TRABAJO DE GRADO

Desarrollar políticas de seguridad en teléfonos inteligentes con sistema operativo Android utilizados en la Policía Nacional.

JOSÉ ALFREDO RAMÍREZ PRADA
Código: 93136250

MARIO AUGUSTO TEJADA RICO
Código: 80055225

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
CIENCIAS DE BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
OCTUBRE DE 2016

TRABAJO DE GRADO

Desarrollar políticas de seguridad en teléfonos inteligentes con sistema operativo Android utilizados en la Policía Nacional.

JOSÉ ALFREDO RAMÍREZ PRADA
Código: 93136250

MARIO AUGUSTO TEJADA RICO
Código: 80055225

Director
JHON FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. UNAD
CIENCIAS DE BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
OCTUBRE DE 2016

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

AGRADECIMIENTOS

Durante el desarrollo del presente trabajo damos un agradecimiento en especial a Dios, por darnos la vida, salud y conocimiento, a nuestra institución, la Policía Nacional de Colombia, ya que fue esta quien nos dio la posibilidad de realizar y llevar a cabo la culminación de nuestros estudios, a nuestras familias y seres más queridos ya que contamos con el apoyo de ellos que nos ven salir cada día adelante, en progreso de nuestro beneficio y en el de ellos.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

El desarrollo del presente trabajo tiene por objeto llevar a cabo el desarrollo de políticas de seguridad para dispositivos móviles con sistema operativo Android, al interior de la Policía Nacional de Colombia, ya que toda vez la tecnología avanza a grandes pasos y sus funcionarios no se quedan atrás en materia de tecnología y su uso.

La Institución cuenta con una gran plataforma tecnológica la cual cuenta con sus políticas de seguridad de la Información, pero no cuenta con políticas en cuanto al uso de la información por medio de dispositivos móviles con sistema operativo Android.

Se ha observado que gran número de personal adscrito a la Policía Nacional cuenta con un Smartphone cuyo sistema operativo es Android, manejando desde allí cuentas de correo empresariales e institucionales, ingreso al portal de servicios institucionales el cual soporta información de carácter confidencial y que es solo de exclusiva utilidad para la institución y de quien la consulta, siendo esta de carácter privado.

El sistema operativo de Google se ha convertido en la plataforma móvil más afectada por el malware, centrando el 99% de las amenazas desarrolladas para Smartphone, motivo por el cual se ve en la necesidad de adecuar y desarrollar políticas de seguridad para dispositivos móviles con sistema operativo Android, al interior de la Policía Nacional de Colombia, ya que la fuga de información es posible mediante ataques a la vulnerabilidades que se presentan en Android o en sus aplicaciones.

1. TITULO

“Desarrollar políticas de seguridad en teléfonos inteligentes con sistema operativo Android utilizados en la Policía Nacional.”

2. DEFINICIÓN DEL PROBLEMA

En los últimos años el uso de dispositivos móviles ha tenido un crecimiento vertiginoso, debido a las múltiples funciones que se pueden aprovechar por parte de los usuarios, todas vez que ofrecen ventajas en movilidad, teniendo en cuenta su fácil conexión a redes inalámbricas, configuración de correo electrónico, navegación en sitios web, instalación de aplicaciones móviles de diversas categorías, acceso a redes sociales, entre otros. Es así que debido a este gran uso de esta tecnología, se ha incrementado en gran medida los ataques a los dispositivos móviles afectando la seguridad de la información de los usuarios.

Los funcionarios de la Policía Nacional, han empleado en gran medida las ventajas de los dispositivos móviles tanto en el ámbito personal como laboral, teniendo en cuenta que desde el año 2014 fueron asignados a nivel nacional dispositivos móviles con sistema operativo Android, observándose el manejo de información institucional en mencionados dispositivos, tal es el caso de configuración de correo empresarial Exchange, configuración de correo institucional Outlook, ingreso al portal de servicios internos "PSI" mediante el cual se tiene acceso a información personal e institucional del funcionario, registro fotográfico de actividades del servicio de policía, registro fotográfico de documentos institucionales. Por lo anterior se ha notado que no hay una política de seguridad de la información para estos dispositivos que garantice la confidencialidad, integridad y disponibilidad de la información institucional, vulnerabilidad que permitiría la fuga de información, ataques de virus, malware, troyanos, ataques de ingeniería social, perdida de la credibilidad e imagen institucional.

Por lo anterior, se requiere desarrollar políticas de seguridad para dispositivos móviles a los funcionarios que tienen acceso por medio de estos dispositivos a información institucional, con el fin de garantizar la confidencialidad de la información.

Problema: ¿Qué políticas de seguridad tiene implementada la Policía Nacional para el uso de teléfonos inteligentes con sistema operativo Android?

3. JUSTIFICACIÓN

Los ataques informáticos dirigidos a teléfonos inteligentes personales de los funcionarios de la Policía Nacional se encuentran el alto riesgo, debido la información institucional administrada en estos dispositivos, en la actualidad no existen políticas de seguridad para dispositivos móviles, exponiendo esta vulnerabilidad a la fuga de información, ataque que puede ser reflejado en el entorno social, debido al nivel de clasificación de la información propia de la institución, conllevando a la pérdida de credibilidad e imagen institucional frente a la nación.

La información es un activo valioso para cualquier organización, la Policía Nacional por medio de la Resolución No. 03049 de 2012 "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía", establece las políticas de seguridad de la información, no obstante los funcionarios de la Policía no aplican adecuadamente el principio de confidencialidad establecido en mencionado manual, toda vez que se está accediendo a información confidencial por medio de dispositivos móviles, el cual puede ser vector de ataque por un ciberdelincuente.

Se requiere minimizar el riesgo al cual está expuesta la información de la institución policial, mediante la implementación de nuevas políticas de seguridad de la información, enfocadas a teléfonos inteligentes utilizados por funcionarios de la Policía Nacional, teniendo en cuenta el vertiginoso crecimiento en el uso de estos dispositivos en los últimos años, políticas las cuales no se encuentran establecidas en la Resolución No. 03049 de 2012 "MANUAL DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION".

4. OBJETIVOS

4.1 Objetivo General

Identificar y definir políticas de seguridad de la información en dispositivos móviles con sistema Operativo Android para los funcionarios de la Policía Nacional.

4.2 Objetivos Específicos

Analizar el nivel de seguridad actual para prevenir la fuga de información a través de teléfonos inteligentes de los funcionarios de la Policía Nacional.

Identificar ataques informáticos dirigidos a dispositivos móviles para interceptar información.

Utilizar herramientas para realizar pentesting para dispositivos móviles con sistema operativo Android.

Establecer políticas de seguridad de la información para teléfonos inteligentes con sistema operativo Android.

Divulgar las políticas desarrolladas en este proyecto por medio de capacitaciones coordinadas con la Policía Nacional.

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

5.1.1 Computación Móvil

Comunicación de diferentes equipos portátiles o móviles de hardware y software, que hacen uso de la computación para realizar diferentes tareas computacionales permitiendo la movilidad y la conexión a otros dispositivos por medio de diferentes tecnologías de comunicación inalámbrica y en la administración de forma óptima del procesamiento, almacenamiento y el consumo de la energía. Entre los dispositivos móviles se encuentran actualmente los computadores portátiles, minicomputadores, teléfonos celulares, Smartphone, Tablets, e-Readers, etc., en general cualquier dispositivo que tenga y permita la conexión a otros dispositivos por medio de diferentes tecnologías de comunicación inalámbrica (Wi-Fi (Wireless Fidelity), GSM (Global System for Mobile), Bluetooth, RFID (Radio Frequency Identification), GPRS (General Packet Radio Service) y Satelital)[1].

5.1.2 Plataforma Android

El sistema operativo Android está basado en el núcleo del sistema operativo Linux, diseñado específicamente para dispositivos móviles[2].

Android es un conjunto de software para dispositivos móviles que incluye un sistema operativo, un middleware o software de conectividad que permite el funcionamiento de aplicaciones distribuidas sobre plataformas distribuidas y diferentes aplicaciones claves. El SDK o Kit de desarrollo de software de Android provee herramientas de desarrollo para crear aplicaciones y las API interfaces de programación de aplicaciones necesarias para desarrollar las aplicaciones en la plataforma Android.

[1] RAMÍREZ, Gabriel. La importancia de la computación móvil: pasado, presente y futuro. Revista Especializada en Telecomunicaciones, Electrónica y Sistemas. Universidad Nacional Abierta y a Distancia. [En línea] [Citado el 15 Octubre, 2014]. Disponible en internet: Volumen 2, Número 2. p. 3.

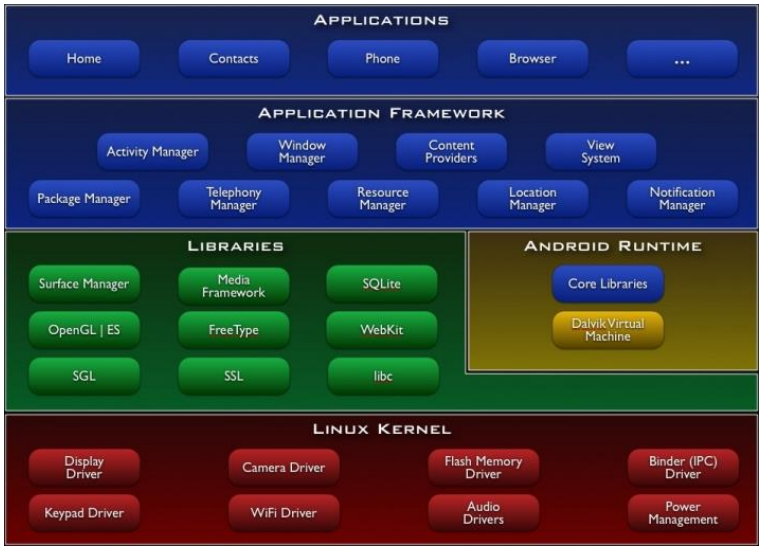
[2] Lección 13: Desarrollo de Aplicaciones [En línea]. Universidad Nacional Abierta y a Distancia, [consultado 08 de Agosto de 2016]. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_13_desarrollo_de_aplicaciones.html

Es una plataforma de software y un sistema operativo que está basado en una versión modificada del sistema operativo Linux, inicialmente fue desarrollado por la compañía Google Inc., después se conformó la fundación Open Handset Alliance, el cual es un consorcio de 48 compañías de hardware, software y telecomunicaciones, la cual es la encargada de proveer estándares abiertos de comunicación para dispositivos móviles, a la cabeza del consorcio se encuentra Google.

La plataforma es de código abierto, la cual permite que cualquier usuario puede modificar el código, crear y desarrollar aplicaciones para el sistema operativo, permite controlar dispositivos por medio de bibliotecas desarrolladlas o adaptados por Google mediante el lenguaje de programación Java.

La Figura 1, se puede observar la arquitectura del sistema operativo Android, el cual está definido mediante cuatro (04) capas: Linux Kernel, librerías, framework de aplicaciones y aplicaciones.

Figura 1. Arquitectura Android



Fuente: http://elinux.org/Android_Architecture

Capas de la arquitectura Android[3]

Linux Kernel: La primera desde la base hacia arriba es el Kernel o Núcleo de Linux aquí se encuentran 8 componentes específicos del núcleo que permiten el funcionamiento del sistema operativo con el hardware del dispositivo móvil, controlador de la pantalla, controlador del teclado, el controlador de la cámara, el controlador del audio, el controlador de la tarjeta de memoria, el controlador de la antena WiFi, el controlador de comunicaciones internas y el administrador de la energía.

Librerías: Las librerías de Android se encuentran en el segundo nivel después del Kernel, aquí se encuentra la librería Surface manager encargada de dibujar las diferentes pantallas, la librerías del entorno de medios controla todos los códec de multimedia, la librería de almacenamiento SQLite encargada de manejar el almacenamiento del dispositivo, la librería OpenGL es la encargada de manejar los gráficos 3D y las interacciones que los gráficos 2D, la librería FreeType es la encargada de administrar las fuentes, la librería WebKit que provee un navegador web que provee las herramientas para el trabajo en dispositivos móviles y pantallas pequeñas, la librería SGL representa las gráficas de Android, la librerías SSL provee los protocolos para la comunicaciones seguras y la librería Libc Incluye todas las cabeceras y funciones según el estándar del lenguaje C. Todas las demás librerías se definen en este lenguaje.

En este mismo nivel se encuentra el Runtime de Android, que está compuesto por dos componentes, el núcleo de las librerías que tiene clases en Java y la máquina virtual de Android Dalvik Virtual Machine.

Framework de Aplicaciones: Representa fundamentalmente el conjunto de herramientas de desarrollo de cualquier aplicación. Toda aplicación que se desarrolle para Android, ya sean las propias del dispositivo, las desarrolladas por Google o terceras compañías, o incluso las que el propio usuario cree, utilizan el mismo conjunto de API y el mismo "framework", representado por este nivel.

Entre las API más importantes ubicadas aquí, se pueden encontrar las siguientes:

[3] Ibíd. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_13_desarrollo_de_aplicaciones.html

Activity Manager: Conjunto de API que gestiona el ciclo de vida de las aplicaciones en Android.

Window Manager: Gestiona las ventanas de las aplicaciones y utiliza la librería Surface Manager.

Telephone Manager: Incluye todas las API vinculadas a las funcionalidades propias del teléfono (llamadas, mensajes, etc.).
Content Provider: Permite a cualquier aplicación compartir sus datos con las demás aplicaciones de Android. Por ejemplo, gracias a esta API la información de contactos, agenda, mensajes, etc. será accesible para otras aplicaciones.

View System: Proporciona un gran número de elementos para poder construir interfaces de usuario (GUI), como listas, mosaicos, botones, "check-boxes", tamaño de ventanas, control de las interfaces mediante teclado, etc. Incluye también algunas vistas estándar para las funcionalidades más frecuentes.

Location Manager: Posibilita a las aplicaciones la obtención de información de localización y posicionamiento.

Notification Manager: Mediante el cual las aplicaciones, usando un mismo formato, comunican al usuario eventos que ocurran durante su ejecución: una llamada entrante, un mensaje recibido, conexión Wi-Fi disponible, ubicación en un punto determinado, etc. Si llevan asociada alguna acción, en Android denominada Intent, (por ejemplo, atender una llamada recibida) ésta se activa mediante un simple clic.

XMPP Service: Colección de API para utilizar este protocolo de intercambio de mensajes basado en XML.

Aplicaciones: En la capa de aplicaciones se ubican las aplicaciones que utilizan todos los recursos del sistema operativo, aquí se encuentra las aplicaciones del teléfono, contactos, navegadores, las aplicaciones que se descargan del Google Play y las aplicaciones que programan los desarrolladores de Android[4].

[4] Ibíd. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_13_desarrollo_de_aplicaciones.html

5.1.3 Historia de Android

Cuando el G1 fue presentado allá por 2008, tanto el teléfono como su sistema operativo eran tan distantes de lo que hoy consideramos un Smartphone real que casi no merece ni esa denominación[5].

En la figura 2 se puede observar el equipo T-Mobile G1, primer equipo basado en Google Android, el cual fue fabricado por la compañía taiwanesa HTC.

Figura 2. T-Mobile G1

Fuente: https://www.wayerless.com/2008/10/w-galeria-t-mobile-g1-android/

Desde entonces, el sistema operativo de Google para móviles ha crecido y recorrido un largo camino para destronar al iPhone como el rey de los Smartphone y posicionarse como el sistema operativo líder en todo el mercado de Tablets y Smartphone.

De este modo y en parte como un homenaje te mostraremos una rápida visión de la historia y evolución de Android a través sus versiones y lo que está aún por venir.

[5] Historia de Android: La Evolución a lo largo de sus versiones [en línea], Mayo 2013, [consultado 08 de Agosto de 2016]. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Pre-Historia de Android

Muchos usuarios creen que Android es un sistema operativo relativamente nuevo en comparación con otros como Symbian, sin embargo este tiene una historia mucho más grande de la que todos pensamos, ya que su existencia data del 2005 cuando era aún propiedad de Android Inc[6].

Su desarrollador en jefe y hasta hace poco ex vicepresidente de Android, había pasado ya por Apple y Microsoft cuando Google compro su empresa en Agosto de 2005, fecha en la cual Android Inc. ya contaba con 22 meses de vida.

Desde esta fecha comienza toda una época de ocultismo que dio pie al surgimiento de grandes rumores y mitos en torno a lo que Google se encontraba preparando en secreto, pero no fue hasta el 5 de Noviembre de 2007 en que el anuncio oficial de Android llego a los medios.

Android 1.0: Apple Pie

Lanzado el 22 de octubre de 2008, el HTC Dream también conocido por entonces como Google Phone fue el primer dispositivo en incorporar el sistema operativo de Google[7].

Este incluyo la primera versión de la Android Market, un Navegador Web, soporte para mensajes de texto SMS y MMS, discador para llamadas, y una aplicación para tomar fotos que no contaba con los ajustes de blancos y resolución.

Además se incluyeron algunas aplicaciones para dar soporte a los servicios de Google más populares como Google Maps con Latitude y Street View, Google Sync para sinronizar Gmail, Contactos y Calendario, Google Search, Google Talk y YouTube.

[6] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

[7] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

En la figura 3 se puede observar la pantalla principal de la versión 1.0 del sistema operativo Android.

Figura 3. Android 1.0

Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-1.0-Apple-Pie.png

Por otro lado, se incluyó una aplicación capaz de acceder a los servidores de correo de terceros con soporte para los estándares POP3, IMAP4, y SMTP.14 que era capaz de sincronizarse con aplicación de Gmail, Google y Google Calendar. Tampoco falto el reproductor de archivos multimedia que por entonces no era capaz de reproducir video

Por ultimo cabe destacar que Android 1.0 ofreció desde sus inicios el soporte para WiFi y Bluetooth, y el popular sistema de notificaciones que aparecen en la barra de estado, con la posibilidad de configurar alertas por ringtone, LED o vibración.

Android 1.5: Cupcake

Con la introducción de Android 1.5 el 30 de abril de 2009, empezamos a oír el nombre de Cupcake en referencia a la primera actualización importante del sistema operativo de Google[8].

[8] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Esta actualización le dio un poco más pulido a Android en algunas áreas pero sus principales características fueron la introducción del teclado virtual en la pantalla (todavía malo) y la posibilidad de insertar widgets.

En la figura 4 se puede observar la pantalla principal de la versión 1.5 del sistema operativo Android, denominada Cupcake, el cual incorpora como principal actualización la introducción del teclado virtual en pantalla y la posibilidad de insertar widgets.

Figura 4. Android 1.5 Cupcake

Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-1.5-Cupcake.jpg

Sin bien los Widgets ya venían implementándose en otros sistemas operativos móviles, como el Samsung TouchWiz, ninguno había sido tan convincente como la aplicación de estos por Android[9].

Claro que le tomó bastante tiempo tener una selección decente de widgets disponibles, pero que finalmente prendió y a decir verdad estos son uno de los grandes diferenciadores para Android, y una de las funciones en las que Google viene trabajando.

