UNIVERSIDAD NACIONAL DE EDUCACIÓN
Enrique Guzmán y Valle
Alma Máter del Magisterio Nacional
FACULTAD DE TECNOLOGÍA
Escuela Profesional de Electrónica y Telecomunicaciones

MONOGRAFÍA

El desarrollo y la seguridad en las aplicaciones móviles

Examen de Suficiencia Profesional Res. N° 0060-2021-D-FATEC

Presentado por:

Gutierrez Torres, Joshwa Erickson Aaron

Para optar al Título Profesional de Licenciado en Educación
Especialidad: Telecomunicaciones e Informática

Lima, Perú
2021

MONOGRAFÍA

El desarrollo y la seguridad en las aplicaciones móviles

Designación de Jurado Resolución N° 0060-2021-D-FATEC

Dr. La Rosa Longobardi, Carlos Jacinto

Presidente

Mg. Chirinos Armas, Daniel Ramon

Secretario

Mg. Quiroz Aguirre, Gualverto Federico

Vocal

Línea de investigación: Tecnología y soportes educativos

Dedicatoria

A Dios, mi madre,

y mi esposa.

Índice de contenidos

Lista de figuras

Introducción

Por medio del siguiente trabajo de investigación titulado “El desarrollo y la seguridad en las aplicaciones móviles”, se pretende revisar los principales campos relacionados al desarrollo de aplicaciones móviles y lo relacionados a la seguridad móvil. Además, promover alternativas de solución que mejoren cada día los dispositivos que tenemos cerca es una misión muy importante. En tiempos en que la tecnología nos sorprende con vertiginosos avances, y el futuro que vimos solo en las películas se hace posible en la palma de nuestra mano, es necesario explicarnos el por qué, el cómo y cuáles con las responsabilidades que trae consigo el adaptarnos a un mundo exponencialmente cambiante.

El desarrollar una aplicación ya no puede ser habilidades de algunos, sino la principal fuente de conocimiento para, día a día, mejorar y cambiar el mundo tecnológico que nos rodea.

Hace no mucho leí que, en los años cincuenta, se utilizó una supercomputadora para enviar hombres a la Luna. Hoy, esas mismas computadoras se utilizan para lanzar cerdos verdes. Palabras como adaptación e innovación deben estar plasmadas en cada idea para impulsar un cambio que genere el avance y exprima el potencial de todos los desarrolladores. Finalmente, presento la aplicación didáctica, síntesis, apreciación crítica y sugerencias, referencias y apéndices.

Capítulo I

Desarrollo de aplicaciones móviles

1.1 Dispositivos móviles

Para considerar como un dispositivo móvil, es necesario tener en cuenta que debe poseer movilidad, capacidad de comunicación inalámbrica e interacción con las personas y tamaño reducido.

A lo largo de los años, la evolución de los distintos dispositivos móviles partiendo desde los inicios de la Segunda Guerra Mundial, en donde la comunicación a través de largas distancias jugó un rol imprescindible. Los teléfonos inteligentes con más y mejores características generaron la aparición y evolución de sistemas operativos y aplicaciones para dispositivos móviles con funciones especializadas para distintas tareas que el usuario desee realizar, entre ellas: productividad, juegos, redes sociales, etc.

Tiempo atrás, solo se consideraba importante la marca del dispositivo, ahora se tiene en cuenta las características de este entre las que resaltan está el procesador, cámara, memoria interna, etc.

De tal forma, se divide a los dispositivos en gama baja, media y alta. Tomando en cuenta también, la capa de personalización que el dueño de la marca imprime internamente. Como principales representantes de marcas relacionadas a dispositivos móviles se tiene Samsung, Apple, Xiaomi y Huawei.

1.2 Sistemas operativos móviles

Los sistemas operativos de móviles tienen la misma función que la de una computadora, sirviendo para controlar los procesos básicos y permitiendo el funcionamiento de las aplicaciones que se instalarán posteriormente. Si bien existieron muchas versiones de sistema operativo entre los que se encuentran Android, IOS, Symbian, Windows Phone, Blackberry OS, Firefox OS, no todas se mantuvieron a lo largo de los años por la exigencia de los usuarios.

En un mercado tan competitivo y cambiante en función de los usos y requerimientos de los usuarios se quedaron como principales representantes Android e IOS. Ahora ya no solo se considera si un dispositivo tiene características especiales, sino la marca que respalda al sistema operativo.

Esto influirá en el sistema operativo del dispositivo y las actualizaciones que reciba a lo largo de su vida útil, pudiendo ser que el dispositivo caiga en la obsolescencia programada y limitando su vida útil a unos cuantos años.

1.2.1 Android.

El sistema operativo Android está basado en Linux, sin embargo, no es lo mismo, ya que no cuenta con la gestión de ventanas nativa, no incorpora soporte para glibc, tampoco permite la mayoría de las aplicaciones de Linux. “Es un sistema orientado a dispositivos móviles, como teléfono inteligente y tablets. Android tiene una gran comunidad de desarrolladores para extender la funcionalidad de los dispositivos” (Martínez, 2011, p.16) En sus inicios fue creado para cámaras digitales profesionales. Posteriormente adquirido por Google e impulsado para ser usado en dispositivos como teléfonos inteligentes, relojes, televisores, etc.

Android tiene dos principales características: Es de plataforma libre y código abierto, lo que permite a los fabricantes de dispositivos utilizarlo sin pagar licencia, esto beneficia al usuario ya que los costos no son tan altos, como si fuera poco permite a desarrolladores realizar modificaciones y/o actualizaciones.

A la fecha, se tiene un registro de más de 700 000 aplicaciones. La última versión publicada del sistema operativo es Android 11.

Figura 1. Logo Android. Fuente: Recuperado de Xatakandroid.com

1.2.2 IOS.

Es el sistema operativo de los dispositivos Apple. “Es un derivado de MAC OS X, a su vez está basado den Darwin BSD.” (Martínez, 2011, p.18).

En sus inicios el sistema operativo IOS se creó solo para el teléfono sin embargo ha sido utilizado en otros dispositivos iPod y tabletas iPad.

A diferencia de Android, que permite el uso en diversos dispositivos de las distintas marcas, así como de las gamas baja media y alta, incluso equipos antiguos, IOS no permite el uso fuera de dispositivos de la marca Apple.

Con el objetivo de sumar funciones a sus dispositivos IOS, permite instalar aplicaciones desde su tienda en línea. El punto más fuerte que tiene IOS es su nivel de seguridad frente al ataque de virus o malware. En su tienda tienen que pasar por un proceso más estricto de validación, lo que genera en un desarrollador muchos

impedimentos para publicar aplicaciones y/o actualizaciones. La versión actual de IOS es 14.4.

Figura 2. Logo IOS. Fuente: Recuperado de Wikipedia.org

1.3 Aplicaciones móviles

Haciendo un símil con una computadora las aplicaciones móviles vendrían a ser los programas que darán una u otra función adicional al dispositivo, con lo que además de las funciones básicas se tiene la posibilidad de instalar aplicaciones de productividad, juegos, redes sociales, almacenamiento basado en la nube, etc.

Las primeras aplicaciones para móviles surgieron a fines de los años 90.

Podíamos verlas en dispositivos con sistemas operativos como Nokia o Blackberry. Aunque en la actualidad se considera como parte imprescindible de un sistema operativo móvil, la agenda, contactos y el ringtone; estas fueron las bases de las aplicaciones.

Para realizar la instalación se tiene que recurrir a la tienda de aplicaciones.

Figura 3. Google Play. Fuente: Recuperado de Cyclonis.com

Figura 4. App Store. Fuente: Recuperado de zdnet.com

La evolución también llegó para los desarrolladores que contaban con mejores herramientas en el desarrollo de las aplicaciones. Para los fines de esta investigación, a partir de ahora solo se hará uso de Android.

1.4 Tipos de aplicaciones móviles

Existen diversas formas de diseñar una aplicación, cada una ofrece distintas características y limitaciones, sobre todo desde el punto de vista técnico. Pese a no parecer tener mucha importancia para el diseñador el tipo de aplicación que se piense diseñar condicionará la parte visual, así como la interacción.

1.4.1 Native App.

Desarrollada en Java, pueden acceder a varias de las diferentes características de los dispositivos. “Son aquellas que han sido desarrolladas con el software que ofrece cada sistema operativo a los programadores, llamado genéricamente Software Development Kit o SDK” (Cuello y Vittone, 2013, p.21). Las ventajas que se esconden en crear aplicaciones nativas están en:

- La cantidad de tiempo que se va a invertir para su desarrollo.
- Son actualizadas frecuentemente lo que permite mejoras o correcciones.
- Permite la posibilidad del uso de las notificaciones del sistema operativo para mostrar avisos al usuario, aun cuando no está haciendo uso de la aplicación.

- No necesitan de internet para su funcionamiento.
- La integración con el dispositivo es completa, esto permite que se pueda hacer uso completo de todas las características del equipo.

1.4.2 Web app.

Una Web App se basa en HTML, JavaScript, y/o CSS ya que se carga en el servidor web y se visualizan con el navegador. No requieren instalación, adicionalmente es posible crear un acceso directo desde la pantalla de inicio.

La variedad de Web Apps es muy amplia ya que engloban desde pequeñas herramientas, software de gráficos, adaptaciones de programas hasta juegos. Un problema con las Web Apps es que no se adaptan correctamente al hardware del dispositivo, sin embargo, funcionan en todos los sistemas operativos y terminales desde los que se acceda con un navegador web. Respecto a los fallos de seguridad se puede solucionar directamente en el software, lo que permite a todos los usuarios acceder de manera más segura.

1.4.3 Aplicaciones híbridas.

Son una mezcla de Native App y Web App. A diferencia de una Web app, las aplicaciones híbridas permiten al usuario acceder usando librerías, como lo haría una Native App.

1.5 Desarrollo de aplicaciones móviles

El proceso de desarrollo para la creación de aplicaciones móviles puede abarcar diversas actividades, desde la idea en sí, hasta la corrección de los errores y/o actualizaciones necesarias para mejorar la aplicación para los distintos dispositivos móviles. “El proceso

de diseño abarca diferentes etapas donde diseñador y desarrollador trabajan simultáneamente" (Cuello y Vittone, 2013, p.18).

