1 Seguridad en Android

Android está asociado a dispositivos móviles y a tablets, también hay ordenadores en los que puede instalarse, pero no es nada habitual, solo para prueba. También se puede tener en Android Boxes (para conectar a las televisiones) y en los AndroidTV (variante de Android exclusiva para conectar a televisiones que está cambiando de nombre a GoogleTV), FireTV (versión de AndroidTV tuneada por Amazon y que funciona con su sistema propio de Android). En los coches últimamente también se está incluyendo Android Auto. También hay relojes con Wear OS, versión Android para relojes hecha por Google, pero solo algunos fabricantes lo usan.

Muchas de las cosas que se van a contar en este curso pueden ser aplicadas en todas partes donde un sistema Android se esté ejecutando, pero aquí solo vamos a centrarnos en los dispositivos móviles.

Los principales aspectos a nivel de seguridad van a ser 3:

- Seguridad física
- Seguridad de acceso al dispositivo
- Seguridad de datos dentro del dispositivo

1.1 Seguridad física de dispositivos

Cuando nos compramos un móvil, nos lo regalan, nos lo financie nuestro operador telefónico, etc. sabemos que es un artículo con un coste alto, no es una barra de pan ni un vaso de cristal que si se rompe no pasa nada y no nos ha costado mucho. En algunos casos los precios de los dispositivos suponen un desembolso muy apreciable y durante un periodo largo de tiempo y es por ello que queremos que nos dure lo máximo posible en las mejores condiciones.

Es por eso que lo primero que buscaremos es proteger físicamente nuestro dispositivo y es aquí donde vamos a empezar a ver que posibles elementos de seguridad podemos añadirle para que así nos dure lo máximo posible.

1.1.1 Que tipos de seguridad física podemos tener en nuestros dispositivos

Vamos a ver que tipos de seguridad física deberíamos tener en cuenta para proteger de la mejor manera nuestros dispositivos.

1.1.1.1 Carcasas y tipos de carcasas

Principalmente se usan para evitar caídas, en función de lo que queramos que resista iremos a carcasas armadas o gorditas, o más finas.

1.1.1.1.1 Rugerizadas

Son las que más protegen el móvil. Son una variante de las carcasas, pero se diferencian de ellas en su aspecto de armazón resistente. Están pensadas para proteger de las caídas más grandes.

1.1.1.1.2 Bumpers

Protegen la zona de impacto ante las caídas. Laterales y cantos, con un bumper puedes salvar tu teléfono sin que tampoco incomode en exceso el uso diario. Son de plásticos diferentes y a veces con otros tipos de materiales, son sencillas. Y las que menos tamaño añaden al dispositivo. Son también bastante flexibles.

1.1.1.1.3 De libro

Este tipo de protecciones que, además de guarecer la parte trasera y los laterales del móvil, dispone de una tapa que pivota sobre el lomo. Como un libro, de ahí el nombre. Son muy

utilizadas en tablets y libros digitales. En móviles se ven menos, pero en china los venden como churros con todo tipo de personalización, aunque la dureza y protección no es la mejor.

1.1.1.1.4 Fibra de carbono

Son las más resistentes, absorben más impacto y lo resisten. Son muy finas y con muy poco peso, pero no cubren todo el móvil, serían más como las de tipo bumper, pero mucho más caras.

1.1.1.2 Protectores de pantalla y sus tipos

Está claro que según el tipo de carcasa que tengamos, es posible que necesitemos completar nuestra protección con algo más. En el caso de las carcasas tipo libro podría no necesitar nada más, pero lo normal es usar una protección en la pantalla.

Es cierto que los fabricantes incluyen unos cristales que ya tienen una protección contrastada, siendo mejor cuando la categoría del móvil es más alta. Esta seguridad viene determinada por el fabricante de la seguridad del cristal y nos sonaran algunas como Gorilla Glass, Dragontail o Dinorex. En todos hay diferentes categorías de calidad y los fabricantes incluyen las mejores en las gamas más altas. Aun así, las gamas más bajas también tienen seguridad en el cristal que montan, pero no es la más alta del fabricante del cristal.

Es cierto que esta seguridad ya incluida en el cristal puede hacernos pensar que no es suficiente (que muchas veces no lo es) y es entonces cuando nos plantearemos añadir una seguridad extra a nuestra pantalla y para ello hay que tener en cuenta que los tipos de pantallas de dispositivos que hay: planos, con bordes curvos, plegables.

Según el tipo de pantalla podemos vernos obligados a usar un tipo u otro, o tal vez poder elegir.

1.1.1.2.1 Cristal templado (vidrio templado)

Suele ser más caro que el otro sistema de protección y ofrece un tacto mejor. El grosor que tenga nos en lo molesto o no molesto que nos sea. Los bordes no son muy cómodos cuando es demasiado grueso. La seguridad no se ve afectada por el grosor, pues depende de cómo se haya fabricado, las capas internas que tenga y la calidad de las mismas.

Los cristales además suelen llevar una capa oleofóbica que repele la grasa natural que tenemos en los dedos y evita que se queden muy marcados los cristales. También repele un poco la lluvia.

1.1.1.2.2 Hidrogel

Es un compuesto de silicona o resina liquida y por tanto la superficie es blanda. Al no ser rígido como el cristal templado su durabilidad es mayor, y al ser blando su absorción de impactos es mayor.

El grosor suele ser mucho menor que un cristal templado y permite adaptarse a las curvas de las pantallas nuevas.

1.1.1.2.3 ¿Cuál elegir?

Comparativa con ejemplos y videos

https://www.youtube.com/watch?v=zLFQ0KzK9Vg

A mayores de todo lo dicho anteriormente:

- Hay protecciones para los cristales traseros de las cámaras, también los hay y se pueden poner incluso con carcasas protectoras.
- Se puede poner un hidrogel en la parte posterior también con diseño personalizado.

1.2 Seguridad de acceso al dispositivo

En nuestro dispositivo llevamos prácticamente todo tipo de información personal, ya sean fotos, documentos, redes sociales, temas monetarios, etc. Es importante que no dejemos acceso fácil a nuestro dispositivo a personas que no deberían acceder a él.

Muchas veces dejamos incluso a personas que conocemos nuestro dispositivo, como pueden ser nuestros propios hijos, pues ellos ven nuestro excesivo uso del dispositivo y quieren usarlo también, como si fuera un juego solo lo que hay en él y no es así, incluso ellos pueden hacer que nuestros datos se publiquen donde no deben, compren cosas que no queremos, pero que habrá que pagar, o eliminen información que no queremos perder. Como regla principal un móvil personal no es un juego y no deberíamos dejárselo a nadie, solo cuando nosotros tenemos control sobre lo que están haciendo o pueden hacer.

