UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Titulo: Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones.
Autores: Pacheco Veliz, Sebastian Exequiel – Piazza Orlando, Carlos Damián
Director: Lic. Venosa Paula
Codirector: Lic. Macia Nicolas
Carrera: Licenciatura en Sistemas - Plan 2007

Resumen

Las amenazas que atentan contra la seguridad de los dispositivos móviles: malware, robo, fuga de información, vulnerabilidades de software y phishing entre otras ponen en riesgo la seguridad personal de los usuarios y de los activos de información de las organizaciones en las que estos trabajan.
Esta tesis trata sobre el impacto del uso de los dispositivos móviles personales en las organizaciones lo cual se conoce como: Bring Your Own Device (BYOD). Este fenómeno constituye un campo de interés para que quienes estudian problemáticas relacionadas a la seguridad de la información en dispositivos móviles, puedan expandir sus análisis a ambientes organizacionales.
Se presentan las líneas de trabajo abordadas, herramientas probadas, guías y buenas prácticas generadas para usar de manera segura dispositivos móviles en una organización.

Palabras Claves

Dispositivos móviles, Seguridad, Amenazas, BYOD (Bring Your Own Device), TI (Tecnologías de Información), MDM (Mobile Device Manager), Política BYOD

Conclusiones

El uso extendido de dispositivos móviles ha hecho que se conviertan de manera activa en una herramienta de trabajo, alojando en ocasiones información crítica y valiosa. La concienciación del usuario es y seguirá siendo un factor determinante para los daños y la exposición al malware. El fenómeno BYOD se presenta como una realidad difícil de restringir y controlar. A la hora de diseñar e implementar soluciones y gestionar la seguridad, se debe abordar la problemática en forma integral.

Trabajos Realizados

Para ayudar a comprender la problemática se realizaron:
- Investigación de problemas de seguridad, tipos de ataques y la metodología BYOD.
- Análisis estadístico acerca de sobre dispositivos móviles y amenazas existentes.
- Análisis de funcionalidades y características de una herramienta de gestión de dispositivos MDM.
- Creación de una política de seguridad para BYOD, como una guía aplicable a organizaciones.
- Creación de una Prueba de Concepto para ejemplificar cómo una aplicación maliciosa podría hacerse de información sensible de un usuario.

Trabajos Futuros

Los trabajos futuros que se proponen son:
Realizar un relevamiento de herramientas MDM actuales, libres y pagas, comparando características y analizando cuales se adecuan mas a una tipo de organización.
Desarrollar una aplicación MDM que sea útil para organizaciones pequeñas y medianas como las PYMES.
dispositivos IoT, conformar un grupo de trabajo que se encargue de analizar la problemática, comparando protocolos de seguridad de empresas que desarrollan nuevos dispositivos IoT.

Fecha de la presentación: Noviembre 2016

Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones.

UNIVERSIDAD NACIONAL DE LA PLATA

Facultad de Informática

Pacheco Veliz, Sebastian Exequiel

Piazza Orlando, Carlos Damian

Tesis presentada para optar al título de

Licenciatura en Sistemas

Director: *Lic. Paula Venosa*

Co-Director: *Lic. Nicolas Macia*

La Plata, 2016

Esta tesis está dedicada especialmente a:
Nuestros padres, por habernos formado y dado todo lo que
necesitábamos en esta vida;
Nuestros amigos y familiares que contribuyen a formarnos profesional, ciudadana y
personalmente.

Agradecimientos

Queremos agradecer a todos los que hicieron posible que hayamos llegado a este punto de culminación de nuestra carrera, familiares y amigos.

Gracias a nuestros directores de Tesina por habernos apoyado en esta propuesta y por habernos guiado para realizarla de la mejor manera posible.

Gracias Nicolás por habernos dado la oportunidad de ser parte del CeSPI, por acercarnos a los directivos del área de Redes e Infraestructura para embarcarnos en lo que fue nuestra primera experiencia laboral y que siempre recordaremos.

Gracias Nicolás y Paula por incentivarnos a participar en los Workshops de Investigadores en Ciencias de la Computación (WICC) 2014 y 2015, y en el Congreso Argentino de Ciencias de la Computación (CACIC) 2016, nuestros primeros proyectos de investigación y presentación en el ámbito de la investigación.

Gracias Paula por elegirnos para ser parte de la creación del taller *"Aprendiendo a estar digitalmente seguros"* en el marco del proyecto *"EXTENSIÓN en vínculo con escuelas secundarias"*.

Gracias a todos los profesores que nos transmitieron sus conocimientos durante todas las cursadas, sin ustedes no podríamos estar en el lugar donde estamos.

Índice general

Marco Teórico

1. Motivación: La necesidad de la seguridad

Hoy en día, los dispositivos móviles son un elemento común en la vida diaria de las personas. A partir del uso masivo de dispositivos móviles, tanto en el ámbito personal como en el laboral, las organizaciones están empezando a considerar más detenidamente el suceso y los potenciales problemas de seguridad que los afectan. Los problemas de seguridad a los que estos dispositivos están expuestos son similares a los que está expuesto una computadora, pero se ven agravados ya que cuentan con una mayor exposición al ser más amplia su comunidad de usuarios, que los utiliza tanto en el ámbito laboral como en el personal.

Al decir datos podemos estar refiriéndonos tanto a información privada del dueño del Smartphone como así también información propia de la organización puesto que el usuario usa el teléfono para conectarse a servicios provistos por esta, lo cual se refiere con el nombre de BYOD. El fenómeno "Trae Tu Propio Dispositivo" (BYOD por sus siglas en inglés, Bring Your Own Device) se basa en la modalidad en la que los miembros de una organización son autorizados a utilizar sus propios dispositivos móviles personales (smartphones, tablets, notebooks, etc) en las actividades de la organización donde trabajan conectados a la red organizacional. El uso de sus dispositivos para realizar sus tareas laborales en la organización provoca que lo que era un dispositivo personal se convierta en parte de la red organizacional, con los problemas que esto podría acarrear.

De acuerdo a varios estudios[1,2,3], un malware[4] que afecte a una computadora o a un móvil puede utilizarse para:

- Robo de Información personal.

- Espionaje de actividad y comportamiento del usuario (Historial de navegación, mensajes, llamadas, ubicaciones, etc.).
- Envío de SMS Premium que generen un costo al usuario, suscripción a servicios Pagos.
- Control remoto el dispositivo (Bot de una Botnet).
- Causar comportamiento destructivo al dispositivo (agotamiento de la batería, reinicios no deseados, consumo de RAM y/o CPU, etc.).
- Enviar spam mediante SMS o emails.
- Robar información personal del usuario y demandando un pago para que el cliente pueda recuperarla (Ransomware).

La problemática presentada se potencia tanto debido al desconocimiento general sobre los problemas de seguridad a los que están expuestos como a la falta de información en las contramedidas que es posible adoptar. Si a ello le sumamos la cantidad de elementos incluidos en los smartphones se dan otros problemas, como los relacionados con el espionaje, puesto que un dispositivo comprometido podría permitir consultar su localización vía GPS, transmitir la información captada por su micrófono o incluso su cámara.

Cuantificando el problema, se pueden sumar los problemas propios de las distintas plataformas de SO móviles a los de las aplicaciones que corren en ellas. Para citar un caso, Android, el sistema operativo para dispositivos móviles más utilizado en la actualidad[5] posee un gran número de versiones, algunas de ellas, hoy en día, sin actualizaciones. De acuerdo a un relevamiento realizado a fines de Febrero de 2015[6], el 58,7% de los celulares Android no tiene soporte y debería ser actualizado como mínimo a la versión 4.4 (KitKat). Además las actualizaciones se ven demoradas debido a que, en primer lugar, Google libera nuevas versiones; luego los fabricantes las adaptan para sus dispositivos; y finalmente las organizaciones de telecomunicaciones lo vuelven a modificar agregando personalizaciones, como ser el logo de la organización. Una vez

finalizado este proceso, el sistema operativo queda liberado. Esto resulta en una convergencia lenta y en ciertos equipos hasta imposible, lo que deja algunos dispositivos vulnerables frente a ataques que explotan vulnerabilidades ya corregidas en versiones posteriores del sistema. Por otro lado, desde la aparición de los Smartphones han ido surgiendo distintas prácticas cuyo objetivo es que el usuario obtenga un control total de su equipo, salteando ciertas restricciones impuestas por el fabricante/desarrollador. Entre estas prácticas podemos mencionar: rootear un teléfono Android, instalar aplicaciones no oficiales, jailbreak de iPhone, etc. Estas prácticas se realizan sin tener en cuenta el impacto que tienen sobre la seguridad de los datos almacenados y transmitidos.

Por lo anteriormente detallado, el fenómeno BYOD constituye una de las amenazas actuales más preocupantes para las organizaciones. Un smartphone comprometido, automáticamente pone en riesgo:

- La clave de la/s red/es a la que el dispositivo se conecta.
- El usuario de la cuenta de correo utilizada.
- El usuario de la cuenta de mensajería instantánea utilizada.
- Accesos VPN que puedan haber configurados.
- Información de contactos personales.
- Información sensible de la organización que se contenga en el dispositivo.

Algunos de los problemas de seguridad pueden mitigarse mediante el uso de software de tipo MDM[7] (Mobile Device Management) el cual permite asegurar, monitorear y administrar dispositivos móviles de manera centralizada. Esto solo puede aplicarse en forma compulsiva sobre los dispositivos que son propiedad de la organización, pero no así sobre los dispositivos personales de los integrantes. Al carecer de la posibilidad de gestionar los equipos, los activos de la organización pueden verse comprometidos tanto cuando circula información por equipos en poder de los miembros de la organización sin el pertinente estado de seguridad, como ante la pérdida o robo de uno de estos dispositivos. Por ejemplo si el dispositivo no posee un PIN o no está protegido por una

contraseña segura, un atacante puede obtener acceso directo al dispositivo, sus datos, e incluso todo el contenido que continúa llegando a través de los servicios que continúen activos. Medidas parciales, como un equipo protegido por contraseña, no lo hacen completamente inmune, puesto que es posible extraer la tarjeta de memoria y si la misma no está fuertemente cifrada, el atacante tendrá acceso a sus datos.
Debido a todo lo mencionado, un dispositivo privado no debe ser considerado fiable para su uso con información de la organización hasta que una adecuada revisión confirme que el mismo cumple todos los requisitos especificados en la política de seguridad organizacional.

En la actualidad, el tema aquí abordado resulta de interés dado que aún no se cuenta con información completa y precisa relacionada a qué medidas adoptar, tanto por parte de los usuarios como por parte de las organizaciones, a fin de preservar la seguridad de la información contenida en los dispositivos móviles. Además, también es de vital importancia el estudio de metodologías y técnicas de análisis que permitan determinar la existencia o no de amenazas reales sobre los dispositivos móviles analizados. Dentro de este marco se realizaron 3 presentaciones de trabajos relacionados al tema en cuestión, WICC 2014 (Workshop de Investigación en Ciencia de la Computación) Universidad Nacional de Tierra del Fuego, Ushuaia, presentación de Poster *"Seguridad en dispositivos móviles, un enfoque Práctico"* en el marco del área Seguridad Informática; WICC 2015 Universidad Nacional de Salta, Salta, Presentación de Póster *"Uso de dispositivos móviles y BYOD: Su impacto en la seguridad"* en el marco del área Seguridad Informática; CACIC 2016 (Congreso Argentino de Ciencias de la Computación) Universidad Nacional de San Luis, San Luis, publicación del paper *"Dispositivos móviles y el fenómeno del BYOD. Su impacto en la seguridad de las Organizaciones"*.

2. Introducción: Plataformas de SO Móviles

En este capítulo nos referiremos a los diferentes Sistemas Operativos que lideran el mercado mundial, entre ellos Android, iOS y Windows Phone; sus características generales, arquitectura y situación actual de los mismos; como es la creación y distribución de aplicaciones para cada SO y las nuevas características de sus Sistemas Operativos más actuales.

Cada plataforma tiene su propia arquitectura de Sistema Operativo, pero todas comparten algunas similitudes, sobre todo cuando se trata del Sandboxing. Sandboxing se refiere al aislamiento de aplicaciones y significa que una aplicación se ejecuta en su propia máquina virtual para limitar el acceso a otras aplicaciones, a zonas de memoria y recursos que no le pertenecen y al sistema operativo. El aislamiento de procesos (del inglés sandbox) es un mecanismo para ejecutar programas con seguridad y de manera separada. Este aislamiento permite controlar de cerca los recursos proporcionados a los programas "cliente" a ejecutarse, tales como espacio temporal en discos y memoria. Habitualmente se restringen las capacidades de acceso a redes, la habilidad de inspeccionar la máquina anfitrión y dispositivos de entrada entre otros. Para utilizar las características del sistema, tales como la conectividad de red, cada característica debe declararse específicamente por la aplicación y debe ser permitido para poder obtener el acceso desde su entorno sandbox. Esta sección proporciona una visión general de la arquitectura de sistema de cada plataforma, sus características más destacadas de seguridad y del proceso de desarrollo de aplicaciones.

El foco central en este trabajo será la plataforma Android ya que, como se mencionó anteriormente, es el SO móvil que predomina en el mercado hace ya varios años, análisis de mercado recientes[8] realizado por la International Data Corporation (IDC), proyecta que la plataforma seguirá en auge y que inclusive su “dominancia” de mercado se incrementará. IDC estima que Android mantendrá su amplio dominio en el sector hacia el año 2019. Des los 81.2 puntos porcentuales de 2015, dentro de cinco años la cuota del SO

móvil de Google crecerá hasta el 82.6%. IOS ira de los actuales 15.8 por ciento a los 14.1%, prevé la consultora. Por su parte, Windows Phone crecerá apenas un 0.1%, de los 2.2 puntos correspondientes a 2015. Por lo que Android resulta de un mayor atractivo a la hora de hablar sobre conceptos de seguridad de plataformas móviles ya que al ser el más masivo, también es lo que más se intenta vulnerar por parte de los atacantes.

Operating System	2015 Shipment Volumes	2015 Market Share	2015 YoY Growth	2019 Shipment Volumes	2019 Market Share	2015 YoY Growth	5 year CAGR
Android	1,161.1	81.2%	9.5%	1,538.1	82.6%	4.8%	7.7%
IOS	226.0	15.8%	17.3%	263.4	14.1%	3.1%	6.5%
Windows Phone	31.3	2.2%	-10.2%	43.6	2.3%	11.4%	4.5%
Other	11.3	0.8%	-16.8%	17.1	0.9%	6.5%	4.7%
TOTAL	1,429.8	100.0%	9.8%	1,862.3	100.0%	4.7%	7.4%

Figura 1. Pronóstico mundial de smartphones por SO (Shipments in millions, Market Share, Year-Over-Year Growth, and 5-Year CAGR)

2.1. Google Android

El proyecto Android es una plataforma de código abierto originalmente desarrollado por Android, Inc. Fue comprado por Google en 2005 y la primera versión fue presentada en 2007 en relación con la fundación Open Handset Alliance (OHA)[9], una organización que crea estándares abiertos para plataformas de dispositivos móviles. La primera versión comercial de Android que salió al mercado fue la versión Android 1.0 Apple Pie (Tarta de Manzana) en el año 2008, introduciendo el Market de Aplicaciones. Actualmente se encuentra en su versión 7.0 Nougat , fue lanzada oficialmente en agosto del 2016. Cuando Android libera una nueva versión de su sistema operativo cada fabricante de móviles (excepto la línea Nexus de Google que trae android por defecto en su versión original sin modificaciones de marcas ni operadoras) adapta el SO agregando toques personales (llamados "shells", son generalmente modificaciones de la interfaz gráfica, logos de inicio, etc) por lo que las actualizaciones tardan un poco más y además dependen de los fabricantes por lo que recién están llegando a algunos modelos de alta gama, en algunos casos no hay fechas y en muchas marcas hay equipos en los que ya se anunció que no

recibirán actualización alguna. Sumado a esto tenemos que considerar que cuando los móviles son comprados a operadoras, estos también realizan modificaciones sobre el SO por lo que las actualizaciones también dependen de las operadoras lo que demora aún más el tiempo de actualización (si es que la operadora la realiza).

Arquitectura del Sistema

La plataforma Android está basada en el sistema Linux (posee un kernel Linux) y ha heredado varios de sus elementos de seguridad. Uno de ellos es la protección basada en el usuario utilizada en sandboxing. Cada aplicación se ejecuta como un proceso separado usando un identificador único (UID), se aísla la aplicación de otras aplicaciones para asegurarse de que sólo puede acceder a sus propios recursos previstos. Por ejemplo, la aplicación A no puede leer los archivos que pertenecen a la aplicación B y viceversa. Una aplicación Android puede hacer uso de varios recursos del sistema. Sin embargo, la mayoría de ellos están prohibidos sin el permiso adecuado. Los permisos son necesarios para tener acceso a las funciones del sistema operativo, como la conectividad a Internet o funcionalidad sensible, por ejemplo, SMS. El permiso para un determinado recurso debe ser declarado explícitamente en el manifiesto de la aplicación y el usuario debe aceptar los permisos más sensibles tras la instalación. Al usuario se le mostrará una lista de todos los permisos que la aplicación ha declarado en su manifiesto, con el fin de proporcionar alguna información sobre el comportamiento de la aplicación. Hay cuatro tipos de permisos y están clasificados por su potencial impacto que podrían tener en el sistema.

- **Normal**: Permisos de bajo riesgo; concede automáticamente sin intervención del usuario o de la notificación en la instalación. Permisos que no son especialmente peligrosos si se obtienen.
- **Peligroso**: Permisos de riesgo medio; concedido por el usuario en la instalación. De lo contrario, no se instalará la aplicación. Los permisos no se pueden conceder de forma selectiva y, por tanto, se conceden todos los permisos o ninguno en absoluto.
- **Firmado**: Permisos de alto riesgo; Estos permisos son poderosos pero no están disponibles para los desarrolladores regulares. Permisos que solo pueden ser

otorgados a otros paquetes que se han firmado con la misma firma que la declarada en el permiso.

- **Sistema o Firmado**: Permisos de firma que también se conceden a los paquetes instalados en la imagen del sistema. Están destinados únicamente a las aplicaciones firmadas por el mismo desarrollador.

La declaración de permisos permite que el sistema pueda monitorear y restringir las aplicaciones que están tratando de comunicarse fuera de su entorno virtual aislado para evitar que aplicaciones maliciosas consigan demasiada influencia sobre el sistema.

El proyecto Android cuenta con su propia máquina virtual (VM) desarrollada para el control de sus aplicaciones. En las versiones anteriores a la 4.4 (kitkat) la máquina es denominada máquina virtual Dalvik (DVM, Dalvik Virtual Machine por sus siglas en inglés), un software de código abierto responsable de gestionar las aplicaciones en Android, a partir de la versión 4.4 se reemplazó por ART (Android Runtime). Las mayores diferencias que existen entre las 2 máquinas virtuales se encuentran en como realizan la compilación/traducción de las aplicaciones a la hora de ejecutarlas[10]. Las aplicaciones de Android se distribuyen en formato .apk. Un .apk es un formato de empaquetamiento que contiene todo lo necesario de la aplicación (imágenes, recursos, manifiestos xml, etc) y lo más importante, las clases de java compiladas en un formato de bytecode conocido como DEX. El formato DEX es independiente de la arquitectura del procesador, por lo que para ser ejecutado necesita traducirse a "código máquina" nativo para el procesador del dispositivo. La diferencia fundamental entre Dalvik y ART es cuando realizan esta traducción o compilación. Dalvik utiliza lo que se llama compilación "justo a tiempo" (just-in-time, o JIT), mientras que ART utiliza compilación previa (ahead-of-time, o AOT)[11]. Con el compilador JIT de Dalvik, cada vez que iniciamos una aplicación, la máquina virtual dinámicamente traduce un parte del bytecode DEX a código máquina. Conforme continúa la ejecución de la aplicación, se compila más bytecode y se almacena en memoria caché. Es por ello que se dice que la aplicación está siendo compilada "justo a tiempo" conforme la usamos. En el caso de ART, las aplicaciones se compilan desde que se instalan en el dispositivo, y ya se deja instalado el

código máquina listo para ejecutarse y sin necesidad de mayor compilación. Está optimizado para funcionar con los dispositivos que se alimentan de la batería y limitados como la Unidad Central de Procesamiento (CPU) o recursos de memoria. Debido a sus bajos requerimientos de recursos la VM puede funcionar eficientemente en varias instancias de máquinas virtuales de forma simultánea, lo que da una buena calidad para la sandboxing. Las Aplicaciones Android están escritas en Java, pero se ejecutan en la VM que provee android (Dalvik o ART), que difiere de la tradicional Java Virtual Machine (JVM) que se utiliza en Java. La compilación puede verse como un proceso de dos pasos: el compilador Java genera el bytecode JVM para compilar el código fuente y almacenarlo como archivos de clase. A continuación, el compilador Dalvik consume los archivos de clase compilados y los vuelve a compilar en un solo archivo índice, que será parte del paquete de la aplicación final para Android (APK).