El trabajo suele estar realizado en constante coordinación entre diseñadores y programadores, teniendo una labor simultánea. Los procesos pueden ser muchos, sin embargo, en el siguiente gráfico se pueden resumir:

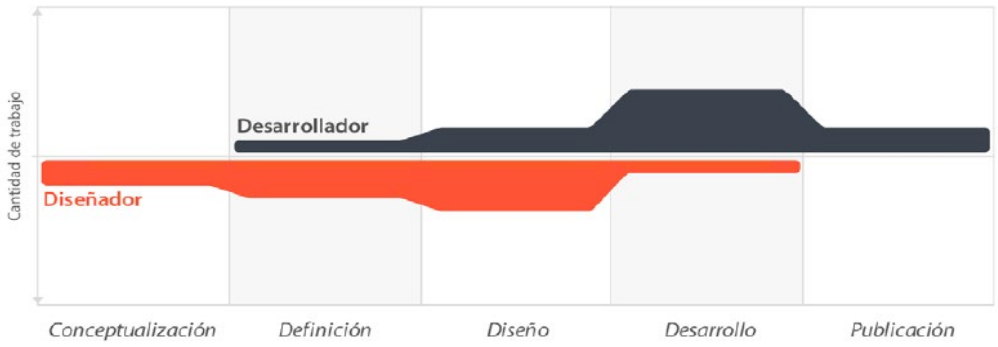


Figura 5. El proceso de diseño de aplicaciones. Fuente: Cuello y Vittone, 2013.

1.5.1 Conceptualización.

Aquí es donde se forma la idea de la aplicación teniendo en cuenta la necesidad que el usuario pueda tener. Se puede dar partiendo de la resolución de un problema u ofrecer un beneficio adicional al usuario.

1.5.2 Definición.

Hace referencia a los usuarios a los que estará diseñada la aplicación. Se debe tomar en cuenta la funcionalidad.

1.5.3 Diseño.

En cuanto se refiere al diseño, la idea es tangibilizar conceptos y definiciones anteriores que permitan la creación de prototipos para ser probados.

1.5.4 Desarrollo.

Es aquí donde el programador genera los diseños y estructura el esqueleto sobre el cual funcionará la aplicación. Posteriormente a la realización del primer prototipo es necesario la corrección de posibles errores y prepararse para publicación y aprobación en las tiendas de aplicaciones.

1.5.5 Publicación.

En este punto es cuando la aplicación finalmente es puesta a disposición de los usuarios. Sin embargo, no finaliza aquí, ya que, por medio de las analíticas, estadísticas y comentarios de los usuarios es que el desarrollador tendrá en cuenta el correcto funcionamiento o no de la aplicación.

1.6 Monetización

"Una aplicación no deja de ser un software, (…), con la llegada del iPhone al mercado se generaron grandes modelos de negocios que hicieron de las aplicaciones algo rentable" (Cuello y Vittone, 2013, p.14.).

La monetización ofrece la posibilidad de obtener dinero por medio de las aplicaciones ya que esto va a depender si la aplicación es gratis, de paga o fremium:

1.6.1 Aplicaciones gratuitas.

El mayor beneficio que se obtiene con una aplicación gratuita es la cantidad de usuarios potenciales a los que es posible dirigirse. "Hay muchos tipos de aplicaciones gratuitas, la mayoría pretende atraer usuarios para que acaben comprando la versión de pago de la aplicación o productos relacionados a ellas" (Ramírez, s.f, p.58).

Basado en la premisa de que “el usuario no tiene nada que perder”, es posible que cualquiera pueda descargar una aplicación gratuita, sin embargo, un punto que a su vez juega en contra es que nadie esperará que una aplicación gratuita sea realmente genial. Para algunos desarrolladores, les ha servido para ir creándose una idea de que es lo que realmente desean sus usuarios. En muchos casos integran publicidad constante, lo que se puede evitar accediendo a la versión de pago. Un ejemplo de aplicación gratuita es TuneIn, la versión gratuita permite la posibilidad de oír diferentes estaciones de radio, sin embargo, la publicidad se encuentra presente, lo que precisamente no resulta molesto ya que con esperar unos cuantos segundos se activa la reproducción y al funcionar como Native App no es necesario tenerla abierta siempre, sino que seguirá reproduciendo en segundo plano.

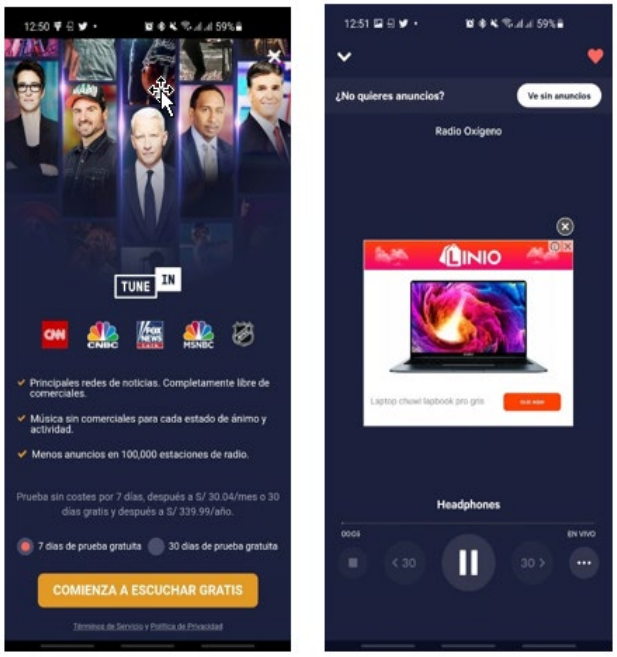


Figura 6. Aplicación TuneIn. Fuente: Autoría propia.

1.6.2 Aplicaciones de pago.

El caso de las aplicaciones de pago es un poco más complicado ya que se requiere de una gran cantidad de descargas para ser rentables. Normalmente un usuario no se arriesga a hacer la compra de una aplicación si es que no la conoce lo que genera una barrera al uso

de la aplicación. Como en la realidad, el usuario es finalmente quien decide si le conviene pagar por una aplicación o usar una alternativa gratuita.

"Que un usuario esté dispuesto a pagar depende de muchas cosas. (…). Si dos aplicaciones son similares (..), pero una de ellas y la otra no, obviamente es más probable que se descargue la aplicación gratuita." (Cuello y Vittone, 2013, p.35).

1.6.3 Aplicaciones fremium.

Es la mezcla de los dos casos anteriores. Lo que permite al usuario utilizar la aplicación de manera gratuita, partiendo un uso básico, y acceder a la posibilidad de recibir funciones avanzadas previo pago.

En muchos casos adquirir la versión de pago facilita la posibilidad de utilizar el 100% de las bondades de la aplicación, como es el caso de Macrodroid, en su versión gratuita permite la posibilidad de usar solo unos cuantos macros, en su versión completa posibilita al usuario el uso completo de la aplicación.

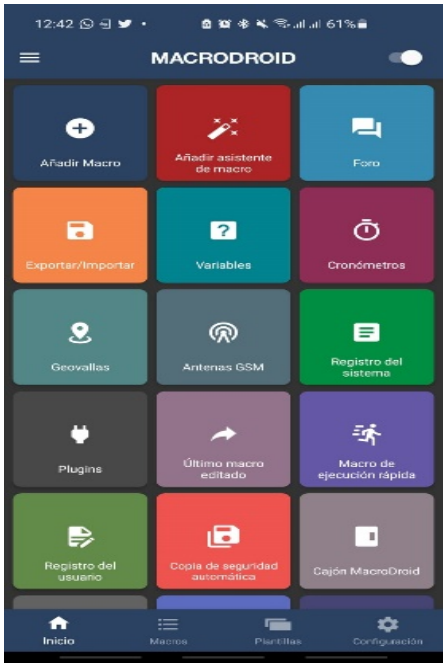


Figura 7. Aplicación Macrodroid. Fuente: Autoría propia.

1.7 Arquitectura de la información

Es la forma de organizar el contenido y las funciones que realice la aplicación.

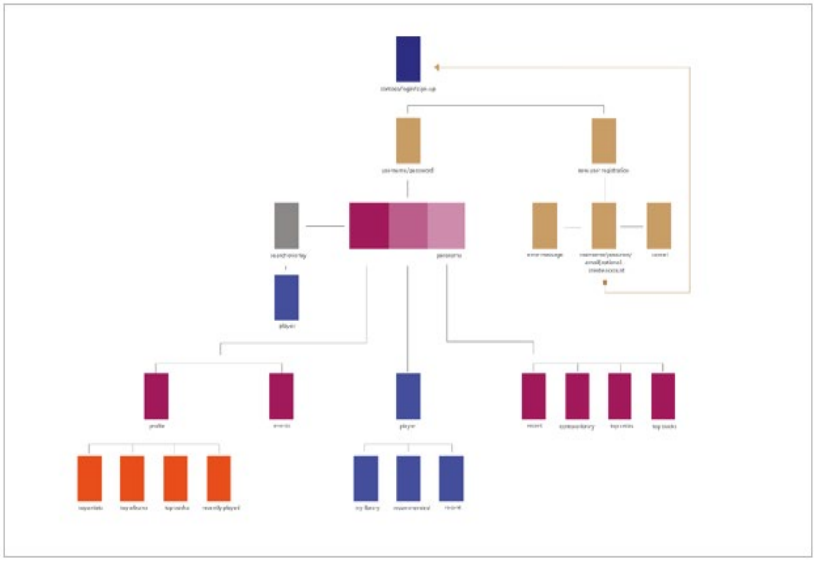


Figura 8. Diagrama de arquitectura de información. Fuente: Autoría propia.

En el gráfico anterior, se observa la forma de organizar la navegación entre una pantalla y otra a través de qué acción se tenga en cuenta seleccionar. El diagrama deja fuera aspectos de diseño ya que se centra visualizar y entender la relación entre contenidos.

1.8 Arquitectura de Android

En Android las actualizaciones suelen suceder muy rápido, en algunos casos semanalmente, permitiendo el uso de nuevas herramientas y bibliotecas.

Por lo general todas las aplicaciones de Android están compuestas de una estructura general en la que intervienen archivos de recursos y vistas, librerías de código, código fuente y Android Manifiest.

A continuación, se muestra un gráfico donde se puede observar por capas la arquitectura de Android. Cada capa usa servicios que brinda las anteriores, posteriormente ofrece sus servicios a capas superiores.

Figura 9. Capas de arquitectura Android. Fuente: Recupera de https//www.Linux

En este nivel se encuentran las aplicaciones por defectos de Android (cámara, agenda, contactos, etc.) además de las que el usuario va instalando posteriormente desde la tienda de aplicaciones o como desarrollo propio. Las aplicaciones de este nivel utilizan los servicios, las API y las librerías de los niveles anteriores. “El núcleo actúa como una capa de abstracción entre el hardware y el resto de las capas de la arquitectura.” (Ladino, s.f., p. 2).

1.8.1 Framework de aplicaciones.

Básicamente son las herramientas de desarrollo de cualquier aplicación. Una API es el conjunto de protocolos para desarrollar e integrar el software de las aplicaciones. Las

API permiten que los productos y servicios se intercomuniquen entre sí. Toda aplicación utiliza el mismo grupo de API y el mismo framework.

