestra privacidad.

7. Orígenes desconocidos para instalar

Es recomendable instalar únicamente aplicaciones a través de Google Play, el repositorio oficial de aplicaciones que Google ofrece a los usuarios cuyos dispositivos tienen sistema operativo Android. Sin embargo, este sistema nos da la posibilidad de instalar aplicaciones mediante archivos conocidos como APK que podremos descargar en otras páginas de Internet y que podrían comprometer nuestra privacidad, debido a que no han pasado los controles de seguridad de Google y, por tanto, no sabemos si hacen lo que dicen o, por el contrario, el código que contiene está desarrollado con fines maliciosos. Es por ello que debemos desactivar la opción que permite instalar aplicaciones que no sean descargadas desde Google Play. Para ello, dentro de Ajustes, accederemos a Seguridad y privacidad > Más ajustes de seguridad > Instalar apps desconocidas y desactivar cualquier fuente sospechosa.



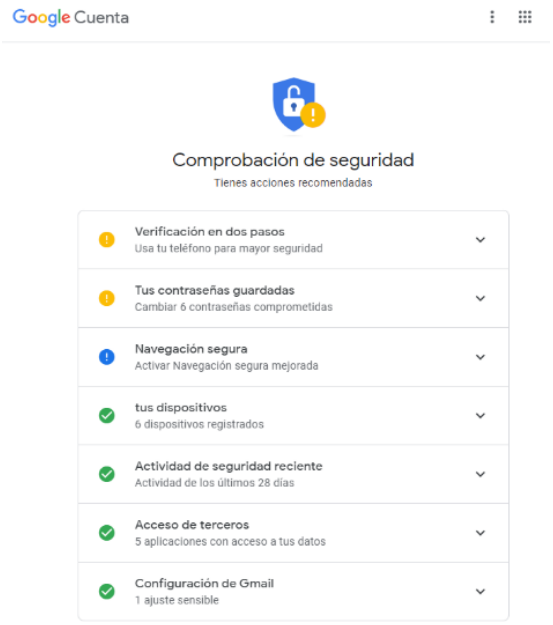


8. Cuenta de Google

Tenemos una funcionalidad extraordinaria a nuestra disposición que nos facilita la revisión y configuración de los aspectos de seguridad y privacidad relacionados con nuestra cuenta de Google, y, por tanto, que nos ayuda a mantener bajo control nuestra información.

MÁS INFORMACIÓN

A esta funcionalidad se accede a través del enlace Ver enlace o directamente desde nuestro dispositivo. En concreto, desde el menú Ajustes > Google > Gestionar tu cuenta de Google y accediendo a la pestaña de 'Seguridad'.



Aquí encontraremos algunas recomendaciones para activar opciones que nos ayudarán a proteger nuestros dispositivos y sus datos almacenados. Entre ellas, destacan:

- Uso de **contraseñas seguras**, deben de ser las más únicas posibles.
- La **verificación en dos pasos**, que nos protegerá de los ciberdelincuentes incluso si estos se hacen con nuestra contraseña. Normalmente el segundo método de verificación suele ser un código enviado al móvil.

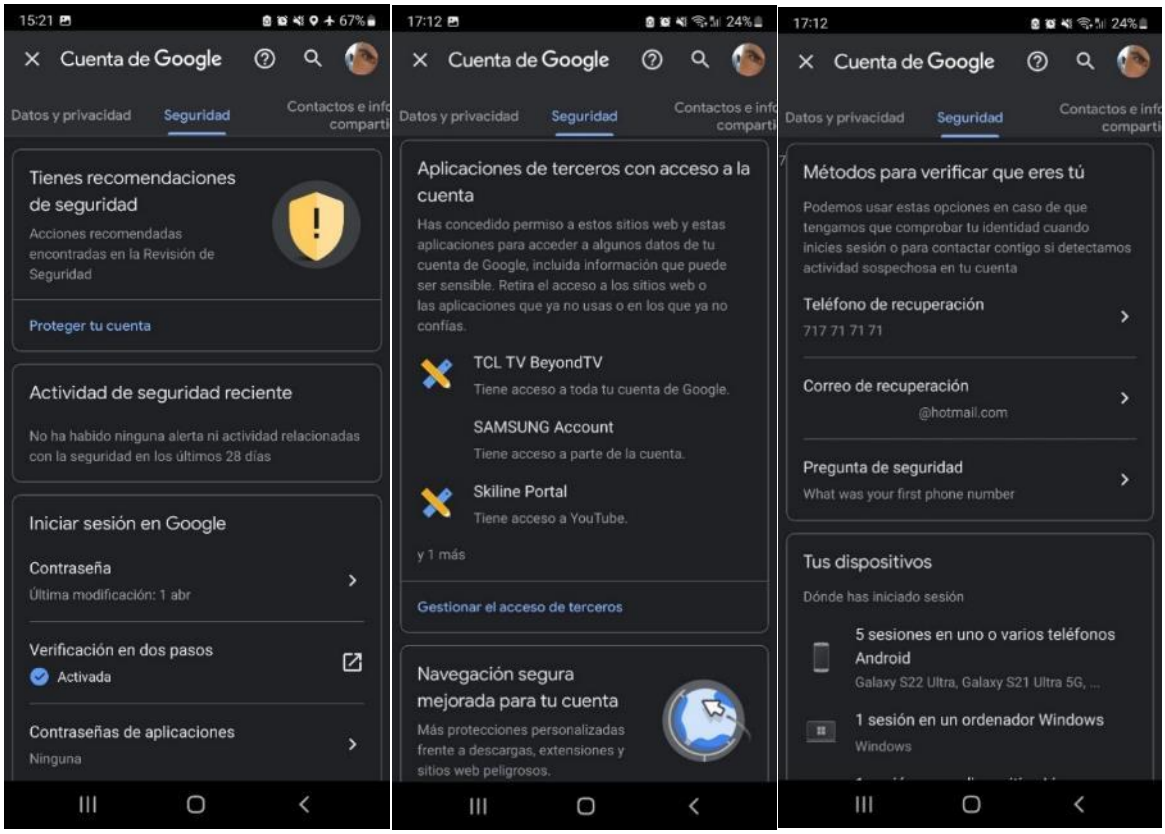
- Conocer las **contraseñas guardadas** en tu cuenta de Google que han sido *hackeadas* y podrían estar al alcance de ciberdelincuentes.