En este caso existen programas launcher que bloquean todo el dispositivo y solo permiten acceder a ciertas aplicaciones sobre las que hemos dado permiso de acceso y solo esas podrán usar.

También hay fabricantes que añaden un 'Modo Niños' donde podemos hacer lo mismo que con un launcher del texto anterior, pero también nos tocara configurar que aplicaciones permitiremos usar y no.

1.2.1 Como proteger para que solo nosotros podamos acceder a nuestro dispositivo

Muchas veces cuando configuramos un móvil nuevo nos aparece una opción de configuración de seguridad, ya sea por pin o patrón. Pero es desde los ajustes del teléfono donde podremos configurar todas las posibles opciones de seguridad en el acceso a nuestro dispositivo.

Los ajustes de sistemas varían según el fabricante y según la versión de Android propia que cada fabricante tiene.

Aquí conviene ver que tipos de Android existen.

1.2.1.1 Que es Android AOSP

AOSP significa Android Open Source Project, o traducido al español Proyecto de código abierto de Android, así pues, este Android AOSP es el código fuente básico en el que se base todo el sistema operativo pensado por Google.

Google empezó a desarrollar Android basándolo en un proyecto de código abierto, esto significa que todo el mundo puede ver, utilizar y modificar el código fuente de Android a su gusto, gratis y sin tener que dar cuenta a nadie.

Google lo hizo así para que Android ganara popularidad y así poder vencer a los sistemas operativos de Windows y de Apple, que en aquellos momentos dominaban el mercado de móviles, acertando en su decisión.

El código fuente de Android contiene lo básico para que funcione:

- Gestor de ventanas
- Gestor de aplicaciones
- Drivers para las cámaras de fotos, GPS, wifi, audio y sensores del móvil
- Sistema para el control de pantallas
- Servicios de reproducción de vídeo
- Servicios de seguridad del sistema, logado en el dispositivo, etc…

Todo esto está disponible para quien que lo necesite, no está restringido a ningún país, ni a ninguna ley, ya que es totalmente código abierto, esta es la gran fuerza de Android respecto a Windows de Microsoft o iOS de Apple que son sistemas totalmente cerrados, cuyo código fuente es privado y nadie lo ha podido ver nunca.

Así pues, en resumen, Android es un sistema de código abierto (AOSP) que cualquier empresa o fabricante puede utilizar sin pagar royalties a nadie. Google tiene una versión propia, donde ha añadido sus servicios y aplicaciones (GMS o Google Mobile Services), y este lo pone a disposición de los fabricantes para que lo utilicen. Google lo tiene actualizado siempre y va por delante de AOSP en todo momento. Es aquí donde Google gana dinero, ya que los fabricantes que usan su versión de Android con sus GMS tienen que pagar por ello.

Al igual que Linux es la base, cada versión sobre Linux es un sistema propio de quien lo hace: Ubuntu, slackware, LinuxMint, etc. Android por debajo está hecho en Linux, pero solo en el kernel.

Así pues, cada fabricante utiliza ese Android de Google y lo tunea, le mete aplicaciones a mayores que consideran necesarias o útiles para sus clientes, y los ajustes los pone como mejor le parece. Es por ello que lo que se diga aquí puede variar de localización y nombre según el fabricante del dispositivo y la versión de su Android que tenga instalado.

Entonces en los Ajustes del sistema, en la opción bloqueo de pantalla, ahí encontraremos las opciones necesarias para configurar el tipo de bloqueo de acceso que consideremos.

1.2.1.2 Huawei usa AOSP

El caso de Huawei es un caso particular debido a una prohibición explicita del gobierno de los EE.UU., el cual no permite usar los GMS a dicho fabricante, por lo cual se han tenido que salir del sistema habitual de Android con servicios Google y tener que implementar sus propios servicios para equiparar el funcionamiento de su Android al de Google.

Los servicios principales que han ‘clonado’ son de localización, de publicidad, de Store de aplicaciones (las aplicaciones tienen versiones específicas para su Store sin los GMS de Google y usando los de Huawei), servicio de correo, mapas, etc.

1.2.2 Tipos de bloqueo

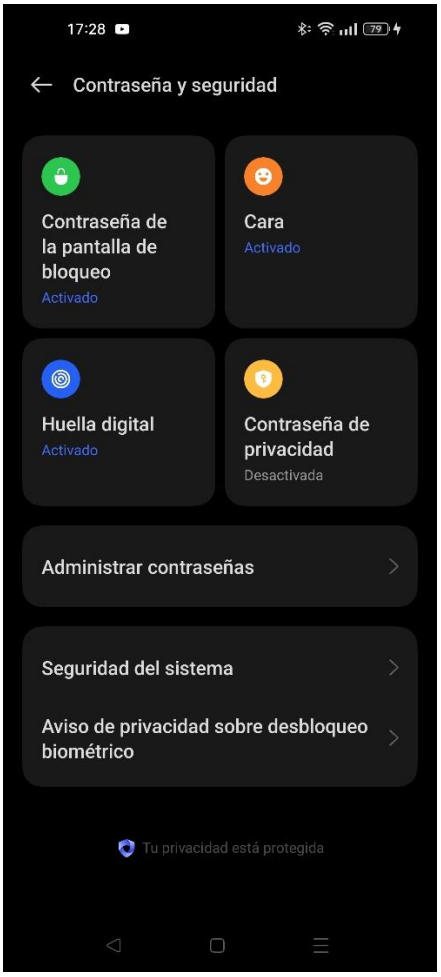
Hablamos de tipos de bloqueo, aunque principalmente son de desbloqueo, pues para nosotros es nuestra manera de desbloquear el acceso y poder acceder a toda la funcionalidad de nuestros dispositivos, pero a su vez en una manera de bloquear el acceso al resto de personas.

Lo principal de un sistema de bloqueo es que este activado y que, en caso de no estarlo, al pasar un tiempo, que este se active automáticamente. Es por eso que la activación automática deberemos tenerla en un espacio de tiempo corto, ya que si nos dejamos un móvil otra persona podría entrar en el durante ese periodo. Lo recomendado en estos casos es elegir un bloqueo a los 30” o al minuto, como máximo.

1.2.2.1 Patrón de desbloqueo

Un patrón de desbloqueo es un código que consiste en unir una serie de puntos (de 4 a 9) en una línea sin levantar el dedo de la pantalla.

Para llegar a él debemos ir a los ‘Ajustes’ de nuestro dispositivo. Una vez ahí en la parte de ‘Seguridad’, o ‘Contraseña y Seguridad’, accederemos a la parte de ‘Bloqueo de pantalla’ o algo similar.



(Las pantallas pueden ser diferentes en función de la versión de Android que tenga nuestro dispositivo y de los colores elegidos.)