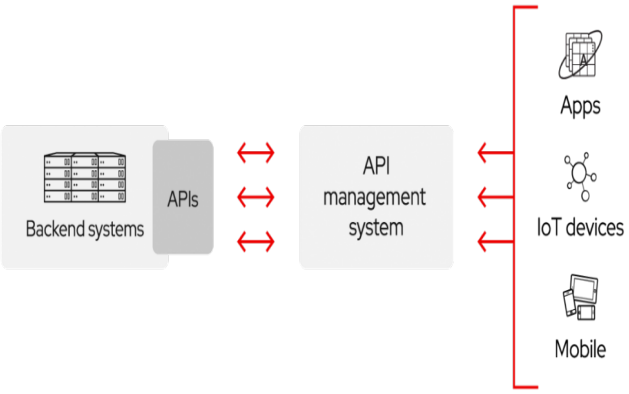


Figura 10. API management system. Fuente: Redhat, 2021.

De entre las API más importantes se pueden indicar:

- Activity Manager: API encargada de gestionar las aplicaciones en Android.
- Window Manager: API encargada de gestionar las ventanas de las aplicaciones, hace uso de la librería Surface Manager.
- Telephone Manager: abarca todas las funcionalidades relacionadas a llamadas, mensajes, etc.
- Content provider: permite a cualquier aplicación compartir sus datos con otras aplicaciones.
- View System: facilita elementos para construir interfaces de usuario (GUI), entre ellas: listas, mosaicos, botones, tamaño de ventanas.
- Location Manager: permite a las aplicaciones conseguir la localización.
- Notification Manager: mediante la que las aplicaciones envían al usuario notificaciones: Llamadas, mensajería, conexión Wifi, etc.

1.8.2 Librerías.

Esta capa contiene las librerías usadas por Android. Éstas han sido escritas con C/C++ y facilitan a Android las principales características. "Tenemos un conjunto de librerías de C y C++ utilizadas por el sistema para varios fines como el manejo de pantalla (Surface manager), mapas de bits, etc" (Catalán, s.f., p.7). Adicional al núcleo basado en Linux, constituyen el centro de Android. Las principales librerías son:

- Librería libc: contiene todas las cabeceras y funciones según el estándar del lenguaje C.
- Librería Surface Manager: encargada de componer los elementos de navegación de la pantalla. Gestiona, además, las ventanas pertenecientes a las aplicaciones activas en cualquier momento.
- OpenGL/SL y SGL: permite el uso de gráficos en 3D y 2D.
- Librería Media Libraries: facilita los códecs necesarios para el contenido multimedia disponible en Android.
- FreeType: permite visualizar y trabajar con distintos tipos de fuentes.
- Librería SQLite: permite la creación y gestión de bases de datos relacionales.
- Núcleo Linux: Android hace uso del núcleo de Linux. Esta capa contiene los principales drivers para que cualquier componente pueda ser utilizado mediante las vinculaciones correspondientes. Cuando un fabricante desea incorporar un hardware es necesario que cree librerías de control dentro del kernel de Linux.

1.9 Wireframe

Es la representación simplificada de una pantalla individual, permite tener una idea de la organización. Básicamente vendría a ser el plano arquitectónico de una casa. Lo más

común es que un diseñador se salte esta etapa, sin embargo, puede traer algunas consecuencias. Usarlos es lo más recomendable porque:

Permite al diseñador evaluar alternativas de interacción y navegación de forma rápida, sin invertir tiempo en el acabado que puede que no funcione como debe al final.

Facilita comunicar ideas, ya que permite hacer un primer vistazo a la aplicación.

1.10 La máquina cirtual Dalvik y ART

Dalvik es una máquina virtual utilizada para la ejecución de aplicaciones y códigos escritos en Java. Básicamente posibilidad que las aplicaciones funcionen en el sistema operativo Android.

En el año 2013 Android lanza su versión KitKat e introduce un sustituto para Dalvik, con el nombre de ART: Android RunTime. La existencia de mejores dispositivos ha posibilitado el desarrollo de ART.

1.11 Lenguaje de programación de las aplicaciones en Android

Las aplicaciones que se instalan en el sistema operativo Android se desarrollan con el lenguaje Java y el Software Development Kit (Android SDK). Adicionalmente se puede hacer uso de otros lenguajes de programación, aplicaciones y extensiones de C y C++. Actualmente se viene trabajando en una actualización del lenguaje de programación llamada Kotlin.

Kotlin, ayuda a prevenir errores comunes durante la programación en Android, pero no es limitante, sino que permite interoperar con Java.

1.12 Interfaz gráfica

Considerada como todo aquello que el usuario puede visualizar y con lo que puede interactuar. Android ofrece diversos componentes de IU compilados que permiten compilar la interfaz gráfica, además también contienen otros como notificaciones y menús.

Capítulo II

Seguridad en las aplicaciones móviles

2.1 La seguridad en las aplicaciones móviles

Al hablar de seguridad en informática, se considera la posibilidad de eventos mediante los que se pueden explotar vulnerabilidades, con el objetivo de saltar la seguridad del sistema ya sea de manera intencional o accidental, pudiendo afectar la integridad del sistema.

Son muchos los datos confidenciales almacenados, desde fotografías o videos personales hasta datos bancarios los que se encuentran almacenados en los dispositivos móviles. En la mayoría de los casos se parte de rootear el dispositivo.

La configuración de seguridad implementada en Android se lleva a lo largo de toda la arquitectura del sistema. Entre los aspectos más importantes destacan:

2.1.1 Application Sandbox.

Android, tiene implementado el principio de mínimo privilegio, lo que facilita solo el uso de determinados permisos para una aplicación, es decir, que no podrá hacer usos de micrófono o cámara si es que el usuario no ha concedido estos permisos. El mecanismo de Application Sandbox asigna un usuario UID para cada aplicación.

2.1.2 Application Singning.

Todas las aplicaciones tienen una firma digital lo que posibilita que sus claves privadas solo sean conocidas por sus desarrolladores. Estos certificados son usados por Android para identificar cuando dos aplicaciones han sido diseñadas por el mismo desarrollador. “Además, se deben incluir certificados que identifiquen el origen de sus claves públicas” (Ladino, s.f., p.2)

2.1.3 Permisos.

Las aplicaciones necesitan que se les otorgue permisos para funcionar correctamente, dependerá del usuario conceder los permisos para cada aplicación durante el proceso de instalación. Incluso cuando una aplicación ya está instalada es posible dar y quitar permisos.

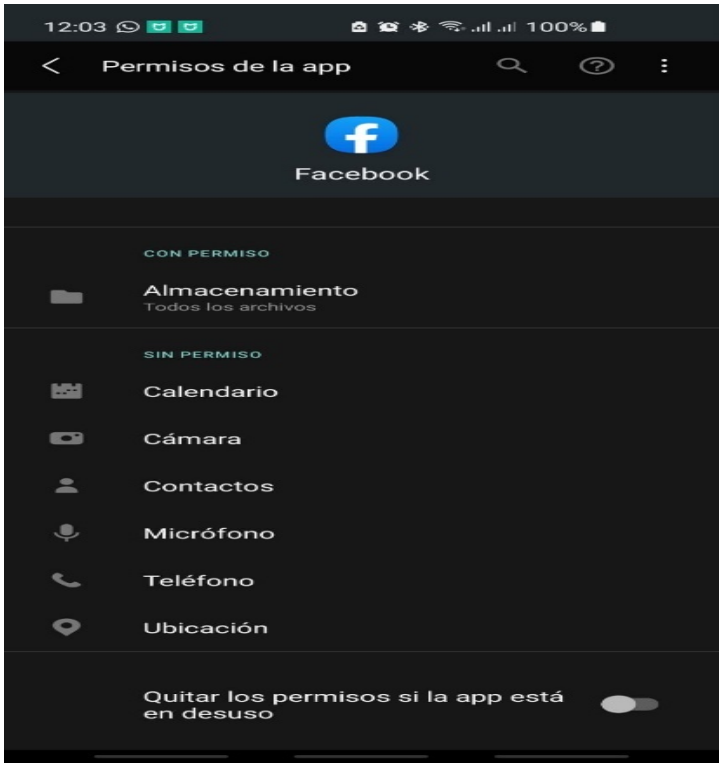


Figura 11. Permisos de aplicación Facebook. Fuente: Autoría propia.

Es importante tener en cuenta que algunos permisos son otorgados por el sistema sin necesidad de consultar al usuario. Razón, por la que es importante no realizar la instalación de aplicaciones fuera de la tienda de aplicaciones oficial.

Las solicitudes de permisos son evaluadas durante el proceso de lanzamiento, luego de agregar las aplicaciones a la tienda de aplicaciones. Si una aplicación solicita el uso de permisos de alto riesgo es necesario que se complete el Formulario de Declaración de Permisos. Si el formulario no es completado, no se permitirá el lanzamiento hasta que se ocupe de la alerta correspondiente. Para completar el Formulario Declaración de Permisos es necesario:

- Evaluar los permisos solicitados, los permisos pueden tener una marca de verificación de las versiones anteriores, sin embargo, es necesario evaluarlos en cada actualización que se publica.
- Específica la funcionalidad de la aplicación, en el listado de casos prácticos.
- Proporciona instrucciones para la revisión de la aplicación. Previo a la publicación el equipo detrás de Google Play revisará la funcionalidad de la aplicación, es necesario que se indique los permisos necesarios para un caso práctico.
- Proporciona un video de un caso práctico. Donde se explica el funcionamiento.
- Facilita instrucciones para acceder al contenido restringido. El equipo detrás de Google Play debe tener acceso a todo el contenido restringido para realizar la verificación de la información utilizada.
- Finalmente, confirma el Formato de Declaración de Permisos.

2.2 Vulnerabilidades en Android

Si bien los beneficios de Android son muchos y muy variados también existen puntos en contra. Al ser un sistema operativo abierto, cualquier usuario puede realizar

modificaciones de las aplicaciones y poner en peligros a otros usuarios. Es necesario que, ante constantes operaciones en la web, descargas, compras, visitas a determinadas páginas se minimicen los riesgos seguridad.

Si bien la mayoría de las aplicaciones se encuentran disponibles en la tienda Google Play, hay desarrolladores que generan aplicaciones de manera independiente y al distribuirlas por sus propios medios se saltan restricciones de seguridad.

Los objetos maliciosos que en su mayoría afectan al sistema operativo Android son:

- Troyanos de SMS
- Exploits para ganar acceso al sistema raíz del teléfono
- Módulos de publicidad

2.3 Tipos de ataque

Existen diversos tipos de ataque que se pueden realizar desde una aplicación o tan solo con ingresar a una determinada página web y presionar en cualquier anuncio contenida en esta.

2.3.1 Ataques al software: Malware.

Es un código que tiene se instala y ejecuta en el dispositivo sin aprobación del usuario. El funcionamiento de este puede ser automático o controlado por otro usuario. Entre los principales se tiene:

- Virus: programa que se encarga de afecta archivos del sistema para modificarlos o dejarlos inservibles. Entre los principales objetivos pueden estar robo de contraseñas o denegar servicios propios del dispositivo.
- Troyano: se oculta dentro de otra aplicación, para pasar inadvertido por el usuario, al instalarse en el sistema cuando se ejecute la aplicación.

