|  |  |  |  |
| --- | --- | --- | --- |
| Casa&Hogar - Home | FacebookC:\Users\Enrique\Pictures\descarga.jpg | **INGENIERÍA DE SISTEMAS** | | **P**  **INICIAL APELLIDO PATERNO** |
| **AUDITORIA DE SISTEMAS** | |
| **EXAMEN FINAL** | | | |
| **NOMBRES** | **APELLIDO PATERNO** | **APELLIDO MATERNO** | |
| **EDSON JAVIER** | **PACO** | **LIMACHI** | |
| **CI.** | **CEL.** | **FECHA** | |
| 5972576 | 73734591 | 02/07/2023 | |

Tabla de contenido

[examen final 2](#_Toc139209547)

[Pregunta 2](#_Toc139209548)

[PROCESO DE DESCARGA DE LA primera aplicación 2](#_Toc139209549)

[Análisis del archivo AndroidManifest 5](#_Toc139209550)

[Proceso de descarga de la segunda aplicación 10](#_Toc139209551)

[Análisis del archivo AndroidManifest 14](#_Toc139209552)

[Conclusiones 16](#_Toc139209553)

# examen final

## Pregunta

Texto

Descripción generada automáticamente

|  |  |
| --- | --- |
| CAPTURAS | EXPLICACION |
| Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico  Descripción generada automáticamente  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente con confianza media  Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación  Descripción generada automáticamente  Tabla  Descripción generada automáticamente con confianza media  Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación  Descripción generada automáticamente    Interfaz de usuario gráfica, Texto, Chat o mensaje de texto  Descripción generada automáticamente  Tabla  Descripción generada automáticamente    Texto  Descripción generada automáticamente | PROCESO DE DESCARGA DE LA primera aplicación  1. Ingresamos al link que nos proporciona 2. Podemos apreciar que no es una pagina oficial 3. Procedemos a descargar el archivo APK 4. Podemos ver que tiene 8487M de descargas y mas de 3000 reseñas 5. En la imagen podemos ver la imagen de la aplicación y del botón de descarga 6. Damos clic al botón de descarga 7. Podemos apreciar que se realizo la descarga cabe destacar que debe ser con la extensión .APK 8. Procedemos abrir la herramienta a utilizar que es el software online APKTOOLS que es desarrollada por JAVA para realizar la reingeniería a las aplicaciones móviles 9. Apreciamos la pantalla de inicio de la aplicación 10. Nos debemos ir la opción que indica en la imagen 11. Procedemos a cargar el archivo 12. Indicamos la ubicación 13. Una vez cargada damos al clic al botón de **upload** 14. Procedemos a ver que empieza a cargar la aplicación por lo cual significa que esta cargando el archivo 15. Una vez finalizado nos da la siguiente opción 16. Nos muestra los archivos de compilados de la aplicación 17. Procedemos a descargar los archivos 18. Damos clic a la opción que nos indica SAVE 19. Damos la ruta donde se guardara los archivos 20. Podemos apreciar que es en formato comprimido .ZIP 21. Podemos apreciar el archivo 22. Procedemos a realizar la extracción de los archivos 23. Una vez finalizado este proceso podemos ver los documentos de compilados del archivo .APK 24. Podemos ver que hay un archivo llamado AndroidManifest 25. Este es el archivo que realizaremos la auditoria 26. Podemos apreciar el archivo .XML que debemos analizar |

### Análisis del archivo AndroidManifest

<uses-permission android:name="android.permission.ACCESS\_NETWORK\_STATE"/>

<uses-permission android:name="android.permission.VIBRATE"/>

<uses-permission android:name="android.permission.ACCESS\_COARSE\_LOCATION"/>

<uses-permission android:name="android.permission.ACCESS\_FINE\_LOCATION"/>

<uses-permission android:name="android.permission.READ\_PHONE\_STATE"/>

<uses-permission android:name="android.permission.READ\_PHONE\_NUMBERS"/>

<uses-permission android:name="android.permission.RECEIVE\_SMS"/>

<uses-permission android:name="android.permission.USE\_BIOMETRIC"/>

<uses-permission android:name="android.permission.USE\_FINGERPRINT"/>

<uses-permission android:name="android.permission.AUTHENTICATE\_ACCOUNTS"/>

<uses-permission android:name="android.permission.GET\_ACCOUNTS"/>

<uses-permission android:name="android.permission.ACCESS\_WIFI\_STATE"/>

<uses-permission android:name="android.permission.CHANGE\_WIFI\_STATE"/>

<uses-permission android:name="android.permission.INTERNET"/>

Usespermission android:name="android.permission.NEARBY\_WIFI\_DEVICES" android:usesPermissionFlags="0x00010000"/>