La ventaja de este modo es la sencillez a la hora de usarlo y que es fácil de acordarse, acabando siendo mecánico en la ejecución, pero su desventaja es que visualmente nos lo pueden averiguar.

1.2.2.2 PIN

Este sistema de seguridad es el más antiguo, lo usamos en todas partes, tarjetas bancarias, de acceso a empresas, a zonas, etc. Y principalmente al encender el teléfono que también nos lo pide para desbloquear el uso de nuestra tarjeta SIM.

Consiste en un código numérico que va desde los 4 a los 17 dígitos, y accedemos a su configuración también desde los ajustes del sistema.

La ventaja es que podemos configurar un código rápidamente y fácilmente recordable, pero por contra nos pueden adivinar dicho código más fácilmente si no es suficientemente fuerte.

1.2.2.3 Contraseña

Posiblemente sea el sistema más seguro de los métodos habituales desde siempre, también el más añejo, y consiste en configurar una contraseña como solemos usar con nuestras cuentas de correo o acceso a redes sociales.

La ventaja es clara, es muy segura si la contraseña es fuerte, pero por el contrario tiene que puede ser difícil de recordar y acabar siendo molesto escribirla continuamente para desbloquear nuestro dispositivo, aparte de que podemos equivocarnos al escribirla y tocara repetirlo de nuevo.

1.2.2.4 Huella dactilar

Aquí empezamos con los sistemas biométricos, que lo bueno que tienen es que una vez configurados son fáciles de usar y casi imposibles de replicar para por parte ajena.

La huella dactilar aún no está implementada en todos los dispositivos. Hace algunos años solo estaba disponible en los dispositivos de más alta gama, pero se ha ido implementando cada vez más y actualmente está en casi todos los modelos nuevos.

Debido a que está siendo una tecnología relativamente nueva, no hay una unificación de cómo debe ser el sensor ni dónde colocarlo, por lo que cada fabricante está desarrollándolo de diferentes maneras para encontrar cual es la que más se ajusta a lo que los usuarios usen, por eso encontramos sensores en teclas de navegación (teclado físico en la parte de debajo de la pantalla), en la tecla de encender o apagar el móvil, botón dedicado en el lateral para la huella, o incluso sensores debajo de la pantalla.

Como consejo, es mejor, a la hora de crear nuestra huella, usar el dedo en múltiples posiciones para así mejorar la capacidad de acierto del sensor.

Como cada fabricante usa su sensor de manera particular, esta parte de configuración y uso es propia de cada uno y puede aparecer de manera distinta en los ajustes para su configuración, aunque dicha configuración estará también en la misma sección que el resto.

Como principal ventaja esta la rapidez a la hora de tener que poner nuestra huella dactilar donde corresponda, así como la casi imposibilidad de que nos clonen una huella dactilar nuestra. Como posibles desventajas tenemos que los sensores puedan ser mejores o peores teniendo que colocar nuestra posición dactilar de una determinada manera para que el sensor lo cuadre con

las huellas capturadas, con lo que nos tocara volver a usar nuestro dedo hasta que sea detectado.

1.2.2.5 Desbloqueo facial

Dado que todos los dispositivos tienen una cámara frontal, los fabricantes han empezado a incorporar otro sistema biométrico que consiste en detectar nuestra cara frente al dispositivo y así poder desbloquearlo.

Esto no es relativamente nuevo ya que existen las cámaras delanteras desde hace años y para ello no se necesita un sensor nuevo, ya que con el mismo uso de la cámara y un software de detección puede hacerse funcional el desbloqueo (existen hardware para la detección).

Lo que si ha ido es evolucionando para que sea cada vez más fiable, pues antes se podía engañar a la cámara con fotos, por ejemplo, o en condiciones de luz malas la cámara no te reconocía, o si usabas gafas de vez en cuando, etc. Ahora funcionan que directamente al levantar el móvil, y ponértelo delante te reconoce y desbloquea el móvil directamente, todo en un instante.

Hay una variante del sistema por cámara y es por infrarrojos, el cual usa una proyección de miles de puntos sobre el rostro para hacer una maqueta exacta de la cara y lo compara con el rostro guardado. Este sistema lo tienen muy pocos teléfonos siendo el más preciso de los sistemas de desbloqueo faciales, de hecho, los últimos Iphone con Face ID los llevan.

1.3 Seguridad de datos del dispositivo

Nuestros primeros datos en nuestro dispositivo son gestionados directamente por el sistema operativo, Android, en este caso, y por eso que lo primero que debemos tener es (siempre que sea posible) nuestro sistema operativo actualizado.

Además, en nuestro dispositivo lo que nos interesa es que la información personal que tenemos en él no nos desaparezca, ya sea por acción humana, es decir nuestra o de alguien que entre en el dispositivo o por acción ajena, que suframos un ataque o una app maliciosa nos perjudique algo.

Que datos nos interesan proteger en un dispositivo:

- Fotos y videos
- Datos personales (contactos, llamadas, sms)
- Mails
- Redes sociales
- Información bancaria
- Datos médicos
- Documentos

Lo primero que deberemos hacer es buscar algún modo de que esta información este salvaguardada en alguna parte y que sea fácilmente recuperable en caso de perdida, y esto lo haremos a través de aplicaciones.

Debemos distinguir aquí las aplicaciones que son propias de Google, de las que no, ya que Google ofrece a sus clientes un espacio de almacenamiento, amplio pero limitado, en su nube, para que puedan guardar cierta información en ella y poder recuperarla fácilmente. Estas apps usan los servicios que Google ofrece, ya sean de pago o gratis.

Las aplicaciones de copia de seguridad que no son de Google tienen el problema (no todas) de que para acceder a cierta zona de los datos se necesitan permisos especiales y de alto rango, y eso solo se puede conseguir únicamente si el teléfono esta rooteado. Aquí es donde Google prioriza sus aplicaciones y les da dichos permisos para poder hacer lo que quiera con la información que tenemos en el dispositivo.

Algunas aplicaciones a mayores que podemos usar para copias de seguridad podrían ser estas: Apps de copia de seguridad

1.3.1 Actualización del sistema

Cuando adquirimos un dispositivo, adquirimos también un servicio de actualizaciones que, según el fabricante, puede ir desde 1 año a 5 años en dicho mantenimiento.