- **Actualización de información de recuperación de cuenta,** asegurarse de recordar los métodos de recuperar la cuenta, tales como números de teléfonos y correos electrónicos alternativos.

- **Actividad de seguridad reciente**, donde podremos ver los últimos cambios de contraseña o en las medidas de seguridad en nuestra cuenta.

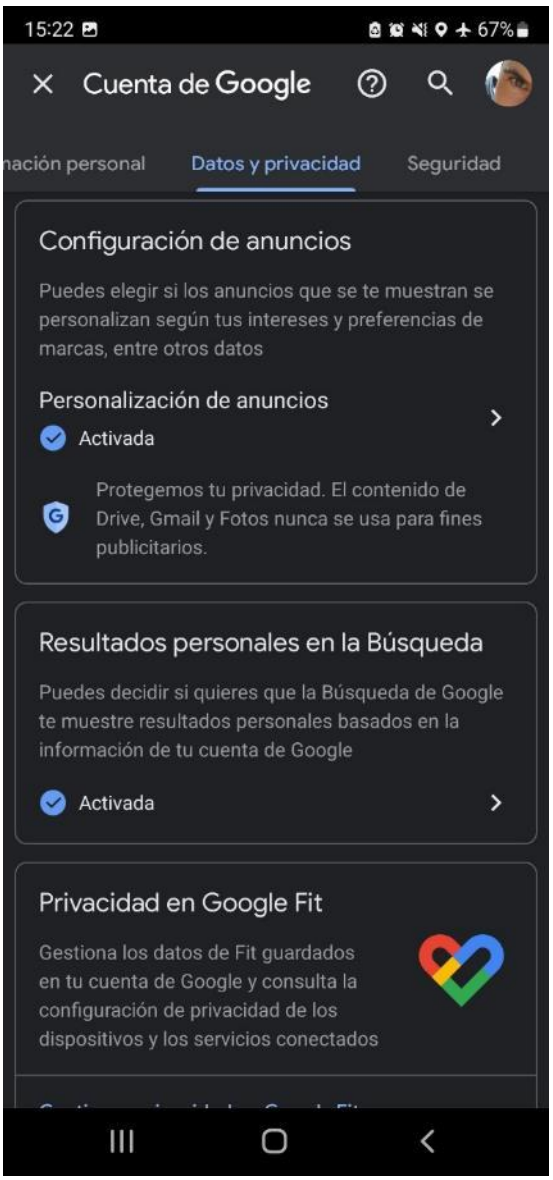
- **Acceso de terceros**, que nos muestra qué aplicaciones tiene acceso a la información de nuestra cuenta.

- **Dispositivos registrados a tu cuenta de Google**, que nos ayudará a revisar rápidamente que todos los dispositivos que acceden a nuestra cuenta e información son conocidos y autorizados.



En el apartado de 'Datos y privacidad', también podremos revisar cuestiones muy interesantes que ayudarán a que nuestra información esté más controlada y protegida.

Por ejemplo, podremos configurar el historial de nuestra cuenta de Google y sus accesos, así como personalizar, o no, los anuncios que recibimos. Desactivar esta opción hará que Google no obtenga datos de nuestra navegación para usarlos más adelante en anuncios dirigidos. Es importante recordar que igualmente veremos anuncios, simplemente que estos no estarán basados en nuestra actividad de navegación y búsquedas.



3. Configuración con iOS

iOS es el sistema operativo propiedad de Apple que podemos encontrar en los dispositivos móviles (iPhone, iPad, iPod touch) de la marca. Millones de dispositivos y usuarios confían en este sistema operativo para almacenar toda su información, y para protegerla, es imprescindible conocer cómo configurar el dispositivo correctamente para asegurar así un nivel adecuado de seguridad y privacidad.