Respecto al arranque del SO, el proceso de inicio de Android puede ser descrito brevemente en seis pasos. Cuando el dispositivo está encendido se ejecutará el código de arranque ubicado en la memoria de sólo lectura (ROM). Se carga el cargador de arranque en la memoria RAM y una vez finalizada la ejecución, se continuará con el gestor de arranque. El gestor de arranque destina una parte separada de la memoria RAM y cargará el gestor de arranque principal en ella. A continuación, los parámetros de bajo nivel se inicializan en el sistema, como la configuración de los sistemas de archivos y asignación de memoria adicional, y si tiene éxito, entonces la ejecución seguirá para cargar el kernel de Linux. El kernel de Linux es responsable de la inicialización del sistema (por ejemplo, inicialización de los drivers). Cuando la inicialización se completa entonces el núcleo se encuentra el archivo init.rc en el sistema de archivos raíz. Este es el nodo raíz de la cual se pondrá en marcha todos los procesos futuro del usuario (o uno de sus hijos). El siguiente y último paso del proceso de arranque es la iniciación y ejecución del servidor del sistema en el cual se iniciarán todos los servicios y administradores de Android. Los diferentes servicios se pueden ver en la figura 2. Una vez que todos los servicios se han iniciado correctamente, entonces el proceso de arranque se ha completado.

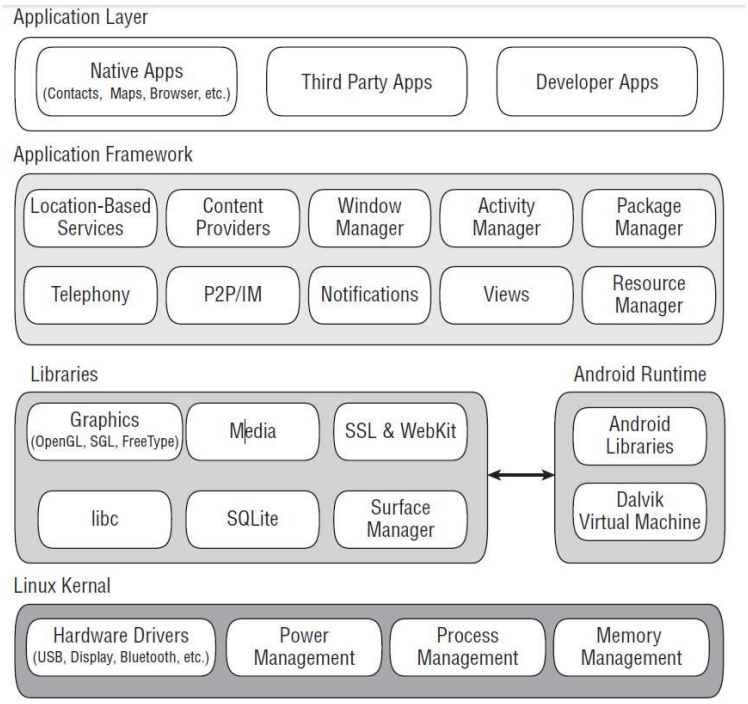


Figura 2. Android Software Stack.

Desarrollo de aplicaciones

La API de Android y el kit de desarrollo de software (SDK) están disponibles públicamente para cualquier desarrollador. No es necesario registrarse para empezar a desarrollar en Android, pero con el fin de publicar y distribuir aplicaciones en Google Play, se requiere una cuenta de Google. Una vez que la cuenta ha sido creada, un desarrollador debe activar la Consola de Desarrollador de Google Play y pagar una pequeña cuota de inscripción para utilizar el servicio. Sin embargo, Google Play no es necesariamente el único canal para la distribución de aplicaciones de Android. La plataforma puede permitir el uso de aplicaciones de terceros si esta opción ha sido habilitada por el usuario. Entonces es posible descargar e instalar aplicaciones desde cualquier fuente disponible.

Con el fin de instalar una aplicación, oficial o de terceros, debe llevar una firma digital emitida por el desarrollador. Si un paquete de aplicación no está firmado, será rechazada por el instalador de paquetes. Es costumbre que antes de que se libere una nueva versión de Android de manera comercial, se libera el SDK para los desarrolladores para así poder

ir adaptando sus aplicaciones a las nuevas versiones o familiarizarse con los cambios que se van a introducir en la nueva versión.

Informe de Google sobre seguridad en Android período 2015

Por segundo año consecutivo Google publica un informe en el que viene a destacar el estado actual de la seguridad en dispositivos Android[12]. El informe brinda una mirada a la forma en que se protege todo el ecosistema Android, las nuevas medidas de seguridad introducidas durante el 2015 y el trabajo realizado con socios y la comunidad de investigación de seguridad en general. Para proteger el ecosistema Android y sus usuarios, Google proporciona un conjunto de servicios de seguridad que se incluyen automáticamente como parte de los Google Mobile Services (GMS). Estos incluyen tanto los servicios basados en la nube como servicios integrados en el propio dispositivo como aplicaciones de Android.

El documento se basa en los adelantos y mejoras en relación a la seguridad en Android realizadas por Google durante el 2015. La compañía destaca que durante el pasado año se ha incrementado su comprensión del ecosistema utilizando sistemas automatizados que incorporan correlación de eventos a gran escala y ejecutando más de 400 millones de análisis de seguridad automáticos por día en los dispositivos con servicios de Google Mobile.

La mayor amenaza sigue siendo la instalación de aplicaciones maliciosas, lo que Google llama Aplicaciones Potencialmente Perjudiciales (Potentially Harmful Applications o PHA), aplicaciones que pueden dañar el dispositivo, dañar al usuario del dispositivo o hacer algo no autorizado con los datos del usuario. El escaneo en busca de malware de más de 6.000 millones de aplicaciones instaladas al día revela una media de menos del 0,5% de los dispositivos tenía algún software de este tipo instalado durante 2015 y esa media desciende a menos del 0.15% en dispositivos que sólo tienen instaladas aplicaciones desde Google Play. Las mejoras realizadas durante el pasado año para hacer más difícil la existencia de aplicaciones maliciosas en Google Play han reducido la probabilidad de instalar una aplicación potencialmente dañina desde la tienda de Google

en un 40% en comparación con el 2014. Las aplicaciones recolectoras de datos han bajado en un 40%, el spyware en un 50% y los "downloaders" en un 50%.

El informe revela que el riesgo de instalar una aplicación desde un repositorio externo a Google Play es máximo. En esta ocasión la compañía llega a calcular que el peligro de encontrar una aplicación maliciosa es hasta 10 veces mayor si la instalación se realiza desde fuera de Google Play.

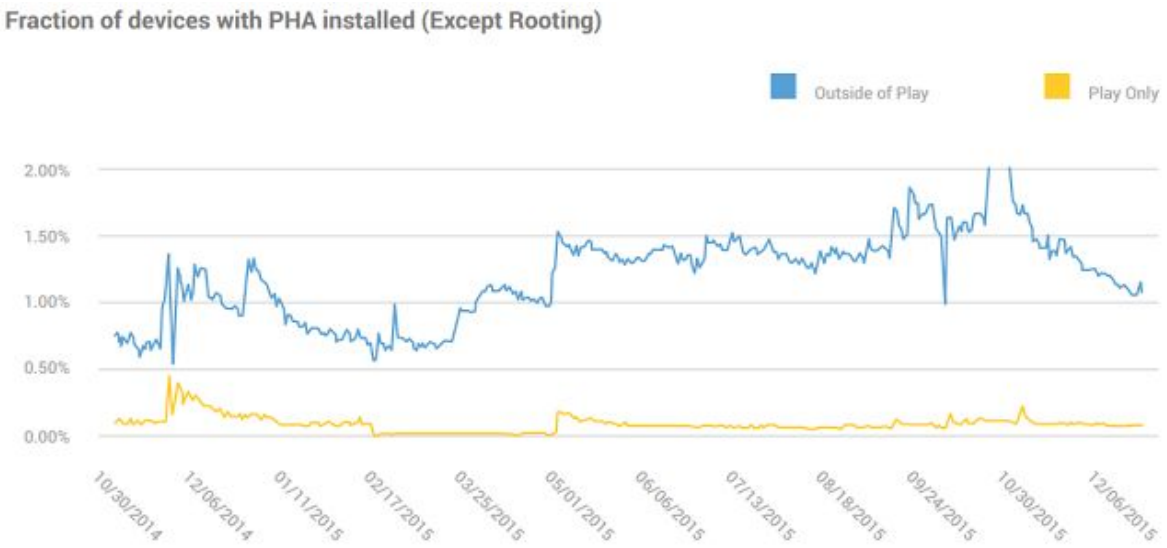


Figura 3.Porcentaje de dispositivos con PHA instaladas

Entre las medidas de protección de Google integradas en el dispositivo en 2015 están:

- **Verify Apps:** Protección contra aplicaciones potencialmente maliciosas.
- **SafetyNet:** Protección frente a la red y amenazas basadas en aplicaciones.
- **Safebrowsing:** Protección frente a sitios web inseguros.
- **Developer API:** Proporcionar a las aplicaciones una forma de utilizar los servicios de seguridad de Google.
- **Android Device Manager:** Protección a dispositivos perdidos o robados.
- **Smart Lock:** Mejorar la autenticación de usuario y protección física.

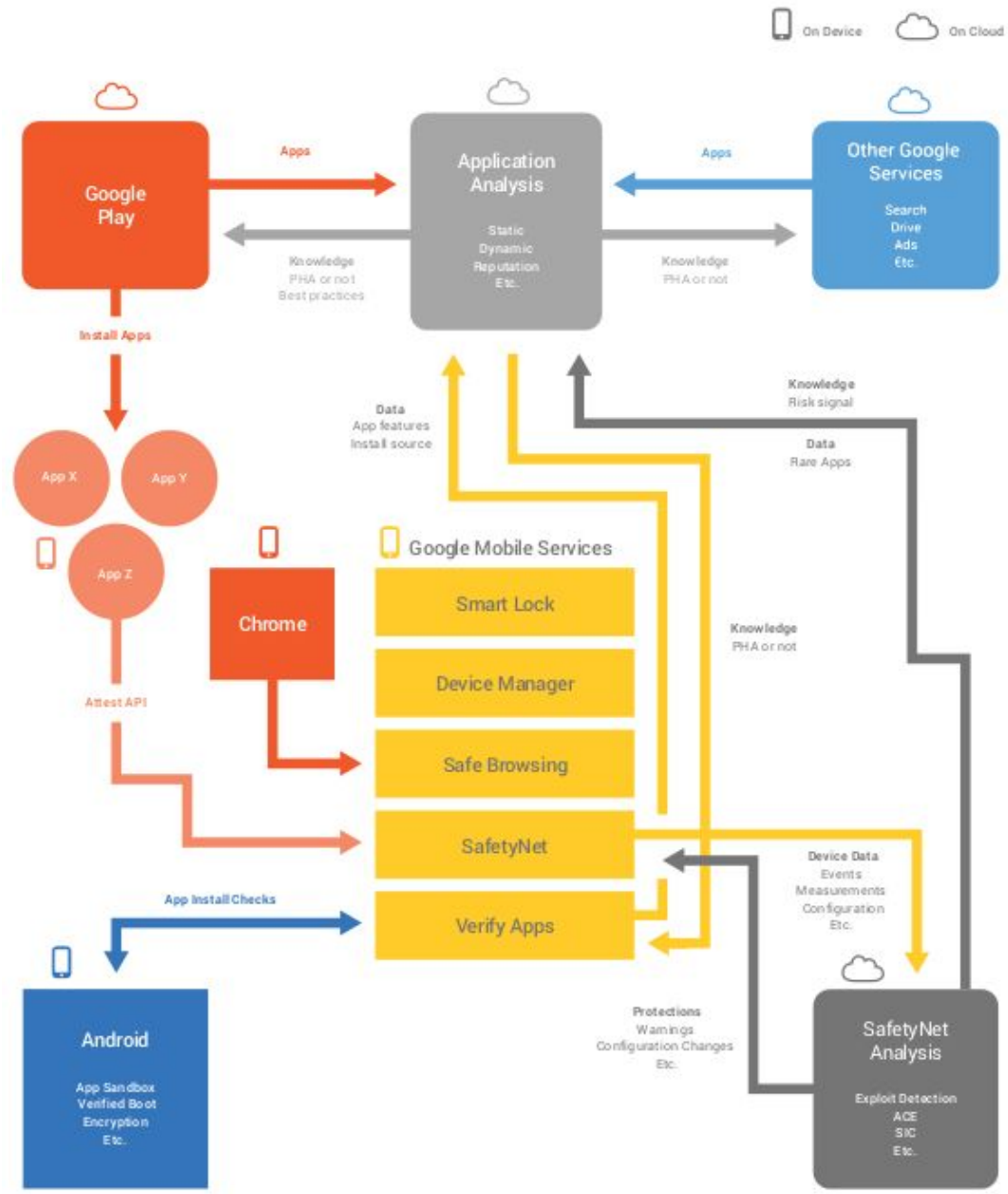


Figura 4. Representación de Servicios

También se destaca el lanzamiento de Android 6.0, conocida como Marshmallow, durante el 2015, y la mejora en la seguridad que el nuevo sistema ha significado. Con soporte para sensores de huellas dactilares, sandbox de aplicaciones, arranque verificado, mejora en la seguridad de usuario, cambios en el modelo de permisos, mayor control de los datos y capacidades que cada aplicación puede acceder. El cifrado es obligatorio para todos los

dispositivos que lo soporten, y se ha extendido para permitir el cifrado de datos en tarjetas SD.

2.2. Apple iOS

iOS es el sistema operativo móvil de Apple. Se basa en la arquitectura de Mac OS X y ha heredado muchas de sus características de seguridad para proporcionar iOS con una base sólida de seguridad[13].

Arquitectura del Sistema

Los dispositivos iOS se construyen con múltiples capas de seguridad, sistemas de protección de los componentes de bajo nivel (firmware, hardware, gestores de arranque, etc.) más componentes de alto nivel (aplicaciones y servicios). Estos utilizan diversos conjuntos de certificados digitales y una cadena de confianza para garantizar la autenticidad de sus componentes de bajo nivel. La integridad de todos los componentes se verifica durante el proceso de arranque para garantizar que el iOS se ejecuta en un dispositivo auténtico de Apple, y esto es posible ya que cada componente ha sido firmado digitalmente por Apple.

En el proceso de arranque, el primer paso es ejecutar el código de la ROM de arranque que también contiene el certificado Apple Root CA que se utiliza para verificar el siguiente paso en el proceso de arranque, el gestor de arranque de bajo nivel (LLB, Low Level Bootloader). Una vez que el LLB ha sido verificado y ejecutado con éxito entonces el siguiente paso del gestor de arranque, llamado iBoot, es verificado por la LLB. La LLB, a su vez verifica el núcleo iOS después de la finalización y así sucesivamente hasta que el sistema esté en funcionamiento (Fig. 5). Si uno de los componentes no se inicia o no se puede verificar, entonces el proceso de arranque se dará por terminado inmediatamente. Un intento de arranque fallido activará el modo de recuperación del dispositivo y el usuario se verá obligado a restaurar la configuración predeterminada de fábrica mediante una PC.

Figura 5. Secuencia de arranque en iOS.

Las características de alto nivel verifican que la integridad de los datos del usuario no se han visto comprometida, por ejemplo, aplicaciones no autorizadas o el propio sistema operativo. Al igual que Android, iOS utiliza sandboxing para aislar cada aplicación del resto del sistema y está prohibido por defecto todas las comunicaciones con otras aplicaciones o el sistema operativo. Una aplicación puede solicitar el acceso a los recursos del sistema al declarar un conjunto de derechos. Los derechos son esencialmente "reglas de entorno limitado" que especifican lo que una aplicación puede acceder fuera de su entorno de pruebas. Así que para tener acceso, por ejemplo, la conexión de red, un desarrollador tiene que declarar el derecho correspondiente. La capacidad de utilizar los derechos es muy restringida para aplicaciones de terceros, y la mayoría de ellos sólo pueden ser utilizadas por las aplicaciones del sistema con el fin de minimizar el riesgo de una escalada de privilegios. Cabe señalar que las aplicaciones del sistema comparten de forma diferente que otros, ya que pueden comunicarse entre sí sin ningún tipo de restricciones específicas.

Apple tiene un esquema de cifrado integrado en su núcleo que no se puede configurar por el usuario. Con el fin de evitar problemas de rendimiento y de batería, cada dispositivo iOS tiene un motor de 256-bit AES de cifrado incorporado y un módulo de algoritmo de hash seguro (SHA-1) incluído en el hardware. El motor de cifrado se implementa estratégicamente entre la memoria RAM y el almacenamiento flash para cifrar y descifrar los datos de manera eficiente.

Cada dispositivo tiene un UID que es una clave de 256 bits y se fusiona en el hardware. La clave es sólo accesible por el motor AES y no puede ser leído por el firmware o software. El UID se escribe en forma permanente en el hardware con el fin de proporcionar una clave que se utiliza para los datos de vinculación criptográfica a un dispositivo específico. Los datos no pueden por lo tanto ser accedidos por otro

dispositivo, incluso si los módulos de memoria reales se eliminan físicamente de un dispositivo y se insertan en otro.

iOS Protección de Archivos

iOS utiliza una jerarquía de claves de cifrado para asegurar que los datos estén protegidos adecuadamente. La tecnología se llama Protección de Archivos de Datos, y está diseñado especialmente para dispositivos móviles. La Protección de Archivos de Datos se asegura de que sólo los datos relevantes para una tarea específica son descifrados. Dado que el cifrado está siempre habilitado en los dispositivos iOS, todos los datos tienen que ser descifrados antes de que puedan ser presentados al usuario a través de la aplicación que los solicitó. El descifrado se realiza dentro del motor AES utilizando los datos proporcionados y su clave correspondiente. Cada archivo está protegido por una clave de archivo único que se envuelve y se almacena en los metadatos del archivo. Además, los metadatos se cifran mediante una clave de sistema de archivos y esa llave está protegida por la clave junto con el UID del dispositivo. El esquema de cifrado fuerte hace que los ataques de fuerza bruta literalmente sean imposibles, ya que tomaría años en descifrarlos.
La clave de archivo se cifra utilizando una clave de clase que es también una descripción del nivel de protección de un archivo en particular. Hay cuatro clases de protección diferentes:

- **Complete Protection**: Esta es una clase de protección muy completa y la clave se genera utilizando el UID y el código de acceso del usuario (contraseña). Los datos sólo se pueden acceder cuando se desbloquea el dispositivo. Cuando se activa la pantalla de bloqueo, la clave de clase se borrará dentro de los 10 segundos y los datos no se podrá leer hasta que el usuario desbloquee el dispositivo de nuevo.
- **Protected Unless Open**: Esta clase permite que los datos sean escritos, incluso si la pantalla de bloqueo se activa y permitiría a los procesos de fondo continuar. Se crea una clave secreta compartida entre la clave del archivo y la clave de clase para mantener el proceso en ejecución y para descifrar los datos, se borrará la clave de clase cuando el dispositivo esté bloqueado.

- **Protected Until First User Authentication**: Esta clase es similar para completar la protección aunque esta clase sólo requiere que el dispositivo sea desbloqueado una vez. La clave de clase de descifrado no se elimina y estará disponible hasta que se reinicie el dispositivo.
- **No Protection**: Esta es la clase por defecto y se selecciona automáticamente si un archivo no solicita otro tipo de protección. La clave de clase se almacena en el almacenamiento borrable y sólo está protegido por el UID. El nombre de esta clase puede ser confuso ya que los datos reales pueden estar cifrados en el almacenamiento. Si un borrado remoto se activa entonces los datos relacionados con esta clase también serán inaccesibles, por lo tanto, se proporciona la protección.

Desarrollo de Aplicaciones

El desarrollo de aplicaciones para iOS es mucho más restrictiva que en otras plataformas. La distribución de aplicaciones es controlado por Apple y bajo condiciones estándar sólo se pueden adquirir a partir de su App Store. Sin embargo, las organizaciones también tienen la oportunidad de utilizar un canal de distribución privada para sus aplicaciones internas utilizando el iOS Developer Enterprise Program (IDEP)[14] para evitar la cadena pública utilizando certificados especiales que les permiten desarrollar aplicaciones para sus miembros y distribuir esas aplicaciones por fuera de la App Store oficial.