Google publica dos tipos de actualizaciones, una corresponde al propio sistema operativo Android, que suele cambiar una vez al año, normalmente en el último cuarto del año. Antes de publicarlo para sus dispositivos, también cede versiones básicas a los fabricantes para que ellos puedan también ir adaptándose a los cambios, mejoras y demás, que esa nueva versión va a tener y así estar al día en sus dispositivos más nuevos. El otro tipo de actualizaciones que publica Google son de seguridad, ya sea para corregir vulnerabilidades detectadas como posibles problemas con cosas básicas del sistema. Estas son enviadas también a los fabricantes. Suelen ser mensuales. Aun así, cada fabricante ajusta esa versión de actualización de vulnerabilidades y pueden publicarlas juntando varias y siendo espaciadas en el tiempo.

Estas actualizaciones nos llegaran como avisos de actualización y normalmente descargan gran cantidad de datos, esto es mejor hacerlo con wifi y con la batería bien cargada por si este proceso demora mucho en hacerse. Normalmente nos pide autorización para actualizar o no y una vez autorizado el proceso ya es automático. También podemos indicar que de manera automática compruebe si hay nuevas versiones y que estas se descarguen automáticamente, aunque esto depende del fabricante también si lo ha implementado así o no.

1.3.2 Stores de aplicaciones

Las aplicaciones también necesitan ser actualizadas, pero de donde podemos instalar una aplicación y donde la podemos actualizar.

De un tiempo a esta parte en los sistemas operativos se incluye una aplicación que agrupa a todas las aplicaciones (que quieren estar) para que puedan ser instaladas en ese sistema operativo, ya sea MacOS, Windows, Linux, iOS o Android.

Estas apps son conocidas como Stores y son los almacenes de todas las aplicaciones que fácilmente son localizables e instalables en el sistema operativo que sea.

Es normal pensar que en nuestros dispositivos solo hay un Store de aplicaciones, que siempre es el Play Store, pero hay que recordar que esta aplicación pertenece a Google y por tanto en los otros Android que solo son AOSP no estará esta aplicación.

Así pues, lo normal es que siempre tengamos instalada nuestra Play Store de serie y no tengamos que hacer nada, pero esto no es así: por ejemplo, Huawei tiene su store propio de aplicaciones, Samsung también, y otras mas como Amazon y otros teléfonos chinos.

Aparte de stores de fabricantes, también existen stores libres que podemos instalar y de los cuales podemos bajar y actualizar aplicaciones.

Aquí es importante saber cual es la app store principal de nuestro teléfono, pues en ella saltaran las actualizaciones automáticas. En caso de haber solo una no habrá duda, pero puede ocurrir que teniendo varias, las apps no llegan a actualizarse, pues no sabrá de cual store de hacerlo.

Es importante saber que los stores como Play Store pasan unos controles, cada vez mas exhaustivos a las aplicaciones que se publican en ellas, tirando muchas de ellas por diferentes causas, ya sea por incumplimientos de servicio, por ser perjudiciales, por decir que hacen unas cosas y luego hacen más por detrás, o por usar unos permisos que realmente no necesitan.

Los stores libres no tienen esa capacidad de control sobre las apps que se publican en ellos y de hecho tampoco cobran por las publicaciones y es por eso que a veces las apps ahí publicadas no son igual de seguras que las publicadas en la Play Store.

Ojo con descargarnos apps alegremente de internet e instalarlas, o descargarlas de un grupo de Telegram y usarlas. Muchas veces estas apps hacen cosas por debajo que no vemos, nos piden permisos que no necesitan y eso es porque hay grupos de hackeo que las descompilan, meten sus programas espías o que hacen cosas que no queremos, las vuelven a compilar y las publican en stores libre (en la Play Store no podrían publican porque los detectan rápido)

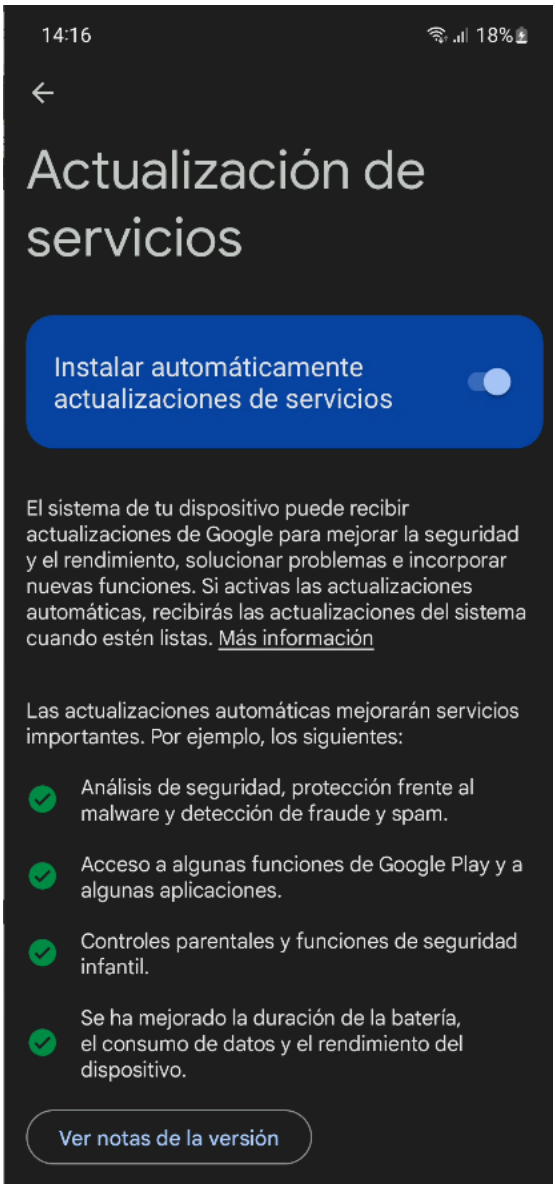
1.3.3 Automatización de actualización en los servicios Google

Lo normal es que las actualizaciones se descarguen, e instalen, de manera automática en segundo plano de nuestro store principal, pero podríamos habilitar o deshabilitar esta característica.

Si por alguna razón queremos desactivarlas lo podríamos hacer de la siguiente manera (puede variar según el fabricante y su versión de Android):

- Entramos en Ajustes
- Entramos en la sección Google
- En los 3 puntos de arriba a la derecha pulsamos y elegimos ‘Actualizaciones de los servicios del sistema)
- Nos mostrara la pantalla donde podremos desactivar o no dicha característica

Por normal, lo suyo es que se deje activado siempre, pero puede haber casos donde nuestro dispositivo se queda antiguo y las nuevas versiones de los servicios de Google no nos funcionen correctamente y ahí es donde deberíamos dejarlo bloqueado.



Aquí nos vamos a detener a ver las otras opciones que nos aparecen en esta pantalla para ver que son cada cosa.

1.3.4 Nube de Google para Android

Hemos visto antes que por configuración podemos hacer que Google automáticamente nos guarde una copia de mucha de nuestra información relevante, algunas cosas de modo automático y otras por indicación nuestra.