Permite el acceder al estado de la conexión de red del movil

Permite controlar vibracion del dispositivo

Permite acceder a la ubicación aproximada del dispositivo

Permite acceder a la ubicación precisa del dispositivo

Permite leer el estado del teléfono como el IMEI y el numero de telefono

Permite leer los números de teléfono asociados

Permite leer y recibir sms

permite usar funciones bometricas como huella o reconocimiento facial

Permite la autenticacion de huella

permite autenticar cuentas de usuario

Permite acceder a cuentas configuradas del dispositivo

Permite acceder al estado de conexión wifi

Permite cambiar al estado de conexión wifi

Permite el acceso a internet

Permit el acceso a dispositivos wifi cercanos

<uses-permission android:name="android.permission.CAMERA"/>

<uses-permission android:name="android.permission.RECORD\_AUDIO"/>

<uses-permission android:name="android.permission.READ\_EXTERNAL\_STORAGE"/>

<uses-permission android:name="android.permission.MANAGE\_OWN\_CALLS"/>

<uses-permission-sdk-23 android:name="android.permission.CALL\_PHONE"/>

<uses-permission android:name="android.permission.ACCESS\_MEDIA\_LOCATION"/>

<uses-permission android:name="android.permission.BLUETOOTH"/>

<uses-permission android:name="android.permission.BROADCAST\_STICKY"/>

<uses-permission android:name="android.permission.CHANGE\_NETWORK\_STATE"/>

<uses-permission android:name="android.permission.FOREGROUND\_SERVICE\_DATA\_SYNC"/>

<uses-permission android:name="android.permission.GET\_TASKS"/>

<uses-permission android:name="android.permission.INSTALL\_SHORTCUT"/>

<uses-permission android:name="android.permission.MANAGE\_ACCOUNTS"/>

<uses-permission android:name="android.permission.MODIFY\_AUDIO\_SETTINGS"/>

Permite leer archivos almacenados externamente al dispositivo

Permite usar funciones de bluetooth (ACTIVIDAD SOSPECHOSA E INNECESARIA)

Permite acceso a la camara del dispositivo

Permite al uso del microfono y grabar audio

Permite accionar llamadas telefonicos entrants y salidas

permite realizar llamadas desde la aplicación

Permite acceder a la ubicacion de los medios FOTOS VIDEOS ETC (ACTIVIDAD SOSPECHOSA E INNECESARIA)

Permite sincronizar datos en segundo plano utilizando un servicio en primer plano.

Permite modificar la configuración de audio del dispositivo.

Permite enviar transmisiones Sticky que se mantiene en el sistema (peligroso)

Permite cambiar el estado de la conexión de red

Permite acceder a la lista de tareas y actividades en ejecución.

Permite instalar accesos directos en la pantalla de inicio.

Permite administrar cuentas de usuario en el dispositivo.

<uses-permission android:name="android.permission.READ\_PROFILE"/>

<uses-permission android:name="android.permission.READ\_SYNC\_SETTINGS"/>

<uses-permission android:name="android.permission.READ\_SYNC\_STATS"/>

<uses-permission android:name="android.permission.RECEIVE\_BOOT\_COMPLETED"/>

<uses-permission android:name="android.permission.SCHEDULE\_EXACT\_ALARM"/>

<uses-permission android:name="android.permission.SEND\_SMS"/>

<uses-permission android:name="android.permission.USE\_CREDENTIALS"/>

<uses-permission android:name="android.permission.WAKE\_LOCK"/>

<uses-permission android:name="android.permission.WRITE\_CONTACTS"/>

<uses-permission android:name="android.permission.WRITE\_EXTERNAL\_STORAGE"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_AUDIO"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_IMAGES"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_VIDEO"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED"/>

<uses-permission android:name="android.permission.POST\_NOTIFICATIONS"/>

<uses-permission android:name="android.permission.WRITE\_SYNC\_SETTINGS"/>

Permite leer las estadísticas de sincronización del dispositivo.

Permite utilizar las credenciales almacenadas en el dispositivo.

Permite leer el perfil de usuario del dispositivo.(SOSPECHOSO)

Permite leer la configuración de sincronización del dispositivo.