1. Bloqueo de pantalla

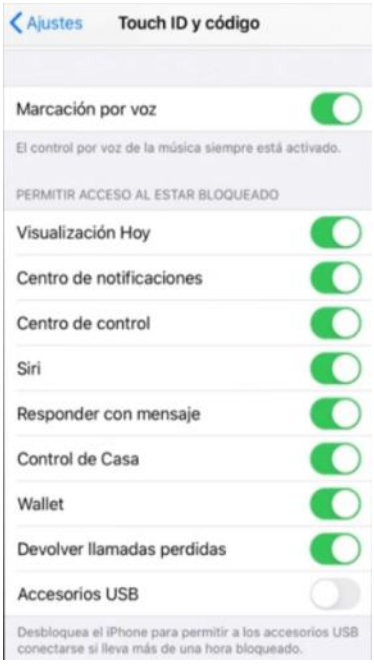
Una de las configuraciones más recomendables y a la vez extendidas por su fiabilidad y la facilidad de configuración es el bloqueo de pantalla, cuyo funcionamiento es extremadamente sencillo: no podremos acceder a ninguna función o información de nuestro teléfono si no lo desbloqueamos con anterioridad.

Disponemos de diferentes métodos de bloqueo para configurar en nuestros dispositivos iOS: **Código, *Touch ID* (biometría mediante huella dactilar), *Face ID* (reconocimiento facial) y *bloqueo de pantalla automático*.**

El método de bloqueo '*Face ID´* , es el más usado en los últimos modelos de iPhone, el cual escanea y reconoce el rostro del usuario para desbloquear la pantalla. El *'bloqueo de pantalla automático'*, bloquea el dispositivo automáticamente pasado un periodo de inactividad.

Para activar alguna de estas opciones, accederemos a Ajustes > Touch ID y código (o Face ID y código, dependiendo de modelo y versión del dispositivo), donde además podremos activar el mismo método de bloqueo para descargas y compras en App Store o para Pagos.

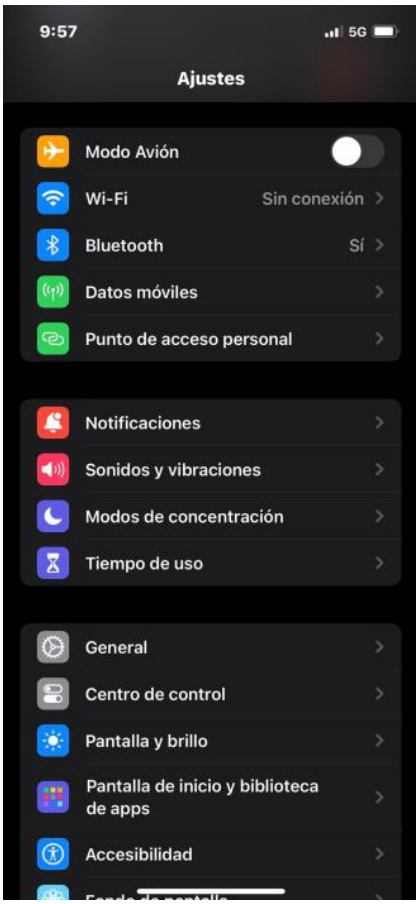
Desde aquí, podremos habilitar que algunas funciones estén disponibles sin necesidad de desbloquear el teléfono. Es recomendable desactivar todas aquellas que no consideremos necesarias para incrementar nuestra privacidad.

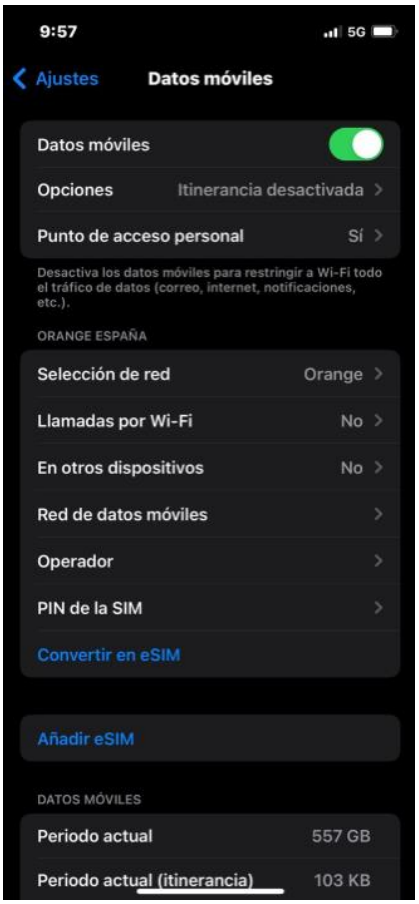


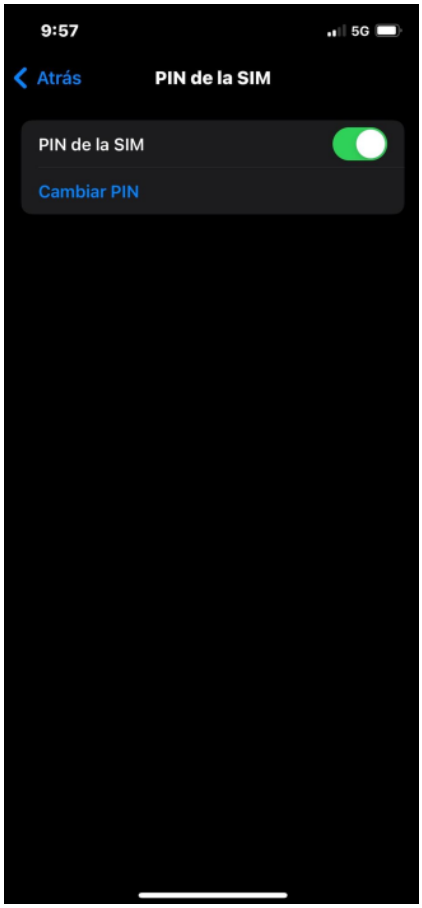
2. Bloqueo de tarjeta SIM

Para evitar que nuestro teléfono pueda ser encendido y utilizado sin nuestro consentimiento, es importante que, además de la pantalla de bloqueo, activemos la opción que nos hará introducir el PIN de la SIM siempre que encendamos el dispositivo.