Los datos que se guardan en la nube nos sirven también para cuando migramos a un nuevo dispositivo, al indicar nuestra cuenta de Gmail, podamos recuperar nuestros datos principales como son:

- Aplicaciones instaladas
- SMS
- Historial de llamadas
- Ajustes del dispositivo (incluidas contraseñas de wifi)

De este modo todo es más fácil cuando sustituimos el dispositivo por uno nuevo.

Google entiende que en sus apps no necesita añadir mas seguridad de acceso, pues ya el usuario es lo suficientemente inteligente para añadir seguridad de acceso al dispositivo, pero aun así muchas apps ofrecen añadir un control de acceso al usuario para que tenga un control a mayores del únicamente configurado por el usuario en el acceso al dispositivo. Es recomendable activar dichos controles de acceso siempre que sea posible.

1.3.5 Cifrado de datos

Los dispositivos Android permiten cifrar todos los datos que están en él. Este proceso de encriptación puede llevar un tiempo importante en función de la cantidad de datos que tengamos en nuestro dispositivo, así que puede ser necesario que en el proceso inicial de encriptación tengamos que tener nuestro dispositivo enchufado a la red, y procurar no interrumpirlo pues podemos corromper los datos si no se terminan de encriptar.

Desde la versión 10 de Android (Android Q) este cifrado es automático e inevitable por parte del usuario, no es opcional, da igual el tipo de dispositivo que sea.

Si nuestro dispositivo es más antiguo y queremos cifrarlo deberemos seguir estos pasos (pueden varias según el fabricante):

- Ir a Ajustes.
- Entrar en Pantalla Bloqueo y Seguridad.
- Toca en «Otros ajustes de seguridad».
- Toca Configuración del sistema.
- Desplázate a Personal.
- Toca Seguridad.
- Desplázate a Cifrado.
- Toca Cifrar “dispositivo”.
- Toca Cifrar “dispositivo” nuevamente.
- Introduce la contraseña o contraseña de la pantalla de bloqueo cuando se solicite.
- Toca Continuar.
- Toca Cifrar “dispositivo”.

Recordemos que esta contraseña nos la pedirá cada vez que encendemos nuestro dispositivo, a mayores de los otros sistemas de seguridad que tengamos activados.

Desde Android 10, el cifrado a usar dependerá de la potencia del dispositivo y si este lleva un chip para cifrado AES, o si no tiene este chip entonces usara un cifrado ChaCha20 por software (aunque es más rápido que el AES)

A partir de Android 10, también se incluye un cifrado TLS 1.3 (como mínimo) para proteger el intercambio de datos entre nuestro dispositivo e internet. No siendo compatible con cifrados más débiles y menos rápidos en su cálculo. Además, añade códecs Bluetooth más fuertes para evitar ataques y también más protección para el núcleo del sistema Android.

1.3.6 Antivirus

Muchas veces, por usar ordenadores, nos acordamos que existen aplicaciones como los antivirus que nos pueden ayudar a evitar problemas. Esperamos que de esa manera no nos entren ataques o aplicaciones maliciosas que nos perjudiquen, pero la realidad es que no los necesitamos.

Tanto en iOS como en Android disponemos de medidas de protección que ya hemos visto que vienen por defecto en nuestros dispositivos y estos antivirus lo único que nos producen es una ralentización del mismo.

La principal de las medidas siempre será instalar aplicaciones del store oficial, Play Store, ya que es donde mas control se hace sobre las aplicaciones antes de publicarlas.

Como tal, un antivirus no nos ayudara mucho, pero estas herramientas vienen con mas aplicaciones y una de ellas es el 'antimalware' y esta parte si nos puede ser útil si navegamos sin mucho cuidado o si pulsamos en enlaces sin querer, que nos pueden llevar a lugares dudosos.

1.3.7 Otras medidas a tener en cuenta

Muchas veces estamos en un sitio, un centro comercial, un aeropuerto, cafetería, etc. y nos ofrecen una red wifi gratuita y abierta. Conectarnos a estas wifis puede ser un error importante pues, aunque la red este creada con malas intenciones si que puede estar mal protegida, con unos niveles adecuados de seguridad, y puede ser utilizada por hackers como puente hacia nuestra información.

Si la red Wifi es falsa entonces ya le dejamos del todo la puerta abierta a quien la haya montado y estaremos totalmente vendidos.

Saber si una red Wifi es buena o falsa no es fácil y lo mejor en estos casos es no usarla y usar nuestros datos contratados con nuestro operador o pedirle a alguien conocido que nos cree una red amiga con su dispositivo para que nos conectemos a través de ella.

- https://www.youtube.com/watch?v=3cB19goAOzI (Chema Alonso)

Otra medida a tener en cuenta es el uso de contraseñas seguras (para servicios o aplicaciones si es que las usamos) y como norma seria que:

- No usemos números fáciles de relacionar: cumpleaños, números de teléfonos, las típicas, etc. que no sean fácilmente deducibles.
- Combinar letras, número y algún carácter especial
- No usar la misma contraseña siempre

También deberemos estar muy atentos al phishing, ya sea a través de nuestro correo electrónico como de los SMS que nos llegan o incluso de mensajes en nuestras redes sociales.

- Siempre sospechar de textos no correctamente escritos, así como de premios y regalos de cosas que no hemos participado.
- Personas que nos contactan que no conocemos o teléfonos que nos indican adivinar quienes son. Nos pedirán dinero y demás, y eso siempre se utiliza con menores.
- Mensajes que instan con urgencia pulsar el link de abajo para hacer tal o cual acción necesaria y rápida para temas bancarios o de cualquier otra índole.

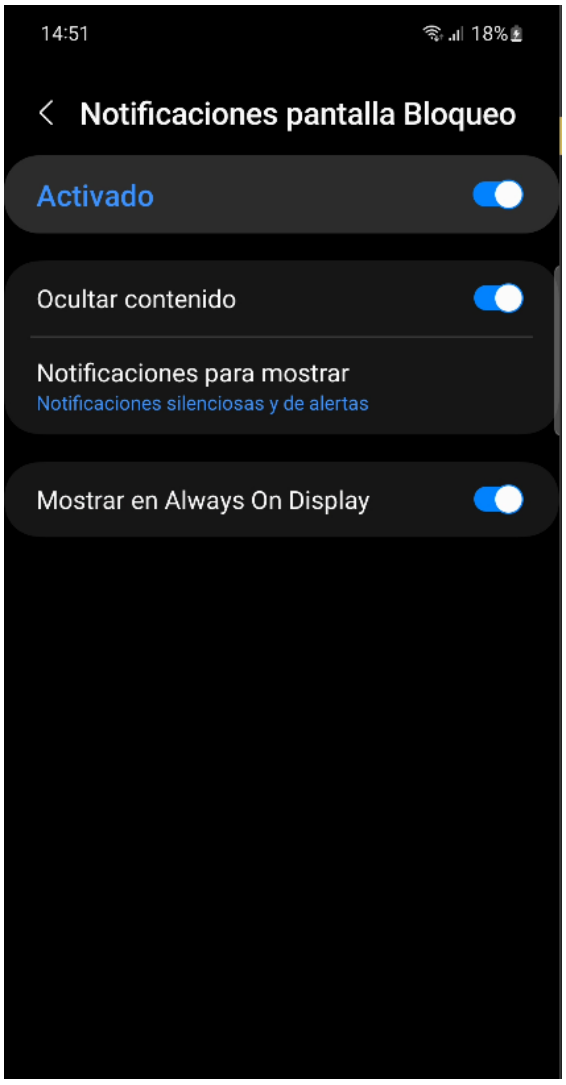
2 Configuración del dispositivo.