[9] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Además se incluyeron otras funciones bastante demandadas por los usuarios como copiar y pegar en el navegador, la grabación de vídeo y reproducción en formatos MPEG-4 y 3GP, la capacidad de subir videos a YouTube directamente, transiciones animadas entre las pantallas, la opción de auto-rotación, auto-sincronización y soporte para Bluetooth A2DP y AVRCP.

Android 1.6: Donut

Luego vino Android 1.6, también conocido como Donut. Esta versión fue en realidad una pequeña actualización, pero vino empaquetaba con un cuadro de búsqueda mejorado, cámara y aplicación de galería, y una renovada Android Market.

La barra de búsqueda, que inicialmente tenía sólo para buscar en la web, ahora le permitía al usuario buscar en otros lugares dentro del dispositivo, como marcadores, contactos, aplicaciones, y mucho más, directamente desde la pantalla principal. El cambio más notable en Donut fue el Android Market que en ese momento renovó su diseño con colores verde y blanco frente a la mirada gris y negro de las versiones anteriores[10].

La nueva tienda resulto un poco más amigable, rompiendo las solicitudes de pago, gratis, y "just in" mientras que también soportaba las capturas de pantalla de las aplicaciones seleccionadas, una característica muy solicitada. La aplicación de la cámara también vio una remodelación, y si bien no era la más bonita, era todavía un paso adelante respecto a lo que estábamos trabajando con anterioridad.

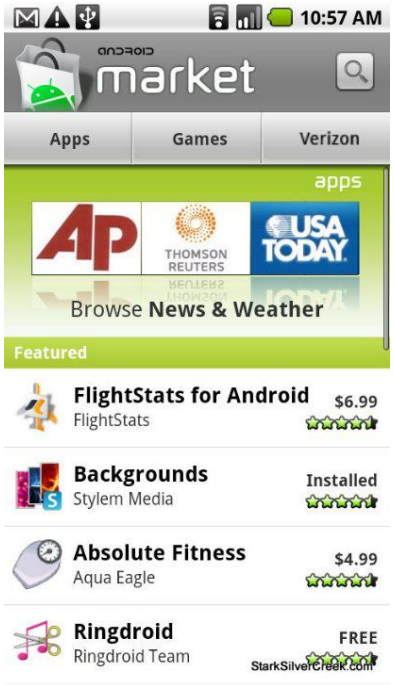
Ahora un usuario podía seleccionar fácilmente la grabación de vídeo sin salir de la aplicación, así como los ajustes que estaban ocultos en la parte izquierda de la pantalla en una barra de menú deslizante lateral. Según el sitio de desarrolladores de Android, la nueva aplicación de la Cámara era un 39% más rápida, y el tiempo entre disparo y disparo fue mejorado en un 28%. Lo único lamentable de la actualización de Android 1.6 fue que no muchos dispositivos la recibieron, y la mayoría como el Droide Eris o Hero saltaron directamente de Android 1.5 y Android 2.1[11].

[10] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

[11] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

En la figura 5 se puede observar la renovada Android market de la versión 1.6 del sistema operativo Android, siendo el cambio más notable de esta versión.

Figura 5. Android 1.6 Donut



Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-1.6-Donut.jpg

Android 2.0: Eclair

Lanzada el 26 de octubre del 2009, la actualización de Android 2.0 Eclair debuto en noviembre de ese mismo año en los Motorola Droid y se trató de un hito muy importante para la plataforma que dio paso al crecimiento exponencial y la atención de las masas[12].

Android Eclair nos sorprendió con su integración social permitiendo sincronizar los contactos de Facebook, y más tarde, Twitter, que le permitió a sus usuarios tener todos sus contactos de todas las redes sociales en un solo lugar.

[12] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Las imágenes de los contactos eran sacadas de una red social, permitiendo que prácticamente ninguno quedara con la foto en blanco, claro está, siempre y cuando formaban parte de una red concreta.

Eclair también trajo el menú de contacto rápido, permitiendo que al tocar la foto de un contacto se deslizara un menú mostrando todas las formas de comunicación con el mismo.

En cuanto a la interfaz de usuarios, también se realizaron mejoras que recayeron básicamente en las animaciones en las transiciones y su fluidez general.

Sin embargo esta actualización no se detuvo allí y nos trajo un puñado de funciones nuevas para la cámara, como el zoom digital, modo de escena, balance de blancos, efectos de color, y el enfoque macro. Sin embargo tendríamos que esperar hasta Froyo para que la aplicación de la cámara se puliera lo suficiente como para darnos la experiencia agradable que tenemos hoy.

Por otro lado, el teclado virtual de Android fue mejorado también con el soporte multitouch, y el diccionario de sugerencias ampliado, que incluía los nombres de nuestros contactos.

El navegador de Android también recibió una actualización, que refinó el aspecto general, sorprendiendo con la nueva función doble toque para el zoom, lo que permitía ampliar la foto sin la necesidad de que los usuarios tengan que depender exclusivamente de los botones más y menos en la parte inferior de la pantalla. La vista de favoritos se modificó también para apoyar las miniaturas, y el navegador comenzó a dar soporte para HTML5.

Finalmente, una de las mayores novedades de Android 2.0 fue Google Maps que recibió el servicio de navegación GPS gratuito, trayendo solo con el lanzamiento una reducción del precio de las acciones de Garmin del 16%, y de Tom Tom del 21%[13].

[13] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Android 2.1

Android 2.1 representa la segunda etapa en la evolución de Eclair con su introducción en el Nexus One. Esta trajo consigo los fondos de pantalla animados e interactivos, siendo ahora hasta 5 escritorios de serie en lugar de los cuales 3 que mostraban las versiones anteriores, que también estrenaban un nuevo modo de navegación en el que con una pulsación larga aparecían las miniaturas de todos ellos[14].

El Nexus One fue también el primer teléfono que extendiera las capacidades de voz existente encontrados en versiones anteriores de Android, dando al usuario la opción de traducir la voz en texto en cualquier campo de texto, así Android comenzaba a dar soporte a la búsqueda a través del reconocimiento de voz. Con esto se incorporó un botón del micrófono en el teclado, que permite hablar en lugar de escribir mensajes de correo electrónico, textos, buscar, y casi cualquier otra cosa que requiriera la escritura.

Android 2.1 también introdujo algunos efectos 3D en el sistema operativo entre los que podemos encontrar el icono para lanzar las aplicaciones, en lugar de la pestaña, que ahora volaban desde las esquinas para colocarse en la pantalla o para la galería de fotos, que ahora mostraba un nuevo aspecto. Ademas ahora basta con un golpecito en el lanzador de aplicación para revelar sus aplicaciones mientras que antes era necesario arrastra hacia arriba la pestaña.

La galería de fotos también vio una importante remodelación en 3D con la ayuda de CoolIris que logro una de las más bonitas aplicaciones integradas para el sistema operativo hasta la fecha.

Android 2.1 (Multi-touch)

A tan solo un mes del lanzamiento del Nexus One, el 12 de enero de 2010, Google lanzo una actualización para el dispositivo en la que se añadía la funcionalidad multitouch en todos los ámbitos del Nexus One, con excepción de las aplicaciones como Gmail[15].

[15] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

De este modo Mapas, fotos, y el navegador tenían soporte para la tan codiciada característica que los usuarios de iPhone habían tenido desde el primer día.

La actualización también añade Google Googles en la lista de aplicaciones pre-instaladas con una nueva una función que utilizaba la cámara para reconocer qué estaba viendo el terminal y lanzar su búsqueda en Internet.

Android 2.2 Froyo

Lanzada el 20 de mayo de 2010, Android 2.2 Froyo fue una de las actualizaciones que consagro al sistema operativo como la competencia de iOS 4 de Apple, dotando a los terminales Android con un notable incremento de la velocidad de todo el sistema, tanto en sus aplicaciones como en la navegación de Internet[16].

Froyo incorpora el motor de Java V8 y ofrece a los usuarios un aumento de velocidad gracias al compilador JIT que permite iniciar las solicitudes más rápido y mejorar el rendimiento general del sistema.

A su vez, Android 2.2 incluye la posibilidad de hacer tretheing, es decir, compartir la conexión 3G a través del wifi del teléfono con otros dispositivos, con la posibilidad de convertir tu móvil en un hotspot.

Una característica que los usuarios habían estado esperando durante años se hace realidad en Android 2.2, y se trata del soporte para Adobe Flash, tanto para el navegador de Internet como para reproducir contenidos multimedia a través del Flash Player.

Una vez que un dispositivo se ha actualizado para Froyo, el reproductor de Flash se puede encontrar en el Android Market, y tiene muy buenos resultados, demostrando así que la tecnología multimedia puede ejecutarse en un teléfono móvil.

[16] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Por ultimo cabe destacar otras características incluidas como la opción para mover las aplicaciones a las tarjeta microSD, una pantalla de inicio ligeramente modificada, nuevos widgets, más mejoras en la galería de fotos, un puñado de características de Exchange, así como la APIcloud-to-device que le permite enviar páginas web y direcciones de Google Maps desde tu ordenador al teléfono.

Android 2.3 Gingerbread

El 6 de diciembre de 2010 Google presentó de forma oficial Android 2.3 Gingerbread, una actualización que se materializaría con el lanzamiento del Nexus S[17].

Gingerbread incorporó una gran cantidad de novedades tanto a estético con una renovada interfaz de usuario con incrementos de velocidad y simpleza, y se preparó para la llegada de los smartphones de doble núcleo al cambiar al sistema de archivos EXT4 y de pantallas más grandes con el soporte para resoluciones WXGA y mayores.

Del lado del usuario, una de las características más notables fue el nuevo teclado virtual que simplificó la entrada de texto y permitió una edición más rápida gracias a la nueva disposición de las teclas y la función para corregir palabras ya ingresadas con sugerencias del diccionario o la opción de cambiarlas mediante voz.

Sin dudas la adquisición de BlindType tuvo que ver en este sentido y le permitió a Google implementar con características como permitir el deslizamiento al teclear, asistencia en la escritura, ajustes personalizados al estilo de escritura del usuario y el "multitouch key-chording", que permite al usuario ingresar rápidamente números y símbolos presionando Shift+ y ?123+, sin necesidad de cambiar los métodos de entrada manualmente.

Por otro lado, Android 2.3 incorporó toda la una gama de funciones que permiten manejar el dispositivo con la voz en lo que se denominó Voice Actions. Estas permitieron enviar mensajes, realizar llamadas, localizar lugares con el GPS, realizar búsquedas convencionales, escuchar música, mandar e-mails y muchos más.

[17] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Además esta actualización incorporó el soporte para llamadas VoIP/SIP, el protocolo basado en una interfaz inalámbrica con el que se podrán pagar diferentes cuentas desde el móvil llamado NFC y una gestión de la energía mejorada.

A su vez Gingerbread incluyó una nueva pestaña de "Running" dentro de Manage Apps que muestra la lista de aplicaciones activas junto con la capacidad y memoria que están consumiendo cada una de ellas[18].

Android 3.0: Honeycomb

El 22 de febrero de 2011 Google comenzó a desdoblar el sistema operativo con la actualización de Android 3.0 Honeycomb y su correspondiente SDK, algo que tendría poca vida debido al alto costo que supone mantener dos plataformas separadas[19].

Basado en el kernel 2.6.36.50 de linux, Honeycomb llego por primera vez en las tablets Motorola Xoom el 24 y sus principales características fueron una renovada interfaz de usuario con una nueva barra de sistema en la parte inferior de la pantalla que permitía el acceso rápido a notificaciones, estados y botones de navegación suavizados y el Action Bar que permitía el acceso a opciones contextuales, navegación, widgets y otros tipos de contenido desde la parte superior.

Además se agregó una nueva interfaz de contactos divida en dos paneles, algo que también calo en la interfaz de correo para simplificar la visualización y organización de mensajes, permitiendo a su vez seleccionar uno o más mensajes.

En la figura 6 se puede observar la pantalla principal de la versión 3.0 del sistema operativo Android, ejecutándose en una tablets, dentro de sus principales características se observa el acceso a notificaciones por medio de la barra de sistema ubicada en la parte inferior.

[18] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

[19] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Figura 6. Android 3.0 Honeycomb

Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-3.0-Honeycomb.png

Por otro lado la actualización de Honeycomb trajo un teclado re-diseñado para pantallas de gran tamaño y se simplificó la función multitarea con una opción que permitió acceder a las aplicaciones recientes que se mostraban en una lista con imágenes para reconocerlas fácilmente.

El navegador también tuvo cambios con la llegada de las pestañas que reemplazaron a las ventanas, la característica de auto completado al ingresar texto y un nuevo modo incógnito que permitió la navegación de forma anónima como el navegador web.

Por ultimo cabe mencionar el soporte para microprocesadores multi-núcleo, la aceleración de hardware, la posibilidad de encriptar todos los datos del usuario, y mejoras en el uso de HTTPS gracias a la incorporación de SNI[20].

[20] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

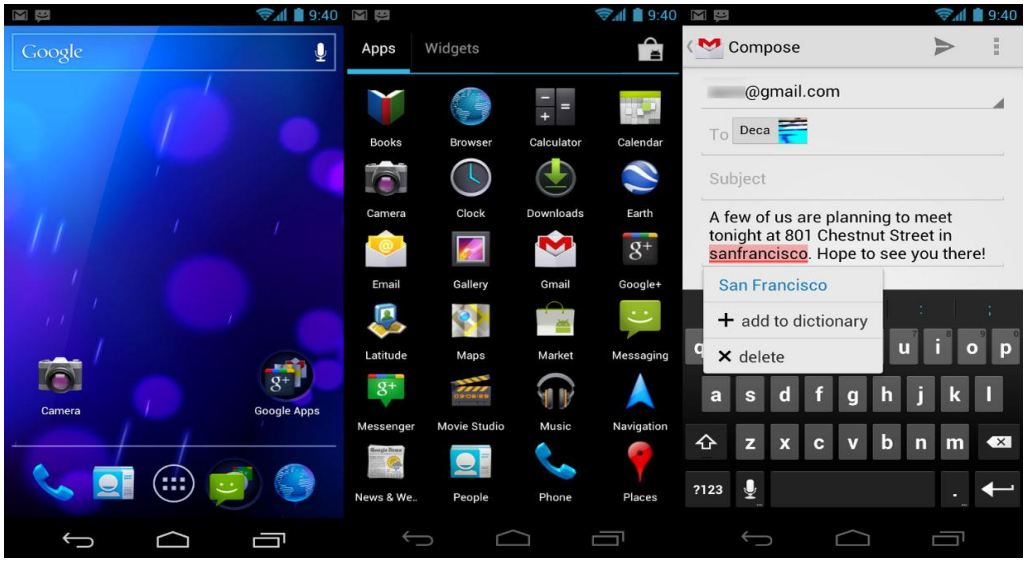
Android 4.0: Ice Cream Sandwich

La llegada de Android 4.0 Ice Cream Sandwich el 19 de octubre de 2011 significó un importante paso en la evolución de Android que no solo vio renovada casi por completo su interfaz de usuario con el nuevo diseño Holo, sino que volvió a integrar el sistema operativo en sus versiones para Tablets y Smartphone[21].

La nueva interfaz de usuario se mostró como la evolución y perfeccionamiento de las ideas de Android 3.0 dándole un poco de esa mirada limpia y futurista. Además Google construyó su propia fuente denominada Roboto y en lugar de botones de hardware, el sistema operativo ofreció sus propios botones virtuales de Atrás, Inicio, y los botones de aplicaciones recientes en la pantalla también para los Smartphone.

En la figura 7 se puede observar la pantalla principal de la versión 4.0 de Android, así mismo el dock de aplicaciones que incluyó una nueva sección para mostrar los widgets de forma separada donde son listados de forma similar a las aplicaciones y se simplificó la posibilidad de crear carpetas, con estilo de arrastrar y soltar.

Figura 7. Android 4.0 Ice Cream Sandwich

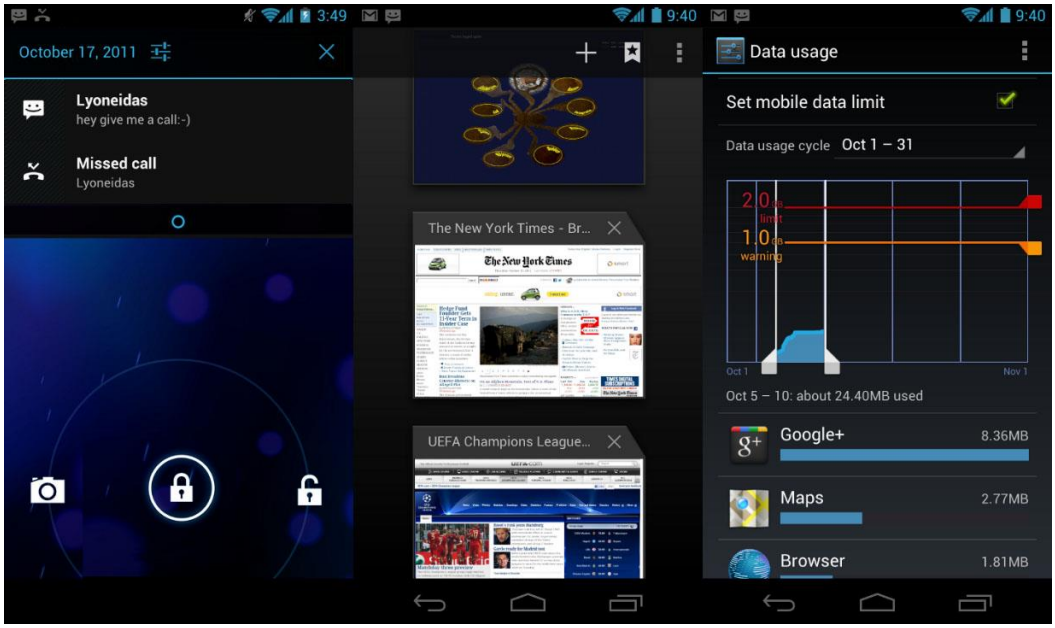


Fuente: http://androidzone.org/wp-content/uploads/2013/05/ics.jpg

[21] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

En la figura 8 se puede observar características adicionales de la versión 4.0 de Android, en la cual no todo tuvo que ver con el diseño en esta versión, Google incluyo algunas mejoras que hoy usamos a diario como la posibilidad de acceder a las aplicaciones directamente desde la pantalla de bloqueo y Google Chrome como navegador por defecto que permitió abrir hasta a 15 pestañas y realizar la sincronización automática con los marcadores de la versión de escritorio. Otra delas grandes novedades fue el desbloqueo facial, característica que permite desbloquear los Smartphone usando el software de reconocimiento facial, algo que luego sería muy criticado por su dudosa seguridad; y una nueva sección de que nos permitió controlar de forma nativa el consumo de datos de todo el equipo y configurar límites para evitar exceder nuestro plan, así como cerrar aplicaciones que están usando datos en segundo plano.

Figura 8. Características Android 4.0



Fuente: http://androidzone.org/wp-content/uploads/2013/05/ICS-2.jpg

Otras aplicaciones nativas mejoradas fueron la cámara que ya no mostró retardo en el obturador y permitió realizar ajustes sobre el time-lapse, seleccionar el modo panorámico y hacer zoom durante la grabación de video que ahora ascendía a los 1080p para dispositivos con Android de serie. Continuando con las características multimedia, Google incluyó de serie una aplicación para la edición de fotos y mejoró la galería con un nuevo diseño y organización por persona y localización[22].