- Spyware: aplicación que recaba información del usuario sin su consentimiento con el objetivo de posteriormente vender esta información a empresa de publicidad.
- Keylogger: aplicación encargada de registrar todas las pulsaciones del teclado. Su principal objetivo apunta a las contraseñas o cuentas bancarias.
- Dialer: código que de manera oculta realiza llamadas con tarifas especiales.

Figura 12. Malware en Android. Fuente: Recuperado de latam.Kasperky.com.

Como principal recomendación para evitar el malware es necesario tener en cuenta:

- Instalar aplicaciones solo desde la tienda oficial de aplicaciones.
- Instalar aplicaciones de desarrolladores de confianza.
- Antes de realizar la instalación verificar las opiniones y calificaciones de otros usuarios que instalaron la aplicación.

Tomar en cuenta los permisos que las aplicaciones solicitan al realizar la instalación. De ser posible, utilizar alguna solución se seguridad de confianza.

2.3.2 Ataques en la web.

Es aquí donde se tienen en cuenta las vulnerabilidades de los navegadores web y posibles mecanismos de seguridad implementados. Existen diversos ataques por medio de la web, pero en este punto solo se revisarán los más resaltantes:

- Phishing: Ataque que cosiste en suplantar una web y hacer creer al usuario que se encuentra visitando una web conocida para robar su información confidencial.
- Clickjacking: Ataque basado en que el usuario interactúa con elementos que normalmente no accedería. Esto podría darse mediante una web superpuesta y que el usuario al acceder a un contenido sea descarga u otro presione sin intención.

Figura 13. Las reparaciones de dispositivos móviles por virus crecen un 20%.
Fuente: Recuperado DealerWorld.

2.4 Rooteo

La posibilidad de rooteo se encuentra disponible en cualquier dispositivo, sin embargo es necesario tener en cuenta que al rootear se le otorgan privilegios de superusuario, desde la instalación de una ROM personalizada a aplicaciones modificadas mejorarán la experiencia del usuario, pero no quiere decir que necesariamente traigan seguridad ya que detrás del desarrollo y/o mejora puede que se encuentre malware listo para activarse en

cuanto el usuario realice la instalación de una ROM personalizada. Con el paso de los años los desarrolladores han ido incorporando las funciones que antes solo se obtenían al realizar el rooteo, por lo que la opción de rooteo ha sido descartada con el tiempo.

2.4.1 Ventajas de rootear el dispositivo móvil.

Dentro de las ventajas al rootear el dispositivo están:

Las actualizaciones, si bien se tenía que esperar a que el fabricante libere la actualización para gozar de las mejoras, el rootear permite la posibilidad de probar las mejoras antes de tiempo con ROMs provenientes de Paranoid Android o LineageOS.

Exprimir las ventajas del dispositivo móvil, es una gran ventaja ya que mediante las configuraciones se dará la posibilidad de exigir mucho más al procesador, obtener fotografías de mejor calidad o extender la vida de la batería.

Activar funciones adicionales, las cuales no se encuentran visibles para cualquier usuario, pero sí que permiten gozar aún más de las bondades del dispositivo móvil.

2.4.2 Desventajas de rootear el dispositivo móvil.

Dentro de las desventajas al rootear el dispositivo están:

Rootear no siempre es tan sencillo, muchas veces, si es que no se tienen algunas bases de cómo es que se realiza un formateo, puede que obstaculice el proceso de rooteo. Si el dispositivo móvil no es muy conocido, el soporte se verá limitado ya que no habrá muchos desarrolladores ni usuarios que puedan brindarte soluciones ante un posible brickeo.

Riesgo de brickeo, esto no siempre ocurre, pero en el caso de ser así, el dispositivo móvil queda inutilizado permanentemente y la única utilidad que recibe el dispositivo móvil es de un bonito y caro pisapapeles.

Al rootear el dispositivo el fabricante puede desentenderse e invalidar la garantía ya que se está modificando el sistema operativo previamente instalado.

Las futuras actualizaciones, si es que las hay, tendrán que realizarse manualmente.

2.5 Mecanismos de prevención

Con la finalidad de estar protegidos es necesario tener en cuenta diversos cuidados entre los cuales están cuidados tan básicos como instalar las aplicaciones desde la tienda de aplicaciones o evitar acceder a sitios que pondrían en riesgo la información personal del usuario.

2.5.1 Tienda de aplicaciones.

En las tiendas de aplicaciones se encuentran publicadas de forma segura las aplicaciones, sin embargo, no quiere decir que todas las aplicaciones que se encuentren acá sean seguras en su totalidad ya que puede que alguna se salte alguna de las barreras de seguridad. Esto a su vez, origina también la demora en la publicación de las aplicaciones, por lo que al ser tanta la cantidad de aplicaciones es necesario que todas pasen por una revisión antes de ser publicada, incluso en sus actualizaciones. Pese a las restricciones y/o recomendaciones para evitar infectar dispositivos con la instalación de aplicaciones no verificadas, los usuarios siguen accediendo a tiendas alternativas donde encuentran las aplicaciones que aún no son publicadas en las tiendas oficiales o aplicaciones modificadas para obtener los beneficios de una aplicación de pago. Entre ellas podemos mencionar:

Figura 14. Mercados de aplicaciones alternativas Android. Fuente: Techtastico, 2020.

2.6 Instalación de aplicaciones fuera de la tienda oficial

Realizar la instalación de aplicaciones fuera de la tienda oficial si es posible, sin embargo, se corre muchos riesgos, los cuales ya fueron mencionados anteriormente. Para realizar la instalación de aplicaciones no oficiales es necesario acceder a las configuraciones de sistema / datos biométricos y seguridad / instalar aplicaciones desconocidas.

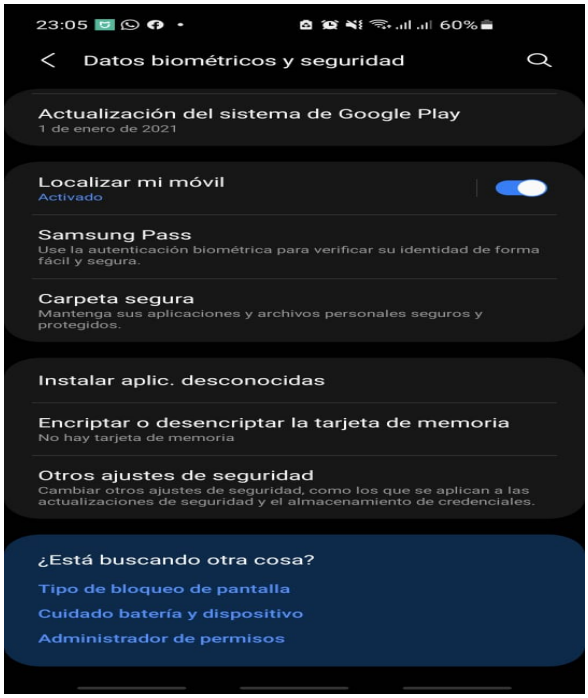


Figura 15. Configuración para instalación de aplicaciones externa a Google Play. Fuente: Autoría propia.

2.7 Recomendaciones se seguridad

Existen muchas recomendaciones al tener un dispositivo móvil, pero las principales son:

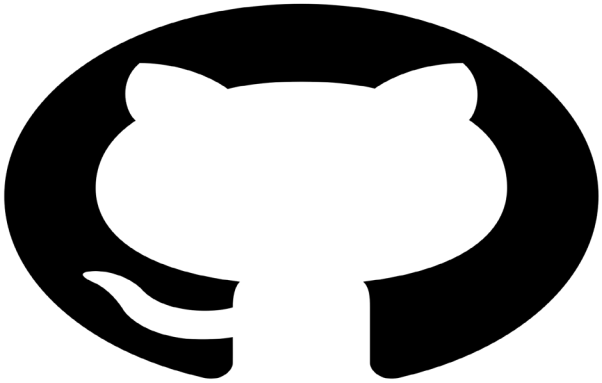
- Actualizar el dispositivo móvil frecuentemente.
- Actualizar las aplicaciones.
- No utilizar patrón de desbloqueo.
- Realizar copias de seguridad.
- Instalar aplicaciones solo desde la tienda de aplicaciones oficial.
- Tener el número IMEI siempre anotado en un lugar seguro.
- No rootear el dispositivo.
- Utilizar antivirus.
- Utilizar software de rastreo o monitoreo.

Aplicación didáctica

Con el objetivo de realizar la aplicación didáctica, se hará uso de los siguientes servicios, programas y aplicaciones:

GitHub

Servicio web para almacenar y administrar código.



GitHub Logo. Fuente: Recuperado de Pngimg.com

APK Icon editor

Editor de íconos para aplicaciones.

Apk Icon Editor. Fuente: Autoría propia.

Brackets

Editor de código gratuito disponible para desarrolladores.

Brackets (Text editor). Fuente: Recuperado de Wikipedia.

Nox Player

Simulador de Android. Basado en Android 5.1.1

Nox Player. Fuente: Recuperado de Uptodown.

Good Barber

Herramienta para la creación de aplicaciones.

GoodBarber. Fuente: GoodBarber

Dell Mobile Connect

Aplicación que permite la visualización de la pantalla del dispositivo móvil en la computadora.

Dell Mobile Connect. Fuente: Recuperado de Dell.