Con el fin de comenzar a desarrollar aplicaciones y subirlos a la App Store, cada desarrollador tiene que registrarse en el Programa de Desarrolladores de iOS para convertirse en un desarrollador certificado Apple. Cada aplicación debe ser firmada digitalmente mediante un certificado Apple Issued que se le da al programador una vez registrado como desarrollador certificado. El certificado es personal y está vinculado a un individuo real u organización. Esto significa que si se presenta una aplicación maliciosa, el desarrollador responsable puede ser identificado por Apple, o si en una aplicación no se encuentra una firma correcta, entonces será rechazada por App Store inmediatamente. Una vez que se presente una solicitud debe ser revisada y aprobada antes de su publicación en el App Store. Apple inspecciona todas las aplicaciones en busca de

comportamiento malicioso potencial y el mal uso de su API interna. Una aplicación que no cumpla con los requisitos será rechazada. Por ejemplo, una razón común para el rechazo se debe a la declaración del derecho innecesario. Aunque la fase de desarrollo y distribución pueden ser restrictivas, Apple ha sido hasta ahora un gran éxito en el mantenimiento de un canal de distribución que es relativamente libre de aplicaciones maliciosas.

2.3. Windows Phone

Windows Phone 8 es la tercera versión de las plataformas Windows Phone. Fue lanzado en octubre de 2012. Windows Phone 8.1, anunciado el 2 de abril de 2014 en la conferencia Build para desarrolladores, es la última versión y definitiva de Windows Phone 8. Fue lanzada el 14 de abril para desarrolladores y a lo largo de mayo y junio para el público en general. Todos los actuales modelos con Windows Phone 8 son actualizables gratuitamente.

El 21 de enero de 2015, se presentó su sucesor, Windows 10 Mobile, con nuevas funcionalidades y mejor rendimiento. Desde que se presentó Windows 10 Mobile al público, Windows Phone 8.1 es la última versión de Windows Phone.

Microsoft decidió volver al mercado y ha puesto mucho énfasis en la funcionalidad del negocio en WP8. Fueron muy populares con su primer sistema operativo móvil, Windows Mobile, que fue un gran éxito en su lanzamiento en el 2002 en las llamadas Pocket PC. Sin embargo, años después, su sucesor Windows Phone 7 no estaba tan preparado para el mercado organizacional. Faltaba soporte para funciones de administración de dispositivos móviles para entornos organizaciones que se habían incluido en Windows Mobile, lo que hizo que su posición dentro de las organizaciones disminuyera considerablemente.

Arquitectura del sistema

Microsoft tuvo dos grandes temas que decidió abordar en el diseño de la arquitectura de seguridad para Windows Phone 8: la fuga de datos y los programas maliciosos. La primera se refiere al almacenamiento incorrecto de datos de la organización y la segunda es la difusión de aplicaciones maliciosas en canales inseguros.

Microsoft añadió algunas nuevas características en WP8 para asegurar un proceso de arranque seguro y para garantizar la seguridad durante el tiempo de ejecución. El arranque utiliza una tecnología llamada Secure Boot para verificar la integridad del firmware. Es una característica que está disponible en la Unified Extensible Firmware Interface (UEFI) que valida un controlador o firmware antes de que se cargue el sistema operativo. Cada componente es criptográficamente firmado y verificado usando una clave de la Plataforma que se ha almacenado en el UEFI[15]. Todos los drivers (o gestores de arranque) no firmados por esta clave no podrán ser cargados. Esta función se utiliza en los ordenadores modernos y es parte del sistema operativo Windows 8. El proceso de arranque también incluye un segundo paso llamado Administrador de arranque de Windows Phone. Esta característica hace la configuración final (iniciando los procesos de background, etc.) que a la larga terminaran el proceso de arranque.

La seguridad en tiempo de ejecución en WP8 se basa en el principio de privilegios mínimos, lo que significa que ni el programa ni el proceso deben tener acceso a información que no es necesario para que se ejecute. Esta función crea una cámara de aislamiento y es básicamente una sandbox. Cada sandbox tiene un conjunto de políticas de seguridad que definen qué capacidades del sistema se deja a la sandbox usar, por ejemplo, la conexión de red. Cada aplicación se ejecuta en su propia sandbox en la que también se da un área de almacenamiento aislado. Todas las capacidades o los permisos se conceden a la instalación y no se pueden cambiar durante el tiempo de ejecución.

WP8 soporta la encriptación completa del dispositivo usando una tecnología llamada BitLocker Drive Encryption para proteger el almacenamiento interno. Sin embargo, no admite el cifrado de almacenamiento extraíble, como Tarjetas Digital (SD). Bitlocker es un software y hardware de aplicación combinado y utiliza un Trusted Platform Module (TPM), un chip dedicado que proporciona operaciones criptográficas seguras en el dispositivo. TPM es responsable de almacenar y proteger la clave utilizada para cifrar el almacenamiento interno. La clave del disco sólo se dará al gestor de arranque del sistema operativo y sólo si todos los componentes de arranque han sido verificadas y cargadas correctamente. Microsoft asegura la protección de la propiedad intelectual con

Information Rights Management (IRM) que evita la pérdida de datos al permitir a los usuarios asignar derechos específicos de usuario a sus documentos. Estos derechos pueden especificar los usuarios que tienen permiso para leer o modificar un documento en particular y para evitar operaciones como copiar y pegar e imprimir. IRM se gestiona mediante Windows Right Management Services (RMS), que es responsable de cifrar y descifrar este tipo de documentos. Una combinación de IRM con RMS proporciona la capacidad de hacer cumplir esta gestión de derechos en, por ejemplo, los e-mails y así evitar que los correos electrónicos y archivos adjuntos se reenvíen a fuera del dominio de la organización.

Desarrollo de Aplicaciones

Microsoft desarrolló un canal de distribución de aplicaciones denominado Windows Phone Store[16], que es similar a la App Store de Apple en cuanto a la presentación y aprobación de las aplicaciones por parte de los desarrolladores[17]. Cada desarrollador debe registrarse para ser provisto de un certificado personal que se debe utilizar para la firma de sus aplicaciones. Una vez que una aplicación se carga a la Windows Phone Store, la identidad de los desarrolladores es verificada por el certificado y se comprueba la aplicación para detectar la ausencia de contenido malicioso en la aplicación y otras violaciones posibles contra las políticas de sandbox.

Microsoft provee un canal alternativo de distribución de aplicaciones para organizaciones en el que se puede distribuir la aplicación interna de la organización (o línea de negocios, LOB) para evitar la presentación de las mismas en la distribución pública. Una organización se registra con Microsoft para obtener todas las herramientas necesarias para desarrollar y distribuir aplicaciones de forma privada. Para garantizar la seguridad de las aplicaciones, Microsoft ha desarrollado un proceso llamado Security Development Lifecycle (SDL). El proceso se aplica a todos los equipos de desarrollo de Microsoft e implica realizar pruebas de penetración, modelado de amenazas y evitar el acceso no autorizado a los recursos. El objetivo es evitar las vulnerabilidades de software y escribir mejor código.

3. Amenazas - Estado actual de la Seguridad

En este capítulo nos referiremos a las amenazas que actualmente afectan a nuestros dispositivos móviles, se realizará una descripción de estas amenazas y se complementarán con noticias actuales que referencian a ataques realizados. Se hablará de las nuevas problemáticas que las nuevas tecnologías como el IoT traerán a la escena.

Los problemas de seguridad a los que los dispositivos móviles están expuestos son similares a los que está expuesto una computadora, pero se ven agravados ya que cuentan con una mayor exposición al ser su comunidad de usuarios más amplia, que los utiliza tanto en el ámbito laboral como en el personal. La problemática se potencia tanto debido al desconocimiento general sobre los problemas de seguridad a los que los dispositivos están expuestos como a la falta de información en las contramedidas que son posibles de adoptar. Si eso lo juntamos con la cantidad de elementos incluidos en los smartphones se dan otros problemas, como por ejemplo los relacionados con el espionaje, puesto que un dispositivo comprometido podría permitir consultar su localización vía GPS, transmitir la información captada por su micrófono o incluso su cámara. En relación a este tipo de problemas es que se realizó la creación de un POC (Prueba de Concepto por sus siglas en inglés) espía del GPS que es explicado en detalle en la sección de Casos Prácticos Realizados, al final del presente documento.

Estas amenazas, suelen estar asociadas a problemas de seguridad en aplicaciones móviles descritos en el Top Ten de OWASP. OWASP Mobile Security Project[18] es un proyecto que tiene la intención de brindar recursos necesarios para que las aplicaciones móviles sean más seguras. A través de este proyecto, el objetivo es clasificar los riesgos de seguridad móviles y proporcionar controles en el desarrollo para reducir su impacto y probabilidad de explotación. El enfoque principal se pone en la capa de aplicación. Si bien se tiene en cuenta la plataforma móvil y los riesgos inherentes al diseño con respecto a los controles y las amenazas, el foco se encuentra en las áreas de desarrollo de aplicaciones. También se fija en consideraciones del lado del servidor y de la infraestructura de

comunicación de las aplicaciones móviles. La idea es enfocarse en la integración entre las aplicaciones móviles, los servicios de autenticación remota, y las características específicas de la plataforma de la nube. La metodología OWASP Mobile resulta interesante para estudiar y aplicar, con la finalidad de disminuir los riesgos y vulnerabilidades y evitar posibles ataques o robos de información.

En la presente sección se intenta explicar las amenazas a los que un dispositivo móvil, y por lo tanto el usuario, están expuestos en la actualidad, así como ejemplos de ataques realizados que concuerdan con las amenazas descritas en la sección.

3.1. Malware

Malware es una clasificación general de software malintencionado en la que se incluyen los virus, rootkits, troyanos, etc., y es más comúnmente relacionado con la destrucción o robo de datos. La definición de malware ha cambiado durante los últimos años y se puede dividir en dos categorías: tradicional o moderno. El malware tradicional se refiere a la forma clásica de malware en la que el objetivo es infectar y propagarse al mayor número de dispositivos posible, al tiempo que maximiza el daño al sistema, sin ningún motivo específico detrás de un ataque. Los malware actuales son más sofisticados y estratégicamente planificados. Un ejemplo de malware moderno son los ataques APT[19] (Advanced Persistent Threat), cada vez más conocidos. Un ataque APT es un ciber-ataque bien planeado con un objetivo específico, como por ejemplo una organización o un sistema de un gobierno. El ataque se lleva a cabo en múltiples pasos para cada una de las metas específicas y es intencionalmente sigiloso con el fin de evitar la detección. Una de las principales diferencias del malware moderno en comparación con el tradicional, es que el malware moderno está dirigido y es sigiloso. El objetivo es elegido específicamente ya que tiene algo de valor para el atacante y evitar la detección es esencial con el fin de llevar a cabo un ataque prolongado. Un ataque APT puede durar durante un largo período de tiempo y mientras más datos detectados puedan ser extraídos mayor se considera la efectividad del ataque.

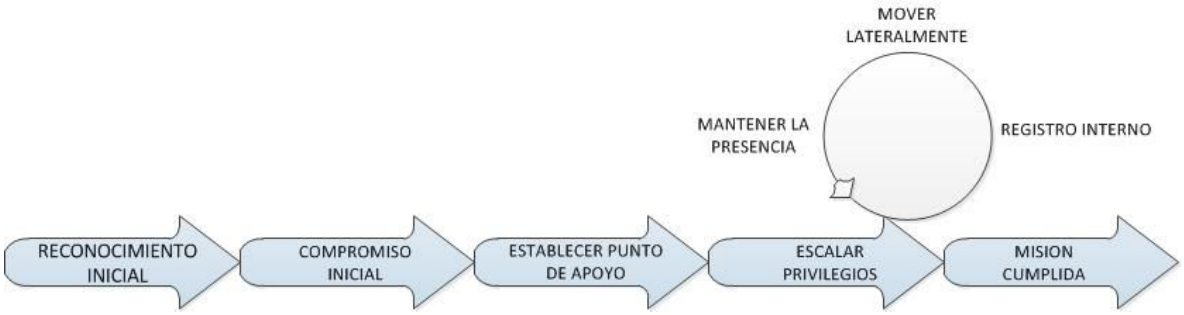


Figura 6. Ciclo de vida APT.

Las características del ciclo de vida APT (Fig. 6) pueden ser descriptas como un proceso secuencial que implica la investigación, la intrusión, la recolección de credenciales, la extracción de datos y la limpieza. El primer paso consiste en la investigación sobre el objetivo con el fin de encontrar puntos débiles, o puntos de entrada, en un perímetro de la organización y para determinar la información de interés que podría ser localizada. Un atacante busca las vulnerabilidades y luego las explota para establecer una penetración inicial utilizando técnicas como phishing o ingeniería social (serán detallados más adelante). Una vez dentro, el malware intenta obtener las credenciales requeridas con el fin de obtener acceso a los datos específicos. Los datos se extraen finalmente. Cuando la extracción se completa entonces el malware se limpia a sí mismo para cubrir sus pasos y no dejar rastros. La intención es intentar de que tome semanas o incluso meses antes de que alguien descubra que un ataque se ha llevado a cabo.

Los autores de malware modernos han comenzado a focalizarse en el desarrollo de malware para dispositivos móviles y Android es la plataforma preferida. Un ejemplo de una APT contra Android tuvo lugar en el año 2013, dirigido contra un grupo activista tibetano[20]. El ataque consistió en el uso de una cuenta de correo electrónico comprometida con la que el atacante se las arregló para enviar un correo electrónico masivo acerca de una conferencia que incluyó un archivo .apk malicioso adjunto. Los datos robados fueron contactos, registros de llamadas, Mensajes SMS, geolocalización y otros datos del teléfono, como el número de teléfono, la versión del sistema operativo, modelo de teléfono y la versión SDK.

Con el pasar de los años, las compañías encargadas de manejar los repositorios de aplicaciones móviles han avanzado en pos de mejorar las características de seguridad provistas por estos repositorios con la finalidad de disminuir los riesgos que se pueden presentar en forma de aplicaciones maliciosa. Aunque mucho ha avanzado respecto a limitar la presencia de malware en repositorios oficiales, ningún sistema es infalible, por lo que continuamente se están desarrollando nuevas técnicas para securizar estos entornos. Como ejemplo, Google no tiene un periodo de aprobación de aplicaciones en Google Play y las aplicaciones enviadas al repositorio quedan inmediatamente disponibles para su descarga. Sin embargo, Google Play no es un santuario para el malware móvil. A principios de 2012, Google presentó un servicio para mejorar la seguridad en Google Play llamado Bouncer. Bouncer es un servicio de escaneo automático que comprueba si hay software potencialmente malicioso y realiza el análisis en una aplicación tan pronto como se carga. Bouncer ejecutará la solicitud dentro de la infraestructura de la nube de Google para simular su comportamiento en un dispositivo Android virtual. La meta fue la de añadir una capa extra de seguridad para hacer frente al aumento de la presencia de malware en Google Play. Pero en junio de 2012, los investigadores de malware conocidos como Charlie Miller y Jon Oberheide[21] publicaron un informe en el que habían sido capaces de infiltrarse en Bouncer y encontraron limitaciones que les permitieron presentar aplicaciones maliciosas y pasar por desapercibidos. Bouncer realiza análisis dinámicos de las solicitudes presentadas y la prueba tiene una duración de cinco minutos. Si se hubieran encontrado ningún contenido o comportamiento malicioso en este punto entonces la aplicación pasaría la prueba. Por lo tanto, los autores de malware son capaces de evitar a Bouncer, ya sea retrasando la ejecución o descargando el contenido malicioso en un momento posterior. Charlie Miller es también conocida por la explotación de la funcionalidad NFC en versiones anteriores de Android para obtener acceso root a un dispositivo simplemente mediante el envío de una etiqueta NFC[22] malicioso.

Con el fin de publicar una aplicación en Google Play debe ser firmada digitalmente por el desarrollador. Sin embargo, no hay requisitos sobre el certificado real y un certificado autofirmado se pueda utilizar. Autofirmados se refiere a un certificado firmado por su

propia clave privada. Esto significa que los desarrolladores pueden crear fácilmente certificados falsos para firmar sus aplicaciones sin revelar ninguna información personal, lo que hace posible la publicación de aplicaciones maliciosas en Google Play de forma anónima. Debido a su falta de revisión de la solicitud por lo que es posible enmascarar aplicaciones maliciosas como existentes, aplicaciones legítimas utilizando una descripción y gráficos similares en Google Play. Esto podría engañar a la mayoría de los usuarios para descargar e instalar la aplicación maliciosa en lugar de la aplicación que en realidad estaban tratando de adquirir. Hoy en día no se pueden subir aplicaciones con gráficos iguales a otra aplicación existente en el store permitiendo una forma visual de identificar y discriminar una aplicación verdadera de una falsa.

3.2 Robo y fuga de datos

La seguridad de la información es esencial para cualquier persona u organización que quiere proteger su información confidencial. Puede ser cualquier forma de información digital, como documentos, presentaciones, cálculos, patentes, registros de miembros, etc., que se pueden clasificar como confidencial. La fuga de datos y el robo en el contexto de los dispositivos móviles se refieren a datos que han sido almacenados en el dispositivo móvil, y la existencia de varias maneras para que estos datos sean filtrados o robados por un tercero. Malware es uno de ellos, pero también puede ser robada por un ataque con acceso físico a un dispositivo, utilizando el correo electrónico o copiando datos a un medio externo. Las memorias de almacenamiento extraíbles que se pueden agregar a los dispositivos móviles son un ejemplo de ataque físico: son de fácil extracción y aunque la tendencia hoy en día es que los dispositivos sean diseñados de tal forma que sea más complejo acceder a esas memorias y retirarlas, con algunas inclusive integradas en la plaqueta electrónica, por insistencia de usuarios, importantes fabricantes están retornando al viejo método de la memoria extraíble.

Las aplicaciones maliciosas pueden rastrear la actividad del usuario mediante la explotación de las características del dispositivo, como el Sistema de Posicionamiento Global (GPS), captura de pantalla, grabación de audio, etc. El uso no autorizado de esta

información también se puede considerar como robo de datos o espionaje, que tiene el potencial de ser utilizado para el espionaje industrial. Un atacante puede espiar a los miembros de una organización en tiempo real, escuchar conversaciones privadas, vigilar la ubicación del usuario o incluso capturar fotos de documentos cercanas para descubrir los datos confidenciales de una organización.

3.3. Vulnerabilidades de software

Las vulnerabilidades de software son un riesgo de seguridad constante para cualquier aplicación o plataforma. En el tiempo entre el descubrimiento de una vulnerabilidad hasta que sea arreglada y parcheada, una aplicación corre el riesgo de ser explotada. Los navegadores Web son un ejemplo típico y que se puede encontrar básicamente en cualquier PC o dispositivo móvil. Si los autores de malware descubren una falla, entonces pueden explotarla con el fin de inyectar código malicioso que puede afectar a millones de dispositivos hasta el momento en que el defecto sea parcheado en el sistema del usuario.

Todos los software en general están destinados a tener algunas vulnerabilidades, ya que son creados por los seres humanos y los seres humanos cometen errores. Ya sea debido a un mal diseño desde su creación o a una mala aplicación, los autores de malware y otros atacantes se esfuerzan por encontrar defectos y, finalmente, explotarlos. Algunos ataques han tenido éxito en versiones anteriores de estas plataformas y algunas vulnerabilidades están esperando a ser encontradas en las versiones actuales.

El uso de los códigos de respuesta rápida (QR) son un ejemplo donde la funcionalidad legítima puede ser explotada por los autores de malware. Un código QR es un código de barras tipo matriz que puede ser escaneado por la cámara de un dispositivo móvil y una aplicación de escáner QR. El código se puede traducir, por ejemplo, en una URL que apunte a un sitio web o a una descarga y que se abre, en casos de manera automática, por el navegador web. Esto puede ser explotado y utilizado para descargar aplicaciones maliciosas. Un atacante puede crear un código QR que incluya una dirección URL a un archivo .apk malicioso y enmascarar el código en un contexto legítimo como un anuncio falso en un sitio web muy conocido. El código no es legible por el usuario, por lo tanto no

puede determinar si el código es legítimo o no antes de que se escanee el código sin poder prever hacia donde lo direccionara el mismo.

Cada 2 años el Open Web Application Security Project (OWASP) publica una lista del Top 10 en vulnerabilidades más comunes; OWASP tiene un área específica para dispositivos móviles (OWASP Mobile Security Project) donde se presentan tanto el TOP 10 vulnerabilidades en plataformas móviles[23] como también guías para desarrolladores con consejos, buenas prácticas, reportes sobre ataques y demás.

Hoy en día se manejan términos como el *0-day vulnerability* (vulnerabilidad de día cero), que se refiere a una nueva vulnerabilidad para la cual aún no se crean parches o revisiones, y que se emplea para llevar a cabo un ataque. El nombre *0-day* (día cero) se debe a que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad. Estas a veces se usan junto a los troyanos, rootkits, virus, gusanos y otros tipos de malware, para ayudarlos a propagarse e infectar más equipos. También se puede encontrar escrito como "0 day", "zero day" y "zero-day".

Las vulnerabilidades de día cero, o zero-day son de las más peligrosas, ya que los atacantes pueden aprovecharse de fallos para los que todavía no hay parche de seguridad.