[22] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Además se mejoró la aplicación People para integrarla con las redes sociales y permitir la actualización de estados e imágenes en alta resolución, se incorporó de forma nativa la posibilidad de tomar screenshots presionado los botones de bloqueo y de bajar volumen y se mejoró la funcionalidad copiar-pegar.

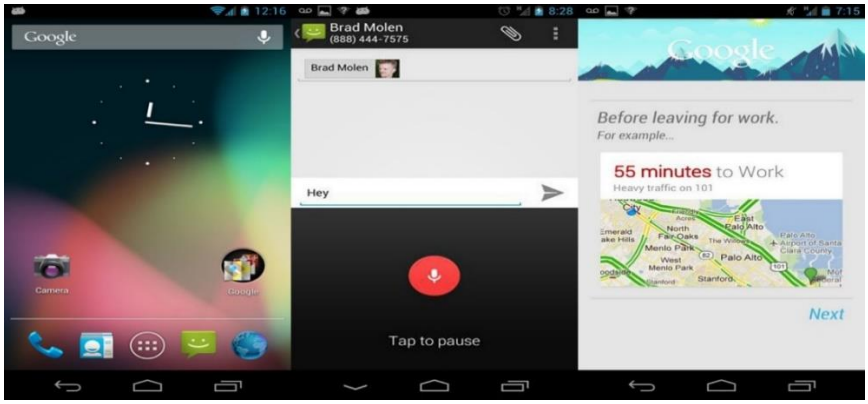
Android 4.1: Jelly Bean

Y así es como llegamos a los tiempos modernos donde Jelly Bean aún resuena como la última actualización importante del sistema operativo de Google que dicho sea de paso, fue presentada el 27 de junio de 2012 y llegó al mercado el 13 de julio con el Nexus 7, el primer Tablet de Google[23].

El objetivo primordial de Android Jelly Bean fue mejorar la estabilidad, funcionalidad y rendimiento de la interfaz de usuario, para lo cual se implementó el núcleo de Linux 3.0.31 y una serie de mejoras en lo que se llamó Project Butter que permitió aumentar hasta 60 FPS las transiciones en la interfaz de usuario, dando una experiencia realmente fluida.

En la figura 9 se puede observar características representativas de la version 4.1 de Android, en la Google mejoró notablemente la barra de notificaciones, una de las características que distinguió a Android desde sus inicios. Esta ahora ofrece una mayor integración ya que permite realizar más acciones desde esta, como realizar llamadas o acceder a diferentes opciones y mostrar información proveniente de las aplicaciones que lanzan la notificación.

Figura 9. Android 4.1 Jelly Bean



Fuente: http://androidzone.org/wp-content/uploads/2013/05/JB-1.jpg

[23] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Google Now fue otra de las grandes características de esta actualización, que junto al Knowledge Graph y la búsqueda por voz mejorada permitió superar ampliamente a Siri, el asistente de Apple, ya que fue capaz de reconocer y predecir nuestros intereses en función del historial de búsquedas.

Los widgets fueron desde los inicios de Android una de sus características distintivas y en esta actualización recibieron cierta atención, ya que se ajustan automáticamente al tamaño de la pantalla si son demasiado grandes para caber en ella

Finalmente otra de las mejoras estuvieron centradas en la entrada de texto, donde, por un lado fue mejorada la entrada por voz que ya no requirió tener una conexión a internet para utilizarla, dado que el intérprete se encuentra dentro del dispositivo; y el teclado predictivo que reconoce hasta cuatro idiomas y es capaz de adivinar la próxima palabra que vamos escribir.

Android 4.2

A tan solo tres meses del lanzamiento de Android 4.1, Google lanzó otra importante actualización aún bajo el nombre de Jelly Bean. Se trató de Android 4.2 que trajo Photo Sphere entre sus principales novedades, una aplicación que nos permite tomar imágenes panorámicas en el plano horizontal y vertical[24].

Pero ello no fue todo, Android 4.2 también trajo lo que hoy conocemos como Gesture Typing, una nueva función similar a Swype que nos permite escribir deslizando el dedo sobre las letras y levantando después de cada palabra. Ademas el teclado anticipa y predice la siguiente palabra, para que pueda terminar las frases enteras con sólo seleccionar las palabras sugeridas, lo cual acelera enormemente la escritura.

Otra de las funciones importantes que llegaron con esta actualización, fue el soporte para múltiples usuarios que pueden tener cada uno su propia pantalla de inicio, fondos, widgets, aplicaciones y juegos incluso con sus propias puntuaciones y niveles.

[24] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Por otro lado, la barra de notificaciones continuó evolucionando gracias a la incorporación de lo que Google llamó Quick Settings, una cuadrícula dividida por varias secciones que nos permiten acceder a las configuraciones de la pantalla, conectividad, sonido, rotación, vibración, volumen, etc; y las notificaciones accionables para más aplicaciones que permiten responder desde la propia barra sin lanzar la aplicación directamente.

Finalmente cabe destacar la posibilidad de incluir widgets en la pantalla de bloqueo, la posibilidad de deslizar con el dedo para ir directamente a la cámara y el soporte para pantallas inalámbricas.

Android 4.3

El 24 de julio de 2013 Google presentó Android 4.3 Jelly Bean, una pequeña actualización que introdujo algunas mejoras de seguridad y rendimiento en el sistema operativo para darle mayor fluidez. De este modo se han introducido mejoras en la representación de formas redondeadas y texto, y la velocidad en que se muestran las imágenes así como el soporte para OpenGL ES 3.0, Bluetooth Smart (o Bluetooth LE) y optimizaciones en vsync timing y el triple buffering[25].

La aceleración de hardware 2D ahora optimiza el flujo de comandos de dibujo convirtiéndolo en un formato GPU más eficiente y reorganizando y uniendo operaciones de dibujo, lo que se suma al procesamiento multiproceso que le permite al procesador utilizar hilos múltiples a través de los diferentes núcleos del CPU en determinadas tareas. En la figura 10 se puede observar la pantalla principal de la version 4.3 del sistema operativo Android.

Además, Android 4.3 ha incorporado el soporte para perfiles restringidos que permite crear ambientes separados para cada usuario en el mismo dispositivo, haciendo que el administrador sea capaz de determinar qué acciones puede realizar cada usuario como descargar aplicaciones de Google Play, realizar compras in-app, jugar a determinado juegos, acceder a ciertas Apps, etc.

[25] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Figura 10. Android 4.3 Jelly Bean

Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-4.3-728x503.jpg

También cabe destacar el nuevo sistema de notificaciones que le permite a las aplicaciones acceder a todas las notificaciones y mostrarlas en la forma que quieran e incluso enviándolas a dispositivos cercanos conectados por Bluetooth.

Pero eso no es todo, Android 4.3 Jelly Bean también añade un nuevo marco de DRM modular, soporte para codificación VP8 integrado, mejoras en el soporte RTL, mejoras en seguridad gracias a SELinux, Google Play Games, mejoras en la entrada de texto, nueva interfaz de la cámara, autocompletado al marcar un número de teléfono, mejor gestión de la batería, y nuevas versiones de las GApps como Gmail, Hangouts, etc.

Android 4.4: KitKat

Lanzado oficialmente el 31 de Octubre de 2013 junto con el LG Nexus 5, Android 4.4 KitKat introdujo una reducción en el tamaño del sistema operativo junto con algunos cambios estéticos menores manteniendo la interfaz Holo[26].

Los cambios que se notaron a primera vista fueron el incremento del tamaño de los íconos y la condensación del texto para una visión más clara y simple. Otro detalle fue la transparencia de la zona de notificaciones que antes era negra, ahora fusionada al resto de la pantalla. Otra funcionalidad añadida fue la del famoso "OK Google" reconociendo nuestra voz una vez desbloqueado el dispositivo. Sumado a

[26] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

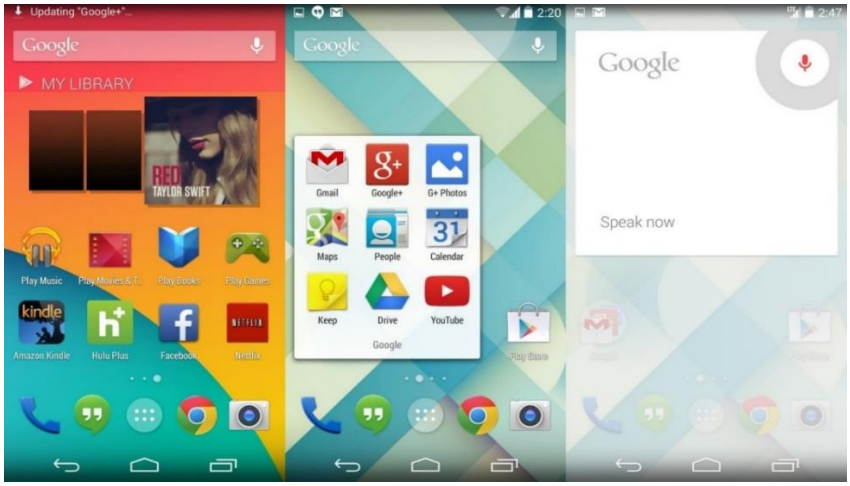
esto, tanto la barra de navegación como la de notificaciones desaparecerían en ciertas aplicaciones para dejarnos ver en pantalla completa.

En cuanto al apartado del rendimiento, Android 4.4 KitKat trajo la implementación de zRAM, en donde se optimizaba el rendimiento para dispositivos con memoria de 512MB de RAM y de esta manera incluir las gamas bajas de los mercados emergentes. Cabe recordar que por aquel entonces GingerBread (Android 2.3) era la versión más utilizada de Android y esto se traducía en serias complicaciones para Google que trataba de impulsar a los fabricantes a incorporar sus nuevas funcionalidades y servicios como así también una experiencia de usuario más fluida que sólo se encontraba en dispositivos con versiones más modernas y de especificaciones más elevadas.

Sumado a esto, Android 4.4 KitKat sustituyó algunos elementos de la interfaz anterior de azul a blanco para darle un aspecto más limpio, las horas del reloj ya no se mostrarían como números en negrita sino de forma más fina tanto las horas como los minutos y un nuevo marco de transiciones y efectos visuales dentro de la interfaz Holo. Dentro de los cambios estéticos se creó un widget para la reproducción de música que se podía controlar desde la pantalla de bloqueo sin la necesidad de ingresas a la interfaz principal.

En la figura 11 se puede observar características relevantes en la versión 4.4 del sistema operativo Android, como el widget para reproducción de música y el reconocimiento de la voz.

Figura 11. Android 4.4: KitKat



Fuente: http://androidzone.org/wp-content/uploads/2013/05/Android-Kit-Kat-Screenshots.jpg

En esta versión se implementó la funcionalidad para que Hangouts sirviera como el servicio de mensajería SMS oficial de Google. Recordemos que esta aplicación se había lanzado poco antes para reemplazar a Google Talk, que era el servicio de mensajería de la firma. Sumado a esto se incorporó un editor de fotos dentro de la galería que nos permitiría recortar nuestras imágenes, ponerles filtros, marcos, ajustarles el brillo y contraste sin la necesidad de aplicaciones de terceros.
En esta versión también se introdujo la implementación de manera opcional para desarrolladores y entusiastas de lo que sería el futuro, la máquina virtual ART que luego suplantaría al Dalvik en versiones posteriores. También se desactivaría el acceso de aplicaciones de terceros a las estadísticas de la batería y se moverían los monitores de actividad de red y señal al menú de ajustes rápidos.

Android 5.0: Lollipop

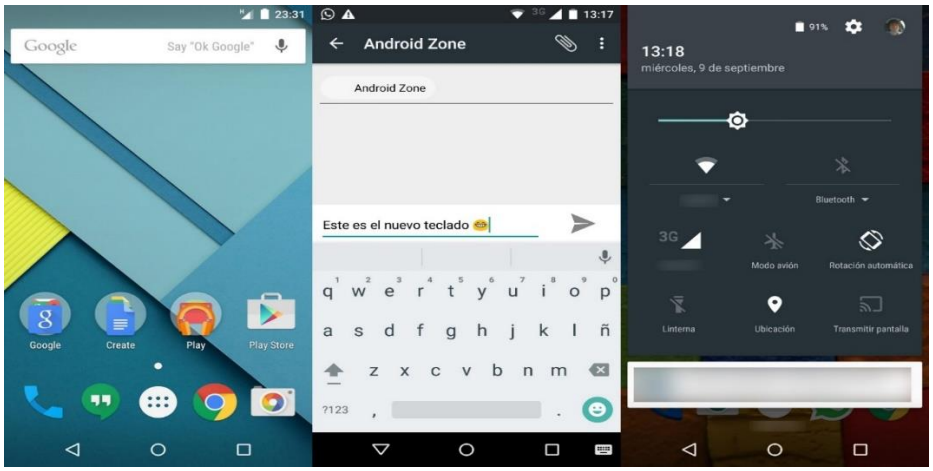
Lanzado el 12 de Noviembre de 2014 junto con el Nexus 6 y el Nexus 9, Android 5.0 Lollipop presentó, dentro de sus cambios, una interfaz de usuario renovada con una serie de innovaciones y nuevas funcionalidades pero lo que se destacó fue su nuevo diseño, el Material Desing que hasta el día de hoy sigue vistiendo el sistema operativo de Google[27].

La idea de Google con Material Desing fue la de renovar la estética de la interfaz de usuario de manera drástica, como lo hizo con Ice Cream Sandiwich y su interfaz Holo. Para ello buscó colores llamativo, un diseño intrépido y una interfaz de usuario donde todas las animaciones y objetos salen de algún lado de la pantalla, como si todo formase parte de un conjunto que es el sistema operativo. En la figura 12 se puede observar algunas características de la version 5.0 del sistema operativo Android, el cual incluye la renovación estética de un nuevo teclado en donde las letras no se dividen por casilleros sino que todas forman parte de un todo, siguiendo con la filosofía estética de este diseño. Sombras detalladas, mucha iluminación y animaciones fluidas componen Material Desing.

Pero no todo fueron renovaciones estéticas en Android 5.0 Lollipop ya que dentro de sus características de funcionamiento también se destaca las nuevas formas de controlar el consumo de batería y las notificaciones. Con respecto a la batería, Lollipop extiende la vida útil del dispositivo hasta 90 minutos con Project Volta, lo cual se puede comprobar en la configuración de la batería del dispositivo.

[27] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Figura 12. Android 5.0 Lollipop



Fuente: http://androidzone.org/wp-content/uploads/2013/05/lollipop-screen.jpg

En cuanto a las notificaciones, Lollipop nos trae nuevas formas de controlar la forma en la que nos aparecen y cómo las recibimos gracias a los perfiles que se configuran por hora y por aplicaciones. En una determinada franja horaria, podremos establecer la prioridad de las notificaciones que querremos recibir, incluso las llamadas entrantes. Sumado a esto, ahora las notificaciones aparecen en un sólo lugar para un acceso más rápido y sencillo.

Otra modificación importante fue la sustitución del Dalvik por parte de ART (Android Runtime), la nueva máquina virtual de Google diseñada para entregar un mejor rendimiento de las aplicaciones. Sumado a esto tenemos los perfiles que nos permite establecer el contenido del dispositivo al cual tienen acceso cada uno, ya sean niños, invitados u otros personalizados. Con los perfiles, el usuario invitado podrá acceder a las aplicaciones básicas como el navegador y la cámara, pero no podrá acceder a los datos personales del usuario original del teléfono o tableta si así no lo deseamos.

La lista de adiciones se completa con varias otras funcionalidades como soporte para procesadores de 64 bit, vectoriales dibujables, soporte para vistas previas de impresión, una nueva pantalla de desbloqueo que ahora ya no soporta widgets para una visual más limpia y sencilla, entrada y salida de audio vía USB, 15 idiomas nuevos y varias otras mejoras no tan relevantes.

Android 5.1

Introducido el 9 de Marzo de 2015, Android 5.1 Lollipop trajo la capacidad de unirse a redes WiFi y de emparejarse con dispositivos Bluetooth desde los ajustes rápidos para reducir la cantidad de pasos, soporte para múltiples tarjetas SIM y llamadas de voz en Alta Definición con otros equipos que cuenten con la misma versión del sistema operativo[28].

Sumado a esto, Android 5.1 Lollipop añade protección de dispositivos bloqueándolos si estos son robados o extraviados hasta que se inicie nuevamente la sesión con una cuenta de Google, incluso si el mismo es restablecido a la configuración de fábrica. También se añaden mejoras de estabilidad y rendimiento junto con otras correcciones menores.

Android 6.0 Marshmallow

Tras meses de misterio suponiendo a qué haría referencia la "M" con la que nombraban el nuevo sistema operativo de Google, finalmente se supo que sería por Marshmallow (Malvavisco). Luego de meses de espera, finalmente Google lanzó Android 6.0 y junto con los nuevos dispositivos Nexus de LG y Huawei[29].

En esta nueva actualización hay cambios muy interesantes que mejoran el rendimiento y la estabilidad del sistema operativo. Entre las principales novedades se destacan Google Now on Tap, permisos de aplicaciones caso por caso, mejoras en la gestión de la batería gracias a Doze, mejoras en las funciones copiar, cortar y pegar, soporte para huellas dactilares, nuevo USB Tipo-C y Chrome funcionando dentro de otras aplicaciones, entre otras.

El 28 de Mayo de 2015 fue lanzada la primera de las tres previews que Google lanzara durante el año en las cuales se pueden observar mejoras en el modelo de permisos. Ahora las aplicaciones ya no conceden automáticamente todos los permisos al momento de la instalación cambiando a un sistema "opt-in", donde los usuarios aceptarán o no que la aplicación acceda a diversas partes de nuestro dispositivo tales como la cámara o los contactos en el mismo momento en el que el programa lo requiera. Las primeras Apps en tener este sistema serán las que forman parte del núcleo de Android con su SDK.

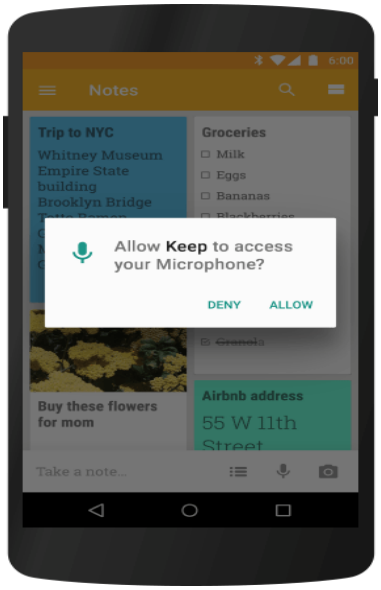
[28] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

[29] Ibíd. Disponible en Internet: http://androidzone.org/2013/05/historia-de-android-la-evolucion-a-lo-largo-de-sus-versiones/

Sumado a esto, como comentamos, una de las más novedosas y buscadas características añadidas es el soporte nativo para el reconocimiento de las huellas digitales, algo cada vez más popular en los dispositivos de alta gama que se está trasladando a la gama media también. Ahora, mediante nuestras huellas dactilares, podremos autenticar nuestra cuenta en el Play Store o Android Play con sólo deslizar nuestro dedo por el dispositivo.