Sesión de aprendizaje

FACULTAD DE TECNOLOGÍA

Departamento Académico de Electrónica y Telecomunicaciones

Título de la sesión: creamos nuestra primera aplicación móvil

I. DATOS GENERALES

1.1. Facultad : Tecnología

1.2. Especialidad : Telecomunicaciones e Informática

1.3. Curso : Telecomunicaciones I

1.4. Promoción : 2021

1.5. Ciclo : 2021-0

1.6. Bachiller : Joshwa Erickson Aaron Gutierrez Torres

1.7. Duración : 45 minutos

1.8. Fecha : 05 de marzo de 2021

II. PROPÓSITO DE APRENDIZAJE

Competencias	Capacidades	Propósito	Evidencia de aprendizaje	Instrumento de evaluación
Gestiona proyectos de emprendimiento económico o social. Se desenvuelve en entornos virtuales generados por la TIC	• Crear propuestas de valor. • Trabaja cooperativamente para lograr objetivos y metas. • Aplica habilidades técnicas. • Evalúa los resultados del proyecto de emprendimiento. • Personaliza entornos virtuales. • Gestiona información del entorno virtual	Desarrollar los procedimientos para la creación de una aplicación móvil y plantear las medidas de seguridad necesarias.	Elaboración de una aplicación móvil.	Lista de cotejo

	• Interactúa en entornos virtuales • Crear objetos virtuales			

III. SECUENCIA DIDÁCTICA

Fase	Actividad	Recursos	Tiempo
Inicio	• El docente da la bienvenida a los estudiantes y se muestra el recurso digital didáctico acerca de casos sobre negocios afectados por las medidas de aislamiento social generado por el virus Covid -19. • Los estudiantes responden a las siguientes preguntas: ¿Conoces algún caso cercano similar a los presentados? ¿De qué manera las implementaciones tecnológicas podrían ayudar en esta situación? • Se elabora una lluvia de ideas con la herramienta Mentimeter para recoger los conocimientos previos de los estudiantes. • El docente presenta el propósito de la sesión: **Desarrollar los procedimientos para la creación de una aplicación móvil y plantear las medidas de seguridad necesarias.** • El docente brinda indicaciones sobre los compromisos para el desarrollo de la actividad.	• Presentación • Mentimeter	5 min.
Desarrollo	• Los estudiantes revisan los principales temas relacionados al desarrollo y seguridad de aplicaciones móviles, con la guía y mediación del docente. • Los estudiantes analizan la guía práctica donde se explican los principales procesos relacionados al desarrollo de aplicaciones móviles. • En forma grupal, los estudiantes consolidan la implementación de su aplicación móvil. • Los estudiantes reflexionan sobre las principales recomendaciones respecto a la seguridad de aplicaciones móviles. • Presentan su aplicación y conclusiones mediante una exposición, la cual es evaluada mediante una lista de cotejo.	• Presentación • Hoja de información • Guía práctica • PC • Software recomendado • Lista de cotejo	35 min.
Cierre	• Los estudiantes completan la ficha de metacognición donde reflexionan sobre los aprendizajes alcanzados. • El estudiante participa del cierre de sesión mediante Mentimeter con las principales conclusiones y compromisos.	• Ficha de metacognición • Mentimeter	5 min.

Evaluación		
Criterio	**Indicador**	**Instrumento**
• Comprensión y aplicación de tecnologías	• Desarrolla una aplicación móvil útil siguiendo las pautas de trabajo. • Reflexiona sobre las medidas de seguridad en el uso de aplicaciones móviles.	• Lista de cotejo

• Habilidades de trabajo en equipo.	• Respeta los aportes de sus compañeros. • Trabaja en equipo.	
• Metacognición	• Reflexiona y evalúa su proceso de aprendizaje	• Ficha de metacognición

IV. BIBLIOGRAFÍA

Garrido, C. (2013). *TFC Desarrollo de Aplicaciones Móviles*. Google Developers

Cuello, J., y Vittone, J. (2013). *Diseñando apps para móviles*. España: Tugamovil

Catalán, A. (2011). *Curso Android desarrollo de aplicaciones móviles*. España: Maestros del web.

Síntesis

La constante evolución de la tecnología exige la adaptación a nuevos dispositivos los que en un inicio parecen complicarnos; sin embargo, con el paso del tiempo, no podemos concebir una vida sin los mismos. Hace treinta años atrás, no pasaba por las mentes de los desarrolladores de aplicaciones que el mundo estaría a unos cuantos toques de pantalla, imágenes, videos, redes sociales, herramientas, juegos, etc. Ahora, se tiene un sinfín de posibilidades. El desarrollo de más y mejores tecnologías permitirá realizar acciones que antes no podíamos; incluso ahora, hacer compras es mucho más rápido, basta con unos cuantos toques de pantalla para luego llegar a casa y tener el producto listo.

Por otro lado, pese a todos los avances de tecnología y la seguridad que se implementa para evitar fraudes electrónicos, es necesario tener en cuenta que es el usuario el que al final decide si o no acceder a una determinada página e insertar sus datos, por lo cual es muy importante que se tenga en cuentan a qué sitio web se ingresa y si es segura. El desarrollo y la seguridad de las aplicaciones móviles van de la mano, principalmente para generar en el usuario la confianza y el aprovechamiento de la tecnología para facilitar sus actividades diarias.

Apreciación crítica y sugerencias

Durante el proceso de revisión de información se analizaron muchos temas vinculados al desarrollo de aplicaciones y se encontraron posibles limitaciones, entre ellas, la más resaltante es el desconocimiento de un lenguaje de programación. Por lo general, aprender a programar puede conllevar muchos años de aprendizaje y práctica, lo cual puede truncar las ideas innovadoras de los desarrolladores. En cuanto al desarrollo de aplicaciones, no deberían existir límites más allá que la creatividad, práctica y experiencia acumuladas.

Por ello, es necesario simplificar los procesos, hacer uso de los repositorios y de las herramientas que faciliten el desarrollo de aplicaciones. Además, tomar como punto a favor el filtro realizado por las tiendas de aplicaciones previo a la publicación, ya que esto evitará que se tengan posibles errores en el futuro al instalar en los distintos dispositivos móviles. Si bien, son unos días de retraso, puede evitar posibles fallos en el futuro.

Respecto a la seguridad en las aplicaciones, hay temas básicos que se deberían tener en cuenta, no solo al usar un dispositivo móvil, sino en cuanto al uso de cualquier dispositivo informático, la mayoría de los usuarios tienen casi toda su información vertida en los dispositivos móviles: fotos y videos personales, números de cuenta, contraseñas, etc. Esta situación, facilitan a los ciberdelincuentes la captación ilegal y uso inapropiado de esta información, ya sea por medio de software o la sustracción de dispositivos.

Una práctica que necesita ser extendida a todos los usuarios, sean de dispositivos móviles o equipos de informáticos, debería ser la instalación de software de rastreo y monitoreo en caso de pérdida del dispositivo. Adicionalmente, la recuperación de contraseñas y bloqueo rápido de cuentas para evitar problemas posteriores. Finalmente, cualquier desarrollador puede crear una aplicación; sin embargo, dependerá de sus

principios éticos darle una finalidad productiva. Por esa razón todo usuario de aplicaciones móviles debe tener en cuenta las medidas de seguridad explicados en esta investigación.

Referencias

Catalán, A. (2011). *Curso Android desarrollo de aplicaciones móviles.* España: Maestros de la Web.

Cuello, J., y Vittone, J. (2013). *Diseñando apps para móviles*. España: Tugamovil

Espacios de México. (s.f.). *Desarrollo de aplicaciones para dispositivos móviles*. México: Ebook.

Garrido, C. (2013). *TFC Desarrollo de Aplicaciones Móviles*. Google Developers

Ladino, A. (s.f.). *Vulnerabilidades y seguridad en el sistema operativo Android*. *libros entre usuarios*. España: UOC.

Martínez, F. (2011). *Aplicaciones para dispositivos móviles*. Valencia. España: Universidad Politécnica de Valencia.

MobileDevGuide. (2016). *D'ont Panic Guía a la galaxia de aplicaciones móviles*. Alemania: Enough Sotware

Ramírez, R. (s.f.). *Métodos para el desarrollo de aplicaciones móviles*. España: UOC.

Sevillano, J. (2018). *Desarrollo de aplicación Android para el intercambio de libros entre usuarios.* España: UOC.

Universidad Piloto de Colombia. (2014). *Desarrollo de aplicaciones para Android*. Colombia: CCIA.

Apéndices

Apéndice A: Lista de cotejo

Apéndice B: Ficha de metacognición

Apéndice C: Hoja de información

Apéndice D: Guía práctica para crear un App

Apéndice A: Lista de cotejo

FACULTAD DE TECNOLOGÍA

Departamento Académico de Electrónica y Telecomunicaciones

LISTA DE COTEJO

Creamos nuestra primera aplicación móvil

Apellidos y nombres: _____

Ciclo: ____ **Promoción:** _____ **Especialidad:** _____

Responde las siguientes preguntas:

N°	Indicador	Sí	No
01	Presenta su aplicación finalizada, siguiendo las pautas de trabajo.		
02	Identifica el tipo de aplicación elaborada.		
03	Describe las características de su aplicación.		
04	Sustenta la utilidad y pertinencia de su aplicación.		
05	Presenta un esquema organizado de su menú de opciones.		
06	Desarrolla el proceso de publicación de su aplicación.		
07	Identifica aplicaciones que ponen en riesgo su dispositivo móvil.		
08	Explica las medidas de seguridad al utilizar aplicaciones.		
09	Respeta los aportes de sus compañeros.		
10	Trabaja en equipo.		

Fuente: Autoría propia.

Apéndice B: Ficha de metacognición

FACULTAD DE TECNOLOGÍA

Departamento Académico de Electrónica y Telecomunicaciones

FICHA DE METACOGNICIÓN

Creamos nuestra primera aplicación móvil

Apellidos y nombres: _____

Ciclo: ____ **Promoción:** _____ **Especialidad:** _____

Responde las siguientes preguntas:

1. ¿Los contenidos explicados te servirán para aplicarlos en tu vida diaria? ¿Por qué?

   _____

   _____

2. Las estrategias planteadas para el desarrollo de aplicaciones, ¿Facilitan el desarrollo de aplicaciones móviles? ¿Por qué?

   _____

   _____

3. ¿Haces uso de alguna estrategia de seguridad?

   _____

   _____

4. ¿Qué nivel de logro de aprendizaje consideras haber obtenido al finalizar la sesión de aprendizaje? ¿Por qué?

Muy bueno	Bueno	Regular	Deficiente

5. ¿Alguna de las herramientas utilizadas en la sesión de aprendizaje te parecieron innovadoras para la implementación en tus clases? ¿Cuál?

Apéndice C: Hoja de información

FACULTAD DE TECNOLOGÍA

Departamento Académico de Electrónica y Telecomunicaciones

HOJA DE INFORMACIÓN

Creamos nuestra primera aplicación móvil

Instrucciones:

Revisa la hoja de información, en ella encontrarás los principales conceptos impartidos por el docente.

Desarrollo de aplicaciones móviles

Dispositivos móviles:

Para considerar como un dispositivo móvil, es necesario tener en cuenta que debe poseer movilidad, capacidad de comunicación inalámbrica e interacción con las personas y tamaño reducido.

Sistemas operativos móviles:

Los sistemas operativos de móviles tienen la misma función que la de una computadora, sirviendo para controlar los procesos básicos y permitiendo el funcionamiento de las aplicaciones que se instalarán posteriormente.

Android	IOS
El sistema operativo Android está basado en Linux, sin embargo, no es lo mismo, ya que no cuenta con la gestión de ventanas nativa, no incorpora soporte para glibc,	Es el sistema operativo de los dispositivos Apple. En sus inicios el sistema operativo IOS se creó solo para el teléfono sin embargo ha sido utilizado en otros dispositivos iPod, tabletas iPad**.**

tampoco permite la mayoría de las aplicaciones de Linux.	

Aplicaciones móviles:

Haciendo un símil con una computadora las aplicaciones móviles vendrían a ser los programas que darán una u otra función adicional al dispositivo, con lo que además de las funciones básicas se tiene la posibilidad de instalar aplicaciones de productividad, juegos, redes sociales, almacenamiento basado en la nube, etc.