Una nueva vulnerabilidad crítica de día cero ha sido descubierto en el kernel de Linux a principios del año 2016. Éste podría permitir a los atacantes obtener acceso root y controlar los sistemas de dispositivos Android o Linux afectados.

Este fallo crítico (denominado CVE-2016-0728) ha sido hallado por un grupo de investigadores de la compañía de seguridad Perception Point, en el informe[24] detallan que esta vulnerabilidad que está presente desde 2012, y afecta a cualquier sistema operativo con Linux kernel 3.8 y posterior, con lo que hay probabilidad de que decenas de millones de ordenadores de 32 y 64 bits estén expuestos a este fallo.

Las versiones de Android KitKat y posteriores también están afectadas, lo que significa que alrededor del 66% de los dispositivos Android están expuestos a esta vulnerabilidad del kernel de Linux.

Un atacante sólo necesita acceso local para explotar esta vulnerabilidad en un servidor Linux. Si es explotada con éxito, el fallo puede permitir a un atacante obtener acceso root al sistema operativo, permitiendo borrar archivos, ver información privada o instalar aplicaciones maliciosas. Esta vulnerabilidad de día cero descubierta lleva tres años sin parchear. El fallo fue reportado al equipo de Linux, por lo que los parches ya deberían estar disponibles en actualizaciones automáticas. En el caso de Android, esta actualización puede tardar un poco más, teniendo en cuenta que muchas actualizaciones no se llevan a cabo de forma automática por los fabricantes.

3.4. Ingeniería Social

En términos técnicos, la ingeniería social se refiere a un ataque en el que se utilizan las habilidades sociales para obtener información, ya sea personal como sobre los sistemas informáticos. Las personas que practican la ingeniería social (estafadores) utilizan la interacción social ya sea para engañar a sus víctimas para que entreguen la información, o manipularlos para que confíen en él o ella y compartan información con el atacante. Podría haber una interacción cara a cara, por teléfono, mensajería, e-mail, etc. Por lo general, el atacante fingirá ser otra persona, por ejemplo, un nuevo empleado en la misma organización como la víctima, un conocido de otro conocido, amigo de un amigo, personalidad pública, etc. Ha habido informes de los atacantes que han logrado obtener información de tarjetas de crédito, los ID de transacción, números de contactos y otros tipos de información que utilizan la finura y técnicas de ingeniería social y podría fácilmente ser utilizado para obtener contraseñas y otras credenciales. El arte del engaño describe varios escenarios de la vida real donde se han utilizado técnicas de ingeniería social en la práctica con ánimo de lucro y de hacking de sistemas informáticos a gran escala.

Este tipo de ataque no es una amenaza específica contra la seguridad informática, sino más bien una cuestión general de seguridad personal que se traslada también a la seguridad móvil.

3.5. Phishing

El phishing es una forma de ingeniería social. Un ataque de phishing es un intento de obtener una parte de la información sensible de los usuarios haciéndoles creer que es por causa legítima. El ataque se inicia normalmente utilizando el correo electrónico o sitios web maliciosos como herramienta primaria o en el caso de telefonía un mensaje SMS o llamada. Un correo electrónico de phishing se disfraza por ejemplo, del banco de la víctima o del departamento de IT de los lugares de trabajo de las víctimas, y pueden contener una investigación respecto a la información personal o financiera, tales como información de tarjetas de crédito y contraseñas. Existe un tipo más sofisticado de ataque de phishing conocido como Spear Phishing. Spear phishing se refiere a los ataques de phishing más específicos donde el objetivo es deliberadamente elegido con premeditación, teniendo como criterio de selección el rol o posición que ocupa en una organización respecto a su nivel de autorización o acceso. El objetivo podría ser aquel que tiene acceso a la información que es necesaria para un atacante en pos de obtener la autorización necesaria para un ataque aún más grande, por ejemplo, un ataque APT.

En el año 2012 se descubrió[25] una nueva vulnerabilidad para la época que afectaba numerosas versiones de sistemas operativos de Google. Se trata de un agujero de seguridad que propicia ataques de phishing a través de mensajes SMS; llamándolo SMIShing. Consiste en que el usuario se descarga en su dispositivo Android una aplicación infectada que se aprovecha de las vulnerabilidades para crear mensajes cortos falsos y enviarlos a los teléfonos móviles de otras personas que figuran en la agenda de contactos. Estos mensajes pueden ser vehículos para realizar ataques de phishing, destinados a recopilar información personal y económica, como números de cuentas, claves y contraseñas. De hecho, la cadena de tiendas Wal-Mart fue protagonista de uno de estos ataques SMIShing. El desencadenante para conseguir los datos personales era reclamar un *"cheque regalo"* (falso) por valor de mil dólares. El texto del mensaje corto distribuido decía *"Querido cliente de Wal-Mart, felicidades, ha ganado un cheque regalo de 1000 dólares. Haga clic en este enlace para reclamar su premio"*. Las víctimas del

engaño que entraban en el enlace acaban en un sitio web fraudulenta que solicita sus datos personales y financieros para “procesar” el cheque regalo.

Figura 7. Mensaje SMIShing

Los ataques de SMS son muy comunes en nuestra región independientemente de que sistema operativo móvil se está utilizando, la mayoría son utilizados para determinar si el número telefónico al que se envió el mensaje hay una persona detrás del mismo, esto se puede ver en los mensajes donde indican que *“te ganaste un auto y si querés más información enviar la palabra OK”*. Con esto el atacante puede determinar que es un número vivo y la persona detrás puede pecar de ingenua ya que respondió el mensaje. También estos mensajes son muy utilizados como estafas, un ejemplo es el mensaje que se recibe *"¡Participás gratis para tu 0km directo de fábrica!", "Financiamos el 100% de tu 0km en cuotas en pesos sin interés"* y frases del estilo son mensajes que reciben miles

de usuarios de telefonía móvil a diario en la Argentina. Basta un simple *"ok"* para, en teoría, obtenerlos. Sin embargo, se trata de potenciales estafas que se envían a diario a los teléfonos de los usuarios.

A principios del 2016[26] se reportó un ataque de spam dirigido a usuarios de Apple, los mensajes afirmaban venir de Apple, pero en realidad estaban diseñados para robar información personal para los propósitos de robo de identidad. Los mensajes utilizaban la ingeniería social, haciéndose pasar por un aviso de Apple cuyo ID iba a expirar en ese mismo momento, para llevar a los usuarios confiados a hacer clic en un enlace a un sitio web de phishing.

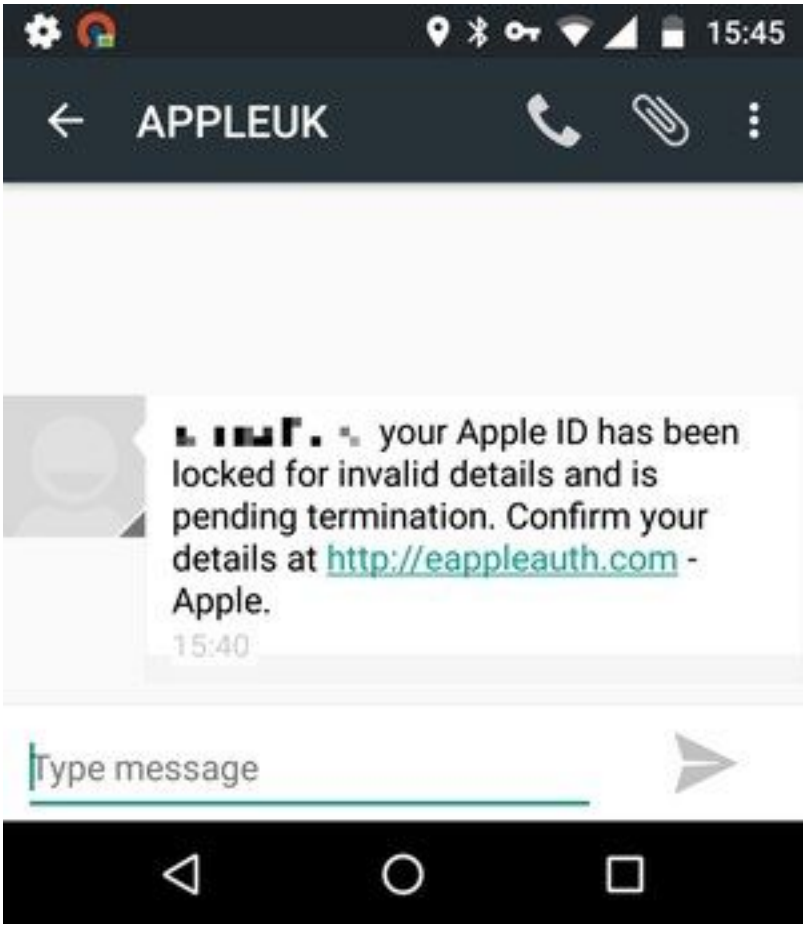


Figura 8. Ataque Apple ID

Los mensaje SMS son aún más convincentes, ya que se refiere a los destinatarios por su nombre, lo más probable engañando a algunos a creer que había una verdadera razón para actuar sobre la alerta y visitar el sitio apuntado por los criminales. El sitio utilizado inicialmente era appleexpired.co.uk, el cual fue bloqueado rápidamente por los principales navegadores web. Otros ejemplos han incluído las direcciones icloudauth.co.uk, mobileicloud.uk, y icloudmobile.co.uk

3.6. Ransomware

Otra amenaza con múltiples ataques que se están registrando en estos últimos años es el ransomware (ransom= rescate, ware por malware). Es un tipo de malware que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo utilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Al igual que otros tipos de malware para Android, a medida que las amenazas de ransomware fueron evolucionando en los últimos años, sus creadores adoptaron muchas de las técnicas que les resultaron eficaces para atacar equipos de escritorio y las aplicaron a la plataforma móvil. El ransomware de bloqueo de pantalla, hoy en día, suele ser del tipo "policial", es decir que intenta asustar a las víctimas para hacer que paguen un **"**rescate" tras acusarlos (falsamente) de almacenar contenidos ilegales en sus dispositivos. El ransomware criptográfico para Android comenzó a usar criptografía fuerte, lo que significa que los usuarios afectados no tienen ninguna forma práctica de recuperar sus archivos secuestrados. Y dado que ahora es más común guardar los datos de uso cotidiano, como las fotografías en el smartphone, en lugar de en la PC, la amenaza de la pérdida de los datos cifrados es mayor que nunca.

El ransomware, como lo indica su nombre, es cualquier tipo de malware que le exige al usuario infectado el pago de una suma de dinero a cambio de la promesa de "liberar" o "rescatar" un recurso secuestrado. Existen dos tipos generales de malware que entran en la categoría de "ransomware":

- El ransomware de bloqueo de pantalla

- El ransomware criptográfico

En el de bloqueo de pantalla, el recurso secuestrado es el acceso al sistema comprometido. En cambio, en el criptográfico, el recurso secuestrado son los archivos del usuario.

Dado que una de las tendencias más notables en cuanto al malware para Android es que sus creadores han estado aplicando las técnicas de malware que resultaron exitosas en Windows, el surgimiento del ransomware para esta popular plataforma móvil era algo lógico y esperado. Como podemos ver en el gráfico de tendencias, las detecciones de ransomware para Android están aumentando[27].

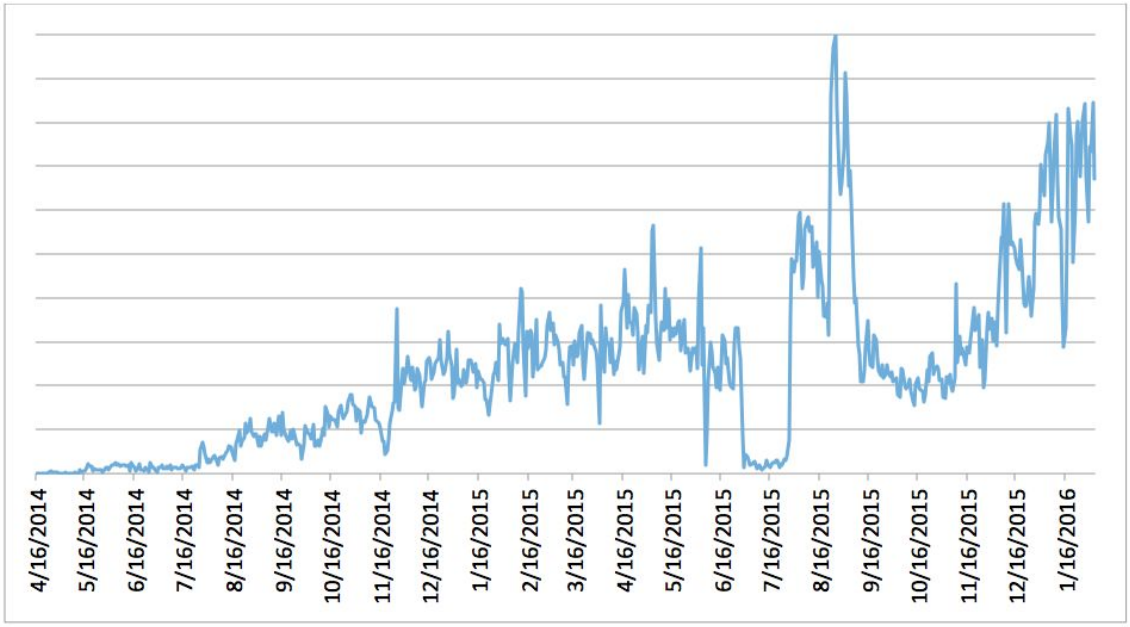


Figura 8. Estadísticas de detección de ransomware para Android, según ESET

Con la creciente cantidad de consumidores que optan por el dispositivo móvil en lugar de la PC, los datos que se almacenan en estos dispositivos son más valiosos, por lo que el ransomware para Android es un atractivo cada vez mayor para los atacantes.

Algunas familias recientes, como Android/Simplocker y Android/Lockerpin, por ejemplo, tuvieron como objetivo de ataque mayormente usuarios en los Estados Unidos.

En el año 2015 se descubrió Simplocker, el primer ransomware para Android activado en Tor que directamente cifra los archivos del usuario. Los investigadores de ESET descubrieron el primer tipo de ransomware de bloqueo de pantalla para Android que bloquea el código PIN.

En los primeros troyanos de bloqueo de pantalla para Android, dicha funcionalidad se suele conseguir poniendo constantemente en un primer plano la ventana de pedido de rescate en un bucle infinito. Aunque se implementaron diversos mecanismos de defensa para bloquear al usuario el acceso al dispositivo, no era tan difícil deshacerse del malware y desbloquear el dispositivo mediante el uso de la aplicación de línea de comandos Android Debug Bridge (ADB), a través de la desactivación de los derechos de administrador, o desinstalando la aplicación maliciosa en Modo Seguro.

Lamentablemente, los creadores de malware redoblaron sus esfuerzos y, con sus nuevos ransomware de bloqueo para Android, detectados por ESET como Android/Lockerpin.A, los usuarios ya no cuentan con una forma efectiva de recuperar el acceso a sus dispositivos sin los privilegios de raíz o sin una solución de administración de seguridad instalada. Además, tienen que restaurar los valores a fábrica, lo que también borra todos sus datos.

Por otra parte, este ransomware también utiliza una molesta táctica para obtener y preservar los privilegios de administrador del dispositivo con el fin de impedir su desinstalación. Este es el primer caso donde se pudo observar este método tan agresivo en un malware para Android.

Android/Lockerpin.A

Después de su instalación exitosa, el malware intenta obtener privilegios de administrador del dispositivo[28]. Esta táctica está siendo utilizada cada vez más por los creadores de amenazas para Android, ya que hace que sea más difícil eliminar la infección.

Las primeras versiones de la familia Android/Locker hacen lo mismo que el resto de los troyanos para Android: se basan en la suposición de que el usuario activará voluntariamente los privilegios elevados.

No obstante, en versiones más recientes, el troyano obtiene los derechos de administrador de dispositivos de una manera mucho más encubierta. La ventana de activación queda tapada por la ventana maliciosa del troyano, que se hace pasar por la "instalación de un parche de actualización".

Cuando la víctima hace clic en esta instalación de aspecto inofensivo, también activa sin saberlo los privilegios de administrador del dispositivo en la ventana subyacente oculta:

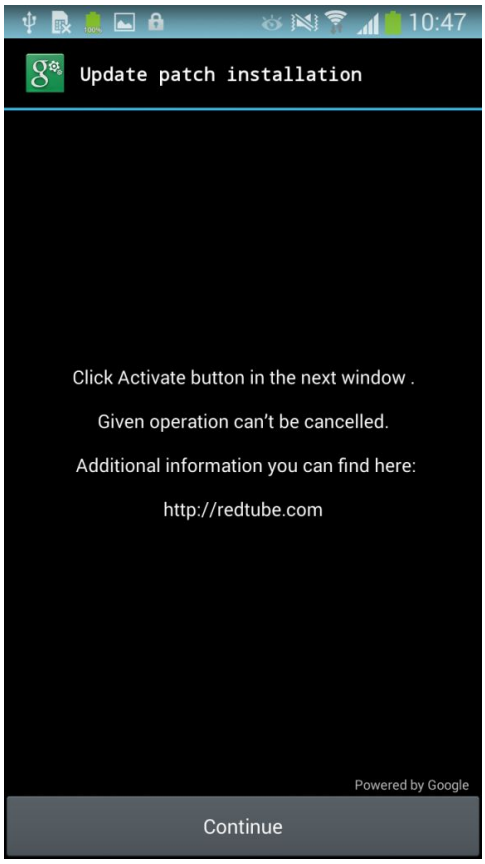


Figura 9. Ventana de activación.

Una vez que el usuario hace clic en el botón, su dispositivo ya está condenado: la aplicación del troyano ya obtuvo los derechos de administrador en forma silenciosa y ahora puede bloquear el dispositivo y, lo que es peor, establecer un nuevo PIN para la pantalla de bloqueo.

No mucho después, se le pedirá al usuario que pague un rescate de USD $500 supuestamente por ver y guardar material pornográfico prohibido:

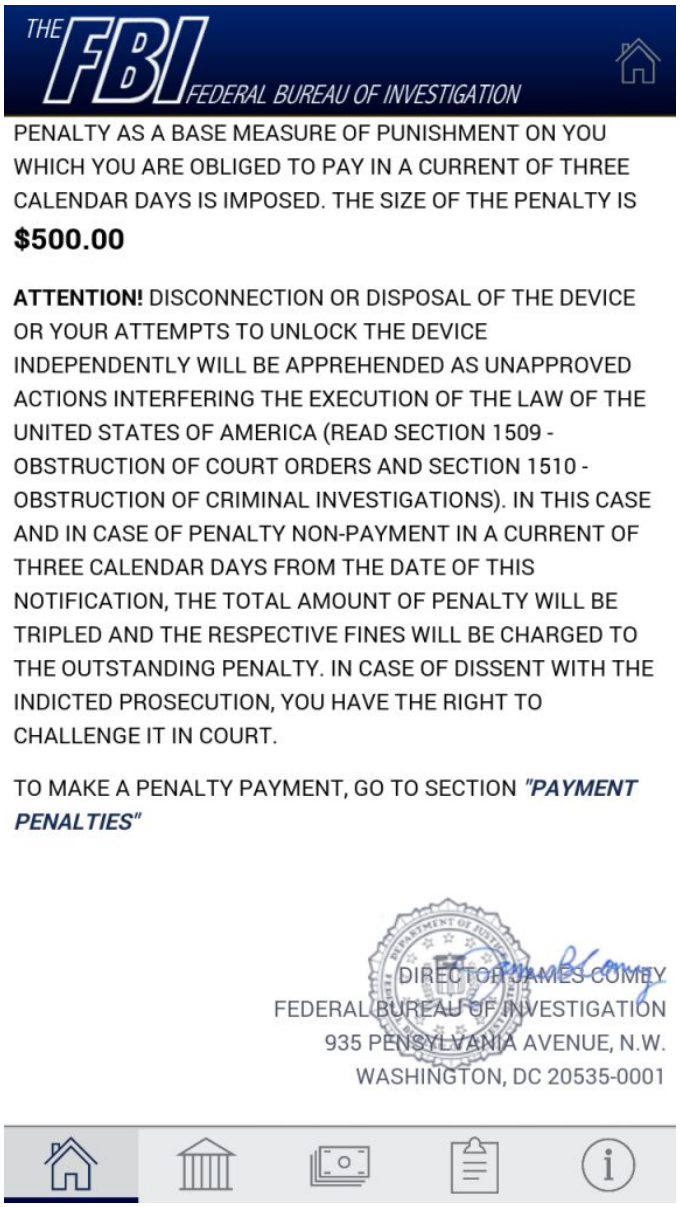


Figura 10. Pedido de rescate

Cuando aparece esta alerta falsa, la pantalla queda bloqueada, de la manera típica de los troyanos bloqueadores de pantalla para Android. El usuario ahora podría desinstalar Android/Lockerpin.A ya sea entrando al Modo Seguro o usando Android Debug Bridge (ADB).