En la figura 13 se puede observar una característica importante de la versión 5.0 de Android, la cual consiste en mejoras en el modelo de permisos, en donde el usuario puede decidir que una aplicación acceda a diversas partes de nuestro dispositivo.

Figura 13. Android 5.0 Lollipop



Fuente: https://www.android.com/intl/es_es/history/#/marshmallow

También tendremos “Doze”, un nuevo sistema de administración de la energía que se complementará con el anterior “Project Volta” para una mejora en la duración de la batería del dispositivo. “Doze” administrará de forma más eficiente las actividades que se ejecutan en segundo plano cuando el sistema operativo detecta que el dispositivo no está siendo tocado físicamente.

Android6.0 Marshmallow también será compatible con el ya famoso y muy bienvenido puerto USB tipo C, el cual es simétrico y se puede conectar de ambos lados. Pero no sólo traerá comodidad a la hora de conectar el dispositivo sino que permitirá una carga hasta 5 veces más rápida.

5.1.3 Seguridad en Android

Phil Schiller, vicepresidente de marketing a nivel mundial de Apple en el año 2013, puso en entredicho la seguridad de Android utilizando un estudio de la compañía F-Secure.

"Estarán seguros fuera de allí". Esta es la frase que utilizó Phill Schiller para criticar la seguridad de Android en Twitter. A la hora de realizar esta crítica, Phill Schiller se basó en el último informe de amenazas móviles de F-Secure en el que afirma que las amenazas para Android continúan incrementándose.

Así, y según el estudio, el 96 por ciento de las nuevas familias y variantes del malware para Android fueron descubiertas en el último trimestre de 2012. Esto supone que en ese trimestre se doblaron los resultados del trimestre anterior en el que, a su vez, ya se obtuvieron cifras récord. Además, una gran parte de esas amenazas era Premium SMS (utilizan los SMS para obtener beneficios).

En el año 2012, el 79 por ciento de todas las amenazas para dispositivos móviles tenían a Android como objetivo, frente al 0,7 por ciento de iOS. F-Secure atribuye el incremento de las amenazas para Android al hecho de que ésta es la plataforma que más está creciendo. En 2012 la cuota que alcanzó Android fue del 68,8 por ciento.[30]

La empresa de seguridad móvil Zimperium ha descubierto el que, probablemente, sea el fallo de seguridad en Android más grave de su historia, afectando a todos los dispositivos por igual y cuyo fix probablemente no llegue ni a la mitad de ellos.

Cada cierto tiempo nos llega noticia de que una nueva vulnerabilidad en Android, y cuyo aspecto más peligroso no es la vulnerabilidad en sí, sino el tiempo que tarda en ser corregido, debido a la usual debacle en actualizaciones en el sistema operativo de Google. Y esta vez, la vulnerabilidad descubierta no es ninguna excepción, como hemos podido ver a través de NPR, la Radio Nacional Pública de EEUU, con una ejecución absurdamente simple pero que potencialmente podría ser muy peligroso para nosotros.

[30] PHIL SCHILLER. La inseguridad de los dispositivos Android [en línea]. Marzo 2013, [consultado 08 de Agosto de 2016]. Disponible en Internet: http://www.pcworld.com.mx/Articulos/28095.htm

Descubierta dicha vulnerabilidad por Joshua Drake, investigador de seguridad en Zimperium (una reputada firma de seguridad móvil), entre el pasado mes de abril y mayo, ésta sería a trav és de un vídeo corto (como los que enviamos a diario a través de WhatsApp o Telegram) con malware en su interior, el cual se aprovecharía del exploit en Android en el momento de llegar al Smartphone de la víctima. "Pasaría incluso antes de oír el sonido del mensaje recibido. Eso es lo que lo hace tan peligroso", afirma Drake.

Drake también afirma que aunque el riesgo es mayor en Hangouts que en la App de mensajería por defecto, debido a que Hangouts procesa el vídeo para que el usuario no tenga que hacerlo poniéndonos así en riesgo, en ningún momento hace falta abrir el archivo para que suframos el exploit: ya con recibirlo el Smartphone se encuentra en peligro. Además, lo verdaderamente preocupante de esto es que, a pesar de que Google ya recibió y aceptó el fix enviado por el propio Drake, el problema es el de siempre: como hacer llegar ese fix a los más de mil millones de dispositivos Android existentes.

Que sólo un 50% de dispositivos Android como máximo recibirán el fix es suficiente para ver que este problema de updates ha de ser corregido.

"Siendo optimistas, entre el 20% y el 50% de dispositivos Android recibirán el fix" afirma Drake, y este dato es demoledor, poniendo en evidencia una vez más el descontrol existente para que las versiones actualizadas lleguen a todos los Android por igual, y cuyo principal culpable no es Google, sino las OEM encargadas de portar sus versiones customizadas, así como las operadoras que frenan aún más el proceso. En cuanto a la cuestión de si estamos en riesgo o no, Drake cree que los hackers no están haciendo uso de esta vulnerabilidad, al menos de momento. Esperemos que los fabricantes y Google se pongan de acuerdo para alcanzar un acuerdo cuanto antes, porque esto nos pone en riesgo a todos.[31]

Seguridad de Android en 2014: más amenazas pero más seguros

Cada vez la seguridad de nuestros Smartphone y Tablets con Android es más y más importante: nuestros dispositivos tienen más datos sensibles sobre nosotros, y las amenazas que quieren hacerse con esos datos van en aumento. Por suerte, Google mejora mucho en este aspecto, y hoy analizamos el informe que el equipo de seguridad de Google ha presentado, analizando todo lo que ha ocurrido en 2014 en materia de seguridad.

[31] MERCHAN, Javier. Este es el fallo de seguridad en Android más grave hasta la fecha [en línea]. Julio de 2015, [consultado 08 de Agosto de 2016]. Disponible en Internet:http://hipertextual.com/2015/07/fallo-de-seguridad-en-android-mas-grave-hasta-la-fecha

Lo cierto es que este informe que se cita es muy extenso, 44 páginas llenas de cifras y estadísticas que sirven para hacernos a la idea de cuál es la salud de la seguridad en nuestros androides, pero hay algunos datos en los que merece la pena pararse y analizar con detenimiento: estas son las cifras de la seguridad en Android durante el año pasado[32].

En la figura 14 se puede observar las amenazas de seguridad más destacadas en el año 2014, según informe del equipo de seguridad de Google.

Figura 14. Las amenazas de 2014: SSL, Fake ID y más

Fuente: http://www.elandroidelibre.com/2015/04/seguridad-de-android-en-2014-mas-amenazas-pero-mas-seguros.html

El año pasado ha estado lleno de amenazas de seguridad, y para muestra sólo tenemos que acudir a nuestra sección de seguridad: han salido varias amenazas preocupantes a lo largo del año que nos han puesto en alerta, y que incluso nos han

[32] PEREZ, David. Seguridad de Android en 2014: más amenazas pero más seguros [en línea]. Abril de 2015, [consultado 08 de Agosto de 2016]. Disponible en Internet: http://www.elandroidelibre.com/2015/04/seguridad-de-android-en-2014-mas-amenazas-pero-mas-seguros.html

hecho profundizar en el funcionamiento de las aplicaciones que nos prometían espiar el Android que quisiéramos. ¿Pero cuáles han sido las amenazas de seguridad que más han destacado en 2014?

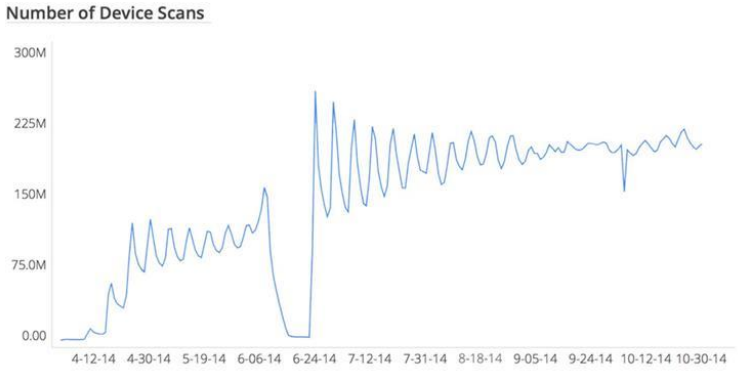
- **Vulnerabilidades en el SSL:** El archiconocido Heartbleed puso en jaque a todo Internet, y Android no llegó a ser una excepción, aunque sólo Android 4.1.1 Jelly Bean se llegó a ver afectado.

- **Vulnerabilidades en Android:** Android por sí mismo tampoco se ha visto exento de fallos: los efectos de FakeID en Android KitKat se han dejado sentir, y ha sido una de las causas por las que Google ha mejorado sus protocolos de protección.

- **Vulnerabilidades en los fabricantes:** Como ya sabemos, la integración de Android es trabajo de los fabricantes: no son parte estricta de la plataforma de código abierto, pero siguen siendo una parte importante de la seguridad de Android. La llegada de SELinux en modo completo con Android 5.0 ha sido una de las grandes soluciones del problema, además de monitorizar las aplicaciones con más detenimiento[33].

En la figura 15 se puede observar el número de amenazas de seguridad que han sido dirigidas al sistema operativo Android, obligando a Google ha implantar diferentes métodos de seguridad

Figura 15. Mejoras de seguridad en 2014: muchas y variadas



Fuente: http://www.elandroidelibre.com/2015/04/seguridad-de-android-en-2014-mas-amenazas-pero-mas-seguros.html

[33] Ibíd. Disponible en Internet: http://www.elandroidelibre.com/2015/04/seguridad-de-android-en-2014-mas-amenazas-pero-mas-seguros.html

Como vemos, no han sido pocas amenazas de seguridad las que han amenazado a Android de una forma u otra, aunque todo esto ha hecho que Google haya implantado diferentes métodos de seguridad y mejorado los existentes. ¿Pero cuáles son esas medidas, exactamente?

Mejoras de las funciones de seguridad de Android: Cifrado completo del dispositivo, autenticado mejorado, uso de perfiles múltiples, SELinux en su versión estricta… las actualizaciones han traído muchas mejoras de seguridad, la pega es que sólo las disfrutan aquellos usuarios que puedan actualizar a las versiones que incluyen estas funciones.

Parches destinados a arreglar el código de AOSP: Durante 2014 han existido 79 vulnerabilidades conocidas: 0 críticas, 30 de alta importancia, 41 de importancia moderada y 8 de poca importancia. 73 vulnerabilidades ya han sido resueltas con aportaciones a AOSP, mientras que las 6 vulnerabilidades restantes se resolverán en la próxima actualización a AOSP.

Mejoras en la seguridad de Google Play: Hay más de mil millones de dispositivos protegidos con Google Play, y todo esto es gracias a los Google Play Services, necesarios para acceder a Play Store. Verificar aplicaciones que instalamos fuera de Google play, revisión de aplicaciones en Play Store, poder mejorar la seguridad sin actualizaciones del sistema, avisos directos a los desarrolladores.

¿Cuál es el futuro de Android en materia de seguridad?

En cualquier caso, muchas de estas vulnerabilidades sólo han sido explotadas por investigadores para comprobar la seguridad de Android, y el nivel de amenazas es muy bajo: menos del 1% de dispositivos Android en 2014 han tenido alguna aplicación potencialmente maliciosa, y menos del 0.15% de usuarios que sólo descargan de Google Play se han visto afectados por alguna aplicación maliciosa.

Google quiere transmitirnos seguridad con estos datos, afirmando que sus sistemas de control funcionan y que no existe ningún peligro para los usuarios de Android que jueguen bajo las reglas que imponen los chicos de Mountain View, incluyendo los dispositivos rooteados por los usuarios. Aun así, todavía hay mucho que mejorar, y esperemos que 2015 sea un mejor año para la seguridad.

5.14 SERIE ISO 27000

Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Existen versiones traducidas al español aunque hay que prestar atención a la versión descargada. El original en inglés y su traducción al francés en su versión de 2014.

ISO/IEC 27001

Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.[34]

ISO/IEC 27002

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR).

[34] ISO 27000. El portal de ISO 27001 en Español. [en línea]. [consultado el 27 de Octubre de 2016]. Disponible en http://www.iso27000.es/iso27000.html.

5.2 MARCO CONCEPTUAL

Se han analizado situaciones que se presentan al utilizar los dispositivos móviles dentro de la Policía Nacional, y se debe adelantar labores de prevención en el campo de seguridad de la información para los Smartphone, implementar políticas de seguridad de la información que conlleven a proteger los datos e información crítica de la institución.

Así mismo debemos tener definido que un Smartphone es un tipo teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional.

Es importante identificar los sistemas operativos utilizados por los Smartphone, los cuales se encargan de administrar la operación entre el hardware y software del dispositivo, creando una experiencia de usuario agradable permitiendo la instalación de aplicaciones, a continuación se describen los sistemas operativos para Smartphone más preferidos por los usuarios, de acuerdo a las ventas registradas en el año 2015:

En el primer lugar se encuentra Android, sistema operativo de Google diseñado con ideología de código abierto, con un dominio en el mercado del 78% en el último trimestre del año 2015, en segundo lugar se encuentra el iOS, perteneciente a la multinacional Apple orientado a dispositivos móviles táctiles como iPhone, iPod, iPad, con un dominio en el mercado de 18%, en tercer lugar Windows Phone, con una presencia en el mercado del 3%.

Al igual Android es un sistema operativo basado en el kernel de Linux diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes o tabletas, y también para relojes inteligentes, televisores y automóviles, inicialmente desarrollado por Android Inc.

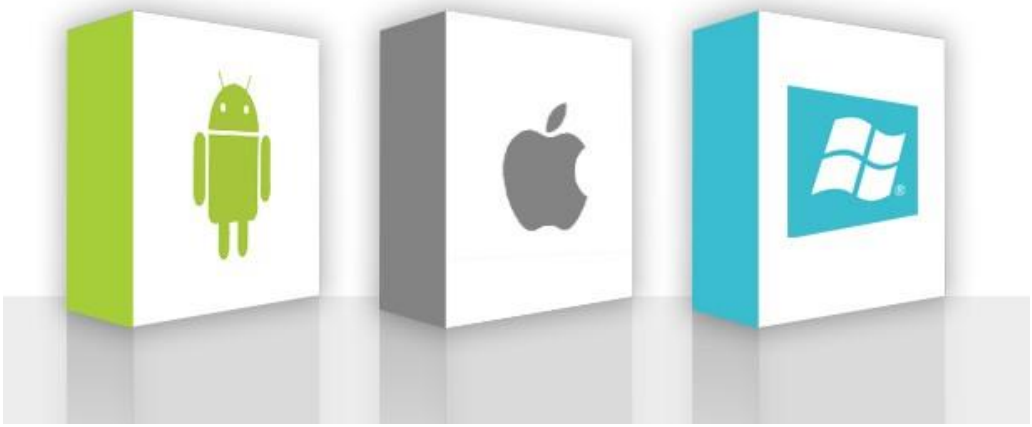
Los dispositivos móviles hacen ya parte de nosotros mismos, almacenan nuestros contactos e información personal y laboral, es por esto que debemos cuidar y proteger lo que almacenamos en ellos.

No solo basta con aplicar pequeñas precauciones de seguridad, como instalar un antivirus, cuidarnos de las estafas, proteger nuestro móvil en caso robo o pérdida,

conectarnos a redes wifi abiertas y/o públicas o por medio de Bluetooth, debemos ir más allá entender que la seguridad en dispositivos móviles es mucho más que estas precauciones.

En la figura 16 se puede observar sistemas operativos más predominantes del mercado para el año 2015, encontrándose en primer lugar el sistema operativo Android.

Figura 16. Mejores Sistemas Operativos Móviles año 2015



Fuente: http://www.tecnologiaparaelmundo.com/wp-content/uploads/2015/08/sistemas-1.jpg

Las tecnologías móviles se componen de diversos tipos de dispositivos los cuales comparten mismas características y funcionalidades, estas traen consigo un desarrollo de servicios nuevos y creación de nuevos mercados, como desarrollo de aplicaciones para dispositivos móviles.

Los Smartphone en sus características principales que incorporan hoy en día, es la capacidad de ejecutar programas y aplicaciones añadiendo así funcionalidad al dispositivo móvil, permite descarga directa de diversos tipo de ficheros.

Hace años atrás los teléfonos móviles no se encontraban vulnerables a muchos riesgos de seguridad al no interconectarse a la red, en la actualidad la mayoría incluye mecanismos para que puedan estar conectados y descargar contenido de internet, leer correo electrónico, etc., por lo tanto, enfrentarse a las iguales amenazas para computadores.

Existen diversas amenazas y vulnerabilidades que se pueden asociar a los dispositivos móviles que llegan a poner en riesgo la seguridad del mismo dispositivo como la información que gestionamos.

Con la aparición de nuevas plataformas de tecnología para móviles, aplicaciones y servicios, así como conexión a través de redes abiertas y privadas, dejan abiertas puertas a novedosas investigaciones de seguridad, las cuales se centran en descubrir vulnerabilidades en estos entornos.

Siempre existirá amenaza de acceso físico a los dispositivos móviles por parte de intrusos, así sea por corto periodo de tiempo, y es uno de los vectores de ataques principales, como para el acceso a la información que se almacena, como para instalación de software de espionaje o malicioso.

Al igual debido por su tamaño y portabilidad y a su uso frecuente fuera de la oficina, siempre existirá la amenaza de que el dispositivo móvil sea robado o se pierda de forma permanente, llevando así a pérdidas económicas notables vinculadas a la terminal y de la información.

Los usuarios de telefonía móvil se han incrementado en los últimos años, debido a que se manejan una gran variedad de aplicaciones que se pueden instalar. Pata garantizar un buen uso y correcto de funcionamiento de los dispositivos, es muy importante estar informados sobre ventajas y desventajas con respecto de las prestaciones que ofrece el teléfono.

5.3 MARCO LEGAL

5.3.1 Ley 1273 de 2009. Ley de delitos informáticos.

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[35]

[35] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05 enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos. En: Diario oficial, Bogotá. 05, enero, 2009. p.1.

Artículo 269A: Acceso abusivo a un sistema informático

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático.

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.[36]

[36] Ibíd. p.1.

Artículo 269F: Violación de datos personales.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269I: Hurto por medios informáticos y semejantes.

El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.[37]

[37] Ibíd. p.2.

6. DISEÑO METODOLOGICO PRELIMINAR

Fase I: Teniendo en cuenta que este proyecto es de carácter propositivo, para esta etapa inicial se hará un análisis de las aplicaciones más utilizadas por los funcionarios de la Policía Nacional, con el fin de identificar las tendencias en el uso de las mismas.

Fase II: Se realizara un análisis por medio de prácticas de penetración, ingeniería social, ataques y análisis de tráfico en Smartphone con sistema operativo Android utilizados en la Policía Nacional, aplicando los objetivos y criterios de un Hacking Ético, ya que en ningún momento se verá afectada ni comprometida la información personal y/o corporativa de cada uno de los Smartphone.