Tipos de aplicaciones móviles		
Native APP	**Web APP**	**Aplicaciones híbridas**
Desarrollada en Java, pueden acceder a varias de las diferentes características de los dispositivos.	Una Web App se basa en HTML, JavaScript, y/o CSS ya que se carga en el servidor web y se visualizan con el navegador. No requieren instalación, adicionalmente es posible crear un acceso directo desde la pantalla de inicio.	Son una mezcla de Native App y Web App. A diferencia de una Web app, las aplicaciones híbridas permiten al usuario acceder usando librerías, como lo haría una Native App.

Desarrollo de aplicaciones móviles:

El proceso de desarrollo para la creación de aplicaciones móviles puede abarcar diversas actividades, desde la idea en sí, hasta la corrección de los errores y/o actualizaciones necesarias para mejorar la aplicación para los distintos dispositivos móviles. El trabajo suele estar realizado en constante coordinación entre diseñadores y programadores, teniendo una labor simultánea. Sin embargo, los más resaltantes son:

- Conceptualización

- Definición
- Diseño
- Desarrollo
- Publicación

Monetización:

La monetización ofrece la posibilidad de obtener dinero por medio de las aplicaciones ya que esto va a depender si la aplicación es gratis, de paga o fremium.

Monetización		
Aplicaciones gratuitas	**Aplicaciones de paga**	**Aplicaciones fremium**
El mayor beneficio que se obtiene con una aplicación gratuita es la cantidad de usuarios potenciales a los que es posible dirigirse.	El caso de las aplicaciones de pago es un poco más complicado ya que se requiere de una gran cantidad de descargas para ser rentables. Normalmente un usuario no se arriesga a hacer la compra de una aplicación si es que no la conoce lo que genera una barrera al uso de la aplicación.	Es la mezcla de los dos casos anteriores. Lo que permite al usuario utilizar la aplicación de manera gratuita, partiendo un uso básico, y acceder a la posibilidad de recibir funciones avanzadas previo pago.

Arquitectura de la información:

Es la forma de organizar el contenido y las funciones que realice la aplicación.

Arquitectura de Android:

En Android las actualizaciones suelen suceder muy rápido, en algunos casos semanalmente, permitiendo el uso de nuevas herramientas y bibliotecas.

Framework de aplicaciones:

Son las herramientas de desarrollo de cualquier aplicación. Una API es el conjunto de protocolos para desarrollar e integrar el software de las aplicaciones.

Librerías:

Esta capa contiene las librerías usadas por Android. Éstas han sido escritas con C/C++ y facilitan a Android las principales características.

Wireframe:

Es la representación simplificada de una pantalla individual, permite tener una idea de la organización.

La Máquina Virtual Dalvik y ART:

Dalvik es una máquina virtual utilizada para la ejecución de aplicaciones y códigos escritos en Java.

En el año 2013 Android lanza su versión KitKat e introduce un sustituto para Dalvik, con el nombre de ART: Android RunTime. La existencia de mejores dispositivos ha posibilitado el desarrollo de ART.

Lenguaje de programación de las aplicaciones en Android:

Las aplicaciones que se instalan en el sistema operativo Android se desarrollan con el lenguaje Java y el Software Development Kit (Android SDK). Atualmente se viene trabajando con la actualización del lenguaje de programación bajo el nombre de Kotlin.

Interfaz gráfica:

Considerada como todo aquello que el usuario puede visualizar y con lo que puede interactuar.

Seguridad en las aplicaciones móviles

Al hablar de seguridad en informática se considera la posibilidad de eventos mediante los que se pueden explotar vulnerabilidades, con el objetivo de saltar la seguridad del sistema ya sea de manera intencional o accidental, pudiendo afectar la integridad del sistema.

Application Sandbox:

Android, tiene implementado el principio de mínimo privilegio, lo que facilita solo el uso de determinados permisos para una aplicación, es decir, que no podrá hacer usos de micrófono o cámara si es que el usuario no ha concedido estos permisos.

Application Singning:

Todas las aplicaciones tienen una firma digital lo que posibilita que sus claves privadas solo sean conocidas por sus desarrolladores.

Permisos:

Las aplicaciones necesitan que se les otorgue permisos para funcionar correctamente, dependerá del usuario conceder los permisos para cada aplicación durante el proceso de instalación.

Vulnerabilidades en Android:

Los objetos maliciosos que en su mayoría afectan al sistema operativo Android son:

- Troyanos de SMS
- Exploits para ganar acceso al sistema raíz del teléfono.
- Módulos de publicidad

Tipos de ataque:

Existen diversos tipos de ataque que se pueden realizar desde una aplicación o tan solo con ingresar a una determinada página web y presionar en cualquier anuncio contenida en esta. Están divididos en: Ataque al software y ataques en la web.

Rooteo:

La posibilidad de rooteo se encuentra disponible en cualquier dispositivo, sin embargo, es necesario tener en cuenta que al rootear se le otorgan privilegios de superusuario, desde la instalación de una ROM personalizada a aplicaciones modificadas mejorarán la experiencia del usuario.

Ventajas y desventajas del rooteo

Ventajas	Desventajas
Las actualizaciones	Rootear no siempre es tan sencillo
Exprimir las ventajas del dispositivo	Si el dispositivo móvil no es muy conocido, el soporte se verá limitado
Activar funciones adicionales	Riesgo de brickeo

Mecanismos de prevención:

Se debe tener en cuenta:

- Instalación desde la tienda de aplicaciones.
- Instalación de aplicaciones fuera de la tienda oficial.
- Recomendaciones de seguridad.

Apéndice D: Guía práctica para crear un App

FACULTAD DE TECNOLOGÍA

Departamento Académico de Electrónica y Telecomunicaciones

GUÍA PRÁCTICA PARA CREAR UNA APP

Creamos nuestra primera aplicación móvil

Instrucciones:

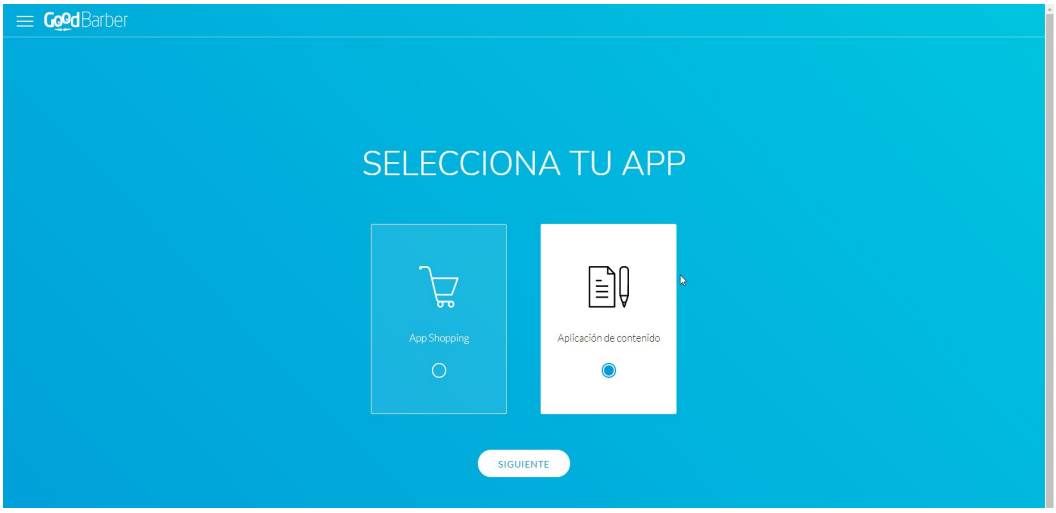
Realiza los pasos indicados para la creación de tu primera aplicación.

Crear mi primera aplicación (Sin saber programar).

1. Acceder a la siguiente dirección: https://www.goodbarber.com/

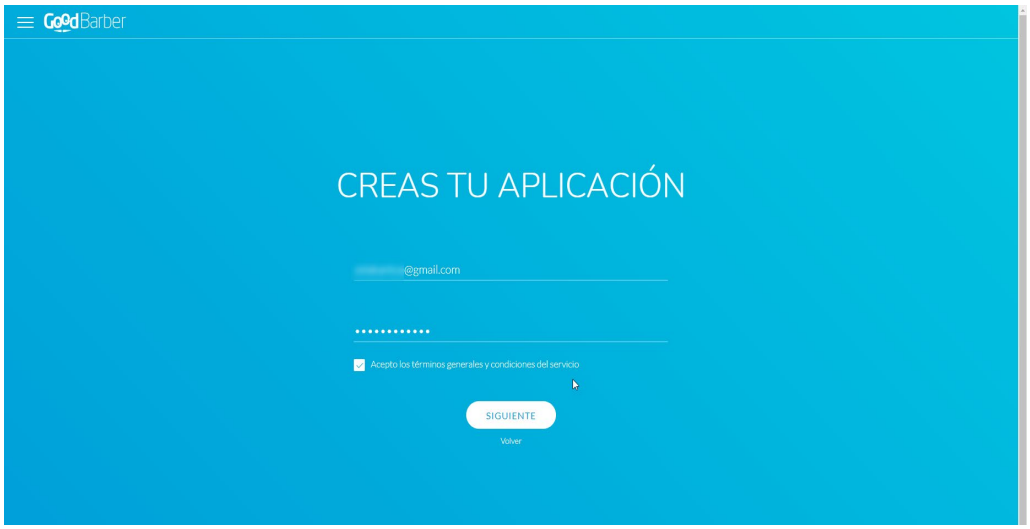
Portada GoodBarber. Fuente: goodbarber.com

2. Clic en el botón “Crea una aplicación”
3. Selecciona el tipo de aplicación que deseas crear (Recomiendo aplicación de contenido). Presiona siguiente:

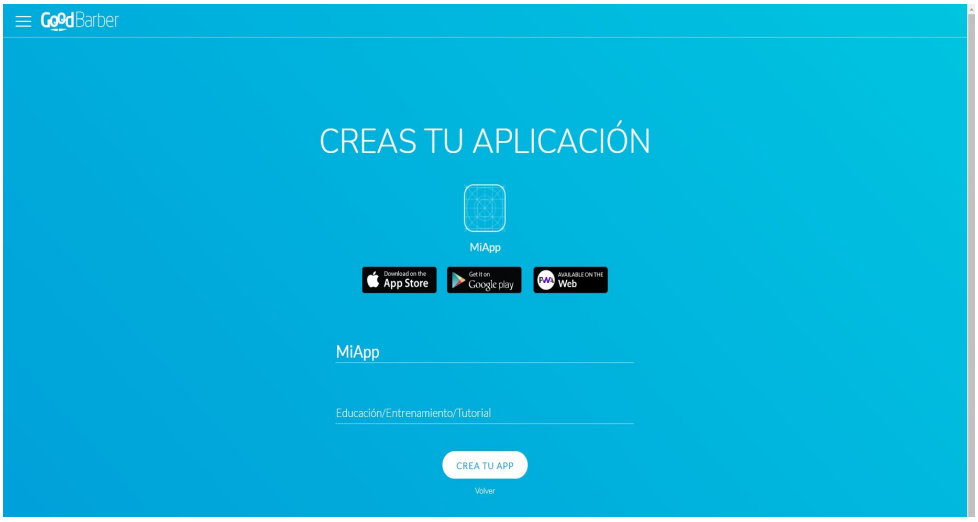


Configuración GodBarber. Fuente: goodbarber.com

4. Inserta los datos solicitados.

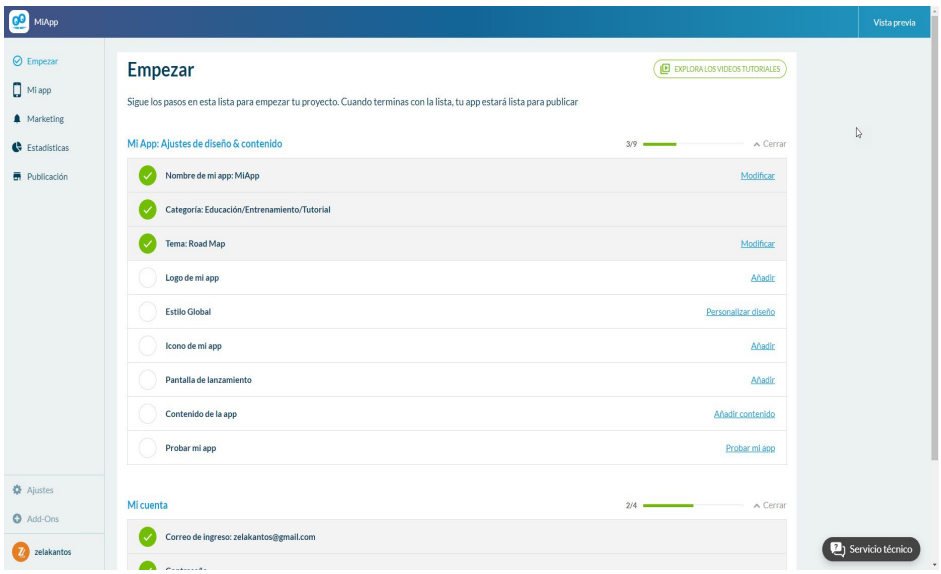


Configuración GoodBarber. Fuente: goodbarber.com



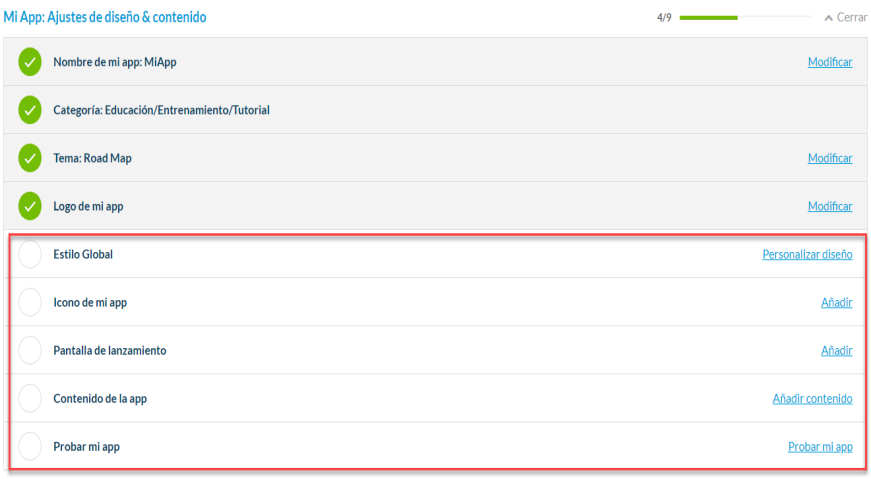
Configuración GoodBarber. Fuente: goodbarber.com

5. Bien, ya registraste tus datos. Ahora aparece la pantalla con las principales configuraciones que se pueden realizar:



Configuración GoodBarber. Fuente: goodbarber.com

6. Es necesario completar todos los apartados según lo que solicita el asistente de la aplicación:

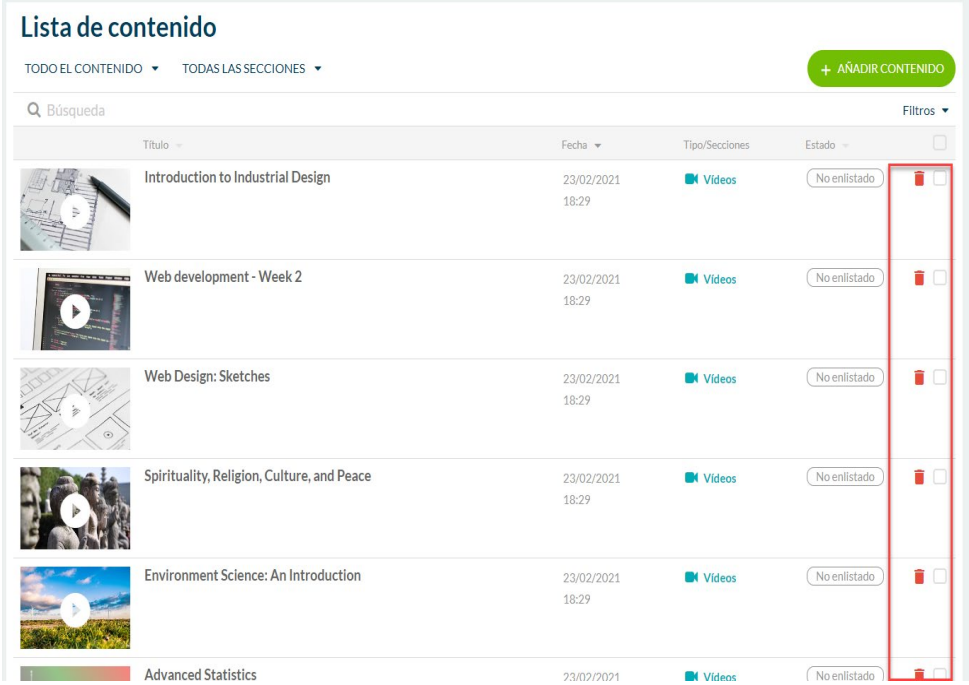


Configuración GoodBarber. Fuente: goodbarber.com

7. Es necesario seguir los parámetros solicitados por la herramienta para que la aplicación sea generada en óptimas condiciones.

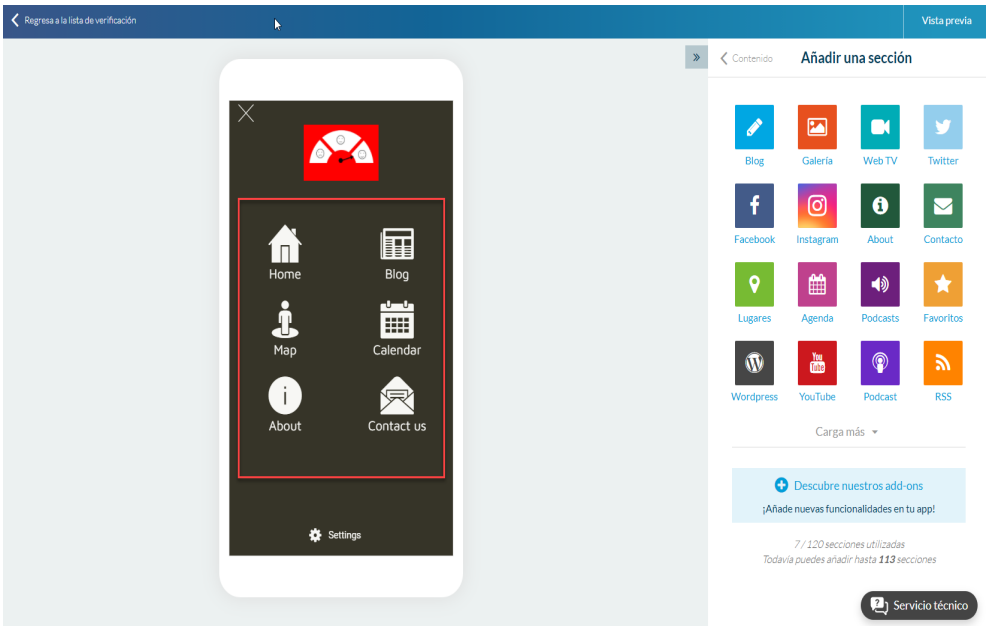
Configuración GoodBarber. Fuente: goodbarber.com

8. Recomiendo eliminar todos los apartados que no utilizarán para la aplicación.



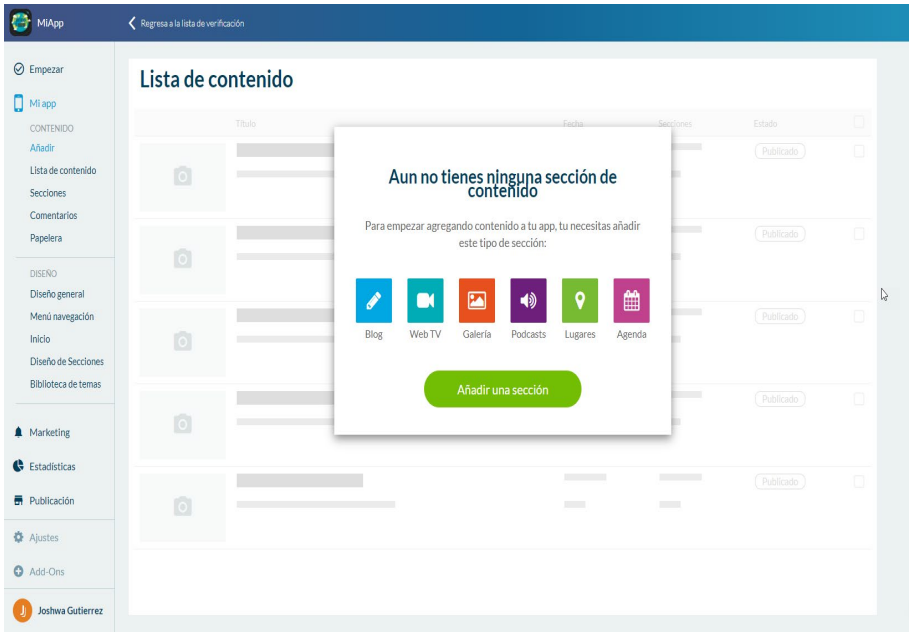
Configuración GoodBarber. Fuente: goodbarber.com