El problema es que, como se restableció el PIN, ni el propietario ni el atacante pueden desbloquear el dispositivo, debido a que el PIN se genera al azar y no se envía al atacante. La única forma práctica de desbloquearlo es restableciendo los valores de fábrica.

El dispositivo ahora se encuentra permanentemente bloqueado y es imposible desbloquearlo sin tener los privilegios de raíz.

Android/Lockerpin.A no solo obtiene los privilegios de administrador del dispositivo de una forma novedosa y encubierta, sino que también utiliza un mecanismo agresivo de autodefensa para asegurarse de que nadie le quite los privilegios conseguidos.
Cuando los usuarios intentan desactivar el administrador del dispositivo para el malware, se producirá un error, dado que el troyano habrá configurado una función de devolución de llamada para reactivar sus privilegios cada vez que alguien intente eliminarlos.
Al igual que cuando el troyano activa por primera vez el administrador del dispositivo, si se hace un intento de eliminar dicho permiso, la ventana Administrador de dispositivos se vuelve a cubrir con una ventana falsa, como se muestra a continuación. Si se hace clic en Continuar, efectivamente se reactivan los privilegios elevados.

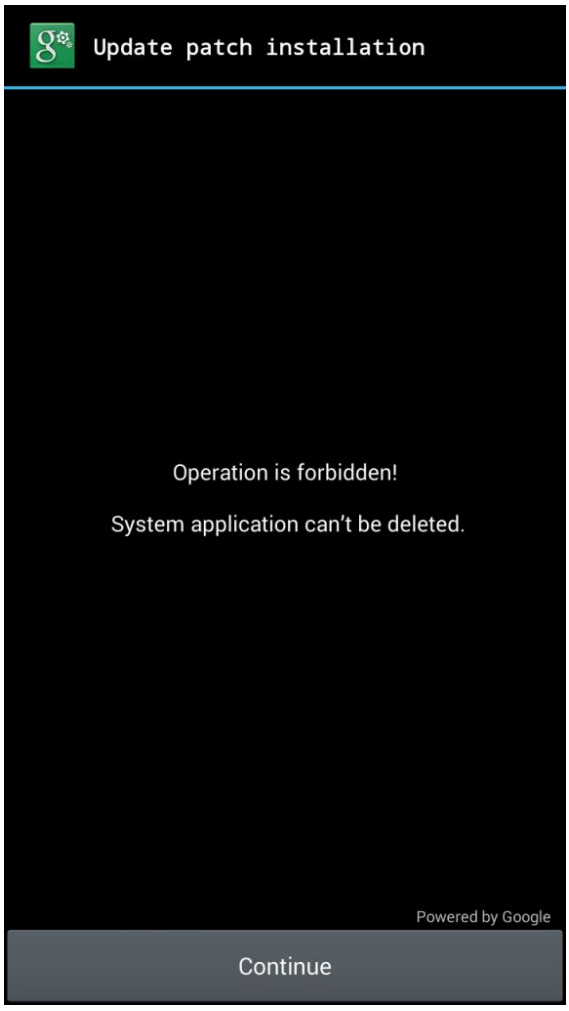


Figura 11. Ventana falsa

Como capa adicional de autoprotección, el ransomware también intenta terminar los procesos antivirus activos, cuando el usuario intenta desactivar sus derechos de administrador del dispositivo.

La única manera de quitar el bloqueo de la pantalla de PIN, sin restablecer el dispositivo a valores de fábrica, es cuando el usuario tiene acceso root del dispositivo o tiene instalada una solución MDM capaz de restablecer el PIN. Si tiene acceso a la raíz del dispositivo, entonces puede conectarse desde una computadora mediante ADB y eliminar el archivo donde se almacena el código de PIN.

Afortunadamente, no se puede descargar esta aplicación desde la tienda oficial de Google Play. Este troyano se propaga a través de mercados de terceros, foros ilegales o torrents.

3.7. Jailbreak en iOS

Los dispositivos iOS parecen ser bastante seguros hasta ahora. Sin embargo, esta declaración sólo se aplica a los dispositivos que no han sido "jailbroken". Se conoce por Jailbreak al método de modificar el sistema iOS con la finalidad de saltarse medidas de seguridad impuestas por Apple en su sistema y acceder a algunas funciones que no están permitidas de manera normal, como puede ser realizar algunas modificaciones visuales del sistema (personalizar más el sistema con fuentes de letra diferentes, iconos) y, la más interesante, habilitar la descarga de aplicaciones que no han sido aceptadas en la App Store o aplicaciones de pago gratuitas vía tiendas no oficiales. Un dispositivo al cual se le realiza el proceso de jailbreak, ya no está limitado a usar la App Store oficial de Apple para conseguir aplicaciones, sino que puede utilizar repositorios de aplicaciones externos (Cydia es uno de los más conocidos). Esto trae consigo el riesgo de que un usuario podría utilizar, sin saberlo, copias de contrabando de aplicaciones legítimas, que resultan atractivas ya que se ofrecen como gratuitas cuando la aplicación original en el App Store tiene un costo, que podrían contener código malicioso. De más está aclarar que esta misma aplicación maliciosa no podría haber ingresado al App Store oficial.

El laboratorio de seguridad informática Hispasec[29] en el día 21 de agosto del 2015 publicó en su servicio diario de información técnica una nueva vulnerabilidad en iOS que afecta a las instalaciones y despliegues organizacionales que hagan uso de sistemas MDM (Mobile Device Management) y que podría permitir el acceso a información confidencial de la organización, como URLs de los servidores, credenciales de acceso como contraseñas de texto plano, etc[30]. El fallo ha sido descubierto por la compañía Appthority y la violación afecta a todos los clientes que utilizan software MDM, así como a todas las aplicaciones móviles distribuidas a través de un servicio de MDM que usen la opción "Managed App Configuration" para establecer y almacenar toda la información y configuraciones privadas. De esta forma, cualquier otra aplicación del dispositivo, podrá

acceder a la información confidencial (como las credenciales de acceso) en formato texto plano.

La mayoría de las compañías emplean un sistema MDM/EMM (Mobile Device Management/Enterprise Mobility Management) para administrar y controlar el acceso a datos, correo y aplicaciones organizacionales en los dispositivos móviles de los miembros. De esta forma lo primero que se hace es crear una cuenta MDM para el empleado e instalar el cliente MDM en su dispositivo móvil. Desde ese momento, todas las aplicaciones organizacionales, así como configuraciones y credenciales se envían a través del MDM al dispositivo. El salto de la sandbox ocurre después de que la configuración se haya enviado al dispositivo, que quedará almacenada en "/Library/Managed Preferences/mobile/"; donde, según el informe de Appthority, cualquier otra aplicación podrá acceder a ella. En teoría solo podrá acceder a los datos la aplicación con el identificador correspondiente. Pero lamentablemente, todos los archivos de configuración pueden ser accesibles por cualquier otra aplicación del dispositivo. Se ha asignado el CVE-2015-5749 a esta vulnerabilidad. La firma notificó la vulnerabilidad a Apple de forma responsable, de forma que esta vulnerabilidad ha quedado solucionada en la actualización a iOS 8.4.1. Por lo que se recomienda a todas las organizaciones que hagan uso de MDM la instalación de esta versión.

También, se ha descubierto en octubre del 2015 un nuevo malware que afecta a dispositivos iOS con y sin jailbreak. Aunque por el momento todo indica que sólo ha afectado a usuarios de China y Taiwán no deja de ser una señal preocupante. El anuncio ha venido de la mano de la compañía Palo Alto Networks, que ha publicado un completo informe[31] sobre el nuevo malware, bautizado como YiSpecter. Según confirmó este malware es diferente a otras muestras anteriores en su capacidad de infectar tanto a dispositivos con jailbreak o sin él a través de comportamientos maliciosos únicos. Concretamente, es el primer malware en circulación que abusa de APIs privadas en el sistema iOS para implementar sus funcionalidades maliciosas. Hay que señalar que el malware afecta principalmente a usuarios iOS de China y Taiwán y se propaga a través de

medios inusuales, incluyendo el secuestro de tráfico de un ISP del país, un gusano de SNS en Windows y la instalación offline de una aplicación y su promoción a través de la comunidad. Por otra parte aunque se confirma que el malware ha estado en circulación durante más de 10 meses, solo un antivirus fue capaz de detectarlo. YiSpecter consiste en cuatro componentes diferentes firmados por certificados de organización. Mediante el abuso de APIs privadas, estos componentes descargaban e instalaban otros desde un servidor de comando y control. Tres de los componentes maliciosos usan trucos para esconder sus iconos del entorno iOS, para evitar que el usuario pueda encontrarlos y borrarlos. Los componentes también usan el mismo nombre y logos de aplicaciones del sistema para engañar a los usuarios de iOS.

Los dispositivos iOS infectados pueden descargar, instalar y ejecutar aplicaciones iOS arbitrarias, reemplazar las aplicaciones existentes por cualquiera que se haya descargado, modificar el funcionamiento de otras aplicaciones para mostrar publicidad, cambiar el motor de búsqueda de Safari, los marcadores o las páginas abiertas. Otra característica es permitir la reinstalación automática del malware incluso si se elimina de forma manual.

YiSpecter es el último de una familia significativa de malware para dispositivos iOS. Ya anteriormente WireLurker[32] había evidenciado la capacidad para infectar dispositivos iOS sin jailbreak mediante el abuso de certificados corporativos. También se habían publicado estudios académicos sobre el uso de APIs privadas para implementar determinadas funcionalidades en aplicaciones iOS. Sin embargo los investigadores de Palo Alto Networks confirman que este es el primer malware iOS encontrado en el mundo real que combina las dos técnicas y ha llegado a causar daño a una gran cantidad de usuarios. Los investigadores han reportado a Apple sus hallazgos para la revocación de los certificados corporativos utilizados. Cabe señalar que con iOS 9 se requiere a los usuarios la configuración manual del perfil de aprovisionamiento considerado como confiable en los Ajustes antes de poder instalar las aplicaciones organizacionales. Esta característica resulta muy útil para evitar incidentes de seguridad mediante el abuso de certificados corporativos. De hecho, la respuesta de Apple[33] ante este incidente se basa en que este malware solo afecta a versiones anteriores de iOS que hayan descargado

malware desde fuentes no confiables. También confirman la corrección del problema en iOS 8.4 y el bloqueo de las aplicaciones identificadas en la distribución del malware.

Otro informe[34] realizado también por la compañía Palo Alto Networks anunció una nueva familia de malware capaz de infectar dispositivos iOS sin jailbreak, a la que bautizaron como “AceDeceiver”. La novedad de AceDeceiver reside en que para lograr su ejecución reside en que en vez de aprovechar el uso de certificados corporativos como otras muestras de malware para iOS de los últimos años, aprovecha un fallo en el diseño del DRM (Digital Rights Management) de Apple. Incluso aunque Apple haya eliminado AceDeceiver de la App Store este sigue reproduciéndose gracias a un nuevo vector de ataque. Según los investigadores de Palo Alto Networks es el primero que abusa de un fallo de diseño en FairPlay, el sistema DRM de protección de Apple. Fairplay es la tecnología de gestión de derechos digitales creada por Apple, para evitar que las pistas de audio protegidas sean reproducidas en sistemas sin autorización. El fallo descubierto permite instalar aplicaciones maliciosas en dispositivos iOS independientemente de si tienen o no tienen jailbreak. La técnica, conocida desde 2013 como "FairPlay Man-In-The-Middle (MITM)", se ha aprovechado para instalar aplicaciones iOS "pirateadas", pero esta es la primera vez en que se detecta su uso para propagar malware.
Apple permite a los usuarios comprar y descargar aplicaciones iOS desde la App Store a través del cliente iTunes del ordenador. Después se puede usar el ordenador para instalar las aplicaciones en el dispositivo iOS. Para probar que la aplicación fue realmente comprada, los dispositivos iOS solicitan un código de autorización para cada aplicación instalada.

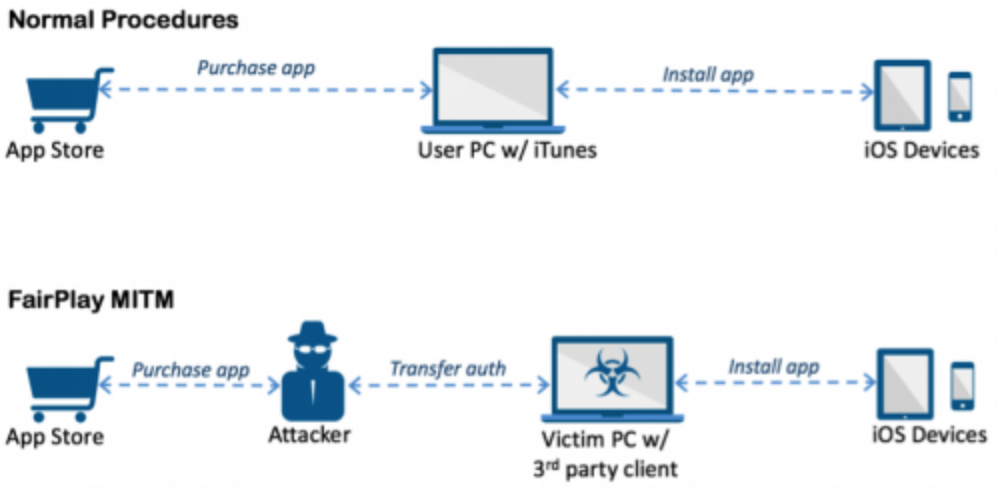


Figura 12. FairPlay MITM

En un ataque FairPlay MITM los atacantes compran una aplicación en la App Store pero interceptan y graban el código de autorización. Además a través de un programa para PC que simula el comportamiento del cliente iTunes, engaña al dispositivo iOS para que crea que la aplicación fue realmente comprada. Por lo tanto, el usuario puede instalar aplicaciones que en realidad nunca pagó, pero el creador del software puede instalar aplicaciones potencialmente maliciosas sin conocimiento del usuario.

Según el informe publicado por Palo Alto Networks hasta el momento han encontrado tres aplicaciones iOS diferentes de la familia AceDeceiver en la App Store oficial entre julio de 2015 y febrero de 2016; todas ellas decían ser aplicaciones de fondos de pantalla (wallpaper). Igualmente, según señalan por el momento AceDeceiver solo muestra comportamientos maliciosos cuando el usuario se localiza en China. Si bien el atacante podría cambiar esto en cualquier momento de una forma sencilla.

A finales de febrero del 2016, tras el aviso de Palo Alto Networks, Apple eliminó estas aplicaciones de la App Store. Sin embargo, el ataque sigue siendo viable ya que FairPlay MITM solo requiere que estas aplicaciones hayan estado disponibles una vez en la tienda. Mientras que el atacante haya podido obtener una copia de la autorización de Apple, el ataque no requiere la disponibilidad actual en la tienda de aplicaciones para su propagación.

3.8. Root en Android

Root, Rooting o "Rootear" se le conoce al método utilizado para darle al usuario los privilegios de Administrador o Superusuario (Superuser) del sistema operativo Android. Este concepto proviene de los SO Unix como Linux, y hace referencia al mismo comportamiento en Android ya que este es en esencia un Linux modificado. El proceso de Root es necesario cuando se quieren ejecutar ciertas aplicaciones que necesitan privilegios especiales para realizar tareas que entran en conflicto con directivas de seguridad impuestas por el desarrollador del SO (En este caso, Google). Al "rootear" un dispositivo Android, lo que generalmente ocurre es que se instala el programa ***su***$_{[35]}$, que permite elevar los permisos de usuario transformándose en el usuario root del sistema. Cada vez que se intenta correr algún programa que necesite utilizar privilegios de superusuario, se invocara *su*. En algunas versiones la instalación de *su* viene acompañada de otra aplicación llamada *SuperSu o Superuser*, que agrega algunos controles y algunas funcionalidades, como hacer aparecer una pantalla pidiendo autorización para correr el proceso que requiere privilegios, guardar la decisión del usuario para el futuro, etc.

¿Porque "rootear"? Hay muchas aplicaciones que requieren que el dispositivo tenga root para funcionar. Por otra parte, los teléfonos nuevos generalmente vienen con aplicaciones pre-instaladas que no se pueden desinstalar (a menos que se sea root). Otra característica es que siendo root se obtiene el control total sobre el sistema Android: se puede manipular cualquier archivo a nivel de sistema, e incluso se puede ser capaz de cambiar de sistema operativo manualmente, instalar versiones modificadas que agreguen funciones o modificar el sistema a niveles avanzados, como cambiar la velocidad del microprocesador. Es este punto el que nos hace prestar especial atención.

Rootear un dispositivo abre la puerta a un número mayor de peligros que los que tiene un dispositivo que se encuentra, digamos, "de fabrica". Las restricciones impuestas por Android a nivel de permisos de aplicación están pensadas para que las zonas de memoria donde puede acceder una aplicación estén delimitadas dentro de su sandbox según los permisos que le fueron otorgados en su instalación, evitando accesos no deseados a

información que la aplicación no tiene que conocer ni modificar. Siguiendo esta línea, en un dispositivo "rooteado", una aplicación maliciosa podría solicitar adquirir privilegios de root lo que le permite ignorar el esquema de permisos (como dijimos, ser root es tener permisos de administrador, lo que hace que las restricciones desaparezcan) y acceder a cualquier parte del sistema aunque no haya declarado y adquirido los permisos necesarios. Una vez que se "rootea" un móvil, hay que tener mucho más cuidado con lo que se instala. Una aplicación con permisos de root tiene la capacidad y la autorización para hacer cualquier cosa en el móvil (instalar un virus, borrar archivos, extraer información y mandarla a otra parte del mundo, dejar el móvil inutilizable, etc.).

3.9. Internet de las cosas, una puerta a las nuevas amenazas

El "internet de las cosas" (IoT por sus siglas en inglés, Internet of Things) se viene manejando desde hace un par de años, y se refiere a la red de dispositivos físicos que cuentan con la tecnología necesaria para comunicarse e interactuar con otros dispositivos o con humanos acerca de lo que los rodea, todo sobre internet.

Hoy en día nos podemos encontrar con ejemplos de estos dispositivos tales como automóviles, sistemas de iluminación, heladeras, sistemas de seguridad de casas, televisores y teléfonos. Estos son quizás los equipos más comunes hoy en dia pero la lista es mucho más extensa e incluso se podría extender al ambiente organizacional, como ser un sistema de control industrial.

Son muchos los electrodomésticos que han evolucionado a tal punto que las últimas generaciones de una gran variedad de ellos incluyen la posibilidad de conectarse a internet para consumir contenidos o intercambiar información que pueda llegar a ser sensible.

Las amenazas siguen la ruta de la tecnología

La posibilidad que IoT se convierta en algo más parecido en "Internet of Threats" (Internet de las amenazas) va a estar ligado en gran medida a dos factores fundamentales: los fabricantes y los usuarios. Hasta el momento las amenazas van a enfocarse allí donde haya una mayor cantidad de usuarios y como esto seguramente no cambie, la seguridad debe depender de otros factores.

Las principales consideraciones que deberían tenerse en cuenta son:

- **Conectividad:** La principal características de estos dispositivos es permitir la interacción en internet, por lo tanto cuidar la forma en que se conectan e intercambian información es primordial.
- **Fácil actualización:** Dado que estas tecnologías emergentes y en desarrollo, será común encontrar vulnerabilidades que deban resolverse una vez que el usuario tiene su dispositivo. Por lo tanto la velocidad de este despliegue y la facilidad de hacerlo será importante para ganarle la carrera a los atacantes.
- **Autenticación:** Al ser equipos que van a estar todo el tiempo conectados a Internet, es muy importante que se garantice que aquellos que interactúan con la información son quienes realmente dicen ser y así evitar fugas de información.
- **Aplicaciones confiables:** Las particularidades de esta tecnología abre muchas posibilidades para desarrollar tareas cotidianas de forma automática. Garantizar que esto no sea aprovechado a través de aplicaciones modificadas de forma maliciosa es necesario para generar confianza en su uso.
- **Cifrado de datos:** Como se maneja información que es sensible, esta debe emplearse de forma segura. Así que cifrarla es una opción para que terceros no puedan accederla para modificarla o robarla.

Brillo y Weave, la propuesta para IoT de Google

Uno de los mayores obstáculos que tiene por delante el Internet de las Cosas reside en el múltiple número de plataformas y objetos, cada uno con su sistema y lenguaje propio, que han de conectarse y comunicarse entre sí. Dicho obstáculo ha sido uno de los mayores a la hora de impedir que el IoT se difunda más rápido, y por ello algunos gigantes de la tecnología llevan meses intentando desarrollar sus propias plataformas, en el conocimiento de que la que resulte vencedora podría adquirir una enorme ventaja sobre sus competidoras.