Fase III: Desarrollo de la definición de Políticas de Seguridad, teniendo en cuenta las vulnerabilidades encontradas y la interpretación de la información recolectada mediante un análisis cualitativo y cuantitativo, buscando a si crear conciencia en cada uno del personal que conforma la Policía Nacional, que la utilización de dispositivos móviles como Smartphone debe ser de forma segura y responsable cuando se maneje información personal y/o corporativa.

6.1 Recopilación de utilidades para analizar APKS

De manera global, existen dos tipos de análisis: estático y dinámico. El primero analiza diferentes aspectos de las aplicaciones sin llegar a ejecutarlas, mientras que el segundo se centra en un análisis basado en el comportamiento de la aplicación una vez ejecutada. De manera habitual, las utilidades y servicios de análisis dinámico incorporan información obtenida a partir de un análisis estático previo.

A continuación se indican algunas de las aplicaciones de uso más extendido que permiten realizar estos dos tipos de análisis, agrupándolas en aquellas que pueden ser ejecutadas en local, previo proceso de instalación, y aquellas que corresponden a servicios online.

En la figura 17 se puede observar aplicaciones para realizar análisis de APK (Android Application Package) a nivel estático y dinámico.

Figura 17. Aplicaciones para análisis de estático y dinámico

Fuente:https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/utilidades_para_analizar_APKS

De manera general, todas ellas pueden utilizarse gratuitamente, a excepción de algún caso en el que se establecen limitaciones si van a ser utilizadas con un fin comercial.

6.1.1 Herramientas locales para el análisis estático

Como reflejan los datos recopilados en el informe sobre la situación del malware para Android, el sistema operativo de Google se ha convertido en la plataforma móvil más afectada por el malware, centrando el 99% de las amenazas desarrolladas para smartphones. De manera global, existen dos tipos de análisis: estático y dinámico. El primero analiza diferentes aspectos de las aplicaciones sin llegar a ejecutarlas, mientras que el segundo se centra en un análisis basado en el comportamiento de la aplicación una vez ejecutada. De manera habitual, las utilidades y servicios de análisis dinámico incorporan información obtenida a partir de un análisis estático previo.[38]

[38] MARTINEZ, Asier. Recopilación de utilidades para analizar APKS [en línea]. Marzo de 2015, [consultado 08 de Agosto de 2016]. Disponible en Internet: https://www.certsi.es/blog/utilidades-para-analizar-apks

Androguard: desarrollada en Python, y por tanto multiplataforma, incorpora gran cantidad de funcionalidades y permite acceder a multitud de características de una APK. Algunas de las opciones más destacadas son:

- Descompilar APKs y por tanto permite el acceso a permisos, Receivers, Activities, Content Providers, Services, Package Name, clases, métodos, etc.
- Indicador de peligrosidad.
- Comparar el código de dos aplicaciones para comprobar la similitud entre ambas. Está disponible en https://code.google.com/p/androguard/.

ApkInspector: también desarrollada en Python, su característica principal es que dispone de un interface gráfico a través del cual se pueden visualizar diferentes aspectos de las APKs analizadas como por ejemplo el AndroidManifest.xml. Está disponible en https://github.com/honeynet/apkinspector/.

APKTool: es una utilidad multiplataforma que permite descompilar y volver a compilar las aplicaciones. Está disponible en https://code.google.com/p/android-apktool/.[39]

APKStudio: es un IDE (entorno de desarrollo integrado) multiplataforma que permite descompilar y compilar APKs. Está disponible en https://apkstudio.codeplex.com/.

Androguarn: es una utilidad cuyo objetivo es detectar y advertir de comportamientos potencialmente peligrosos. Para ello, analiza multitud de aspectos de las APKs como por ejemplo:

- Posibilidad de exfiltración de información sensible como configuraciones del dispositivo móvil, geolocalización, credenciales de acceso Wi-Fi, información de contactos, etc.
- Posibilidad de envío de SMS Premium o capacidad para realizar llamadas.
- Capacidad de grabación de video y audio.

Los reportes generados tienen un diseño muy intuitivo y claro. Está disponible en https://github.com/maaaaz/androwarn.

[39] Ibíd. Disponible en Internet: https://www.certsi.es/blog/utilidades-para-analizar-apks

Dex2Jar: permite convertir un fichero .APK en uno .JAR de manera que se pueda visualizar el código de la aplicación. Está disponible en https://code.google.com/p/dex2jar/.

JD-GUI: es una herramienta con interface gráfica que permite interactuar de una manera intuitiva con ficheros con extensión .CLASS. Está disponible en http://jd.benow.ca/.

JAD: Es una aplicación multiplataforma que permite convertir ficheros .DEX en ficheros .CLASS. Está disponible en http://varaneckas.com/jad/**.**

6.1.2 Herramientas locales para el análisis Dinámico

DroidBox: es una utilidad por línea de comandos, la cual permite el acceso a multitud de información como por ejemplo:

- Comunicaciones establecidas por la aplicación.
- Posibilidad de exfiltración de información sensible.
- Mapa que muestra el comportamiento de la APK.
- Comparar el código de dos aplicaciones para comprobar la similitud entre ambas.

Está disponible en https://code.google.com/p/droidbox/**.**

6.1.3 Servicios online análisis estático

Virustotal: analiza las aplicaciones con más de 50 motores antivirus. Así mismo, realiza un análisis estático de las mismas con Androguard e incorpora diferentes módulos como ExifTool o TrID para obtener información adicional. Dispone tanto de una API pública con limitaciones como de una API privada. El servicio es accesible en https://www.virustotal.com/.[40]

[40] Ibíd. Disponible en Internet: https://www.certsi.es/blog/utilidades-para-analizar-apks

AndroTotal: el servicio está en fase BETA. Analiza las aplicaciones con varios motores antivirus, menos que Virustotal. Además, muestra información como los permisos y las activities de la aplicación analizada. El servicio es accesible en http://andrototal.org/.

6.1.4 Servicios online para el análisis Dinámico

APKScan: Muestra gran cantidad de información: Información general: hashes, tamaño, etc.

Análisis con Virustotal: capturas de pantalla de la aplicación en ejecución, captura del tráfico de red, posibilidad de exfiltración de información, dispone de una API privada. El servicio es accesible en http://apkscan.nviso.be/.

Mobile Sandbox: permite acceder a la información habitual de un análisis estático como permisos solicitados, receivers, services, content providers, etc. y muestra de una manera intuitiva la información a la que accede la aplicación, por lo que se pueden observar claramente los riesgos que supone la instalación de la misma. El servicio es accesible en http://mobilesandbox.org/.

Akana: es un entorno interactivo online que muestra la información típica de un análisis estático junto con el análisis de Virustotal. El servicio es accesible en http://www.mobiseclab.org.

Anubis: junto con la información característica de un análisis estático, muestra otra como el tráfico de red, captura de pantalla de la aplicación en ejecución, cadenas significativas, etc. El servicio es accesible en http://anubis.iseclab.org/.

Existen varias distribuciones que recopilan éstas y otras utilidades para realizar los análisis anteriormente descritos. De todas ellas, destacan las siguientes:

Santoku: es un entorno basado en Linux que incorpora un gran número de utilidades entre las que se encuentran muchas destinadas al análisis de malware para dispositivos móviles. Está disponible en https://santoku-linux.com/.[41]

[41] Ibíd. Disponible en Internet: https://www.certsi.es/blog/utilidades-para-analizar-apks

Android Reverse Engineering (A.R.E): es una máquina virtual con multitud de herramientas expresamente diseñadas para el análisis de aplicaciones para Android. Está disponible en https://github.com/hannoL/AREsoft.

MobiSec Lab: es un entorno basado en Ubuntu que incluye la infraestructura necesaria para realizar el análisis de aplicaciones. Está disponible en http://sourceforge.net/projects/mobisec/files/.

En el caso de no disponer de muestras y querer conseguir algunas para probar las herramientas que se han descrito en el artículo, es posible obtenerlas a partir de diferentes orígenes:

APK Downloader: es un servicio online que permite descargar aplicaciones de Google Play. Está disponible en http://apps.evozi.com/apk-downloader/.

MyAPPSharer: es una utilidad disponible en Google Play que, una vez instalada en el dispositivo móvil, permite extraer otras aplicaciones instaladas en el terminal.[42]

Contagio Mobile: el popular blog de malware para Android, dispone de un gran número de muestras que pueden ser descargadas para poder analizarlas.[42]

6.2 Pruebas vulnerabilidades sistema operativo Android

El entorno de trabajo configurado para la identificación de vulnerabilidades de los dispositivos móviles con sistema operativo Android, consiste en una red wifi, 01 equipo Motorola G16 primera generación con sistema Android 5.0.2 Lollipop, 01 equipo Motorola G8 primera generación con sistema operativo 4.4.4 Kitkat.

6.2.1 zANTI

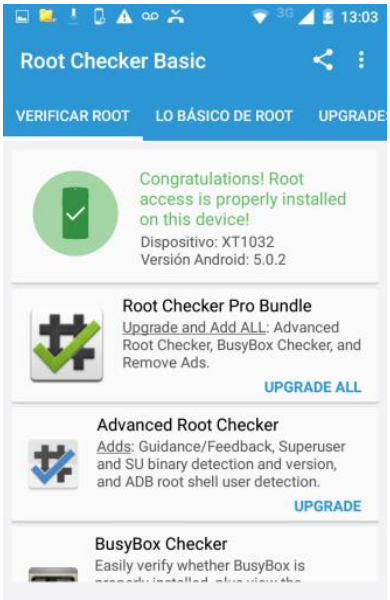
Las pruebas de penetración iniciales, corresponden a identificar vulnerabilidades presentadas en los dispositivos móviles, los cuales son conectados a redes wifi libres, mediante la utilización de la herramienta zANTI, previa configuración de los permisos root (superusuario) en el equipo Motorola G16.

[42] Ibíd. Disponible en Internet: https://www.certsi.es/blog/utilidades-para-analizar-apks

zANTI es una herramienta de seguridad bajo entorno de sistema operativo Android, la cual permite realizar pruebas de penetración a redes wifi, encontrando vulnerabilidades aprovechadas para atacar los puertos de los dispositivos conectados en una red wifi, estas vulnerabilidades pueden ser encontradas igualmente en dispositivos móviles con sistema operativo Android.

Esta herramienta surge de la evolución de la famosa suite dSploit. Posee distintas secciones desde donde permite realizar técnicas como Man In The Middle (MITM), interceptar el tráfico de una red y modificar la dirección MAC, con un enfoque defensivo y de manera que te ayude a mantener una protección proactiva. [43]

En la figura 18 se puede observar por medio de la aplicación Root Checker Basic que el dispositivo se encuentra rooteado, es decir con acceso de súper usuario, el cual permite control total sobre los archivos e instalación de aplicaciones.
Figura 18. Verificación root dispositivo

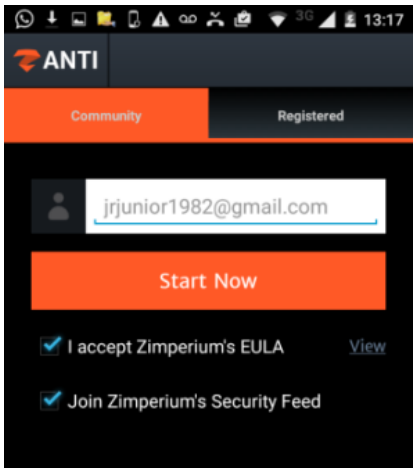


Fuente: el autor

En la figura 19 se puede observar la instalación de la herramienta zANTI en el dispositivo móvil Android, con el fin de iniciar las pruebas correspondientes.

[43] PAUS, Lucas. 5 herramientas actualizadas para pentest desde tu Android [en línea]. Enero de 2015, [consultado 08 de Agosto de 2016]. Disponible en Internet: http://www.welivesecurity.com/la-es/2015/01/22/5-herramientas-pentest-android/

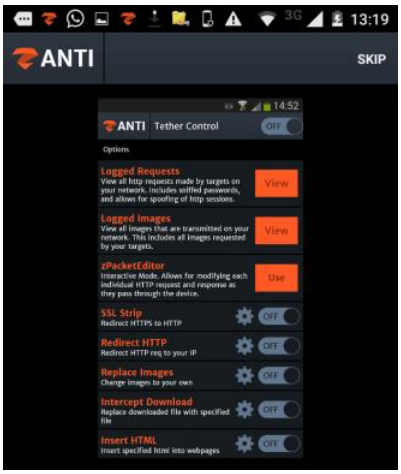
Figura 19. Instalación herramienta zANTI



Fuente: el autor

En la figura 20 se puede observar la ejecución de la utilidad zTether de la aplicación zANTI, mediante el cual se logra crear un punto de acceso Wifi y controlar de esta forma el tráfico de la red, evidenciándose una zona wifi creada desde el dispositivo móvil, desde la cual se pueden conectar los demás dispositivos móviles.

Figura 20. Utilidad zTether



Fuente: el autor

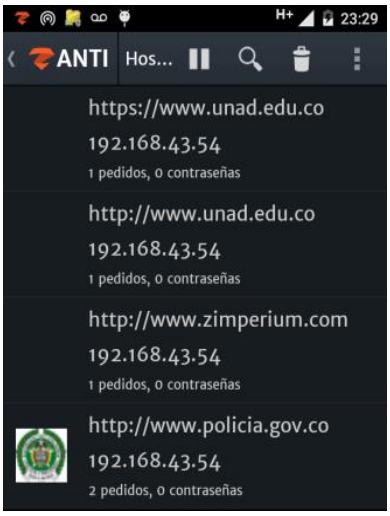
En la figura 21 se puede observar la conexión del equipo Motorola G8 a la zona wifi creada anteriormente denominada “Claro”, y de esta forma obtener el tráfico de este dispositivo.

Figura 21. Conexión zona wifi

Fuente: el autor

Una vez activado el control zTether, seleccionamos la "opción" Logged Request", en la figura 22 se puede observar todas las solicitudes HTTP (HyperText Transfer Protocol) realizadas desde el dispositivo Motorola MG8 (dispositivo de la víctima), la cual puede contener contraseñas y otra información sensible.

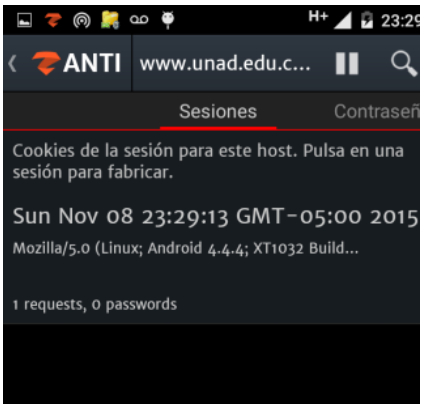
Figura 22. Solicitudes HTTP



Fuente: el autor

En la figura 23 se puede observar el acceso al registro de actividades por medio de la aplicación zANTI para obtener más detalles, como por ejemplo sesiones, solicitudes, y agentes de usuarios.

Figura 23. Registro de actividades



Fuente: el autor

En la figura 24 se puede observar los agentes de usuarios enviada por los clientes en las cabeceras de las peticiones HTTP, esta utilidad permite iniciar un ataque Zetasploit en la dirección IP identificada.

Figura 24. Agentes de usuario

Fuente: el autor

6.2.2 Prueba de penetración aplicación myMail

Se realiza pruebas de penetración a la aplicación de correo electrónico “myMail”, la cual permite gestionar fácilmente cuentas de correo de Outlook, Exchange, en el caso de la institución las cuentas institucionales son configuradas en este aplicativo muy fácilmente, se realizará pruebas estáticas y dinámicas.

Herramienta Apktool

Por medio de esta herramienta se realizara análisis estático a la aplicación myMail, se realiza configuración de ésta herramienta, así como la configuración de las variables de entorno para la ejecución de la herramienta por medio de la consola de comando de Windows.

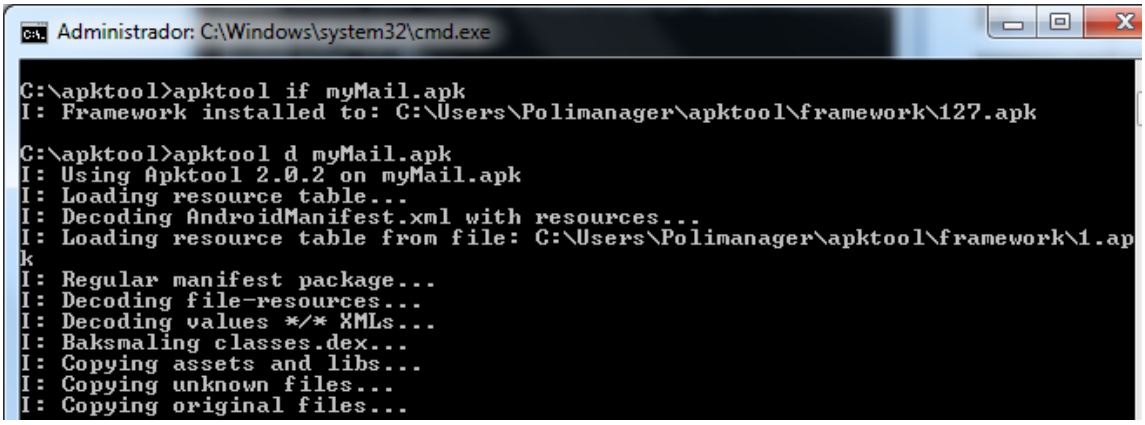
En la figura 25 se puede observar la creación del directorio en la unidad C: de Windows denominada “Apktool”, con el fin de configurar el entorno de trabajo.

Figura 25. Directorio Apktool

Fuente: el autor

En la figura 26 se puede observar la descompilación de la aplicación “myMail” por medio de la consola de comando de Windows, a través del siguiente comando: apktool if myMail.apk.

Figura 26. Descompilar y compilar APK

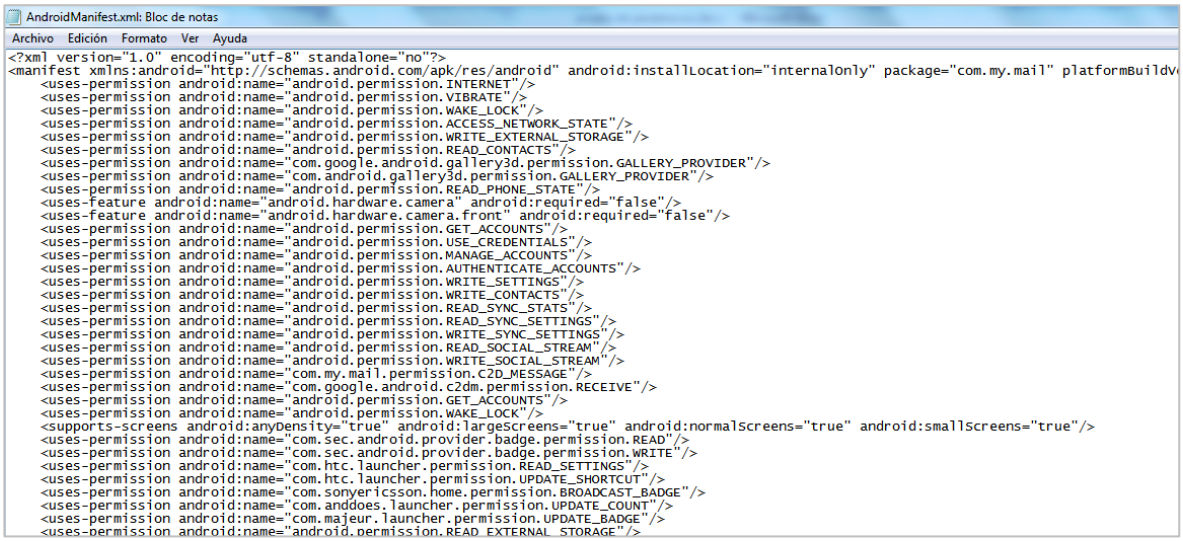


Fuente: el autor

Seguidamente realiza la compilación de la apk, por medio del siguiente comando: apktool d myMail.apk.