9. Además, eliminar las secciones de las que no se hará uso.



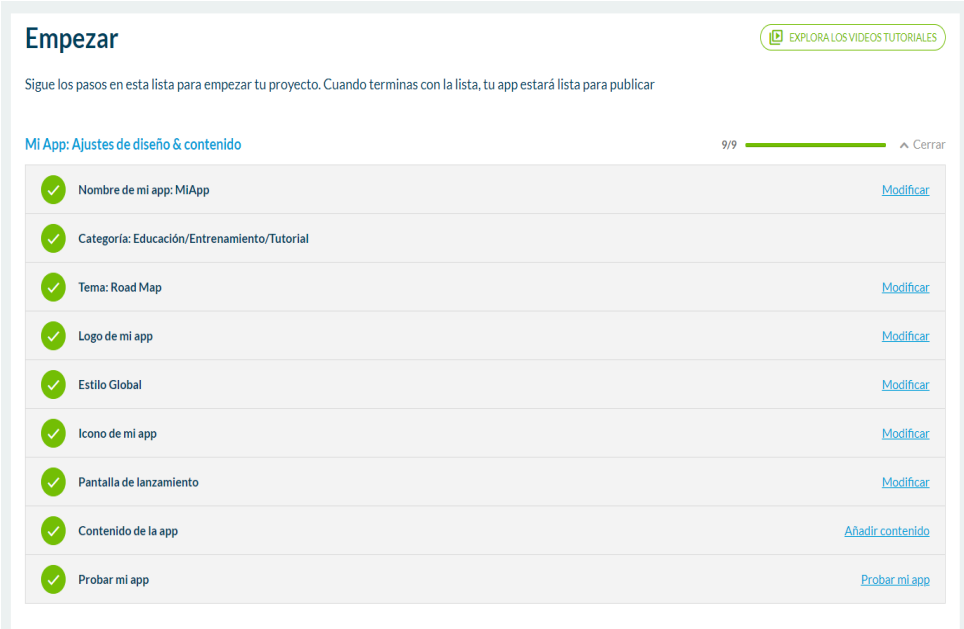
Configuración GoodBarber. Fuente: goodbarber.com

10. Ahora puedes ir agregando cada sección que necesites para tu aplicación:



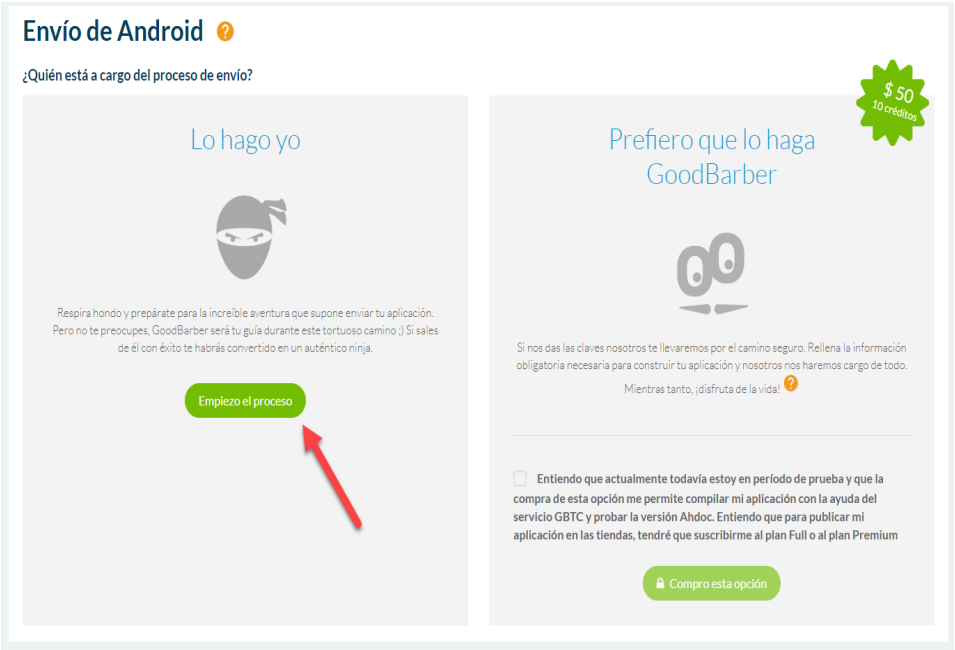
Configuración GoodBarber. Fuente: goodbarber.com

11. Para realizar la publicación de la aplicación es necesario completar todos los campos requeridos.



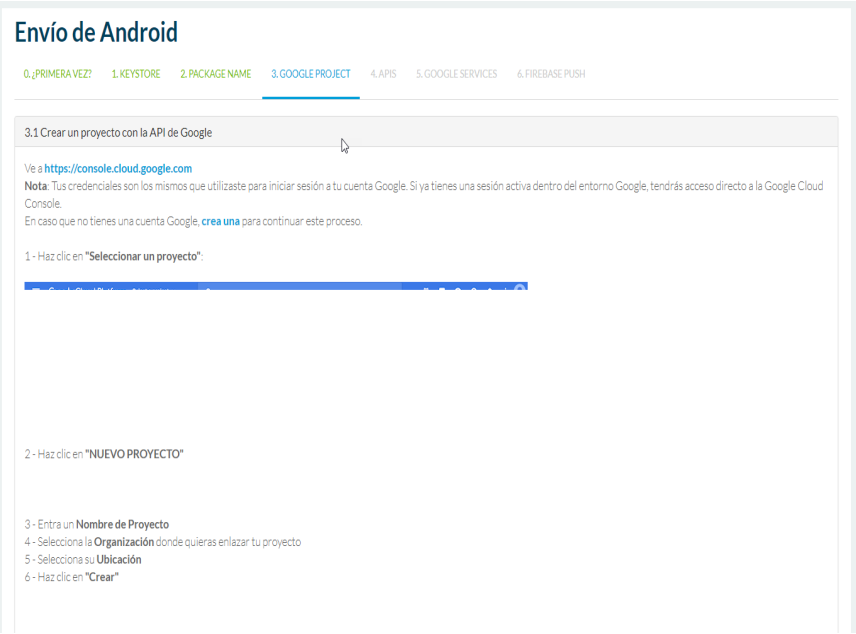
Configuración GoodBarber. Fuente: goodbarber.com

12. Inicia el proceso:



Configuración GoodBarber. Fuente: goodbarber.com

13. Sigue los pasos para la publicación de tu primera aplicación.



Configuración GoodBarber. Fuente: goodbarber.com

14. Además, no olvides revisar la declaración de permisos para la publicación.

Declara permisos para tu app

Las solicitudes de permisos se evalúan durante el proceso de lanzamiento, después de agregar los APK o paquetes de aplicaciones. Si tu app solicita el uso de permisos sensibles o de alto riesgo (p. ej., SMS o Registro de llamadas), deberás completar el Formulario de Declaración de Permisos y recibir la aprobación de Google Play.

Acerca del proceso

El Formulario de Declaración de Permisos se muestra durante el proceso de lanzamiento si la app incluye un APK o paquete de aplicación que solicite permisos para los cuales no se haya proporcionado una Declaración de Permisos a Google Play.

Si tienes paquetes de aplicación o APK activos que requieran una Declaración de Permisos, incluidas las versiones en los segmentos de prueba interna, abierta o cerrada, se mostrará una alerta en el menú de la izquierda, en **Presencia en Google Play Store** > **Contenido de la app**. No podrás publicar cambios en tu app, incluidas las modificaciones de la presencia en Google Play Store (p. ej., Ficha de Play Store, Precios y distribución), hasta que te ocupes de esta alerta mediante la creación de un lanzamiento que incluya una Declaración o quite los permisos.

Considera la opción de desactivar los segmentos de prueba abierta, cerrada o interna que no estén en uso en ese momento en caso de que no cumplan con esta política.

Si publicas apps mediante la API de publicación para desarrolladores de Google Play, consulta estas instrucciones especiales.

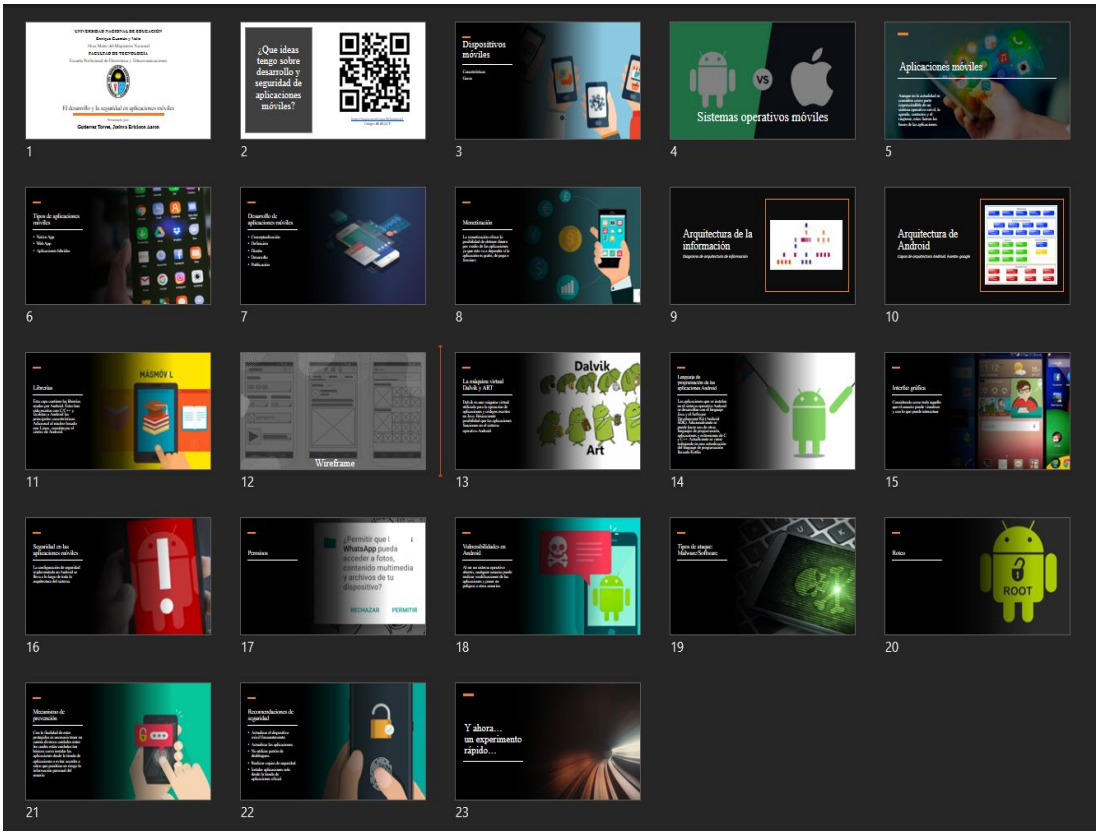
Declaración de permisos. Fuente: support.google.com

Carátula de Curso Android Desarrollo de aplicaciones móviles. Fuente: Autoría propia.

Carátula Diseñando apps para móviles. Fuente: Autoría propia.

Carátula Desarrollo de aplicaciones para dispositivos móviles: Como crear una aplicación útil. Fuente: Autoría propia.

Carátula Don't Panic Guía a la galaxia de aplicaciones móviles. Fuente: Autoría propia.



Presentación para estudiantes. Fuente: Autoría propia