Permite recibir la notificación de que el dispositivo ha terminado de arrancar.

Permite programar alarmas exactas en el tiempo.

Permite envio de SMS

Permite escribir en el almacenamiento externo del dispositivo.

Permite leer archivos visuales seleccionados por el usuario almacenados en el dispositivo.

Permite mantener el dispositivo despierto para evitar que entre en suspensión.

Permite modificar o agregar contactos en el dispositivo.

Permite leer archivos de audio almacenados en el dispositivo.

Permite leer archivos de imágenes almacenados en el dispositivo.

: Permite leer archivos de video almacenados en el dispositivo.

<uses-permission android:name="android.permission.REQUEST\_INSTALL\_PACKAGES"/>

<uses-permission android:name="android.permission.FOREGROUND\_SERVICE"/>

<uses-permission android:name="android.permission.USE\_FULL\_SCREEN\_INTENT"/>

<uses-permission android:name="com.android.launcher.permission.INSTALL\_SHORTCUT"/>

<uses-permission android:name="com.android.launcher.permission.UNINSTALL\_SHORTCUT"/>

<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>

<uses-permission android:name="com.google.android.gms.permission.AD\_ID"/>

<uses-permission android:name="com.google.android.providers.gsf.permission.READ\_GSERVICES"/>

<uses-permission android:name="com.sec.android.provider.badge.permission.READ"/>

<uses-permission android:name="com.sec.android.provider.badge.permission.WRITE"/>

<uses-permission android:name="com.htc.launcher.permission.READ\_SETTINGS"/>

<uses-permission android:name="com.htc.launcher.permission.UPDATE\_SHORTCUT"/>

<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST\_BADGE"/>

Permite recibir mensajes de Google Cloud Messaging.

Permiso de desinstalación de accesos directos específico para el lanzador de Android.

Permite ejecutar un servicio en primer plano

Permite solicitar la instalación de paquetes en el dispositivo.

Permite acceder al ID de publicidad de Google.

Permite utilizar ventanas de intento de pantalla completa.

Permiso de instalación de accesos directos específico para el lanzador de Android.(SOSPECHOSO Y PELIGROSO

Permite leer servicios de Google Play.

Permiso de lectura de insignias específico para dispositivos Samsung.

Permiso de escritura de insignias específico para dispositivos Samsung.

Permiso de lectura de configuración específico para dispositivos HTC.

Permiso de actualización de accesos directos específico para dispositivos HTC.

Permiso de transmisión de insignias específico para dispositivos Sony Ericsson.

permission android:name="com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE"/>

<uses-permission android:name="com.huawei.android.launcher.permission.READ\_SETTINGS"/>

<uses-permission android:name="com.huawei.android.launcher.permission.WRITE\_SETTINGS"/>

<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE\_BADGE"/>

<uses-permission android:name="com.whatsapp.permission.BROADCAST"/>

<uses-permission android:name="com.whatsapp.permission.MAPS\_RECEIVE"/>

<uses-permission android:name="com.whatsapp.permission.REGISTRATION"/>

<uses-permission android:name="com.whatsapp.sticker.READ"/>

<uses-permission-sdk-23 android:name="android.permission.ANSWER\_PHONE\_CALLS"/>

<uses-permission-sdk-23 android:name="android.permission.READ\_CALL\_LOG"/>

Permiso de inserción de insignias específico para dispositivos Sony Mobile.

Permiso de lectura de configuración específico para dispositivos Huawei.

Permiso de escritura de configuración específico para dispositivos Huawei.

Permiso de cambio de insignias específico para dispositivos Huawei.

Permiso de transmisión específico para la aplicación WhatsApp.

Permiso para recibir mapas específico para la aplicación WhatsApp.

Permiso de registro específico para la aplicación WhatsApp.