Posteriormente, en el directorio podremos acceder a una carpeta denominada con el mismo nombre de la aplicación, para abrir el archivo “AndroidManifest.xml” y obtener información con respecto a los permisos requeridos por la aplicación “myMail”.

Figura 27. Permisos requeridos por la aplicación



Fuente: el autor

Tabla 1. Permisos myMail

Permisos requeridos por “myMail”	
INTERNET	AUTHENTICATE_ACCOUNTS
VIBRATE	WRITE_SETTINGS
WAKE_LOCK	WRITE_CONTACTS
ACCESS_NETWORK_STATE	READ_SYNC_STATS
WRITE_EXTERNAL_STORAGE	READ_SYNC_SETTINGS
READ_CONTACTS	WRITE_SYNC_SETTINGS
READ_PHONE_STATE	READ_SOCIAL_STREAM
GET_ACCOUNTS	WRITE_SOCIAL_STREAM
USE_CREDENTIALS	READ_EXTERNAL_STORAGE
MANAGE_ACCOUNTS	UPDATE_BADGE

En la figura 27 se puede observar los permisos requeridos por la aplicación “myMail”, por medio del archivo AndroidManifest.xml visualizado por medio del block de notas.

Las vulnerabilidades encontradas en la aplicación MyMail, descritas en la tabla 1, permite identificar los siguientes permisos solicitados, los cuales representan alto riesgo de amenaza:

El permiso WRITE_EXTERNAL_STORAGE, como vulnerabilidad en la cual la aplicación puede leer, modificar y eliminar cualquier dato ubicado en el almacenamiento externo, convirtiéndose en un alto riesgo para el usuario, toda vez que puede haber almacenada información sensible para el usuario.

El permiso READ_EXTERNAL_STORAGE, permite leer archivos almacenados en el almacenamiento externo.

El permiso READ_PHONE_STATE representan vulnerabilidad para el usuario ya se puede obtener acceso a información acerca de logs del teléfono incluyendo información privada, así mismo se puede determinar IMEI, el número telefónico del usuario y serie del teléfono.

El permiso INTERNET, permite establecer conexiones de internet, este permiso es importante validar para aplicación se concede, ya que puede ser empleado por un malware para envío de datos desde el dispositivo.

El permiso READ_CONTACTS, permite leer información sobre los contactos del dispositivo, números de teléfono y correo electrónico.

Igualmente sobresale el permiso CAMERA, el cual permite tomar fotos y grabar videos, siendo innecesarios para la finalidad de la aplicación.

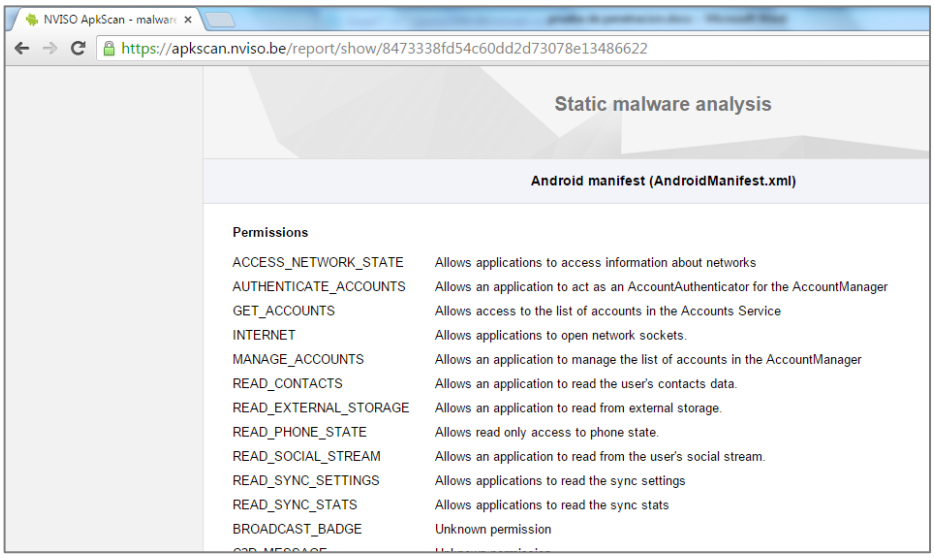
El permiso RECEIVE_SMS, permite a la aplicación recibir y procesar SMS

Herramienta APKScan

Esta herramienta para análisis estático y dinámico online, permite visualizar una gran cantidad de información de la aplicación, incluye análisis con virustotal, captura de pantalla de la aplicación en ejecución, captura tráfico de la red y posibilidad de ex filtración de información.

En la figura 28 se puede observar el análisis estático realizado a la aplicación "MyMail" por medio de la herramienta APKScan, con el fin de identificar por permisos requeridos por esta aplicación utilizada para acceder al correo institucional del dominio @policia.gov.co y @correo.policia.gov.co.

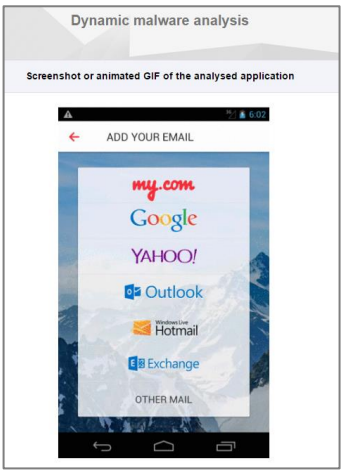
Figura 28. Permisos AndroidManifest.xml



Fuente: Los autores

En la figura 29 se puede observar la ejecución del análisis dinámico, esta herramienta ofrece la opción de capturas de pantallas de las aplicaciones analizadas, verificación de servicios, actividad de almacenamiento de archivos, actividad de conexiones abiertas en la red, actividad criptográfica, fuga de información.

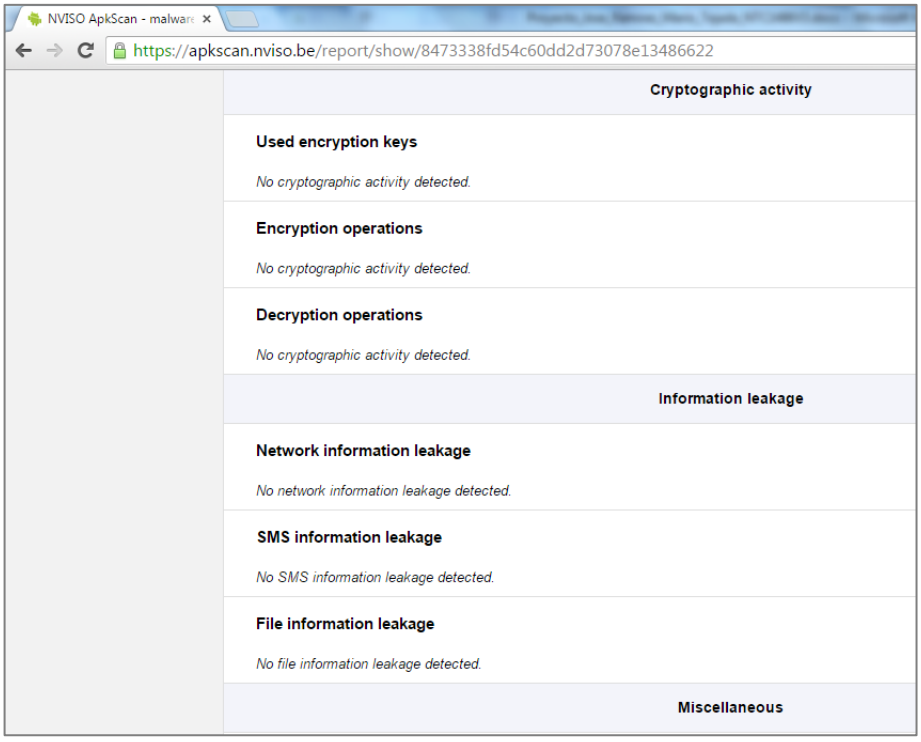
Figura 29. Captura de pantalla de la aplicación apkscan



Fuente: Los autores

En la figura 30 se puede observar el informe del análisis dinámico de la aplicación "MyMail" por medio de la herramienta APKScan, el cual no detecta ningún tipo de fuga de información de la aplicación analizada.

Figura 30. Informe de fuga de información



Fuente: Los autores

6.2.3 Prueba de penetración aplicación Ahorrando

Esta aplicación para dispositivos móviles Android, fue publicada por la Oficina de Telemática nivel central a principios del año 2015, a través de la intranet se dispuso un enlace para la descarga por parte del personal de la institución policial, este aplicativo permite administrar los gastos mensuales, de acuerdo a los ingresos de cada policial, y de esta forma contribuir a la educación financiera. Particularmente ingresando por medio de esta aplicación con el usuario y contraseña de dominio institucional, automáticamente la aplicación tiene acceso al ingreso mensual de nómina de mencionado usuario.

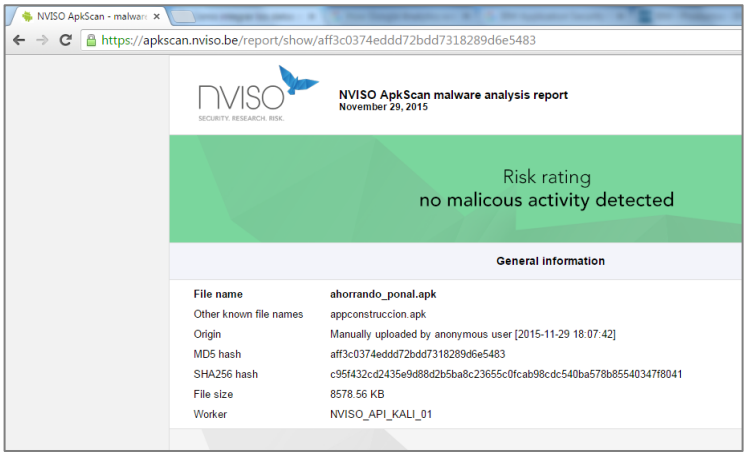
En la figura 31 se puede observar la pantalla principal de la aplicación “Ahorrando”, en la cual solicita el usuario y contraseña de dominio institucional para iniciar sesión en la aplicación.

Figura 31. Aplicación Ahorrando

Fuente: Los autores

En la figura 32 se puede observar que por medio de la herramienta online APKScan, se lográ realizar un pentest para identificar las vulnerabilidades de seguridad de la aplicación “Ahorrando”.

Figura 32. Análisis herramienta apkscan



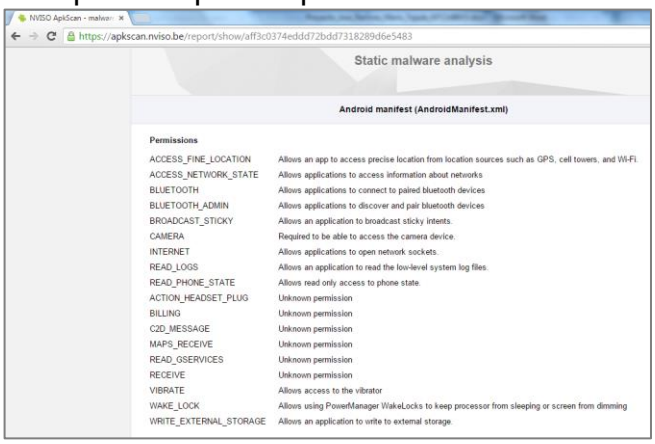
Fuente: Los autores

Tabla 2.Permisos APK Ahorrando

Permisos requeridos por “Ahorrando”
ACCES FINE LOCATION
ACCESS_NETWORK_STATE
BLUETOOTH
BLUETOOTH_ADMIN
BROADCAST_STICKY
CAMERA
INTERNET
READ_LOGS
READ_PHONE_STATE
VIBRATE
WAKE_LOCK
INTERNET
VIBRATE
WAKE_LOCK
WRITE_EXTERNAL_STORAGE

En la figura 33 se puede observar los permisos solicitados por la aplicación “Ahorrando” a través de un análisis estático con la herramienta APKScan, por medio de archivo AndroidManifest.xml.

Figura 33. Permisos requeridos por la aplicación “Ahorrando”



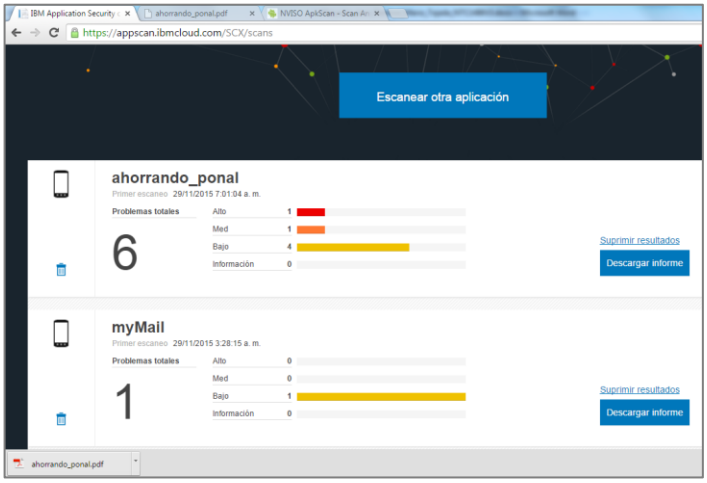
Fuente: Los autores

IBM Application Security Analyzer – Mobile

Se realizó analisis de la aplicación “Ahorrando” por medio de la herramienta IBM Security AppScan Mobile Analyzer, con el fin de identificar vulnerabilidades de seguridad.

En la figura 34 se puede observar el análisis de la aplicación “Ahorrando” por medio de la herramienta online IBM Security AppScan Mobile Analyzer, se evidencia seis (06) problemas de seguridad, categorizados en 3 escalas de gravedad: alta, media, y baja.

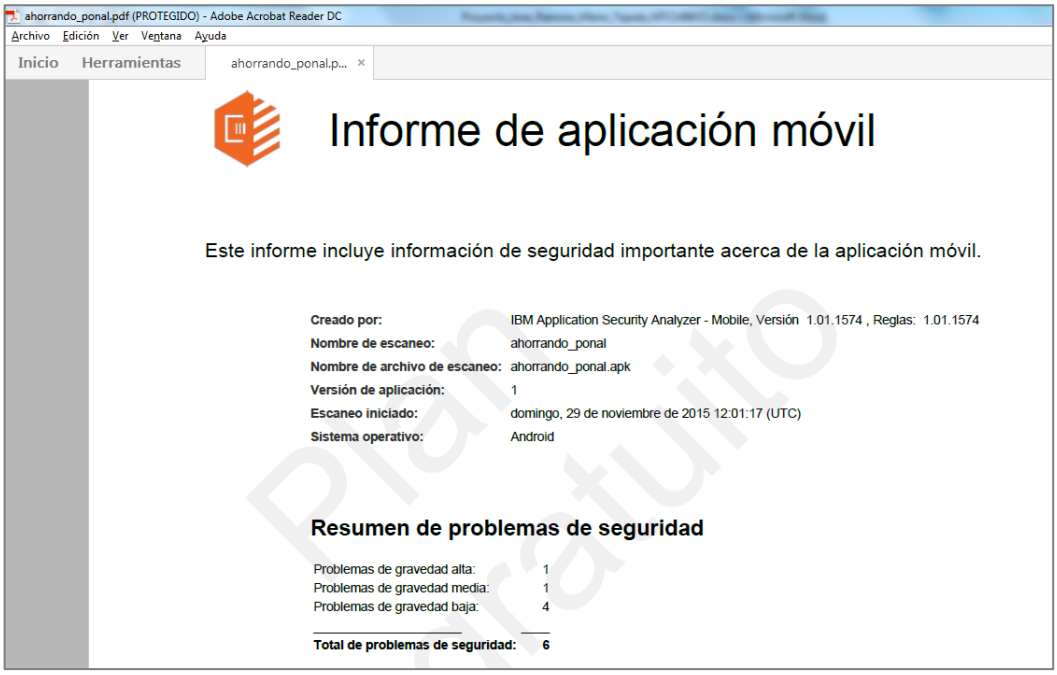
Figura 34. Escaneo de la aplicación “Ahorrando”



Fuente: Los autores

En la figura 35 se puede observar el informe de seguridad realizado a la aplicación “Ahorrando”, por medio del cual se identifica un total de seis (06) problemas de seguridad, categorizados en tres (03) niveles.

Figura 35. Informe aplicación “Ahorrando”



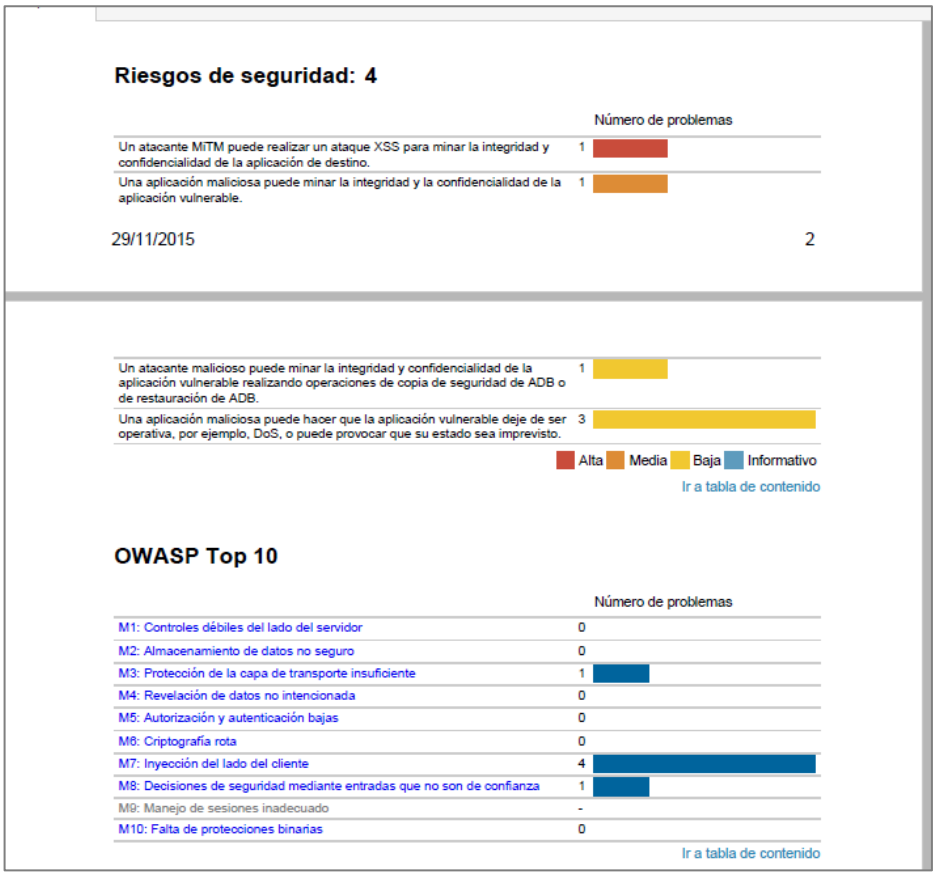
Fuente: Los autores

Los problemas identificados por la herramienta descrita corresponden a:

- Script entre sitios (XSS) a través de MiTM (Man-in-the-Middle)
- ConnectManipulation
- Distintivo de copia de seguridad habilitado
- Bloqueo en código Java

En la figura 36 se puede observar los riesgos de seguridad identificados en la aplicación “Ahorrando”, relacionados la protección insegura en la capa de transporte, inyección del lado del cliente, decisiones de seguridad mediante entradas que no son de confianza, que afectan la confidencialidad, integridad y disponibilidad de la información administrada por la aplicación.