Para ello, entraremos en Ajustes > Datos móviles > PIN de la SIM o Bloqueo SIM, donde nos deberemos asegurar de que la opción está activa.





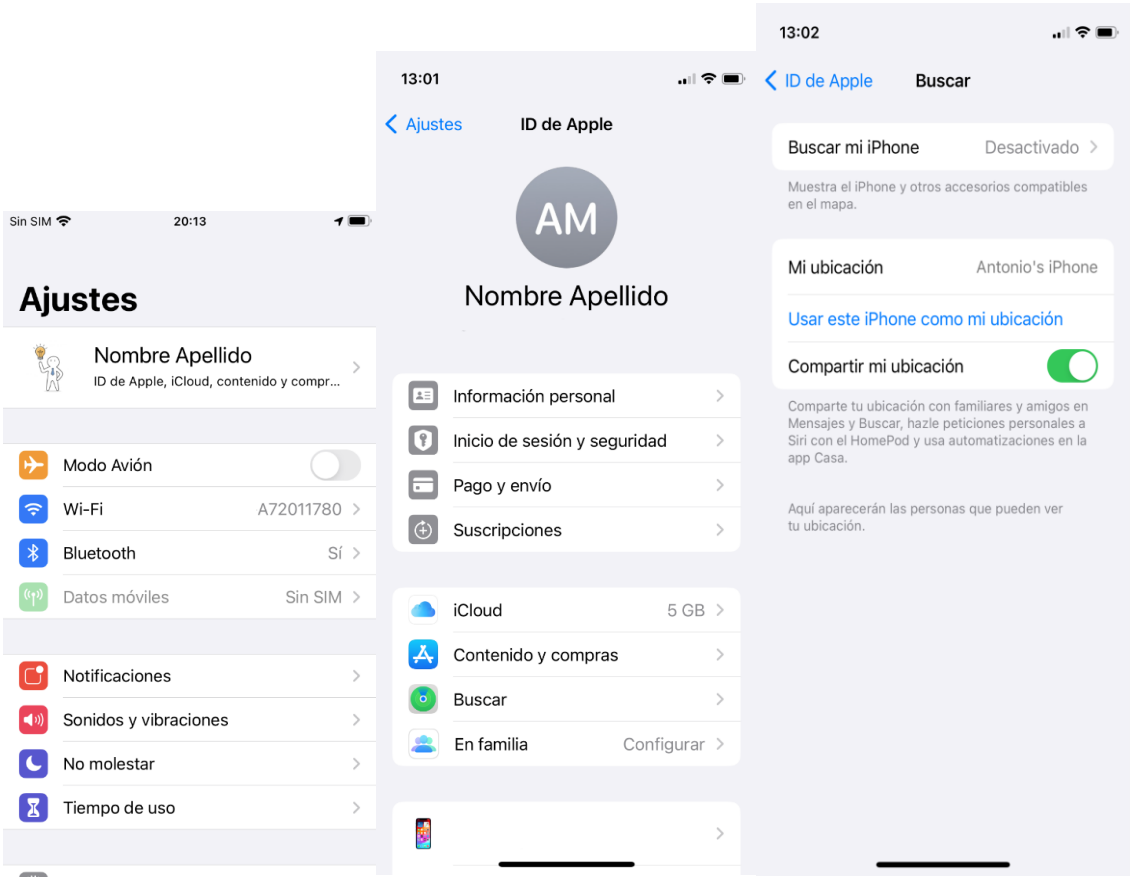


3. Buscar mi iPhone

'Buscar mi iPhone' es una función integrada en iOS, que nos permitirá saber dónde se encuentra nuestro dispositivo de forma remota a través de un ordenador u otro dispositivo, conectándonos a nuestra cuenta iCloud o usando la aplicación '*Buscar´* desde otro dispositivo iOS. Además, nos ofrece tres acciones de manera remota que son: reproducir un sonido, bloquear el teléfono o borrar todos los datos almacenados.

Existe también la función '*modo perdido´*, para que bloque de forma remota el dispositivo a través de un código de acceso publicando un mensaje personal en la pantalla principal.

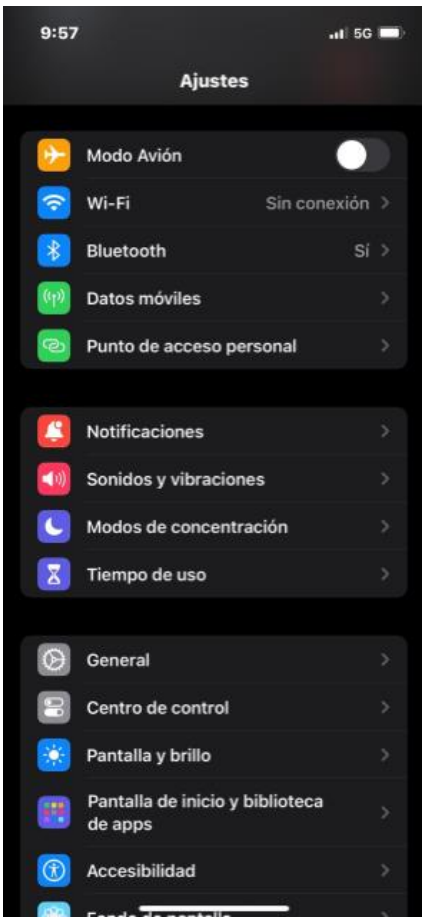
Para asegurarnos de que esta funcionalidad está activa, accederemos a Ajustes > ID de Apple > Buscar y activaremos la opción 'Buscar mi iPhone'.