Permiso de lectura específico para la aplicación WhatsApp para leer pegatinas.

versión SDK 23): Permite responder llamadas telefónicas desde la aplicación.

versión SDK 23): Permite leer el registro de llamadas del dispositivo.

|  |  |
| --- | --- |
| Capturas | Explicación |
| Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico  Descripción generada automáticamente  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente con confianza media  Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente con confianza baja  Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico  Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto  Descripción generada automáticamenteInterfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Texto, Carta  Descripción generada automáticamente  Interfaz de usuario gráfica, Aplicación  Descripción generada automáticamente  Interfaz de usuario gráfica  Descripción generada automáticamente  Interfaz de usuario gráfica, Texto, Aplicación  Descripción generada automáticamente  Tabla  Descripción generada automáticamente      Tabla  Descripción generada automáticamente con confianza baja    Texto  Descripción generada automáticamente | Proceso de descarga de la segunda aplicación  1. Procedemos a realizar el ingreso al link proporcionado 2. Podemos ver el 84.5M descargas que se le realizo y 1838 reseñas que tiene la aplicación 3. Procedemos a ver la pagina de descarga 4. Procedemos a dar clic al botón de descarga 5. Procedemos abrir la herramienta web utilizada para la auditoria 6. Procedemos a ingresar a esta opción es muy importante 7. Cargamos el archivo .APK descargado 8. Damos a la ruta del archivo 9. Esperamos a que cargue 10. Damos a la opción de upload y empezara el trabajo 11. Procedemos a ver que la aplicación se recarga la aplicación 12. Esto indica que está procesando la operación 13. Al finaliza la operación podemos ver que nos da un erro indicando que la ruta este mal del archivo, pero ante verificaciones estaba todo normal y se realizo los pasos indicados para le laboratorio 14. Se realizo el intento con una versión más antigua y non indica el mismo error por los cual se optó por otra aplicación 15. Se realizo la descarga del mismo sitio web indicado por la pregunta 16. Ingresamos a la opción para realizar la descarga de la aplicación INSTAGRAM 17. Podemos apreciar que no es una página oficial 18. Procedemos a descargar el archivo APK 19. Podemos ver que tiene 3132M de descargas y más de 2121 reseñas 20. En la imagen podemos ver la imagen de la aplicación y del botón de descarga 21. Damos clic al botón de descarga 22. Podemos apreciar que se realizó la descarga cabe destacar que debe ser con la extensión .APK 23. Procedemos abrir la herramienta a utilizar que es el software online APKTOOLS que es desarrollada por JAVA para realizar la reingeniería a las aplicaciones móviles 24. Apreciamos la pantalla de inicio de la aplicación 25. Nos debemos ir la opción que indica en la imagen 26. Procedemos a cargar el archivo 27. Indicamos la ubicación 28. Una vez cargada damos al clic al botón de **upload** 29. Procedemos a ver que empieza a cargar la aplicación por lo cual significa que está cargando el archivo 30. Una vez finalizado nos da la siguiente opción 31. Nos muestra los archivos de compilados de la aplicación 32. Procedemos a descargar los archivos 33. Damos clic a la opción que nos indica SAVE 34. Damos la ruta donde se guardará los archivos 35. Podemos apreciar que es en formato comprimido .ZIP 36. Podemos apreciar el archivo 37. Procedemos a realizar la extracción de los archivos 38. Una vez finalizado este proceso podemos ver los documentos de compilados del archivo .APK 39. Podemos ver que hay un archivo llamado AndroidManifest      1. Este es el archivo que realizaremos la auditoria |

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

### Análisis del archivo AndroidManifest

Estos son algunos de los permisos que el APK requiere por lo cual analizaremos los más importantes y peligrosas

<uses-permission-sdk-23 android:name="android.permission.ACCESS\_WIFI\_STATE"/>

<uses-permission android:name="android.permission.INTERNET"/>

<uses-permission android:name="android.permission.ACCESS\_NETWORK\_STATE"/>

<uses-permission android:name="android.permission.WAKE\_LOCK" violationExplanation="Need wake lock when user using SUP" violationType="MOS\_BLOCKED\_PERMISSION\_WAKE\_LOCK"/>

<uses-permission android:name="android.permission.GET\_ACCOUNTS"/>

<uses-permission android:name="android.permission.USE\_CREDENTIALS"/>

<uses-permission android:name="android.permission.RECEIVE\_BOOT\_COMPLETED"/>

<uses-permission android:name="android.permission.VIBRATE"/>

<uses-permission android:name="android.permission.FOREGROUND\_SERVICE"/>

<uses-permission android:name="android.permission.USE\_FULL\_SCREEN\_INTENT"/>

<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>

<uses-permission android:name="android.permission.BLUETOOTH"/>

<uses-permission android:name="android.permission.CAMERA"/>

<uses-permission android:name="android.permission.READ\_CONTACTS"/>

Permiso de acceso al estado de la conexión wifi

Permiso de conexion a internet

Permiso a estado de la red

Obtener cuentas almacenadas en el dispositivo

Usar credenciales almacenas en el dispositivo

Recibir notificación al reinicio del dispositivo

Control de la vibración del dispositivo

Ejecutar un servicio en Segundo plano

Mostrar ventanas emergentes en la pantalla completa

Recibir mensajes de Google Cloud Messaging.