La configuración de nuestro dispositivo es esencial para poder estar lo mas seguros y protegidos en nuestro uso diario del mismo. Para ello es muy importante conocer cada una de las partes de configuración del dispositivo, así como el funcionamiento de todos los servicios a los que nuestro dispositivo esta conectado por defecto.

2.1 Notificaciones

Una información que a veces es mejor proteger de personas ajenas son las propias notificaciones que las aplicaciones pueden mostrar. Estas notificaciones muchas veces muestran información parcial, o completa, al usuario sobre mensajes o cosas que son personales y que quisiéramos considerar que no deberían ser vistas por otros.

Es por ello que también en la sección de ajustes deberemos ir a la sección de Notificaciones para configurarlas como queremos que se muestren realmente. Aquí recomendamos que se active la 'Ocultación de contenido' para que no se muestre dicha información.



2.2 Clonador del sistema

Con el tiempo se nos da el caso de que tenemos que cambiar de móvil, y nos encontramos que volver a tener configurado el nuevo dispositivo tal como estaba en anterior es una labor costosa en tiempo y que puede que no nos permita tener la información que teníamos en ciertas aplicaciones tal como estaba en el anterior dispositivo.

De un tiempo a esta parte, muchos fabricantes ya incluyen clonadores o migradores de sistema, de modo que volver a tener nuestro nuevo dispositivo tal como estaba el anterior es sumamente cómodo y fácil.

También Google ayuda en este sentido pues directamente guarda las aplicaciones que ya tenemos instaladas en nuestro dispositivo (si se han descargado de Play Store) para ser directamente instaladas en el nuevo al inicializarlo con nuestra cuenta de Gmail.

2.3 Localización del dispositivo desde una cuenta.

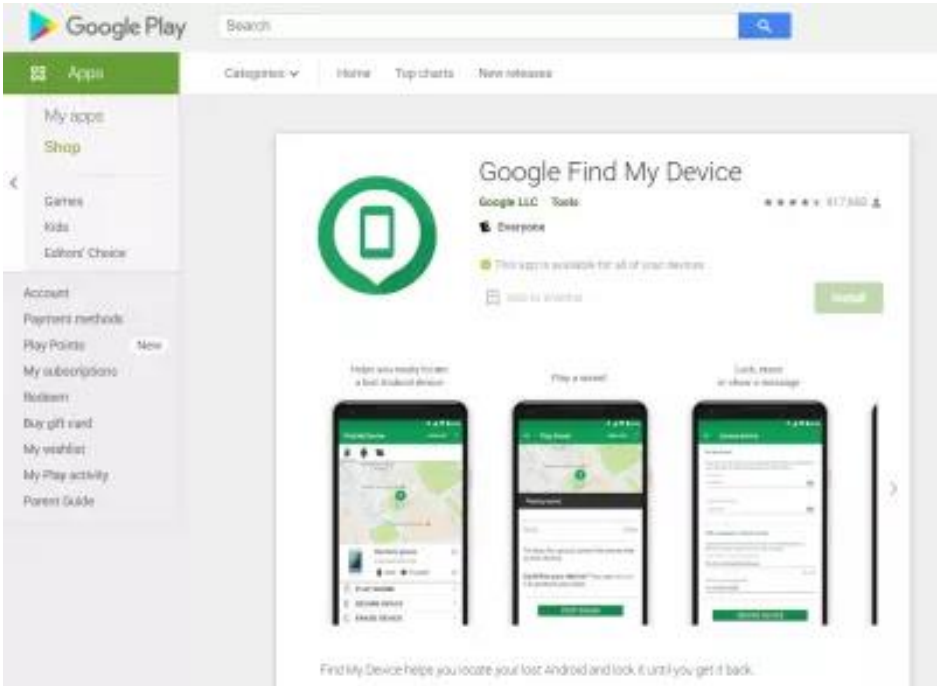
Tanto Google como el fabricante del dispositivo (si no es Google) ofrecen al usuario poder dar de alta su dispositivo para poder ser localizado en cualquier momento. Eso se hace en la configuración del dispositivo en los ajustes del sistema, tal como se indicó en la sección de ajustes.

Si por un casual estamos ante la necesidad de localizar alguno de nuestros dispositivos deberemos recordar con que usuario esta funcionando para poder localizarlo. Eso lo haremos desde una pagina web:

https://myaccount.google.com/intro/find-your-phone?hl=es

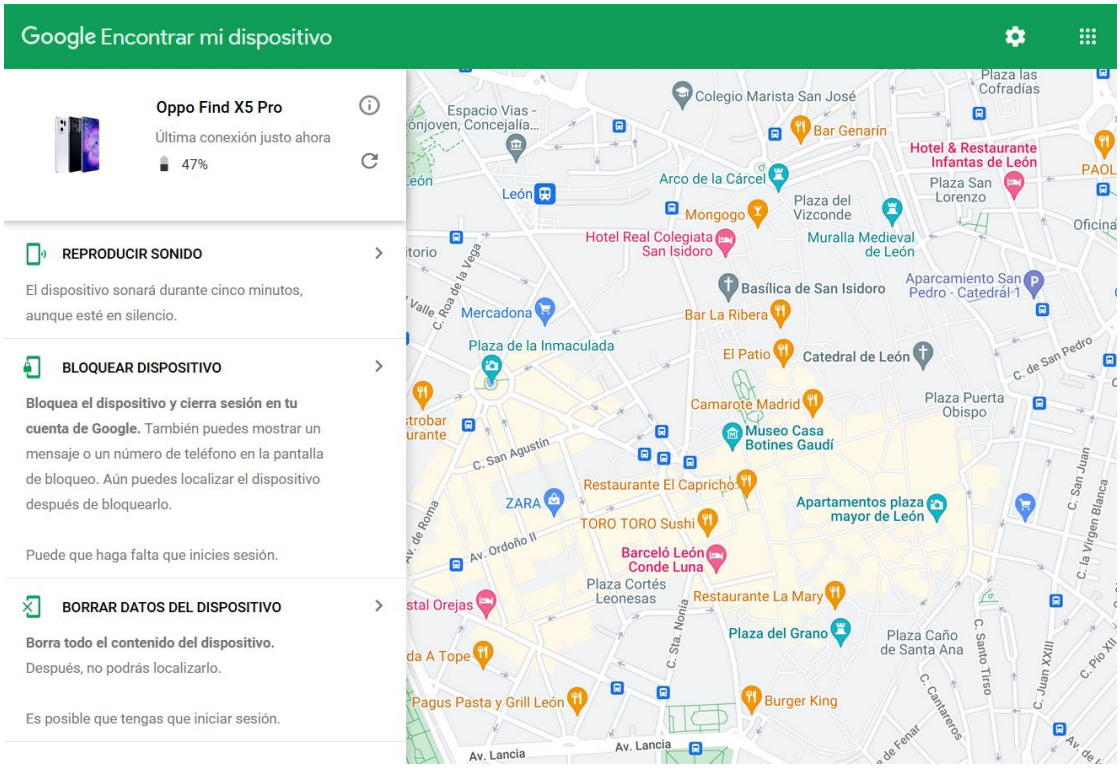
o desde la pagina que tenga el fabricante del dispositivo a nuestra disposición.

También es posible instalar una aplicación en nuestro dispositivo desde el que podemos localizar el resto de nuestros dispositivos y realizar las operaciones que necesitemos remotamente sobre ellos.



Si vamos a la web de Google veríamos una pantalla parecida a esta una vez nos registremos en ella con nuestra cuenta de Google.

Al pulsar sobre uno de ellos accedemos a la siguiente pantalla:



También podemos localizar la última posición a través de la línea temporal en Google Maps. Es decir, tendríamos que ir a localizar nuestra línea temporal y ver la última posición que nos da y ahí será donde este localizado el dispositivo.

3 Gestión de permisos en las aplicaciones

Todos conocemos que las aplicaciones necesitan o piden permisos, ya sea cuando se instalan o cuando son usadas. Es cierto que estos permisos pueden realmente ser necesarios para el correcto funcionamiento de las aplicaciones pero puede que algunas pidan permisos de mas para cosas que realmente no necesitan o que los pidan para otros fines que no nos han indicados en las funcionalidades de la aplicación.

3.1 Que son los permisos de las aplicaciones

Los permisos pueden dar a las aplicaciones el control sobre el dispositivo, llamadas telefónicas, acceso a la cámara, al micrófono, a mensajes SMS, conversaciones, fotos, localización, etc. Suelen estar relacionados con privacidad, ya que lo que no sea acceso a algo privado no a necesitar de pedir permisos y puede usar libremente es espacio que Android da a cada una de las apps independientemente.

Hay permisos que no son necesarios que el usuario los acepte manualmente, las apps los piden y estos se dan de manera automática, pero los mas sensibles si que se le solicita al usuario que los acepte. Hay algunos que incluso dan la opción de que solo se puedan usar en el momento de uso de la aplicación y no cuando no este siendo usado por el usuario, esto dependerá del tipo de permiso y la versión Android que tenga el dispositivo, pues cada versión pone mas condiciones a las apps para el uso de permisos. Es por ello que siempre es mejor tener la última versión de Android que nuestro fabricante nos provea.

3.2 Controlador de permisos

El controlador de permisos es una parte de Android que indica a cada aplicación a lo que puede o no puede acceder. En el momento de instalar una app este controlador es el que da la opción de permitir o denegar los permisos que solicita.

3.3 Permisos sensibles

Debemos tener especial cuidado cuando una aplicación nos solicita permiso de alguno de los siguientes grupos:

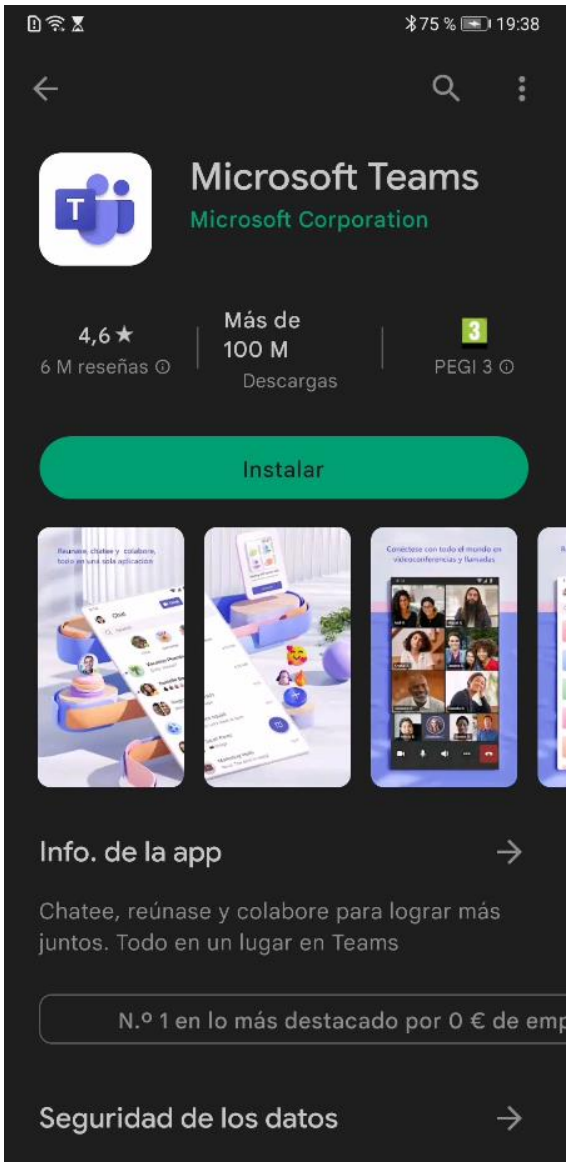
- Sensores corporales
- Calendario
- Cámara
- Contactos
- Localización
- Micrófono
- Llamadas
- Envío de mensajes

- Acceso al almacenamiento

Deberemos prestar atención a si la aplicación consideramos que realmente necesita dicho permiso o lo vemos irrelevante para su funcionamiento.

3.4 Comprobar permisos de una aplicación antes de instalarla

Si usamos Play Store (otros Stores también permiten esto mismo, pero otros no), podemos ver que permisos pide una aplicación antes de instalarla. Al seleccionar una aplicación podemos ver que incluye una sección de 'Seguridad de los datos' donde nos informa de los datos que recoge (permisos que nos va a solicitar para ello) y también que hace con esos datos.