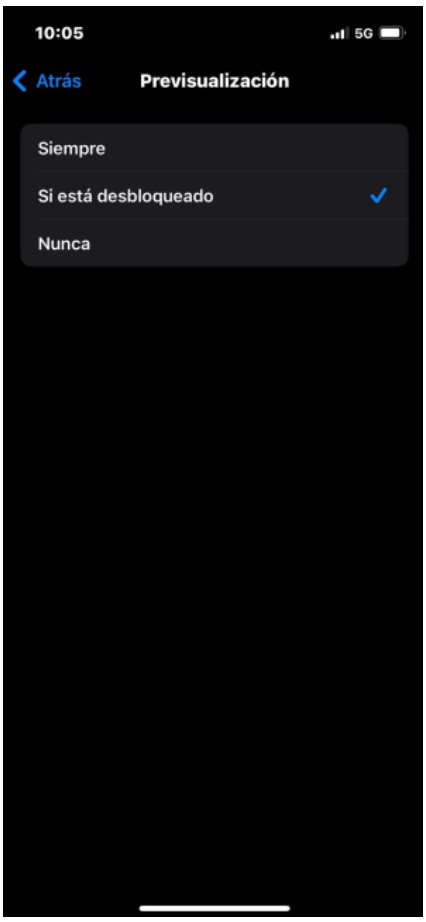


4. Notificaciones

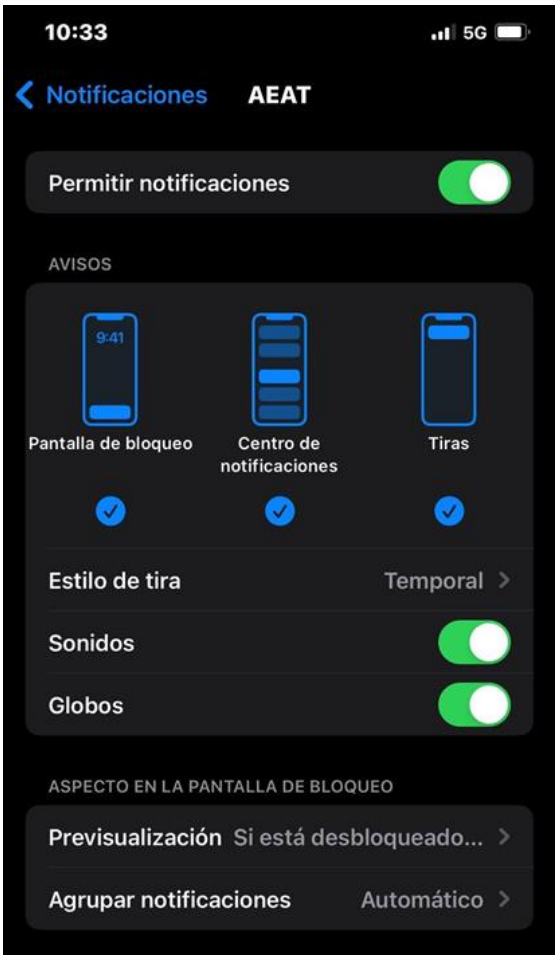
Si queremos impedir que otras personas puedan ver las notificaciones e información que aparecen en nuestra pantalla, es importante que configuremos las notificaciones para que no muestre previsualizaciones de la información recibida.

Para ello, dentro de Ajustes, pincharemos en Notificaciones > Previsualización. Una vez en ese menú, podremos seleccionar 'Nunca' para evitar recibir previsualizaciones en las notificaciones. Aunque, también se puede elegir la opción '*Si está desbloqueado´*, con esta opción las notificaciones aparecerán únicamente cuando el dispositivo este desbloqueado.