Leer información de los contactos

Acceder a la cámara

Funciones de bluetooth

<uses-permission android:name="android.permission.READ\_PROFILE"/>

<uses-permission android:name="android.permission.ACCESS\_FINE\_LOCATION"/>

<uses-permission android:name="android.permission.RECORD\_AUDIO"/>

<uses-permission android:name="android.permission.MODIFY\_AUDIO\_SETTINGS"/>

<uses-permission android:name="android.permission.READ\_EXTERNAL\_STORAGE"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_IMAGES"/>

<uses-permission android:name="android.permission.READ\_MEDIA\_VIDEO"/>

<uses-permission android:name="android.permission.WRITE\_EXTERNAL\_STORAGE"/>

<uses-permission android:name="android.permission.ACCESS\_MEDIA\_LOCATION"/>

<uses-permission android:name="android.permission.POST\_NOTIFICATIONS"/>

<uses-permission android:name="com.google.android.gms.permission.AD\_ID"/>

<uses-permission android:name="android.permission.READ\_PHONE\_STATE"/>

<uses-permission android:name="android.permission.READ\_PHONE\_NUMBERS"/>

<uses-permission android:name="com.android.launcher.permission.INSTALL\_SHORTCUT"/>

<uses-permission android:name="com.android.launcher.permission.UNINSTALL\_SHORTCUT"/>

<uses-permission android:name="com.instagram.direct.permission.PROTECTED\_DEEPLINKING"/>

Leer perfil de usuario

Acceder a la ubicación del dispositivo

Graba audio con el microfono

Modificar configuración de audio

Leer contenido de almacenamiento externo

Lee imágenes almacenadas en el dispositivo

Leer videos almacenados

Escribe en el almacenamiento externo

Acceder a la ubicación de los archivos de multimedia

Permite publicar notificaciónes en el dispositivos

Permite ID de publicaciones de Google

Lee estado del telefono

Lee números almacenados en el dispositivo

Instalador acceso directos en el lanzador de android

desinstala acceso directos en el lanzador de android

Permiso de acceso a enlaces profundos protegidos de Instagram Direct.

<uses-permission android:name="com.instagram.direct.permission.DIRECT\_APP\_THREAD\_STORE\_SERVICE"/>

<uses-permission android:name="com.facebook.services.identity.FEO2"/>

<uses-permission android:name="com.htc.launcher.permission.READ\_SETTINGS"/>

<uses-permission android:name="com.htc.launcher.permission.UPDATE\_SHORTCUT"/>

<uses-permission android:name="com.huawei.android.launcher.permission.CHANGE\_BADGE"/>

<uses-permission android:name="com.sonyericsson.home.permission.BROADCAST\_BADGE"/>

<uses-permission android:name="com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE"/>

<uses-permission-sdk-23 android:name="android.permission.UPDATE\_APP\_BADGE"/>

<uses-permission-sdk-23 android:name="android.permission.CALL\_PHONE"/>

Permiso de acceso al servicio de almacenamiento de hilos de la aplicación Direct de Instagram.

Permiso de identidad de servicios de Facebook.

Permiso de lectura de configuración específico para dispositivos HTC.

Permiso de actualización de accesos directos específico para dispositivos HTC.

Permiso de cambio de insignias específico para dispositivos Huawei.

Permiso de transmisión de insignias específico para dispositivos Sony Ericsson.

Actualizar insignias de aplicaciones (requiere SDK 23 o superior).

Realizar llamadas telefónicas (requiere SDK 23 o superior).

## Conclusiones

Como conclusión a la auditoria de las dos aplicaciones llegamos a que hay muchos permisos extraños e innecesario para el funcionamiento por lo cual es muy importa tener el control de los permisos que se le da en las aplicaciones con el dispositivo y tener actualizado las versiones de Android ya que vienen en conjunto de actualizaciones de parches de seguridad.

La segunda conclusión llega es que siempre en mas seguro realizar la descarga e instalación de las aplicaciones de una fuente oficial ya que de fuente de terceros pueden venir con una reingeniería realizada e implementado código malicioso. Cabe recalcar que no siempre es necesario que el código malicioso este en la versión descargada si no puede ver con alguna actualización del APK