Figura 36. Problemas de seguridad



Fuente: Los autores

Vulnerabilidades OWASP Aplicación “Ahorrando”

M3. Proteccion insegura en la capa de transporte

Un atacante MiTM puede realizar un ataque XSS a través de MiTM (Man-in-the-Middle) para atacar la integridad y confidencialidad de la aplicación de destino, se recomienda validar la entrada del usuario, utilizar canales de comunicación seguros, se recomienda No habilitar nunca JavaScript en el navegador incluido, si no es necesario.

M7: Inyección del lado del cliente

Una aplicación maliciosa puede atacar la integridad y la confidencialidad de la Aplicación.

M8: Decisiones de seguridad mediante entradas que no son de confianza

Se presenta tipo de problema bloqueo en codigo java, cuyo riesgo de seguridad implicaria que una aplicación maliciosa puede hacer que la aplicación deje de ser operativa.

6.2.4 WhatsApp Sniffer

Es un aplicativo que rastreador de paquetes y que de manera muy automática se obtienen chats de Whatsapp que se encuentren en el momento en la red, es decir que si estamos conectados por una red Wifi y ejecutamos la aplicación, podemos obtener todas las conversaciones de Whatsapp que este circulando por la red en ese momento. WhatsApp Sniffer desde hace bastante tiempo no se encuentra disponible en la play store de google.

Para poder instalar y ejecutar WhatsApp Sniffer necesitamos permisos de supe usuario (root) y busybox para que pueda funcionar sin ningún inconveniente

Al momento de tener ya instalado whatsappsiffer debemos hacer click o pulsar sobre la opción “start” y luego no solicitara permisos de superusuario, luego de conceder los permisos solicitados por el aplicativo empezara a buscar las conversaciones por whatsapp en la red a la cual estemos conectados. En el momento que capte alguna conversación aparcera listas en la pantalla principal del aplicativo.

En la figura 37 se puede observar la pantalla principal de la aplicación WhatsApp Sniffer, la cual explota fallas de seguridad presentadas en la aplicación WhatsApp relacionada con la encriptación de los mensajes enviados por medio de las conversaciones de los usuarios.

Figura 37. Aplicación WhatsApp Sniffer

Fuente: http://www.redeszone.net/whatsapp/sniffer-tutorial-para-aprender-a-utilizar-whatsapp-sniffer.

La última versión de WhatsApp cifra los mensajes[44]

Un miembro del soporte de WhatsApp ha confirmado que a partir de la última versión de este programa, las conversaciones estarán cifradas.

Una gran noticia para todos los usuarios de esta popular aplicación para móviles que nos permite comunicarnos de forma gratuita a través de mensajes (siempre y cuando tengamos internet, ya sea por WiFi o tarifa de datos).

En el mismo mensaje ha declarado que ellos no almacenan ningún historial de conversación en sus servidores, únicamente almacenan los mensajes hasta que el usuario está disponible y de esta forma entregárselos.

Debido a esta actualización se mitigó este sniffer.

[44] DE LUZ, Sergio. La última versión de WhatsApp cifra los mensajes…según su FAQ [en línea]. Agosto de 2012, [consultado 26 de Octubre de 2016]. Disponible en Internet: http://www.redeszone.net/2012/08/26/la-ultima-version-de-whatsapp-cifra-los-mensajes-segun-su-faq/

Cifrado de extremo a extremo

El cifrado de extremo a extremo de WhatsApp asegura que solo tú y el receptor puedan leer lo que es enviado, y que nadie, ni siquiera WhatsApp lo logre hacer. Tus mensajes están seguros con un candado y solo tú y el receptor cuentan con el código/llave especial para abrirlo y leer los mensajes. Para mayor protección, cada mensaje que envías tiene su propio candado y código único. Todo esto pasa de manera automática; sin necesidad de ajustar o crear chats secretos especiales para asegurar tus mensajes.

El sistema fue desarrollado por Open Whisper Systems y se basa en una plataforma llamada Text Secure.[45]

Según publica Gizmodo, Tex Secure es capaz de crear una llave privada única (lo que WhatsApp llama código de seguridad único), asociada al dispositivo móvil y que es necesaria para descifrar el mensaje que llega cifrado.

Text Secure, además, cambia de llave cada vez que se envía un nuevo mensaje mediante una tecnología llamada Forward Secrecy. La clave del asunto es que las llaves privadas solo se alojan en el dispositivo del usuario, lo que impide que Whatsapp pueda obtener esas claves.

6.2.4 USB Rubber Ducky

Este hardware permite la imitación de un teclado por medio de un ataque HID, para los dispositivos móviles, esta amenaza se orienta hacia la tarjeta micro USB, se aprovecha una vulnerabilidad de los dispositivos como lo es la comunicación del usuario con el dispositivo denominada dispositivo de interfaz humana, este ataque se logra por medio de un “payload”, gracias a un archivo compilado en binario por medio de un lenguaje de programación.

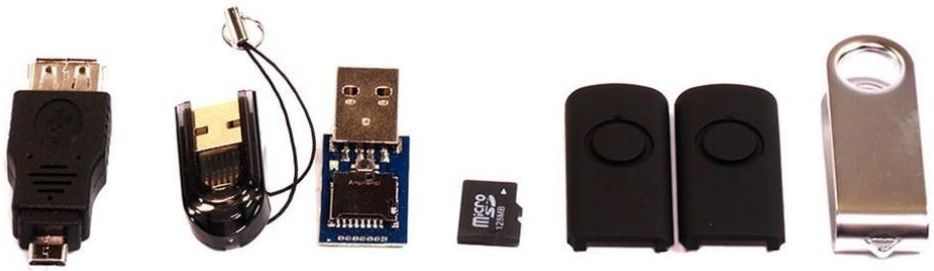
Este tipo de ataque basado en ingeniera social, se aprovecha del eslabón más débil de la seguridad informática, es decir los usuarios, ya que el ataque se pude llevar a

[45] WhatsApp: ¿Qué significa el mensaje de cifrado "de extremo a extremo"? [En línea]. Abril de 2016, [consultado 26 de Octubre de 2016]. Disponible en Internet: http://www.t13.cl/noticia/tendencias/tecnologia/que-significa-nuevo-mensaje-esta-apareciendo-whatsapp

cabo en unos cuantos minutos, debido al descuido de equipo o dispositivo móvil, dejando en riesgo la información sensible, sin dejar ninguna sospecha a la víctima.

USB Rubber Ducky es una herramienta hardware de hacking, internamente tiene un procesador, aunque a simple vista parece un USB, aunque emula ser un teclado, de tal forma que cuando se conecta a un ordenador/dispositivo éste lo reconoce como un teclado y ejecuta las instrucciones que tenga cargadas en una memoria SD que lleva.[46]

Figura 38. Contenido USB Rubber Ducky



Fuente: http://www.securityartwork.es/2015/12/23/me-parecio-ver-un-lindo-patito-usb-rubber-ducky/

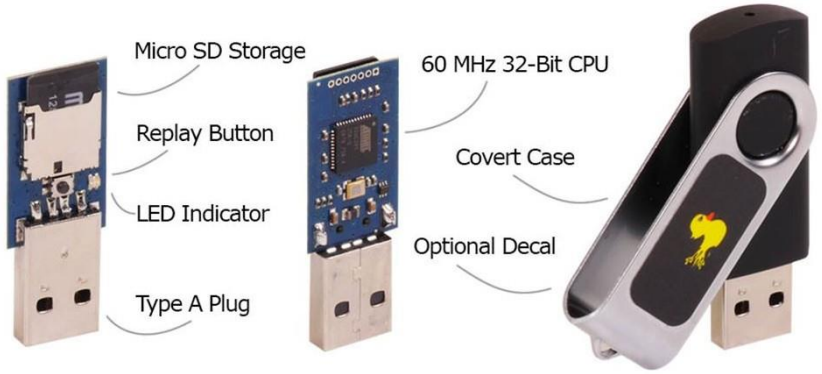
De izquierda a derecho tenemos las siguientes partes:

1. Adaptador de USB micro-B
2. Adaptador o lector de tarjetas microSD
3. USB Rubber Ducky
4. Tarjeta micro-SD
5. Carcasa de USB

Las especificaciones del USB Rubber Ducky se pueden ver en la figura 39.

[46] OLMEDO, Yolanda. USB Rubber Ducky [En línea]. Abril de 2016, [consultado 26 de Octubre de 2016]. Disponible en Internet: http://www.securityartwork.es/2015/12/23/me-parecio-ver-un-lindo-patito-usb-rubber-ducky/

Figura 39. Detalles técnicos USB Rubber Ducky



Fuente: http://www.securityartwork.es/2015/12/23/me-parecio-ver-un-lindo-patito-usb-rubber-ducky/

Funcionamiento USB Rubber Ducky[47]

1. Lo primero que debemos hacer es insertar la tarjeta microSD en el adaptador/lector de tarjetas, que es donde cargaremos el payload.
2. Escribiremos el payload en un fichero de texto.
3. Cargaremos el payload en la tarjeta MicroSD.Para ello utilizamos el Encoder para compilar y cargar el payload que hemos desarrollado. La ultima versión disponible del Encoder es la versión 2.6.3, el cual está basado en Java y debemos tener instalado.La instrucción para cargar el payload en la tarjeta SD sería la siguiente:

Figura 40. Instrucción para cargar el payload

```
javar -jar duckyencoder.jar -i nuestropayload.txt -o /rutaUSB/inject.bin -l resources es.properties

-i: input del payload de entrada.
-o: ruta hacia la tarjeta microSD donde cargaremos el payload, por defecto el nombre es inject.bin.
-l: parámetro de configuración del idioma del teclado.
```

Fuente: http://www.securityartwork.es/2015/12/23/me-parecio-ver-un-lindo-patito-usb-rubber-ducky/

[46] Ibíd. Disponible en Internet: http://w ww.securityartwork.es/2015/12/23/me-parecio-ver-un-lindo-patito-usb-rubber-ducky/

Dentro de la carpeta Encoder tenemos una carpeta llamada Resources con los idiomas disponibles de configuración del teclado. Si no se especifica idioma, por defecto utiliza “us.properties”.

Otras opciones para compilar el payload es mediante interfaz gráfica con EncoderGUI y también a través de este generador online.

4. Una vez se ha generado correctamente el binario, colocaremos la microSD en el USB Rubber Ducky.
5. Ya lo tenemos todo listo, ya sólo nos queda conectar el USB Rubber Ducky en el ordenador víctima y dejar que se ejecute automáticamente el binario.

6.2.5 IMSI CATCHER

Son dispositivos para interceptar comunicaciones en redes de telefonía celular GSM, funcionan como torres móviles falsas, este tipo de ataque conocido como MITM (Main in the Middle), permite por medio de una estación virtual interceptar comunicaciones de un teléfono móvil, consiste en una antena de telefonía móvil que actúa como falsa estación base, ubicando durante la transmisión entre el dispositivo móvil atacado y las torres proveedoras de servicio de telefonía, representa una amenaza para los dispositivos móviles, teniendo en cuenta que por medio del IMSI CATCHER se puede identificar todos los dispositivos alrededor, interceptar llamadas, mensajes de texto, así como tomar el control de dispositivo por medio de un malware enviado vía MSM.

Aunque en un inicio su uso fue reservado para cuerpos militares o de inteligencia, como la CIA o el Ejército de los Estados Unidos, actualmente se ha popularizado en agencias estatales y locales estadounidenses. También en otras partes del mundo se ha reportado su uso y adquisición, como el Reino Unido y México.

Estos aparatos se denominan así porque acopian la Identidad Internacional del Suscriptor de Móvil (IMSI), un número único que permite identificar globalmente a un teléfono, el operador al que está suscrito y el usuario al que pertenece. Normalmente el IMSI no se transmite y pertenece como un número confidencial.[47]

[47] 5 datos que debes saber sobre los IMSI catchers o stingrays [en línea]. Junio de 2016, [consultado 08 de Agosto de 2016]. Disponible en Internet: https://r3d.mx/2016/06/20/5-datos-que-debes-saber-sobre-los-imsi-catchers-o-stingrays/

¿Qué uso se conoce de los IMSI catcher?

La publicación Scientific American reconoce su uso bajo tres circunstancias. Primero, agentes pueden utilizar el simulador para rastrear un número de celular y conocer su ubicación.

Segundo, se puede utilizar un IMSI catcher para seguir a un objetivo de vigilancia aunque no se conozca el número de teléfono. Este método implica que el simulador sea encendido periódicamente en distintas ubicaciones conocidas del usuario, así se busca conocer qué dispositivos utiliza esta persona. Al momento de encender el dispositivo, este recolecta indiscriminadamente información y datos de todos los teléfonos que se conecten en esa zona.

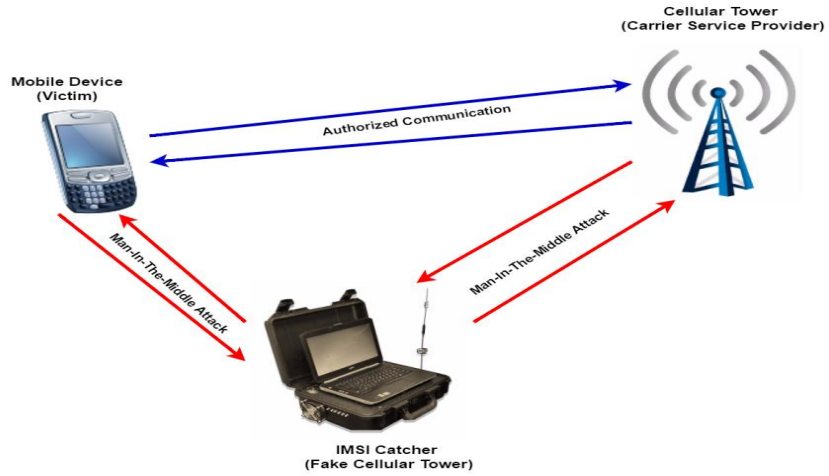
Tercero, se conoce el uso de los IMSI catchers en manifestaciones y protestas sociales para recolectar información de los asistentes.

¿Cómo funciona IMSI Catcher?

IMSI receptor actúa como una torre celular falsa entre la torre original del proveedor de servicios y los usuarios de dispositivos móviles, que transmitió la señal de radio de alta frecuencia y su radio cubre de larga distancia. Será engañar a los dispositivos móviles en el pensamiento de que es la única antena de telefonía móvil en la zona con señal fuerte y dispositivos móviles elegir para conectarse con IMSI receptor (antena de telefonía móvil falso con señal fuerte). Una vez que los dispositivos móviles se conectan al colector IMSI, todo dispositivo móvil transita entre la torre de servicio original y proporcionar a los usuarios de dispositivos móviles, sería totalmente sin cifrar. Por lo tanto, IMSI receptor puede ahora realizar "(MITM) man-in-the-middle" ataques para interceptar tráficos de dispositivos móviles y rastrear el movimiento de los usuarios de dispositivos móviles.[48]

[48] KAREDIA, Rahil IMSI Catcher [en línea]. Abril de 2016, [consultado 26 de Octubre de 2016]. Disponible en Internet: http://iisecurity.in/blog/imsi-catcher/

Figura 41. Funcionamiento IMSI Catcher



Fuente: http://iisecurity.in/blog/imsi-catcher/

7. PERSONAS PARTICIPANTES EN EL PROYECTO

Responsables del proyecto: MARIO AUGUSTO TEJADA RICO, JOSE ALFREDO RAMIREZ PRADA.

Director del proyecto: Ingeniero JOHN FREDDY QUINTERO TAMAYO

8. RECURSOS DISPONIBLES

Talento Humano: Director del trabajo de grado, asesores, personal de las oficinas de Telemática del Departamento de Policía Huila y Escuela Nacional de Operaciones Policiales San Luis Tolima.

Recursos Financieros: Este proyecto no requiere dinero teniendo en cuenta que pertenecemos al área de Telemática de la Policía Nacional.

Recursos institucionales: Equipos de cómputo, instalaciones policiales, impresora, teléfonos inteligentes.

9. RESULTADOS E IMPACTOS ESPERADOS

9.1 POLITICAS DE SEGURIDAD

Teniendo en cuenta las vulnerabilidades a las que se encuentran expuestos los dispositivos móviles con sistema operativo Android utilizados en la Policía Nacional, los datos deben estar protegidos en todo momento y ese es nuestro objetivo principal, las aplicaciones móviles son un método principal de acceso a los datos, visualizarlos, almacenarlos y enviarlos, mientras más aplicaciones se utilizan más datos confidenciales existen dentro de nuestros dispositivos móviles. Tanto aplicaciones como datos deben contar con ciertos controles y métodos de protección adecuados, con el fin de ser implementados para la actualización del Manual de Seguridad de la Información de la Policía Nacional, teniendo en cuenta que se encuentra desactualizado de acuerdo a la norma ISO 27001, y por consiguiente se deben adoptar las políticas de acuerdo a los objetivos de control establecidos en el anexo "A" ISO/IEC 27001:2013.[49]

9.1.1 Aspectos Organizativos de la Seguridad de la Información

Con respecto al objetivo de control "Dispositivos para movilidad y teletrabajo" perteneciente a este dominio, de dará aplicación al siguiente control:

Política de uso de dispositivos para movilidad

El uso de dispositivos móviles con sistema operativo Android con fines institucionales, será únicamente los asignados por la Policía Nacional, de acuerdo a las siguientes directrices supervisadas por la Oficina de Telemática de la Policía Nacional:

- Configurar adecuadamente el acceso y bloqueo del dispositivo
- Instalación de antivirus autorizado y actualizado
- Cifrado de la información
- Permisos de instalación de aplicaciones solo por personal autorizado de la Oficina de Telemática y solo de fuentes conocidas.
- Restricción de conexión de dispositivos USB

[49] ISO 27000. El portal de ISO 27001 en Español. [en línea]. [consultado el 27 de Octubre de 2016]. Disponible en http://www.iso27000.es/download/ControlesISO27002-2005.pdf

9.1.2 Seguridad Ligada a los Recurso Humanos

Con respecto al objetivo de control “Durante la contratación” perteneciente a este dominio, de dará aplicación a los siguientes controles:

Concienciación, educación y capacitación en seguridad de la información

La Oficina de Telemática de la Policía Nacional realizará capacitaciones a todo el personal de la unidad sobre la seguridad de la información en dispositivos móviles con sistema operativo Android, con el fin concienciarlos sobre los riesgos presentados por la inaplicabilidad de las políticas de seguridad.