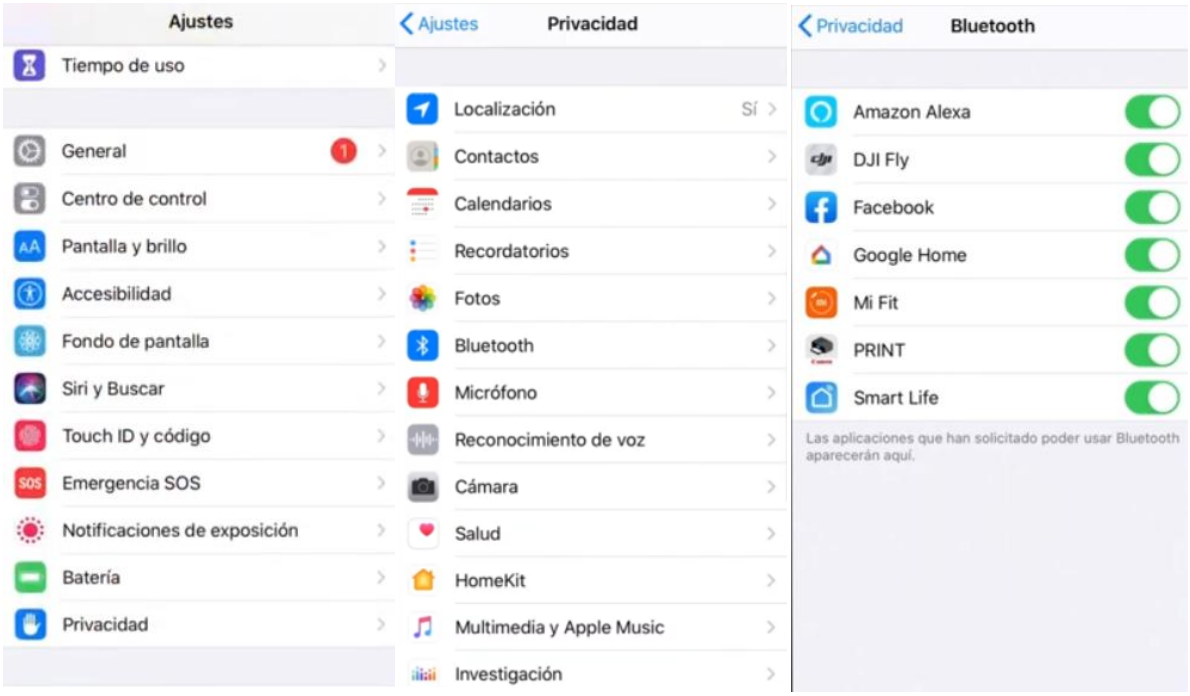


En el mismo menú, podremos además seleccionar cada una de las aplicaciones y decidir individualmente si queremos recibir notificaciones o no.

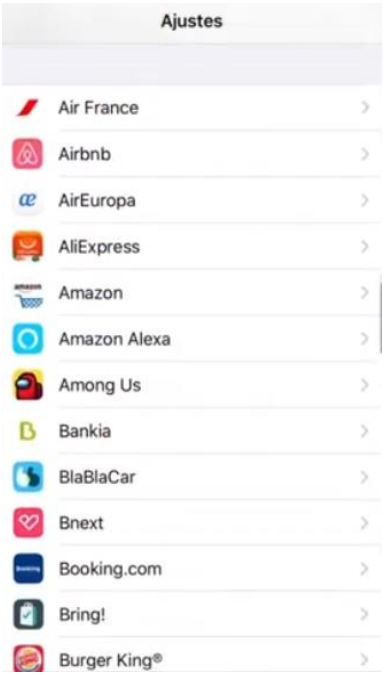


5. Permisos de acceso

Otra de las opciones que nos dan más control sobre nuestro dispositivo y nuestra privacidad son los permisos de acceso. Gracias a esta opción, podremos decidir qué aplicaciones tienen acceso a las diferentes funcionalidades del dispositivo. De este modo, las aplicaciones sólo podrán acceder a la información que necesitan para su actividad. Para configurarlo, accederemos a Ajustes > Privacidad y seguridad. Una vez ahí, veremos todas las funcionalidades y podremos acceder a cada una de ellas. También ver la lista de aplicaciones con permiso para hacer uso de ellas.

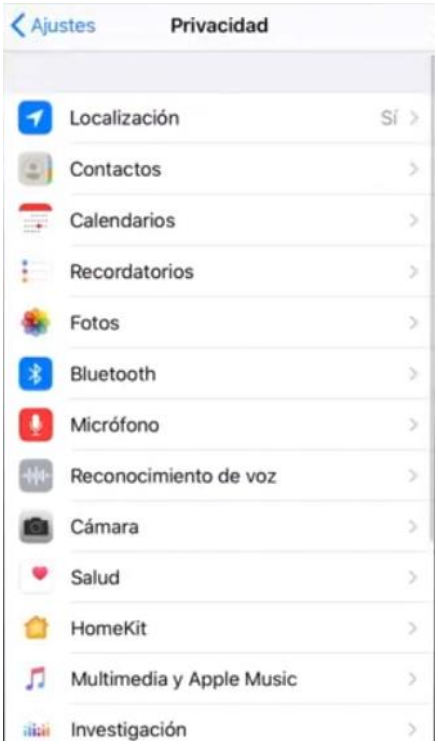


Otra opción para comprobar los permisos que cada aplicación es a través de Ajustes y buscando directamente la lista de aplicaciones instaladas. Seleccionando cualquier de ellas, aparecerán los permisos otorgados.



6. Ubicación

Es recomendable no compartir nuestra ubicación, o al menos, restringir qué aplicaciones y cuándo tienen acceso a dicha información. Para configurarla, entraremos en Ajustes > Privacidad y seguridad > Localización. Podremos desactivar la localización de manera general, desactivando 'Localización'.



También podremos permitir acceso a la ubicación de manera independiente y específica para cada una de las aplicaciones con las siguientes opciones: nunca, preguntar la próxima vez o al compartir, cuando se use la app o siempre.

Dentro de los ajustes de Localización, encontramos la opción 'Compartir mi ubicación', que es recomendable desactivar para evitar que otros dispositivos y usuarios puedan conocer nuestra localización en todo momento.