Brillo es un sistema operativo basado en Android que permitirá llevar a cabo todo tipo de tareas propias del IoT. El sistema se ha diseñado para que sea muy sencillo y precisa muy pocos recursos, lo que le permitirá conectarse con dispositivos simples en un intento de

llegar a la mayor cantidad de objetos posible. El sistema fue anunciado por Google en mayo del 2015. Brillo se comunicará con los dispositivos del IoT mediante Wifi y Bluetooth Low Energy, y lo hará en el lenguaje Weave. Weave sería un lenguaje con vocación universal, ya que se pretende que se pueda conectar a todo tipo de disponibilidad aunque no utilicen Brillo.

Weave es un protocolo de comunicaciones estandarizado que respalda el descubrimiento, el abastecimiento y la autenticación de modo que los dispositivos puedan conectarse e interactuar unos con otros, con Internet y con sus plataformas móviles. El protocolo Weave ayuda a los desarrolladores de IoT a incrementar el alcance de las aplicaciones móviles en el mundo físico. Los desarrolladores pueden generar una aplicación para controlar múltiples dispositivos que aprovechen los servicios de Google.

4. Seguridad de Dispositivos Móviles, Buenas Prácticas

En este capítulo nos referiremos a las técnicas que podemos aplicar para proteger nuestros dispositivos móviles de ataques y amenazas. Desde técnicas básicas de bloqueo de pantalla hasta la encriptación de información en el dispositivos y nuevas formas de autenticación. Cada técnica será explicada y frente a qué amenazas son de gran ayuda.

Como se ha visto en la sección de amenazas, hay varios tipos de ataques que se dirigen a los dispositivos móviles y múltiples vulnerabilidades que deben tenerse en cuenta a la hora de pensar en proteger los dispositivos personales.
Los principales principios comunes en el debate sobre la seguridad de la información son: Confidencialidad, Integridad y Disponibilidad.

- Confidencialidad: Los datos sólo deben ser leídos por sus usuarios previstos y autorizados.
- Integridad: Los datos sólo deben ser modificados por sus usuarios previstos y autorizados.
- Disponibilidad: Usuarios autorizados siempre deben ser capaces de acceder a los datos que tienen acceso.

Lo que dicen es que sólo los usuarios con credenciales adecuadas deben ser capaces de leer, modificar y acceder a los datos privados en cualquier momento. Estos tres principios resumen los requisitos que deben cumplirse a fin de proporcionar un nivel aceptable de seguridad.
En este capítulo, se presentan las buenas prácticas más importantes que un usuario debe llevar a cabo para asegurar sus dispositivos móviles. Cada sugerencia se deriva de uno o más de los principios anteriores. Estas soluciones son persistentes a lo largo del informe y están destinadas a proporcionar una idea sobre medidas para protegerse contra los ataques descritos en la sección de amenazas latentes. En relación a los temas que serán abordados

a continuación, se presenta en la sección de Casos Prácticos Realizados un análisis estadístico hecho en base a datos recolectados, durante la participación de los Tesistas en el Proyecto de Extensión "Extensión en Vinculación con Escuelas Secundarias", llevado a cabo por la Facultad de Informática UNLP durante los años 2015 y 2016, en el ámbito del taller "Aprendiendo a estar Digitalmente Seguros", bajo la coordinación de la Lic. Paula Venosa.

4.1. Política Screen-lock (Bloqueo de Pantalla)

La capacidad de configurar una pantalla de bloqueo mediante un PIN, patrón de puntos, contraseña o biometría es una característica común en los dispositivos móviles para aumentar la seguridad y la privacidad del usuario proporcionando un mecanismo de autenticación para evitar que un atacante pueda tener acceso directo a los contenidos del dispositivo. Por lo general, varios métodos de bloqueos de pantalla están disponibles en las diferentes plataformas y el usuario puede decidir cuál utilizar según su preferencia.
Una política de bloqueo de pantalla está configurada definiendo cual es el nivel mínimo de longitud del PIN o contraseña aceptable implementando entropía. La entropía es una medida de la seguridad de la contraseña y su resistencia contra ataques de fuerza bruta. Una política de bloqueo de pantalla, por lo tanto no debe ser demasiado simple o fácil de predecir. Una política adecuada de bloqueo de pantalla para dispositivos móviles debe incluir lo siguiente:

- Requisito de bloqueo de pantalla: Los usuarios deben tener un PIN o contraseña activada en el dispositivo.
- Alta entropía: Especificar una longitud mínima, número de letras, dígitos, símbolos, etc.
- Intentos fallidos: Si se hacen demasiados intentos de inicio de sesión fallidos, limpie el dispositivo.
- Temporizador de Bloqueo de pantalla: Tiempo de inactividad antes de bloqueo de pantalla se active.

Esto evitará que usuarios no autorizados tengan acceso directo a las aplicaciones y archivos, y prohíbe la fuerza bruta y ataques de diccionario, de esta manera se mejora

significativamente la confidencialidad e integridad de los datos del usuario cuando se configura una política de contraseñas.

La fortaleza de cada método de bloqueo depende de la implementación que cada SO haga. La longitud del PIN, la cantidad de puntos de un Patrón, la cantidad de caracteres y tipos de una contraseña determinarán cuan seguro será el método. A modo de ejemplo, si tomamos la opción de Patrón presente en Android, según el análisis realizado por *Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith* en su documento *"Smudge Attacks on Smartphone Touch Screens"*[36] la cantidad de patrones posibles dadas las limitaciones provistas por el sistema son 389.112 y mediante un análisis de la pantalla táctil de un dispositivo utilizando distintas técnicas fotográficas, análisis de imágenes, exposiciones lumínicas, se presentan opciones factibles de ataques de fuerza bruta sobre el patrón y hasta de obtención del patrón a partir de estos análisis de imágenes.

4.2. Bloqueo remoto, tracking y borrado de la información

Los dispositivos que se utilizan en una organización con frecuencia tienen más probabilidades de contener algún tipo de datos sensibles que los que son de uso personal. Estos datos no tienen porqué ser sólo documentos o archivos, las credenciales para los servicios de correo electrónico o VPN también pueden estar disponibles. Ya sea un dispositivo organizacional o uno personal, la propiedad intelectual y la privacidad de los datos está en riesgo si un dispositivo se pierde o es robado. Una manera eficaz de proteger el dispositivo y la confidencialidad e integridad de los datos es un bloqueo remoto, una manera de realizar un seguimiento geoposicional del dispositivo y una política de limpieza mediante un método de borrado remoto. Esto permitirá que un usuario o un administrador pueda activar de forma remota el bloqueo del dispositivo, conocer la ubicación o iniciar un borrado que elimine todo el contenido del dispositivo.

La función de bloqueo remoto tiene como fin prohibir el acceso directo al dispositivo y el borrado remoto intenta asegurar que los datos ya no están en riesgo. Debe tenerse en cuenta que en un dispositivo bloqueado los datos todavía están disponibles y todavía están

en riesgo, por lo tanto el borrado es una opción más segura y casi indispensable si lo pensamos para la implementación en una organización.

Un ejemplo de estas funcionalidades es la herramienta provista por Android llamada "*Android Device Manager*". Esta herramienta viene integrada en todos los dispositivos Android y brinda 4 funcionalidades:

- Hacer sonar el dispositivo.
- Localizar el dispositivo (depende que el dispositivo tenga la localización activada).
- Bloquear el dispositivo.
- Borrar el dispositivo (tiene algunas limitaciones respecto a la tarjeta SD).

Se accede mediante la cuenta de google que se registra en el dispositivo entrando a "*https://www.google.com/android/devicemanager*"

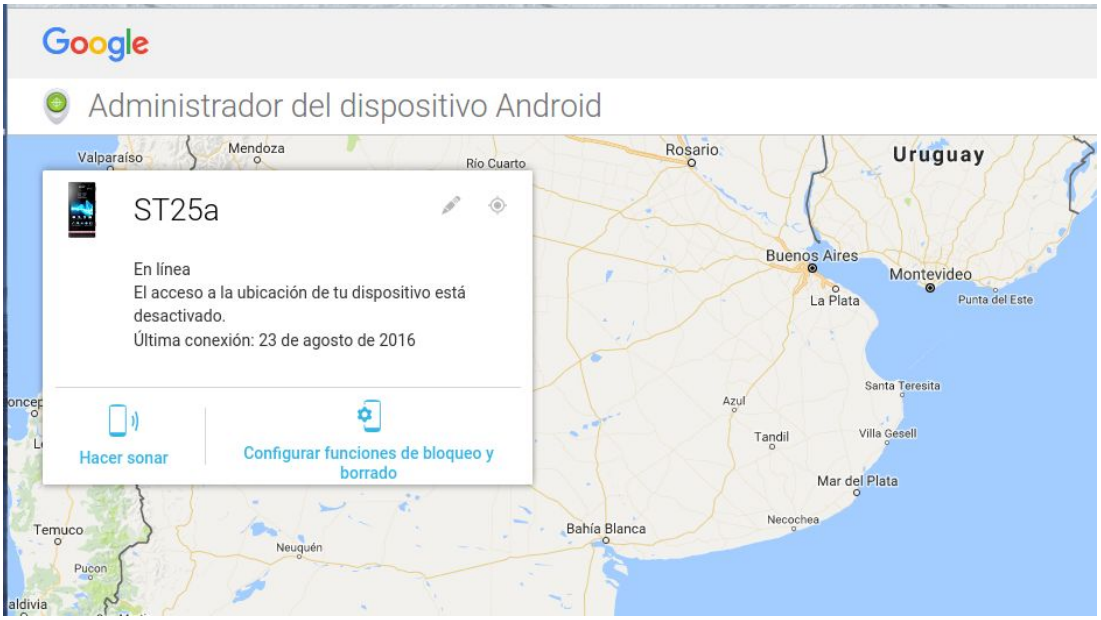


Figura 13. Panel de Android Device Manager

4.3. Encriptación o cifrado de datos

El cifrado de datos es una técnica clásica para la protección de la información digital y se utiliza para garantizar la confidencialidad de los datos. En seguridad del dispositivo móvil implica principalmente dos tipos de cifrado: cifrado del dispositivo y cifrado de red.

Cifrado de dispositivo se refiere a la encriptación de los datos almacenados en la memoria no volátil. Como se mencionó en la sección anterior, incluso si el bloqueo de la pantalla se activa en un dispositivo este sigue siendo vulnerable, por ejemplo a los ataques sin conexión. Un ataque sin conexión hace referencia a ataques que están dirigidos directamente contra el hardware del dispositivo con el fin de extraer los datos, ya sea directamente desde la memoria de acceso aleatorio (RAM) o al almacenamiento persistente sin tener la necesidad de acceder al SO dispositivo mediante los métodos normales. El cifrado de dispositivos se utiliza para proteger los datos de texto sin formato y se recomienda para prevenir que estos datos sean extraídos en el caso de un ataque sin conexión. Esto proporciona la confidencialidad de los datos en dispositivos móviles, aún considerando que no protege contra la extracción de datos real. Aunque un atacante se haga con los datos almacenados mediante un ataque sin conexión, a menos que el atacante logre descifrar los datos obtenerlos le es inútil ya que no podrá leerlos. Dependiendo del esquema de cifrado y de su robustez, el resultado de aplicar un cifrado del almacenamiento del dispositivo será prevenir o retrasar a un atacante de hacerse con los datos de manera legible e interpretable.

El cifrado de red de datos de la capa de red proporciona protección durante el transporte a través de redes no confiables (como Internet). El protocolo de transferencia de hipertexto seguro (HTTPS) y de red privada virtual (VPN) son ejemplos de protocolos y servicios que pueden ser utilizados para hacer cumplir este nivel de seguridad y para evitar el espionaje, así como la fuga de datos. HTTPS es una versión segura del Protocolo de transferencia de hipertexto (HTTP) que utiliza características de cifrado para cifrar la cabecera y la carga útil (datos) de un paquete HTTP. También es ampliamente utilizado para la autenticación del lado del servidor con el fin de probar la identidad de un servidor mediante la presentación del cliente (usuario) con un certificado válido. Inicialmente un proceso de negociación se lleva a cabo para generar las claves necesarias para cifrar el tráfico. Este proceso es sobre una base de uno a uno, lo que significa que se realiza una negociación entre cada servidor que un usuario desea establecer una conexión. Otra alternativa para la comunicación de red segura es utilizar una conexión VPN. Una VPN

simula una interfaz de red virtual que permite a los usuarios acceder de forma remota a los recursos y servicios en una red interna. La interfaz virtual encapsula un paquete IP dentro de otro paquete IP que se utiliza como contenedor entre dos puntos finales en una red insegura, conocido como un túnel VPN y generalmente la información dentro del túnel vpn viaja de manera cifrada para aumentar la seguridad del canal. Ni HTTPS ni VPN puede proporcionar protección a los datos que se encuentran almacenados en un dispositivo, pero proporcionan un canal seguro que se puede utilizar para el transporte de datos.

4.4. Control de aplicaciones

Las funciones que se describieron en las secciones anteriores son ejemplos recurrentes de los mecanismos de protección que se utilizan contra las amenazas externas. Pero no protegen contra amenazas internas, como las aplicaciones maliciosas que se podrían instalar negligentemente por parte del usuario y, finalmente, podrían robar datos utilizando métodos legítimos. Estas aplicaciones podrían haberse instalado sin el conocimiento del usuario, utilizando correos electrónicos de phishing, ingeniería social o cualquiera de los métodos descritos en la sección anterior de amenazas.

El mercado ofrece una amplia gama de dispositivos de diferentes fabricantes y con varios tipos y versiones de sistemas operativos. La mayoría de los proveedores de sistemas operativos móviles no permiten que las aplicaciones que se distribuyen desde un tercero puedan ser utilizadas en sus dispositivos, y sólo permiten las que se distribuyen en su tienda oficial ya que a la hora de publicar una aplicación en los repositorios oficiales se realiza un proceso de análisis que implica la prueba y revisión de código de la aplicación que pretende ingresar al repositorio con el fin de evitar la publicación de contenido malicioso. El proceso difiere entre diferentes proveedores y todos ellos tienen diferentes ideas sobre cómo realizar la distribución de las aplicaciones. En particular Android se diferencia del resto porque presenta la opción de habilitar o deshabilitar el permiso para que se puedan instalar aplicaciones desde fuentes que no sean su tienda oficial. Ello implica que posee mayores riesgos que las demás plataformas, al hacer “más fácil” que el

usuario cometa un error; instalando una aplicación maliciosa, que se hace pasar por otra cosa, desde una fuente externa. Sin embargo, los repositorios oficiales no están completamente libres de peligros por lo que siempre es recomendable realizar una revisión de las aplicaciones antes de instalarlas independientemente del medio desde donde se obtengan. Un ejemplo de una revisión simple es observar los permisos que la aplicación necesita para funcionar. Tomemos por ejemplo la aplicación para usar el led del flash del dispositivo como linterna *Tiny Flashlight*[37]. Esta aplicación para Android está disponible en el PlayStore hace mucho tiempo y no presenta comportamientos maliciosos informados. Los permisos que solicita son para instalarse y funcionar son:

Figura 14. Permisos de Tiny Flashlight

Si a la hora de instalar una aplicación que hace uso del led como una linterna esta solicitara permisos por ejemplo para usar el GPS, para realizar llamadas o acceder a datos de navegación, el usuario ya tiene una buena base de información para sospechar que la aplicación posee intencionalidades diferentes a las que informa.

A nivel organizacional, además de la revisión de aplicaciones es recomendable proporcionar una lista negra o lista blanca de aplicaciones. El concepto de una lista negra se describe como una lista de prohibidos, mientras que una lista blanca se refiere a una lista permitidos. Una lista negra de aplicaciones hace referencia a aplicaciones que se

encuentran prohibidas dentro de la organización, una lista blanca exactamente lo contrario. Se utiliza una lista negra para minimizar el riesgo de instalar aplicaciones maliciosas o inapropiadas. Se utiliza una lista blanca para determinar un listado de las únicas aplicaciones permitidas que deberían ser instaladas. A nivel de uso personal el usuario propietario del dispositivo es quien debe permitir el uso de las aplicaciones a su elección. Por tanto, un lista negra es la opción preferida y también se puede complementar con una lista de aplicaciones.

4.5. Técnicas y Aplicaciones para reforzar la seguridad

Existen en todas las plataformas, distintas herramientas cuyo fin es mejorar la seguridad de los datos contenidos en un dispositivo móvil. Estas herramientas muchas veces brindan algunos aspectos de seguridad que las plataformas no proveen y por esto merecen ser mencionadas. En particular y a modo ejemplificador nos haremos referencia a 2 tipos de aplicaciones: Antivirus y Vaults (bóvedas).

Los Antivirus de dispositivos móviles cumplen la misma función que en las PCs, protegiendo al dispositivo del malware. Los antivirus realizan escaneos de las aplicaciones instaladas para controlar la ausencia de comportamiento malicioso. Mantienen una base de datos acerca de las aplicaciones maliciosas conocidas para la plataforma, la cual actualizan regularmente. Brindan funcionalidades para la eliminación de malware, el control de tráfico de red, bloqueo de aplicaciones, tracking de dispositivo, bloqueo remoto, eliminado remoto de información, escucha remota, firewall, entre otros. Resulta interesante mencionar que debido a la cantidad de funcionalidades críticas que presentan, los permisos que solicitan es bastante grande. Un extenso análisis[38] realizado por *AV-Comparatives* compara funcionalidades provistas por distintos antivirus moviles, explicando cómo son llevadas a cabo y puede resultar atractivo para el lector. Entre los antivirus móviles más conocidos se encuentran: *"Avast Mobile Security"*, *"McAfee Mobile Security", "AhnLab V3 Mobile Security"* entre otras.

Las Vaults o bóvedas, son aplicaciones que se hicieron famosas por su funcionalidad de cifrar y proteger por contraseña archivos y/o el acceso a aplicaciones. Las aplicaciones de

este tipo, proveen un almacenamiento más seguro dentro del dispositivo móvil para archivos sensibles. La funcionalidad básica de las aplicaciones tipo Vault radica en la capacidad de almacenar de manera cifrada archivos que solo pueden ser accesibles mediante el ingreso de una contraseña para descifrarlos. De esta manera un usuario podría almacenar en una Vault protegida por contraseña la información sensible que almacena en su dispositivo móvil, agregando un nivel más de seguridad. Las funcionalidades más comunes implementadas por las vaults son: galerías privadas, vaults con protección por contraseña, fotografia en caso de contraseña incorrecta (si se ingresa una contraseña incorrecta para acceder a una vault, la herramienta hace uso de la cámara frontal para sacar una foto de quien intentó acceder y la almacena en la vault), bloqueo de aplicaciones con contraseña, falsas bóvedas como señuelos, copias de seguridad en la nube, etc. Algunas aplicaciones tipo Vault famosas son "*Vault-Hide SMS, Pics & Videos"* de *NQ Mobile* y *"Vaulty"* de *Squid Tooth LLC*.

A la hora de proteger el acceso a cuentas de servicios que se acceden desde un dispositivo móvil cuyas credenciales podrían ser robadas por algún malware o algún ataque de otro tipo, una de las técnicas más simples de hacerlo es a través de la Verificación en dos pasos o Autenticación en dos pasos (Two Factor Authentication o 2FA). El sistema de 2FA es una de las versiones de la metodología de Multi-Factor Authentication (MFA)$_{[39]}$ cuyo propósito consiste en la utilización de múltiples factores de autenticación para poder confirmar la identidad de que quien quiere acceder a datos sensibles es realmente la persona autorizada para hacerlo. Este sistema no vuelve imposible el robo de información, pero añade una capa más de seguridad si alguien intenta acceder a una cuenta donde por ejemplo se tienen datos personales o donde pudieran hacerse pasar por el verdadero dueño de la cuenta. El uso de múltiples factores de autenticación para probar la identidad está basado en la premisa de que quien no esté autorizado a ingresar a los datos sensibles será incapaz de proveer todos los factores requeridos para el acceso. Si en un intento de autenticación al menos 1 de los factores falta o es incorrecto, la identidad no puede

confirmarse y el acceso no es permitido. Entre los factores utilizados para MFA podemos mencionar:

- Factores de Conocimiento: “Algo que el usuario conoce”, como contraseñas, PIN, preguntas secretas. Son el factor más utilizado
- Factores de Posesión: “Algo que el usuario tiene”, como tokens de seguridad USB o tarjetas.
- Factores de Inherencia: “Algo que el usuario es”, datos biométricos como una huella dactilar o el iris.