- Debido a las fallas de seguridad presentadas en las aplicaciones de mensajería instantánea, los usuarios deberán abstenerse en enviar información clasificada de la Institución por mensajería Whatsapp u otra aplicación similar.
- Crear copias de seguridad de forma periódica

Proceso Disciplinario

La vulneración de las políticas de seguridad establecidas para dispositivos móviles con sistema operativo Android asignados por la Policía Nacional, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo a los procedimientos establecidos para cada caso.

9.1.3 Gestión de Activos

Con respecto al objetivo de control “Responsabilidad sobre los activos” perteneciente a este dominio, de dará aplicación al siguiente control:

Inventario de los activos

Los dispositivos móviles con sistema operativo Android, serán identificados dentro del inventario de activos de la Policía Nacional.

Propiedad de los activos

Los activos pertenecientes al inventario son de propiedad de la Policía Nacional.

Devolución de los activos

Todos los funcionarios de la institución que tengan asignado dispositivos móviles con sistema operativo Android, deberán entregar a la Oficina de Telemática el respectivo activo y subsanar las novedades presentadas debido al mal uso por parte del funcionario.

Con respecto al objetivo de control “Manejo de los soportes de almacenamiento.” perteneciente a este dominio, de dará aplicación al siguiente control con el fin garantizar la confidencialidad, disponibilidad e integridad de la información institucional:

Soportes físicos en tránsito

Los dispositivos móviles deberán estar protegidos de accesos no autorizados, garantizando su custodia en todo momento, y dejándolos fuera del alcance de personas no autorizadas.

9.1.4 Control de accesos

Con respecto al objetivo de control “Gestión de acceso a usuario” perteneciente a este dominio, de dará aplicación al siguiente control:

Gestión de los derechos de acceso asignados a usuarios

La Oficina de Telemática deberá establecer un patrón de bloqueo o contraseña para acceder a los dispositivos institucionales entregados a los funcionarios, así mismo configurar la activación del bloqueo de pantalla en determinado tiempo con el fin de garantizar la confidencialidad de la información del dispositivo.

9.1.5. Cifrado

Con respecto al objetivo de control "Controles criptográficos" perteneciente a este dominio, de dará aplicación al siguiente control:

Política de uso de los controles criptográficos

La Oficina de Telemática de la Policía Nacional determinará el nivel requerido de cifrado y la longitud de las claves criptográficas a utilizar.

9.1.6 Seguridad Física y Ambiental

Con respecto al objetivo de control "Seguridad de los equipos" perteneciente a este dominio, de dará aplicación al siguiente control:

Mantenimiento de los equipos

El mantenimiento de los dispositivos móviles será realizado únicamente por personal autorizado por la Oficina de Telemática, teniendo en cuenta las siguientes directrices:

- Elaboración y cumplimiento de acuerdo al cronograma de mantenimiento de los dispositivos móviles.
- Uso de un sistema de información para el registro de los mantenimientos realizados.

- Eliminación de manera segura la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.

Seguridad de los equipos y activos fuera de las instalaciones

El uso de dispositivos móviles fuera de instalaciones Policiales se permitirá para quienes tengan asignado y bajo su responsabilidad estos elementos y autorizados por la oficina de Telemática de la Policía Nacional, y estos deben protegerse mediante el uso de los siguientes controles:

- Evitar conectar los dispositivos móviles a redes Wifi abiertas o públicas.
- Cifrado de datos
- Restricciones en Aplicaciones
- Restricción de conectarlos a dispositivos USB
- No Descuidar dejando al alcance de personas no autorizadas, nuestro Smartphone sin una debida contraseña o patrón de desbloqueo
- No permitir el uso del dispositivo móvil por personas ajenas, en caso de ser necesario tener configurado la opción de múltiples usuarios ó usuario invitado, sin otorgar acceso a información y aplicativos del perfil de usuario del propietario.

9.1.7 Seguridad en la Operativa

Con respecto al objetivo de control “Copias de Seguridad” perteneciente a este dominio, de dará aplicación al siguiente control:

Copias de seguridad de la información

Las copias de seguridad estarán a cargo del responsable del dispositivo móvil, la Oficina de Telemática supervisará la frecuencia en la ejecución de las copias de seguridad.

9.1.8 Normas para uso de Dispositivos Móviles

Establecer configuraciones acordes para los dispositivos móviles institucionales o personales y que hagan uso de los servicios provistos por la Policía Nacional.

Establecer métodos de bloqueo para dispositivos móviles institucionales y que serán entregados y asignados a los funcionarios de La Policía Nacional. Igualmente configurar estos dispositivos para que después de un lapso de tiempo de inactividad salten automáticamente a modo de suspensión y se active el bloqueo de la pantalla el cual solicitara el método de desbloqueo configurado

Se debe activar la opción de cifrado de memoria de almacenamiento de cualquier dispositivo móvil institucional con el fin de hacer imposible copia o extracción de datos si no se conoce el método de desbloqueo.

Activar códigos de seguridad para las tarjetas SIM de los dispositivos móviles institucionales antes de ser asignados a los funcionarios y almacenar estos códigos en un lugar seguro.

Configurar una solución de copias de seguridad para aquella información contenida en los dispositivos móviles de la institución

9.1.9 Acciones que afectan la Seguridad de la Información en Dispositivos Móviles con Sistema Operativo Android

Permitir el uso de nuestro dispositivo móvil por personas ajenas, en caso de ser necesario tener configurado la opción de múltiples usuarios o usuario invitado, sin otorgar acceso a información y aplicativos del perfil de usuario del propietario.

Conectar nuestro dispositivo a redes Wifi abiertas o públicas, ya que representa un riesgo en la transmisión de los datos, teniendo en cuenta que se puede obtener información confidencial del dispositivo por medio de aplicaciones con las cuales se puede ingresar de manera ilícita, en consecuencia se debe evitar guardar información clasificada de la Institución en nuestro Smartphone

Enviar información de carácter clasificado o restringido por correo electrónico sin una debida autorización y/o protocolos establecidos.

No establecer un patrón de bloqueo o contraseña para acceder a los dispositivos institucionales entregados a los funcionarios, así mismo no configurar la activación del bloqueo de pantalla en determinado tiempo con el fin de garantizar la confidencialidad de la información del dispositivo.

Realizar o establecer acciones para eludir controles establecidos en la configuración de seguridad.

No ejercer un Control de aplicaciones por parte de personal de Telemática, debemos establecer una lista negra de aplicaciones y asegurarnos de que ninguna de estas aplicaciones se puedan ejecutar en el dispositivo móvil y utilizar el restos de aplicaciones.

Instalación de aplicaciones de fuentes desconocidas, se deben instalar aplicaciones únicamente desde sitios oficiales de los dispositivos móviles institucionales.

10. BIBLIOGRAFIA

SILES, Raúl. Seguridad de dispositivos móviles Android. . [en línea]. 2013. [consultado 03 de octubre de 2015]. Disponible en internet: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/453-Seguridad_Android/453SeguridadenAndroidmay13.pdf

ENJOY SAFER TECHNOLOGY. Tendencias 2015 el mundo corporativo en la mira. [en línea]. 2014. [consultado 03 de octubre de 2015]. Disponible en internet: http://www.welivesecurity.com/wp-content/uploads/2015/01/tendencias_2015_eset_mundo_corporativo.pdf

TREND-MICRO. Amenazas de seguridad para empresas, el estilo de vida digital y la nube. Predicciones de Trend Micro para 2013 y años posteriores. [en línea]. 2013. [consultado 03 de octubre de 2015]. Disponible en internet: http://www.trendmicro.es/media/misc/2013-predictions-security-threats-es.pdf

PAUS, Lucas. Herramientas actualizadas para pentest desde tu Android. ESET We Live Security [en línea]. 2015. [consultado 03 de octubre de 2015]. Disponible en internet: http://www.welivesecurity.com/la-es/2015/01/22/5-herramientas-pentest-android/

TORRES, Alejandro. hackeando con USB Rubber Ducky. [En línea]. 2014. [consultado 24 de noviembre de 2015]. Disponible en Internet: http://www.hackingmexico.mx/hackeando-con-usb-rubber-ducky/

ROMANO, Agustín y LUNA, Carlos. Descripción y análisis del modelo de seguridad de Android. Universidad de la Republica. [En línea]. 2013. [consultado 03 de octubre de 2015]. Disponible en Internet: https://www.colibri.udelar.edu.uy/handle/123456789/3475

CALERO ASENCIOS, Raúl. Modelo de seguridad para mitigar los problemas derivados de las vulnerabilidades en dispositivos móviles Android con respecto a los principios de integridad, confidencialidad y disponibilidad [en línea]. Trabajo de grado Ingeniero de Sistemas. Bogotá D.C.: Pontificia Universidad Javeriana. Facultad de Ingeniería, 2013. 119 p. [consultado 03 de octubre de 2015]. Disponible en Internet: http://hdl.handle.net/10554/12667

ANEXOS

Anexo A. Acta de divulgación de políticas de seguridad en teléfonos inteligentes con sistema operativo Android utilizados en la policía nacional

MINISTERIO DE DEFENSA NACIONAL
POLICIA NACIONAL
DIRECCION DE SANIDAD
SECCIONAL DE SANIDAD HUILA

TODOS POR UN NUEVO PAÍS

Fecha:	Neiva, 05 de Septiembre de 2016		
Hora de inicio:	08:30 am	**Hora de finalización:**	08:00 am
Lugar:	Auditorio Seccional de Sanidad Huila		

ACTA No. _____/ SECSA– GADFI - 5-2.92

QUE TRATA DE LA DIVULGACION DE POLITICAS DE SEGURIDAD EN TELÉFONOS INTELIGENTES CON SISTEMA OPERATIVO ANDROID UTILIZADOS EN LA POLICÌA NACIONAL

ORDEN DEL DÍA

1. Verificación de asistentes
2. Lectura del acta anterior **(No Aplica)**
3. Verificación de los compromisos **(No Aplica)**
4. Divulgación de Políticas de Seguridad en Teléfonos Inteligentes Con Sistema Operativo Android Utilizados En La Policía Nacional

Propósito Principal:

En los últimos años el uso de dispositivos móviles ha tenido un crecimiento vertiginoso, debido a las múltiples funciones que se pueden aprovechar por parte de los usuarios, todas vez que ofrecen ventajas en movilidad, teniendo en cuenta su fácil conexión a redes inalámbricas, configuración de correo electrónico, navegación en sitios web, instalación de aplicaciones móviles de diversas categorías, acceso a redes sociales, entre otros. Es así que debido a este gran uso de esta tecnología, se ha incrementado en gran medida los ataques a los dispositivos móviles afectando la seguridad de la información de los usuarios.

Los funcionarios de la Policía Nacional, han empleado en gran medida las ventajas de los dispositivos móviles tanto en el ámbito personal como laboral, dispositivos móviles con sistema operativo Android, observándose el manejo de información institucional en mencionados dispositivos, tal es el caso de configuración de correo empresarial Exchange, configuración de correo institucional Outlook, ingreso al portal de servicios internos "PSI" mediante el cual se tiene acceso a información personal e institucional del funcionario, registro fotográfico de actividades del servicio de policía, registro fotográfico de documentos institucionales. Por lo anterior se ha notado que no hay una política de seguridad de la información para estos dispositivos que garantice la confidencialidad, integridad y disponibilidad de la información institucional, vulnerabilidad que permitiría la fuga de información, ataques de virus, malware, troyanos, ataques de ingeniería social, perdida de la credibilidad e imagen institucional.

Por lo anterior, se requiere divulgar políticas de seguridad para dispositivos móviles a los funcionarios que tienen acceso por medio de estos dispositivos a información institucional, con el fin de garantizar la confidencialidad de la información.

POLÍTICAS DE SEGURIDAD

- No Descuidar dejando al alcance de personas no autorizadas, nuestro Smartphone sin una debida contraseña o patrón de desbloqueo, así mismo se deberá configurar adecuadamente el acceso y bloqueo del dispositivo.
- No permitir el uso de nuestro dispositivo móvil por personas ajenas, en caso de ser necesario tener configurado la opción de múltiples usuarios o usuario invitado, sin otorgar acceso a información y aplicativos del perfil de usuario del propietario.
- Debido a las fallas de seguridad identificadas en el sistema operativo Android, es primordial que los usuarios instalen las actualizaciones disponibles del dispositivo a la última versión disponible, esto con el fin de corregir fallas de seguridad.

- Teniendo en cuenta las vulnerabilidades encontradas en algunas aplicaciones, se requiere no instalar aplicaciones desconocidas, ya representa riesgos en la seguridad de la información, siempre tener desactivado la instalación de fuentes desconocidas.

- La plataforma del sistema operativo Android permite verificar los permisos solicitados por las aplicaciones, es necesario validar los permisos innecesarios y sospechosos.

- Debido a las fallas de seguridad presentadas en las aplicaciones de mensajería instantánea, los usuarios deberán abstenerse en enviar información clasificada de la Institución por mensajería WhatsApp u otra aplicación similar.

- Evitar conectar nuestro dispositivo a redes Wifi abiertas o públicas, ya que representa un riesgo en la transmisión de los datos, teniendo en cuenta que se puede obtener información confidencial del dispositivo por medio de aplicaciones como zANTI, en consecuencia se debe evitar guardar información clasificada de la Institución en nuestro Smartphone.

- Supervisar y monitorear la instalación de un software antivirus en los dispositivos móviles.

- Cifrar el sistema completo en Android, igualmente la información de la memoria de almacenamiento y del dispositivo, con el fin de evitar la fuga de información institucional en caso de acceso no autorizado.

- Configurar la seguridad del navegador web, para ayudar a prevenir ataques, evitando igualmente visitar sitios desconocidos.

- Crear copias de seguridad de forma periódica, con el fin de permitir la recuperación ante pérdida de datos.

- Control de aplicaciones, debemos establecer una lista negra de aplicaciones y asegurarnos de que ninguna de estas aplicaciones se puedan ejecutar en el dispositivo móvil y utilizar el restos de aplicaciones.

- No debemos seguir hipervínculos dudosos de correos, mensajes o de sitios web.

- Bloquear aplicaciones que contengan información personal y empresarial.

Elaboro por: Subintendente. Nelio Augusto Tejada Rico
Fecha elaboración: 05/09/2018
Ubicación F:\Archivo 2018\
Carrera 22 Sur No. 26ª – 21
Barrio Fronteras del Milenio
deuil.clima-almac@policia.gov.co
www.policia.gov.co

MINISTERIO DE DEFENSA NACIONAL
POLICÍA NACIONAL
DIRECCION DE SANIDAD
SECCIONAL DE SANIDAD HUILA

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Fecha:	Neiva, 05/09/2016		
Hora de inicio:	06:30	**Hora de finalización:**	08:00
Lugar:	Auditorio Seccional de Sanidad Huila		

ACTA No. ________/ SECSA– GADFI - 5-2.92

QUE TRATA DE LA DIVULGACION DE POLITICAS DE SEGURIDAD EN TELÉFONOS INTELIGENTES CON SISTEMA OPERATIVO ANDROID UTILIZADOS EN LA POLICÍA NACIONAL

ASISTENTES

GR.	NOMBRES Y APELLIDOS	UNIDAD O DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
PT	Edwer Cedeño Rivas	SECSA	Planeación	edwer.cedeno@ [illegible]	3125569419	[signature]
IT.	Gimondi Bravo Gonzalez	SECSA	Planeación	gimondi.bravo@	3124553024	[signature]
SI	Wilson Meldoz Torres	SECSA	Contratos	wilson.meldoz@correo.	3123382435	[signature]
IT	Juan Carlos Sepulveda	SECSA	Contratos	carlos.sepulveda@	3118610774	[signature]
	Maria Camilo Escobar	Secsa	Contratos	[illegible]@hotmail.	3209640962	[signature]
PT	Lina Cristina Guzman	SECSA	Secretaria	lina.guzman4644@	3138844022	[signature]
ST	[illegible]	Secsa	[illegible]	[illegible]	3209786000	[signature]
AG.	Efuer Giovanni Gonzalez	SECSA.	Conductor	efuer.gonzalez@correo.	3143866427	[signature]
PT	Karen Eliana [illegible]	SE[illegible]	[illegible]	Karen [illegible] 2[illegible]	316488[illegible]	[signature]
IJ	Yenny Garcia Bonilla	SECSA	Tesorera	yenny.garcia	3102733581	[signature]
PT	Victor Escalante	Secsa	Aux enfermería	victor.escalante@	3224844600	[signature]
CPS	Alexander Trujillo Gaona	Secsa	Eventos M.	almoto[illegible]@hotmail.	3134194710	Alexander T.T.

GR.	NOMBRES Y APELLIDOS	UNIDAD O DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
PT	Jesica Patricia Reyes Arteaga	Tesorería	Auxiliar	jesica.reyes@correo.policia.gov.co	3162350520	
PT	evelyn morales lozada	cuentas	cuentas	evelyn.morales5408@	3124970750	
CS	DANIEL GARCIA MIRANDA	SECSA	BIOMEDICO	danielgarcia.miranda@	3183512636	DANIEL GARCIA M.
SI.	LUISA FDO. VALENCIA C.	SECSA	AUX ENFERMERA	luisa.valencia@	3106660003	LUISA FDO
TS-24	CARLOS CARDENAS	SECSA	AUX ENF	704.garcia1967@	3138394770	
PT	EIMER JORGES RAMIREZ	SECSA	ESTUFETA	eimer.jorges@	3214923493	
PT	Andres Silva Hoyos	Secsa	Dail	fernando.silva1459	3106132693	
PT	YAMID DEIVAR HURTADO	SECSA	AUXILIAR	yamid.osorio@	3133509024	
PT	oscar salvador montero	SECSA	Almacen	oscar.salvador	3229477639	
IT	James Garcia Hernandez	SECSA	Seguridad	jamesgarcia@correo.policia	3004726869	
PT	Yuly catalina Rodriguez	SECSA	AUX ENFERM	yuly.Rodriguez2725	3184355589	Yuly Rodriguez.
SARG	OSIRIS VARGAS	SECSA	FISIOTERAPEUTA	OSIRIS.VARGAS@	3203451274	
PT	JULIAN TRUJILLO CALDERON	SECSA	CENTINELA	julian.trujillo3771	3207470405	
PT	EVERT ROMERO C	SECSA	CENTINELA	evert.romero1491@	3004265152	
PT	JOHANA CASTELLANOS	SECSA	Coordinadora PIP	leidycastellanos1801@	3115403490	