7. Siri y el uso de datos

Siri es un asistente de voz que apareció por primera vez el 4 de octubre de 2011 en la presentación del nuevo iPhone 4S. Este asistente, nos ayuda con las tareas cotidianas e información que necesitemos, pero para conseguir que nos ayude de una manera más eficiente, nuestra privacidad se puede ver comprometida ya que analiza el uso que hacemos de cada una de nuestras aplicaciones.

Para desactivar esta opción en las aplicaciones en las que no queremos que Siri analice nuestro comportamiento, entraremos a Ajustes > Siri y Buscar. Allí encontraremos un listado de todas nuestras aplicaciones y en cada una de manera individual desmarcaremos la opción 'Aprender de esta app'.

También, se puede desbloquear varias funcionalidades de Siri según nuestras preferencias, para ello hay que entrar en Ajustes > Siri y Buscar. En esta pantalla podremos activar o desactivar las siguientes opciones:

Como hemos aprendido a lo largo de este capítulo, existen una serie de configuraciones necesarias si queremos que la privacidad de nuestra información no se vea comprometida. Para ello, te pediremos aplicar algunas de las configuraciones explicadas anteriormente.

4. Cómo actuar en caso de robo o pérdida de dispositivos

Por desgracia, todos conocemos casos de pérdidas o robos de dispositivos que nos dejan de repente en una situación de incertidumbre y desamparo, y es que nuestros dispositivos se han convertido casi en una extensión de nuestro cuerpo, y por supuesto, en nuestro principal almacén de información.

Es por ello que en este capítulo trataremos de dar una serie de pasos y consejos a seguir en caso de que nos veamos envueltos en tan desafortunado suceso.

Primer intento de contacto

Es importante recordar que, en estas situaciones, es primordial actuar con rapidez, ya que es muy posible que hayamos dejado el móvil olvidado en algún sitio, o que simplemente se nos haya caído del bolsillo.

En este caso, lo que se suele hacer es llamar a nuestro número y enviar un mensaje de texto dando instrucciones de cómo devolverlo o dónde dejarlo, ya que es posible que haya caído en manos de alguien que quiere devolverlo, pero no sabe cómo ni dónde.

Sin embargo, si este primer intento no es exitoso, deberemos tratar de localizar el dispositivo lo antes posible desde las propias posibilidades que nos dan los fabricantes y los diferentes sistemas operativos.

Localizar el dispositivo

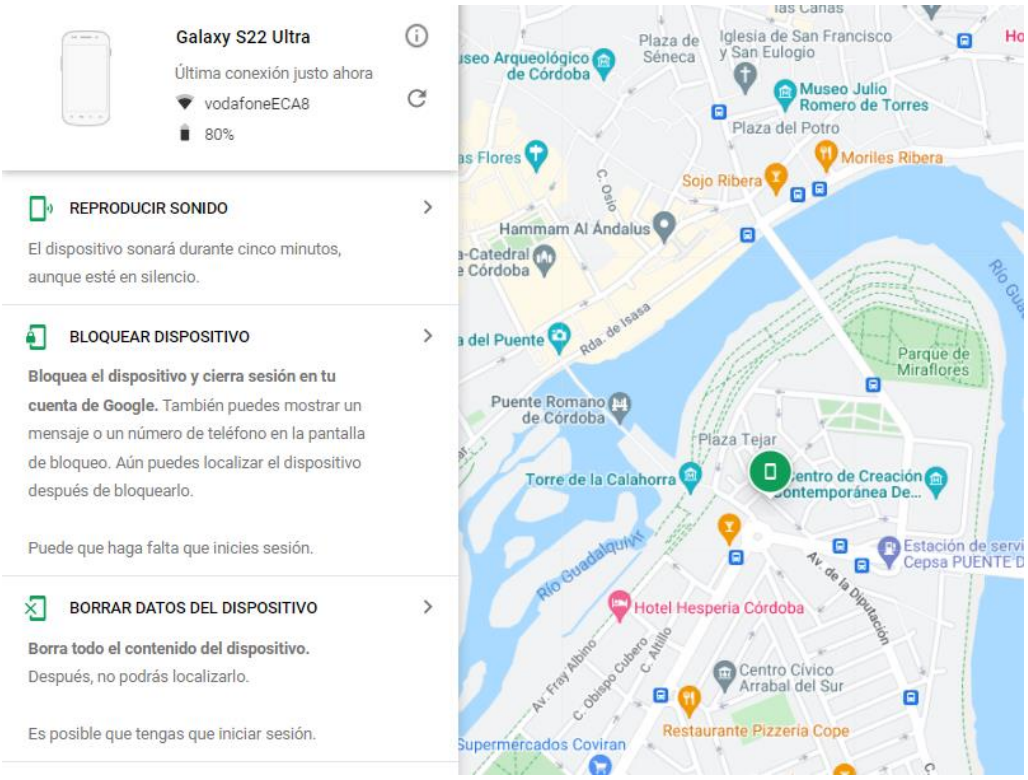
La funcionalidad de rastrear y encontrar nuestros dispositivos en caso de pérdida o robo ha ganado visibilidad en los últimos años, y el número de usuarios que la conocen y la tienen activa ha crecido de manera exponencial. Ya sea en Android, mediante la función 'Encontrar mi dispositivo' de Google, o en iOS con 'Busca mi iPhone'.