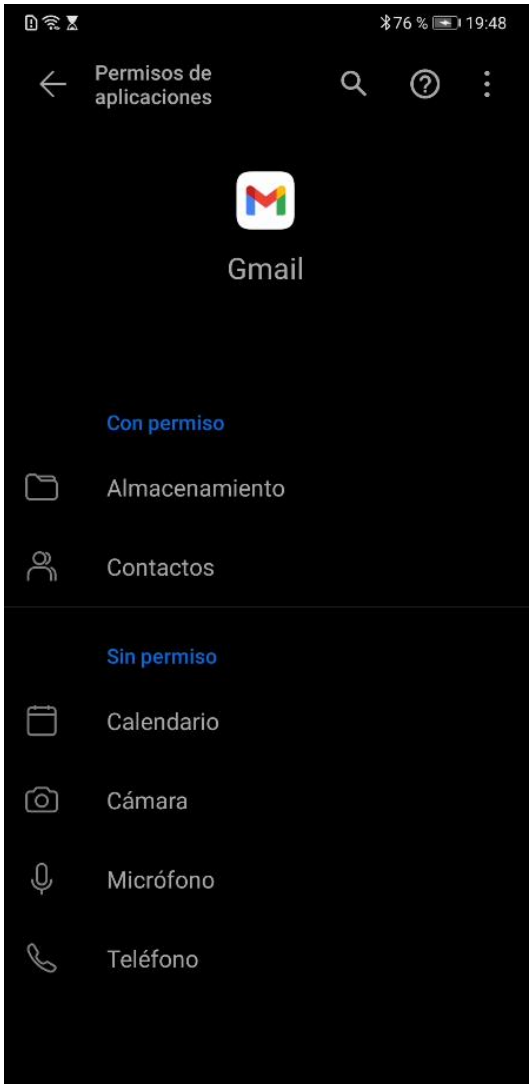
Si la app es confiable podemos estar seguros de que los va a usar bien. Si son de otro tipo puede que digan que harán algo, pero luego puede usar la información que consiga para otra cosa.

3.5 Donde ver los permisos de las aplicaciones (Controlador de permisos)

Android nos permite gestionar los permisos de cada aplicación ya sea para revocarlos como para concederlos en caso de que sea necesario. Esto lo vamos a encontrar en los ajustes de Android en la sección de Aplicaciones. En ella podemos ir a la aplicación que queramos y dentro acceder a los permisos que afectan a dicha aplicación.

Según el fabricante del dispositivo, en su capa de personalización de Android, puede añadir mas secciones en los Ajustes de Android, en los que incluso puede accederse a un permiso concreto y ver que aplicaciones lo tienen permitido, facilitando así encontrar posibles aplicaciones que no usamos y que realmente están usando permisos que no necesitan.

También hay que saber que las ultimas versiones de Android detectan, si el usuario no indica lo contrario, cuando una aplicación lleva tiempo sin usarse y pasado un tiempo revoca todos los permisos que se le habían dado, como medida de seguridad.



4 2FA

Es normal que desde nuestro dispositivo podamos acceder a servicios (Gmail, calendar, servidores privados, etc. etc.) a través de aplicaciones instaladas, así como desde nuestros ordenadores.

Normalmente para entrar a estos servicios nos piden una contraseña, de las características que sean, pero se ha visto que muchas veces esta seguridad puede ser saltada por ataques humanos, es decir, nos envían un correo y caemos en la trampa, o nos preguntan por teléfono datos de nuestra contraseña, o incluso nos la encuentran apuntada en alguna parte de algún servicio que ha sido atacado. O incluso esa contraseña la hemos usado en muchos sitios y alguno ha sido atacado y esa contraseña es usada en muchos otros sitios para probar si también entran.

Al final nos vemos desprotegidos y es por esos que se implemento una nueva forma de validar acceso a servicios: el 2FA (autenticación en dos fases).

Algunas de las ventajas de 2FA

- No se necesita utilizar un generador de tokens de hardware. Estos a menudo se pierden o extravían.
- Los generadores de códigos de acceso son mucho más eficaces que las contraseñas tradicionales. Estos generadores son más seguros porque dos códigos de acceso nunca son iguales.
- La entrada masiva de códigos de acceso impide que ciberdelincuentes ataquen datos confidenciales y obtener acceso a ellos.
- El proceso es fácil de administrar y utilizar.

Métodos usados para autenticarse:

- Tokens de hardware
- Verificación por SMS
- Notificaciones push
- Autenticación basada en voz

4.1 Uso de Autenticator y similares

En nuestro dispositivo podemos disponer de una app centralizadora de tokens que nos ayuda a gestionar todo este tipo de procesos. La principal de todas ellas es Google Autenticator, pero existen muchas más, siendo una alternativa también muy buena la app de Microsoft Autenticator.

5 Otras cosas a tener en cuenta

5.1 Pagos por NFC

En muchos teléfonos, antes únicamente en los ‘gamas altas’, pero ya en casi todas las gamas, nos aparece una especificación que para algunos es un poco extraña y para otros ya empieza a ser muy conocida. El NFC

NFC o Comunicación del campo cercano, es una tecnología de comunicación inalámbrica de corto alcance, en concreto de unos 15 cm como máximo.

En el posible uso de esta tecnología encontramos la posibilidad de sincronizar un móvil con un altavoz, validad un billete de tren o bus, uso de etiquetas o tags NFC que permiten definir acciones solo con pasar sobre ellas…. Y sobre todo… pagar como tarjeta contactless.

El chip NFC esta casi siempre en dispositivos móviles, pero últimamente también empieza a aparecer en relojes

Ya sea desde el propio móvil, como a través de relojes. Hay que poner bloqueo siempre para que no salte sin pedir desbloqueo del tipo que sea.

Desde Android 9 la autenticación biométrica está permitida para el uso de aplicaciones y es por ello que tendremos que hacer uso de la autenticación explicita (por ejemplo, poner el dedo en el lector de huellas) para poder continuar con esa aplicación (Google Pay por ejemplo)

Desde Ajustes del sistema, en la sección donde está la configuración de NFC podremos elegir cual será la aplicación de pagos que queremos que responda cuando vamos a realizar un pago por NFC, puede ser nuestra aplicación bancaria de confianza, la de Google Pay (Wallet) o la que nos ofrece el fabricante del dispositivo (Samsung Pay).

5.2 Cuanto tarda en averiguar por fuerza bruta tu contraseña

https://www.xataka.com/seguridad/sabemos-que-tarda-hacker-averiguar-tu-contrasena-fuerza-bruta-da-miedo