Uno de los métodos más utilizados en servicios de uso masivo, como facebook o servicios de google, es 2FA usando los teléfonos móviles o smartphones como “algo que el usuario tiene”, cumpliendo el rol de segundo factor de autenticación. A la hora de autenticarse a un servicio con 2FA activado que hace uso de un teléfono móvil, el usuario deberá ingresar por ejemplo su usuario y contraseña y además un código dinámico temporal de un solo uso que le será entregado mediante SMS. La seguridad radica en que los códigos enviados por SMS se generan de manera aleatoria en el momento que se solicita el acceso, y pasado un período corto de tiempo se eliminan para evitar que sean comprometidos. Frente a un nuevo acceso, se generará y enviará un nuevo código al dispositivo. La ventaja de este método es que no se necesita memorizar claves extras, ni llevar siempre encima un token, sino solo el teléfono móvil. Algunas de las desventajas son que el dispositivo podría ser robado, el sms interceptado, o que en un lugar sin cobertura la persona correcta no podrá autenticarse ya que el código SMS no llegaría al dispositivo.

La mayoría de las personas solo utilizan un nivel de protección (contraseña) para sus cuentas. Gracias al sistema 2FA, si un atacante descubre una contraseña, necesitará también el teléfono o el token de seguridad para poder ingresar a la cuenta. Como se dijo, con el sistema 2FA se protege la cuenta con un elemento que se conoce (la contraseña) y un elemento que se tiene (el teléfono o token), añadiendo un elemento más de seguridad al solicitarnos un código de comprobación junto al nombre de usuario y la contraseña en el momento de iniciar sesión. Si por ejemplo consideramos el caso de 2FA donde se utiliza un código que se envía a un número de teléfono cuando se quiere acceder al servicio, a la

vez que se protege la cuenta se puede saber si alguien trata de entrar en ella en un momento dado ya que el sistema enviará el código al dispositivo que el usuario tiene en su poder.

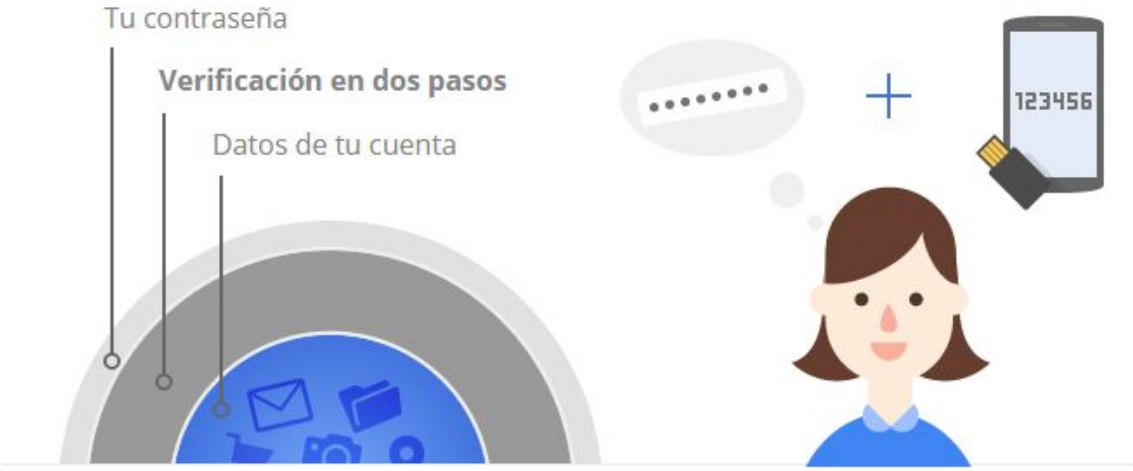


Figura 15. Mobile Two Factor Authentication.

5. Seguridad de la organización, el fenómeno BYOD

En este capítulo nos referiremos al nuevo paradigma que entra en escena en las organizaciones, el BYOD. Se presentan el análisis de características, los nuevos aspectos de seguridad y cómo mitigar los ataques mediante una política organizacional clara. Se describirán los pasos necesario para la creación de una política de mitigación, que lo constituye y cómo mantenerla activa en la organización. Se describirán las nuevas amenazas que el BYOD representa dentro de una organización y cómo las diferentes áreas que comprenden una organización tendrán que trabajar para mitigar estos problemas.

Bring Your Own Device (BYOD), que traducido al español significa "trae tu propio dispositivo", es un nuevo fenómeno cultural y tecnológico que incentiva a los miembros de una organización utilizar sus propios dispositivos móviles personales en las actividades de la organización donde trabaja conectado a la red organizacional.

El fenómeno del BYOD[40] es una tendencia que se expande cada día en las organizaciones de todos los tamaños gracias a la reducción de precios de dispositivos móviles tales como smartphones, tablets y laptops. Hoy en día es muy común que los miembros de una organización hagan uso de sus dispositivos móviles personales para realizar sus labores en la organización donde brindan sus servicios, y lo que era un dispositivo personal se convierte en parte de la red organizacional. La razón por la que ocurre esto es que la tecnología que se usa en casa es tan buena como la que se usa en la organización. Algo que ha contribuido a esta tendencia es la explosión de smartphones y tablets en los hogares y que la tecnología usada en casa y en la oficina puede estar interconectada. Es tal este fenómeno que en Estados Unidos muchas organizaciones llegan a ofrecer a sus miembros cierta cantidad de dinero para que ellos se compren la computadora o smartphone que más les atraiga, con la idea que quien trabaja cómodo, trabaja mejor.

Para los administradores de los departamentos de TI (Tecnologías de Información) esta tendencia resulta problemática a la hora de llevar a cabo las políticas de soporte y seguridad porque ahora hay dispositivos variados sobre los que no poseen control dentro del radar organizacional que solicitan conectarse a las redes organizacionales, lo que conlleva a un potencial riesgo para la seguridad de la información sensible que pertenece a la organización.

Innovación, inteligencia e inversión, son los tres pilares sobre los cuales las organizaciones necesitan apostar sus estrategias organizacionales. Para lograr enlazar estos tres pilares, los departamentos de TI son fundamentales en la creación de plataformas que permitan interconectar a los actores involucrados en la consecución de dichas estrategias. En un futuro, donde todo estará interconectado, la ubicuidad de dispositivos acelerará un incremento en el desarrollo de servicios para un usuario móvil y que está permanentemente conectado. La implementación de una infraestructura inteligente, que permita gestionar la variedad de dispositivos móviles conectados a la red organizacional, implicará un uso racional de los recursos tecnológicos que poseen las organizaciones.

Según varios estudios, para el año 2020, el concepto que tenemos hoy en día de oficina desaparecerá y el volumen de la información digital se multiplicará por $30_{[41]}$ debido a los cambios tecnológicos que estamos experimentando en estos momentos. Que el volúmen de información se multiplique en un factor de 30 para el 2020 implica la necesidad de llevar a los extremos las medidas de seguridad para evitar fugas de información que puedan darse a través de los múltiples dispositivos interconectados a la red organizacional.

Con la introducción de tecnologías móviles más seguras y capaces y con el inevitable crecimiento en la adopción de la nube (cloud computing) en la vida organizacional y personal el concepto actual de oficina irá desapareciendo. El patrón de trabajo que persistirá será el híbrido, porque la oficina se usará como un lugar para reuniones y networking, bajo la modalidad presencial, semipresencial o virtual. Y el trabajo desde el hogar tendrá una aceptación cultural mayor.

Ante el fenómeno del BYOD las organizaciones se han visto obligadas a actualizar sus plataformas de servicios, pero el envejecimiento de los sistemas heredados de back office[42] (labores informáticas y de comunicaciones, de gestión de recursos humanos, contabilidad o finanzas) tiene como consecuencia que el 79% de las organizaciones no puedan racionalizar adecuadamente sus entornos tecnológicos y las plataformas que dependen de ellos.

Lo anterior está ocurriendo a pesar de que las organizaciones reconocen el gran poder de agente de cambio que las tecnologías involucran en un mercado en continuo cambio. En Europa las organizaciones líderes en diferentes áreas confiesan que se ven tentados a adquirir la última tecnología disponible, aunque todavía no se haya alcanzado la funcionalidad plena de la existente. Esto conlleva a denotar que existe una laguna entre las inversiones que han sido destinadas a las tecnologías de front y back office, porque se está destinando más inversión en nuevas tecnologías a nivel de front office mientras que las inversiones de back office decaen. Este enfoque dispar de la administración de las TICs implica que los procesos del negocio queden expuestos a cuellos de botella, riesgos de seguridad o duplicación de esfuerzos.

Cuando hablamos de BYOD, hacemos referencia a una tendencia consolidada y ante la cual las organizaciones deben hacer un análisis de riesgos para tomar un posición al respecto. La adopción de esta tendencia por parte de las organizaciones puede traer, como mencionamos, grandes beneficios relacionados con la disminución de los gastos en infraestructura, la comodidad de los empleados para el manejo de la información y por tanto el incremento de la productividad, pero a su vez enfrenta a la organización a nuevas amenazas que deben ser gestionadas; las principales y quizás más preocupantes son la fuga de datos y el acceso no autorizado a la información.

Es así como las organizaciones para enfrentar estos retos deben establecer una mezcla entre políticas claras para el manejo de la información y el uso de herramientas adecuadas que permitan la gestión de la seguridad de la misma. Estas dos medidas deben complementar con un adecuado plan de divulgacion y educacion para que todos los

niveles de la organización conozcan las restricciones alrededor del manejo de la información.

Debido y en relación a este fenómeno es que se presentan en la sección de casos prácticos realizados el análisis de una herramienta para el manejo de dispositivos móviles y un ejemplo de política para BYOD como complemento del análisis y descripción del fenómeno y las dificultades este trae aparejadas.

5.1. BYOD: Características de un nuevo paradigma

A continuación se presentan con más detalle algunas de las nuevas características que deben analizarse a la hora de tomar la decisión de enfrentar el establecimiento de una política de BYOD en una organización con el fin de poder manejar los nuevos entornos organizacionales. Cabe mencionar desde un primer momento que cualquier política de BYOD, para ser eficiente, debe tener un punto importante en la capacitación de usuarios respecto a los temas que se presentan a continuación.

Uso de los dispositivos móviles

Dado que los empleados llevan sus dispositivos personales a la organización, además de darles un uso personal, lo más usual es que los utilicen para la revisión del correo electrónico organizacional y como apoyo a las tareas del trabajo. A esto se suma que para poder acceder a la información organizacional desde sus dispositivos personales, los empleados utilizan en su mayoría las redes WiFi que tiene la organización. Además, el hecho de manipular este tipo de información permite que sea almacenada en los dispositivos personales, y en general no se tienen en cuenta las precauciones necesarias para eliminarla. Finalmente, al ser un dispositivo personal no suele contar con controles como el cifrado de la información, una medida de seguridad que puede llegar a evitar que caiga en manos incorrectas si el dispositivo se extravía o es robado.

Cambios en la gestión de Infraestructura

A raíz de los nuevos usos para los dispositivos personales (vinculados con información organizacional), se plantean también nuevos retos para departamentos de TI en cuanto al

manejo de sus recursos para garantizar la seguridad de los datos de la organización. Estas nuevas formas de manejar la información implican que las organizaciones deban prestar mucha más atención a la forma en que los usuarios se conectan a las redes de la organización para manipular la información, y se preocupen cada vez menos por la infraestructura física. No obstante, se generan nuevos riesgos que se deben gestionar adecuadamente para garantizar la seguridad de la información, con el objetivo de proveer mejores y más altos niveles de rendimiento y un control más preciso para los diferentes tipos de dispositivos.

Gestionar los recursos

Los análisis de riesgos deben partir de la clasificación de la información con el objetivo de establecer, por ejemplo, cuáles son los datos sensibles que requieren mayores niveles de protección; a qué información se puede acceder desde dispositivos personales; a cuál por fuera de la red de la organización; y a cuál debe restringirse el acceso total. Con estos datos se logrará establecer cuáles son las medidas de control más adecuadas para garantizar la seguridad de la información, ya sean de tipo tecnológico o a nivel de estructura y procedimientos. Toda esta gestión de riesgos debe estar complementada con un adecuado plan de educación para que todos los empleados conozcan las implicaciones del uso de sus dispositivos personales, los riesgos a los que están expuestos y las medidas de seguridad que deben tener en cuenta.

Trabajo remoto

A raíz de la posibilidad de manejar información laboral en dispositivos personales, nacieron tendencias como el homeworking, es decir, la posibilidad de trabajar desde el hogar y a través de un equipo personal, tienen un impulso importante. Esta cuestión implica que las organizaciones contemplen diversos panoramas, como la manipulación de información laboral en dispositivos que pueden no estar protegidos adecuadamente. Si bien esta tendencia permite ahorrar costos operativos para las organizaciones y brindar un mejor ambiente a los empleados, es necesario que consideren opciones para que los

usuarios tengan sus dispositivos protegidos con una solución de seguridad y con las aplicaciones actualizadas para prevenir infecciones.

Manejo de la información

Si el empleado manipula información de la organización en su dispositivo personal, debe estar claro qué pasará con ella una vez terminada la relación contractual, ya que es muy complicado tener la seguridad de que la información será eliminada. Las acciones de control en estos casos pueden apoyarse en aspectos contractuales, como la firma de acuerdos de confidencialidad o medidas más estrictas en relación al tipo de información que se pueda descargar y almacenar en dispositivos personales.

Gestión de aplicaciones y dispositivos

El reto para las organizaciones es garantizar que los dispositivos, a través de los cuales se accede a la información, cuenten con aplicaciones seguras que no pongan en peligro la integridad de la información. Además, el área encargada de la seguridad de la de información dentro de la organización debe tener políticas definidas que permitan especificar el uso que los empleados le pueden dar a los recursos de la organización a través de sus dispositivos personales. De esta manera, se logra controlar y gestionar los recursos de red, pues estos se convierten en un punto de falla que podría permitir la intrusión ilegal a los sistemas de la organización.

5.2. Aspectos de seguridad en el uso del BYOD

En cuanto a seguridad el fenómeno de BYOD no está libre de riesgos. El utilizar dispositivos propios para acceder a redes organizacionales, que a su vez podrían usar un software no recomendado por la organización, representa un gran riesgo para la seguridad de los datos y a su vez un reto para el personal que trabajan en TI. Asimismo, el comportamiento o los malos hábitos de seguridad de los usuarios pueden escaparse del control del departamento de TI en la medida que crezcan los BYOD en la red organizacional. Sin embargo, aunque entendemos que las redes organizacionales contienen información muy importante para las organizaciones y la seguridad de los datos

debería ser una prioridad de protección, muchas organizaciones han abrazado el concepto de BYOD[43] sin pensar en las consecuencias de seguridad.

Es necesario asegurar la solidez de los sistemas desde adentro, logrando que el entorno esté altamente protegido, independientemente de dónde provenga la petición de acceso y esa buena práctica debe venir acompañada de adiestramientos y educación al usuario a quien se le autoriza que traiga su dispositivo personal.

Por otra parte, el que los miembros utilicen sus propios dispositivos para el trabajo es algo que debe estar controlado. Por lo que se recomienda que la implantación del BYOD no se deje a la espontaneidad, sino que se planifique.

El personal de TI debe conocer y entender las necesidades de los miembros, pero valorando la conveniencia de poner en marcha un plan de BYOD, entendiendo a la vez que es trabajo de todos evaluar las ventajas y calcular los costos de planificación y de protección de datos.

En una encuesta desarrollada por la organización Fortinet, y realizada en más de quince países, se encontró que cerca de 42% de los encuestados indicaron la pérdida de datos y la llegada de software malicioso a sus redes fue a consecuencia del BYOD.

Asimismo, Fortinet reportó[44] que *"más de uno de cada tres trabajadores, un 36%, admitieron que han infringido o infringirían la prohibición de usar sus dispositivos personales con fines laborales"*. A pesar de ello, cuando se autoriza el uso corporativo de éstos, dos de cada tres encuestados consideran que deben ser ellos mismos y no el departamento de sistemas de la organización los responsables de la seguridad de los aparatos.

De manera que queda establecido que este asunto de la seguridad es una responsabilidad de todos sus usuarios, no importa el aparato tecnológico que utilicen para acceder a la información.

Todos los riesgos del BYOD provienen principalmente del hecho de que es el propio usuario quien gestiona sus propios dispositivos personales. Esto implica que la

organización, propietaria de los datos, tiene menos control sobre el dispositivo que accede a estos datos que si este fuera de la organización.

Con el BYOD se amplía el espectro de dispositivos que pueden acceder a los datos, dificultando el control y administración de este tipo de tecnología. Por otro lado, ante la variedad de dispositivos que existen, hay que valorar el uso que se les da, sus características de seguridad implícitas y a que datos pueden tener acceso. Así que, a través de diferentes tipos de ataque a los dispositivos móviles personales un ciberdelincuente podría obtener usuarios y contraseñas de acceso a servidores, cuentas de correo, servidores ftp o directamente obtener archivos almacenados en el propio equipo o a algún otro dispositivo o recurso de red al que se tenga acceso. Estos ataques pueden producir:

- Pérdida de datos directa desde el dispositivo: robo/eliminación/modificación de archivos accesibles desde el dispositivo.
- Robo de identidad que permita el acceso a diferentes servicios de la organización.

Estos riesgos hacen que a la hora de gestionar los datos se deban controlar distintos parámetros referentes a la seguridad de los datos de la organización teniendo en cuenta:

- A qué datos se tiene acceso desde los dispositivos móviles.
- Donde pueden estar almacenados los datos.
- Cómo se transfieren los datos.
- La posibilidad de fuga de datos.
- El uso personal y de negocio de forma simultánea.
- La capacidad y configuración de seguridad del dispositivo.
- Qué hacer si el propietario del dispositivo renuncia de su puesto de trabajo.
- Cómo tratar la pérdida, robo de un dispositivo.

Ahora se debe gestionar hasta donde se permite al usuario acceder a los datos desde dispositivos más variados con tecnologías que no siempre estarán actualizadas y sin garantías de estar securizadas.

Las amenazas a dispositivos móviles y que pueden comprometer los activos de información de la organización son las siguientes:

Malware: Programas maliciosos creados para manipular el funcionamiento normal de los sistemas sin el conocimiento ni consentimiento de los usuarios. Estos programas tratan de alterar el funcionamiento normal del equipo así como la información que contienen o manejan. El objetivo de estos ataques pueden ser múltiples: uso del sistema para realizar actos delictivos, obtención de datos pero lo que en el trasfondo siempre estará presente en la mayoría de ataques es un fin económico. Por lo tanto, tratan de ser lo más silencioso para poder actuar el máximo tiempo posible. A través de un ataque malware al dispositivo un atacante podría:

- Acceder a información sensible (datos o credenciales).
- Usar el móvil dentro de una red zombie.
- Cifrar, borrar o modificar archivos.
- Infectar la red organizacional.

El malware puede infectar un dispositivo móvil de diversas formas:

- Explotando una vulnerabilidad de cualquier programa instalado en el sistema.
- Ingeniería social: Incitando al usuario a que realice algún tipo de acción. Se utiliza sobretodo en correos de phishing, aunque encontrarse en otro tipo de ataques de ingeniería social.
- A través de un archivo malicioso que puede llegar adjunto en un mensaje, archivo en una web, carpetas compartidas.
- Dispositivos extraíbles que contienen copias del malware que se ejecuta automáticamente una vez se conecta el dispositivo extraíble.

Privilegios y permisos de las aplicaciones: Cuando se instala una aplicación en un dispositivo móvil la aplicación requiere que se acepten una serie de permisos que, supuestamente, son necesarios para funcionar correctamente. En el caso de aplicaciones en android de no aceptar estos permisos la aplicación no se instalará. La mayoría de veces, los usuarios, suelen aceptar estos permisos sin ni siquiera haberlos leídos, por lo que no se analiza donde tendrá acceso la aplicación que se está instalando. Como una aplicación puede solicitar permisos para prácticamente cualquier función del dispositivo

(acceso a las herramientas del sistema, acceso a la red de datos, acceso a la lista de contactos, acceso al historial web) un programador podría encubrir en una simple aplicación algo más que lo que se cree que se está instalando.

Simplemente aceptando este exceso de permisos y privilegios en una aplicación podemos provocar que la aplicación ayude a un atacante a:

- Robar información sensible (datos o credenciales).
- Cifrar, borrar o modificar archivos.
- Usar el dispositivo móvil usando cualquier de sus capacidades (envío de mensajes, conexión a internet, etc)

Ataques a través de redes wifi: La flexibilidad y movilidad que aportan las redes inalámbricas ha hecho que actualmente se use el sistema wifi como el sistema más elegido para la conexión de datos en edificios y espacios abiertos. El uso del aire como medio de transmisión provoca que la señal enviada llegue no solo al dispositivo destino sino a muchos otros que puedan estar dentro del alcance. Tanto los dispositivos que sostienen esta red y las señales de comunicaciones que transfieren están expuestos a diversos ataques:

- Sniffing: Es uno de los ataques más sencillos. consiste en la intercepción de datos inalámbricos que se están emitiendo en una red wifi. La forma más habitual es a través de un software que captura la información de red pese a que también puede realizarse por hardware. Aquel tráfico que no esté cifrado, o lo esté con un sistema débil será accesible para el atacante.
- Análisis de tráfico: El atacante obtiene información con solo examinar el tráfico y sus patrones.
- Spoofing: El atacante se hace pasar por un punto de acceso y el cliente piensa estar conectándose a una red WLAN verdadera.
- Modificación: El atacante borra, manipula, añade o reordena los mensajes transmitidos.