Estas funciones integradas en los sistemas de los dispositivos nos permitirán saber dónde se encuentra nuestro dispositivo de forma remota a través de un ordenador u otro dispositivo, conectándonos a nuestra cuenta de Google o iCloud. Además, nos ofrecen otras opciones adicionales que veremos en detalle a continuación.

Para acceder a la citada funcionalidad, se puede hacer a través de cualquier navegador, entrando a la página web de nuestra cuenta de Google, para dispositivos

Android, https://myaccount.google.com/find-your-phone, o en la cuenta de iCloud para dispositivos de Apple https://www.icloud.com/find.

Captura del sistema operativo de Apple, iOS



Captura del sistema operativo de Google, Android

Además de la ubicación del dispositivo, que podremos ver sobre un mapa, también veremos otras opciones disponibles, muy similares en ambos sistemas operativos.

- **Reproducir un sonido:** esta función es muy útil, ya que hará sonar nuestro dispositivo aunque se encuentre en silencio, por lo que podremos escucharlo si lo hemos perdido cerca de nosotros y no podemos llamarlo o se encuentra silenciado.
- **Bloquear el dispositivo o 'Modo perdido':** si no somos capaces de encontrar el dispositivo, es una buena opción bloquearlo. Esto mostrará un mensaje a pantalla completa en el teléfono que podrás elegir, como un número de teléfono al que llamar, para que la persona que lo encuentre pueda ponerse en contacto contigo.
- **Borrar datos:** en el peor de los casos, si lo damos por perdido y preferimos asegurarnos de que nuestros datos privados no pueden ser accedidos de ninguna manera por terceros, esta opción borrará todos los datos que tengamos almacenados en nuestro dispositivo. A continuación, explicamos más en detalle en qué consiste.

Borrado remoto, qué es y cuándo debemos utilizarlo para proteger nuestra privacidad

La opción de borrado remoto es quizás la más drástica de todas, ya que es una funcionalidad que nos permite garantizar que, en caso de pérdida o robo de nuestro dispositivo, toda la información existente en el mismo puede ser borrada desde cualquier otro dispositivo con conexión a Internet, evitando así que una tercera persona pudiera acceder a nuestra información confidencial almacenada en el dispositivo, o hacer uso de nuestras cuentas de correo u otras.

Así pues, es una opción recomendable solo si nos encontramos en una situación en la que estamos seguros de que no recuperaremos nuestro dipositivo y que además existe un riesgo de que la información que contiene pueda ser accedida.

Aunque esta funcionlidad puede ser muy útil en la situación que hemos descrito en el párrafo anterior, es importante recordar que el borrado de datos será irreversible, y sólo podremos recuperar nuestros datos si tenemos una copia de seguridad de los mismos en otro dispositivo o soporte de almacenamiento, ya sea en la nube o un disco duro externo, por ejemplo.

Informar al operador

Contactar con el servicio de atención al cliente de tu proveedor móvil informandoles de la situación de pérdida o robo, ya que ellos pueden bloquear la SIM, además del IMEI, evitando de este modo su uso.

¿Robo o hurto? Denuncia en la comisaría más cercana

A pesar de que todo lo explicado anteriormente nos puede ayudar a recuperar nuestro dispositivo, y a asegurarnos de que nuestra información no acaba en manos ajenas, es importante recordar que, si la pérdida de tu dispositivo se debe a un robo o hurto, debes denunciar de inmediato el suceso ante las Fuerzas y Cuerpos de Seguridad del Estado.

Para interponer la denuncia deberás tener a mano el número de identificación del dispositivo (IMEI).

Este número puede ser encontrado de estas formas:

- Dentro de los ajustes del dispositivo, buscando por IMEI
- Marcando el código *#06#
- En la caja del dispositivo.
- A través de 'Encuentra mi dispositivo' en Android (dentro de 'Encuentra mi dispositivo', pulsando en el icono de información (i) a la derecha del nombre del dispositivo) y en appleid.apple.com para iOS (Menú 'Dispositivos' y seleccionando el dispositivo concreto del que se quiere obtener la información > apartado 'Información').

Además de ser imprescindible para interponer la denuncia, con el IMEI y la propia denuncia podrás solicitar a tu operadora el bloqueo del terminal para evitar que se use con otra tarjeta SIM.

Cambiar las contraseñas de tus cuentas

Además de realizar la denuncia es importante recordar que existe la posibilidad de que un tercero que tenga nuestro dispositivo haya podido acceder a nuestras cuentas de redes sociales, correos electrónicos o aplicaciones bancarias si no lo teníamos bloqueado con algún mecanismo, por lo que debemos proceder a cambiar todas las contraseñas, en especial aquellas en las que almacenamos información privada.

Consultar objetos perdidos o establecimientos cercanos

No debemos olvidar que hay mucha gente con buenas intenciones, que han podido encontrar tu dispositivo, pero no saben qué hacer con él, por lo que buscarán algún establecimiento cercano o lo dejarán en objetos perdidos de hoteles, aeropuertos, estaciones, etc. dependiendo de dónde se haya producido la pérdida.

Por lo tanto, siempre es una buena práctica preguntar en lugares donde potencialmente podrían haber dejado el dispositivo, así como volver a preguntar o llamar pasados unos días por si alguien lo ha encontrado con posterioridad.