- Reactuación: El atacante inyecta en la red paquetes interceptados utilizando un sniffer para repetir operaciones que ya habían sido realizadas.
- Denegación de servicio: El atacante puede utilizar el servicio wifi generando interferencias que produzcan errores en la transmisión hasta que la velocidad caiga hasta hacerla casi inutilizable.

A partir de estos ataques se podría leer, insertar y modificar mensajes entre dos usuarios o sistemas. Para el caso que nos ocupa este ataque podría realizarse cuando el trabajador de la organización esté usando su dispositivo móvil desde alguna red desconocida y quizás insegura como podría ser la wifi de un bar o de un aeropuerto.

Atacando a una red wifi se podría:

- Robar información sensible (datos o credenciales).
- Desviar correos a otro destino, modificarlos y enviarlos o no al destinatario, con el perjuicio que provocan estos actos para la organización. Con esto podrían perjudicar la relación con clientes, añadir malware a los correos, etc.

Ataque a bluetooth: Como en el caso anterior, el uso del aire como medio de transmisión hace que la señal enviada no solo llegue al destino sino también a los dispositivos dentro de un alcance. Un atacante puede aprovechar el uso del bluetooth para realizar diversos ataques a los dispositivos que lo tengan activo. Con la redefinición del estándar de emparejamiento entre dispositivos bluetooth se ha conseguido rebajar en gran porcentaje el número de ataques a esta tecnología. Pese a ello aún es posible realizar ciertos ataques. Como ejemplo, algunos de ellos:

- Bluebug: es una vulnerabilidad causada por un error en la implementación de la pila de Bluetooth gracias al cual es posible conectarse al puerto serie RFCOMM del teléfono móvil y enviar comandos AT que serán ejecutados en el terminal GSM. Explotando esta vulnerabilidad, un atacante podría realizar llamadas, obtener la agenda de contactos y de llamadas, acceder al servicio SMS y muchas cosas más.

- BlueSnarf: permite extraer archivos de un teléfono móvil sin previa autorización del propietario. Con este ataque un atacante puede obtener los contactos, el calendario y otros datos de otro usuario.

Como en los casos anteriores nos encontramos con un tipo de ataque que puede acarrear problemas serios para la organización y sus datos, ya que un atacante podría:

- Robar información.
- Enviar mensajes o realizar llamadas no deseadas.

Ingeniería social: Un ataque de este tipo consiste en la manipulación de las víctimas con el fin de obtener información confidencial o para convencerles de que realicen alguna acción que comprometa su sistema. Gracias a las formas de comunicación en línea que hay actualmente (redes sociales, correo) este tipo de ataques están en aumento. La ingeniería social se sustenta en el principio de que el usuario es el eslabón débil. A través de los dispositivos móviles se pueden realizar diferentes tipos de ataques de ingeniería social, por ejemplo:

- Llamada suplantando identidad: Recibir una llamada de nuestro supuesto departamento TI que después de una serie de preguntas y de ganarse nuestra confianza nos pregunte por nuestro password del correo.
- Phishing attacks: Uno de los métodos más usados. Fraude informático que utiliza el mail, SMS y web, para convencer a la víctima de que revele cierta información (datos de la organización, contraseñas) o realice cierta actividad como entrar en una web falsa.

A través de un ataque de ingeniería social un atacante podría:

- Obtener información sensible (datos o credenciales).
- Infectar con malware el dispositivo móvil y este a la red organizacional.
- Obtener un pago de la organización.

Ataques a 2G/3G/4G: A través de estos estándares de comunicación de telefonía tradicional también pueden llevarse a cabo ciertos ataques para perjudicar al propietario del dispositivo móvil o bien a la organización donde trabaja.

En 2G la seguridad es prácticamente nula y sus protocolos y algoritmos de cifrado presentan multitud de vulnerabilidades permitiendo a un atacante.

- Ataques de escucha pasiva que permiten la intercepción, escucha de llamadas, suplantación de identidad y obtención de SMS.
- Ataques de escucha activa donde el atacante actúa como una estación base falsa que actúa sustituyendo a la del operador sin que la víctima detecta anomalía.
- Ataques de denegación de servicio a ciertos usuarios y semipermanentes.

En 3G la seguridad es más elevada, pese a ello se puede llevar un ataque de denegación de servicio que obliga al dispositivo móvil a cambiarse a 2G y una vez conectado a 2G se podría llevar a cabo alguno de los ataques descritos anteriormente. También es vulnerable a ataques man-in-the-middle y se ha demostrado que se puede acceder a datos e identidades a través del eavesdropping, consiste en la escucha pasiva de una comunicación de forma que un atacante puede capturar información privilegiada y claves para acceder con posterioridad a más información.

Para 4G, basada en tecnología IP, existen también una serie de ataques que no hacen de esta tecnología una tecnología libre de vulnerabilidades. Estos ataques son:

- Ataques a los recursos de radio, pudiendo provocar una denegación de servicio.
- Ataques man-in-the-middle.
- Ataques eavesdropping.

A través de los ataques que se pueden llevar a cabo a través de 2G, 3G, y 4G un atacante podría:

- Denegar el servicio a un dispositivo concreto.
- Obtener información sensible (datos o credenciales) a través de escuchas telefónicas.

Ataques a NFC: Esta tecnología permite la transmisión e intercambio de datos de forma inalámbrica entre dispositivos móviles próximos a los 20 cm de forma instantánea y sin necesidad de emparejamiento entre ellos. Se usa mayoritariamente para realizar pagos sin necesidad de usar tarjetas o dinero en efectivo, intercambio de datos y automatización de tareas como ejecutar aplicaciones o realizar llamadas.

NFC tiene una serie de vulnerabilidades con las que un atacante podría:

- Robar información sensible (datos o credenciales).
- Cifrar, borrar o modificar el contenido de los archivos o los propios archivos.
- Descargar malware e infectar el equipo y la red organizacional.
- Intersección, lectura y modificación de los datos que se transmiten entre dispositivos mediante un atacante man-in-the-middle.

Robo o pérdida del dispositivo móvil: A partir del robo de un dispositivo móvil un atacante podría acceder a todos los datos del dispositivo móvil y a todos aquellos datos remotos accesibles desde el propio terminal.

Así que, podemos afirmar que todos los tipos de tecnologías inalámbricas que podemos encontrar en un dispositivo móvil son vulnerables y que en mayor o menor medida permiten a un atacante obtener información y datos del mismo dispositivo móvil o de otras ubicaciones. Esto hace que se haga indispensable un correcto uso del dispositivo por parte de los usuarios y a que la organización aporte el máximo de recursos posibles a la protección de sus datos, a la consideración de sus trabajadores y a la ayuda en la correcta administración y uso de los dispositivos móviles. Una correcta política en los aspectos anteriores permitirá a la organización y a los trabajadores tener un nivel elevado de seguridad.

5.3. Políticas de mitigación

Los dispositivos móviles pueden sufrir ataques que provoquen robo o pérdida de datos organizacionales o personales, robo de identidad o denegación de servicio que impidan un uso normal del terminal. Además, si permitimos que cada usuario utilice su dispositivo,

nos encontramos con que la red organizacional ya no estará conformada por un conjunto de dispositivos uniformes (mismo hadware, mismo sistema operativo, mismo software), sino que tenemos que gestionar dispositivos de diferentes marcas, con diferentes sistemas operativos, cada uno de ellos con diferentes aplicaciones desconocidas instaladas. Esto hace que la administración de la seguridad de cada dispositivo no se pueda hacer dispositivo a dispositivo y que se necesite centralizar este control de la seguridad.

Teniendo en cuenta las premisas anteriores la opción más interesante es la de controlar desde la red organizacional qué tipo de dispositivo está accediendo a la red, como lo está haciendo, qué aplicaciones tiene instaladas, qué sistemas de conexión tiene activados, si tiene activado el antivirus, si tiene alguna aplicación sospechosa, donde quiere acceder.

Con las necesidades que surgen hay una líneas claras en las que la organización debe trabajar para mantener una red de dispositivos móviles segura:

- Definición de política de uso y gestión.
- Uso de aplicaciones Mobile Device Management (MDM).
- Concientización del usuario

Definicion de politicas de uso y gestión

Una política BYOD es un conjunto de reglas que gobiernan los aspectos relacionados con el uso de dispositivos personales para acceder y utilizar recursos de la organización.

Una política es algo específico para cada organización puesto que debe basarse en los requerimientos de la organización, su perfil de riesgo y su situación, pero en esta sección describiremos los aspectos generales que debe cubrir.

Si en la organización ya existe una política de movilidad organizacional, deberá revisarse para incorporar la política BYOD. Así mismo, deberemos revisar otra políticas que también se verán afectadas (negocio, seguridad, acceso a recursos, regulatorias y legales, RRHH, etc.).

A la hora de definir la política, es conveniente tener en mente que lo que impulsa los programas de movilidad organizacional es la necesidad de proporcionar acceso seguro y transparente (es decir, con la mejor experiencia de usuario) a los recursos organizacionales en cualquier momento, en cualquier lugar y desde cualquier dispositivo.

Las iniciativas de movilidad deben contribuir a facilitar la continuidad del negocio, mejorar la colaboración, simplificar el teletrabajo y mejorar la satisfacción de los empleados.

La política BYOD debe revisarse periódicamente (cada 6-12 meses) para asegurar que se adapta en todo momento a la organización y sus necesidades de negocio. También va a ser necesario estar al corriente de los cambios tecnológicos que la afectan (nuevas funcionalidades o nuevos dispositivos, aplicaciones y servicios de consumo; innovaciones y tendencias en los sistemas de gestión MDM, EMM; nuevas amenazas de seguridad, medidas de protección y mitigación, etc.).

La política debe ser clara, concisa, realista, sostenible y adaptada a los usuarios que la van a utilizar. Una política que pretende influenciar el comportamiento de los empleados no puede estar escrita en un oscuro lenguaje técnico ni alejarse de la cultura y estilo de la organización.

Aunque en un principio la elaboración de la política pueda parecer una tarea abrumadora, hay que tener en cuenta que la peor política es la ausencia de política. Cuando los empleados saben qué se espera de ellos, cuáles son los comportamientos aceptables y las consecuencias del incumplimiento, es menos probable que rompan las reglas y, en caso de hacerlo, los planes de contingencia definidos con anterioridad en las políticas permitirán actuar con rapidez y minimizar el impacto negativo.

Cualquier persona que participe en el programa BYOD debe firmar explícitamente sus condiciones de uso.

Pero las políticas por sí mismas no son suficientes para evitar las consecuencias del incumplimiento de las normas, ya sea por error, accidente o decisión voluntaria del usuario. Necesitaremos herramientas que nos ayuden a hacer cumplir las políticas, como pueden ser los sistemas de gestión de dispositivos móviles (Mobile Device Management, MDM), sistemas de gestión de aplicaciones móviles, etc.

Integrantes que deben participar en la definición de una política BYOD

Como hemos visto hasta ahora, un programa BYOD afecta a muchas áreas de la organización más allá del área de TI. A la hora de crear la política es importante contar

con la participación de todas. Muchas organizaciones carecerán de la estructura organizativa necesaria para crear estas políticas y deberán crearla en profeso para asegurar la gobernanza necesaria para implementar con éxito el programa.

Estas son las áreas que deberían participar en la definición de la política. Según el tamaño de la organización, algunos de estos roles podrían coincidir en una única persona:

- Representantes de las áreas de negocio y de los usuarios.
- Recursos humanos.
- Área legal y de regulación.
- Área de TI:
    - Seguridad.
    - Red.
    - Mensajería y comunicaciones unificadas.
    - Operaciones de servidor.
    - Administración de servicios de TI.
    - Desarrollo y mantenimiento de aplicaciones.
    - Soporte al usuario.

Análisis y gestión del riesgo de la información y la actitud de la organización hacia el riesgo

La seguridad de la información debe ir de la mano de los riesgos de la información. Esto permitirá alinear el área de TI con los objetivos de negocio de la organización.

La tecnología avanza a velocidades vertiginosas, y las amenazas también. Es necesario establecer un marco de referencia adecuado para entender y gestionar estos nuevos riesgos para la organización que están en contínua evolución. Por ello, se recomienda seguir una estrategia estructurada de gestión del riesgo para afrontar los riesgos de forma sistemática.

En primer lugar, tenemos que diferenciar entre riesgo y seguridad. Podemos ver el riesgo de la información como una parte de la gestión de riesgos organizacionales, y la seguridad como el habilitador.

El riesgo definiría dónde vamos y la seguridad determinaría el cómo.

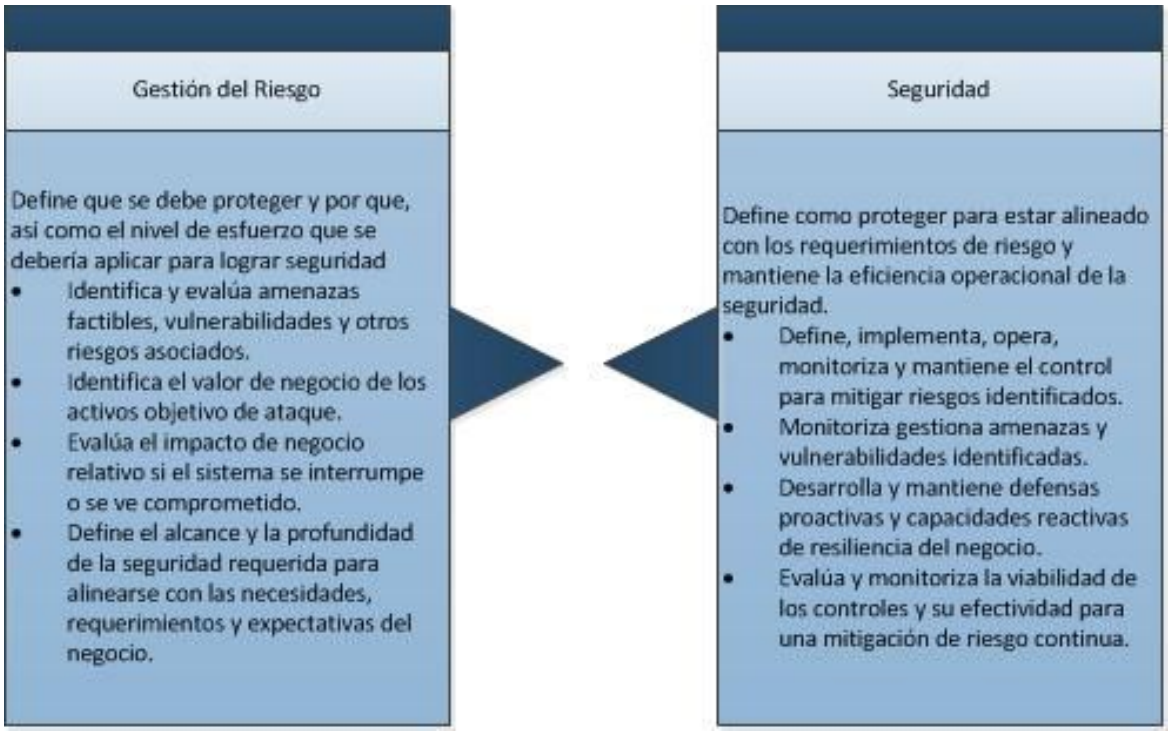


Figura 16. Gestión del Riesgo vs Seguridad

Primero, debemos entender la actitud hacia el riesgo de la organización, es decir, el nivel de riesgo que la organización está preparada para aceptar. Examinar a fondo lo que más le importa y por qué.

La actitud hacia el riesgo no es fácil de concretar, cada organización puede tolerar niveles de riesgo diferentes. Sin embargo, es importante que la organización establezca una definición común de sus riesgos y que se prepare en función de la probabilidad y el impacto de las amenazas conocidas. La organización debería definir el máximo nivel de tolerancia al riesgo en cada área de riesgo antes de determinar acciones.

La actitud hacia el riesgo a veces se expresa a través de una "declaración de actitud hacia el riesgo", un documento que sirve de guía a la organización en las labores de gestión de riesgos. Esta declaración debería basarse en las perspectivas y preocupaciones de todas las áreas implicadas, así como en las prioridades y estrategias organizacionales actuales.

A continuación, debemos detallar los perfiles de riesgo de la información en la organización que, entre otros, implicará contemplar aspectos como:

- decidir y acordar lo que se considera un riesgo aceptable;

- la identificación de todos los activos físicos y lógicos de la organización, manteniendo un inventario preciso de activos, incluyendo aquellos que se acceden o almacenan en dispositivos móviles, (lo que no se conoce no se puede proteger);
- la clasificación de los activos (información pública y confidencial, por ejemplo), para identificar los objetivos y requerimientos de las medidas de control. No todos los recursos tendrán que protegerse de la misma forma ni necesitan accederse o almacenarse en dispositivos móviles;
- definir los incidentes que son significativos (por ejemplo si un incidente implica la pérdida de algunos datos puede no ser significativo para la organización, por lo que el coste de proteger los datos no debería superar el valor de los datos);
- qué se considera una pérdida aceptable;
- priorización de los riesgos;
- análisis realista de amenazas y vulnerabilidades alineadas con el negocio (incluyendo impacto en el negocio y probabilidad de ocurrir);
- el impacto material en el negocio, que puede variar en cada organización, considerando el impacto económico, en la reputación o en el cumplimiento de legislación y normativas;
- el impacto en la cadena de suministro o en el ecosistema de partners y colaboradores;

Para elaborar el perfil de riesgo de la organización en el programa BYOD es necesario conocer muy bien el negocio de la organización, así como el entorno legal y regulatorio en el que se mueve. Por ello, estos perfiles de riesgo deben estar vinculados al análisis y actividades organizacionales de gestión de riesgos, y el área de TI deberá trabajar estrechamente con esas áreas.

Una vez elaborados los perfiles de riesgo de la información, tanto el área de negocio como el área legal deberán firmarlos. Estos perfiles definirán las medidas a tomar para reducir la probabilidad de riesgos (medidas preventivas), y las acciones a emprender en caso de producirse un incidente (planes de contingencia). Definiremos los requerimientos a nivel

tecnología y sistemas de control a implantar en el programa, en base a un enfoque que evalúe las amenazas y alinee las defensas a los riesgos.

Detalle de plataformas, sistemas operativos y dispositivos aceptados en los diferentes grupos de usuarios/roles definidos

Es necesario dejar claro a los usuarios si dentro del programa BYOD se aceptarán todo tipo de plataformas, sistemas operativos y dispositivos, o si, por el contrario, el área de TI sólo dará acceso y soporte a determinados dispositivos. Esta información hay que definirla para cada grupo de usuarios identificado.

El área de TI puede determinar la lista de dispositivos, sistemas operativos y versiones admitidos en función de las necesidades de seguridad, control, aplicaciones y soporte de la organización, puesto que las funcionalidades admitidas van a variar mucho según sistema operativo y dispositivo utilizado.

Si la organización va a implementar una solución MDM/EMM, debemos asegurarnos de que los dispositivos aprobados están soportados por el sistema de gestión.

También será necesario definir las condiciones y plazos de actualización de los dispositivos, así como la obligatoriedad de la actualización. Es posible que el área de TI quiera estudiar si nuevas versiones de los sistemas operativos móviles son compatibles con las aplicaciones organizacionales instaladas en los dispositivos o con el sistema MDM antes de permitir que los usuarios actualicen sus dispositivos. Del mismo modo, es posible que se descubra una vulnerabilidad de seguridad que se corrige con una actualización y que el área de TI deba requerir que los usuarios actualicen de inmediato sus dispositivos.

Igualmente será necesario especificar en la política las consecuencias de no seguir la pautas establecidas por el área de TI (por ejemplo, no disponer de soporte técnico si no se usa un hardware de dispositivo que cumpla los mínimos requerimientos, interrupción del acceso a la red si no se cumplen las condiciones de seguridad, etc.).

Estas especificaciones deben revisarse periódicamente por el área de TI.

Controles de seguridad y gestión

En la parte más técnica de la política deberemos especificar cuestiones como los requerimientos para el acceso a la red, las configuraciones de seguridad recomendadas y obligatorias, los controles de seguridad y gestión que se aplicarán sobre el dispositivo y los datos, (incluyendo el posible reseteo o borrado del dispositivo), la monitorización y auditorías que se efectuará sobre el dispositivo, las aplicaciones permitidas y no permitidas, las posibles restricciones en el acceso a datos organizacionales, etc.

Aspectos relacionados con el área de RRHH, como contenido y remuneraciones

Un capítulo importante a abordar a la hora de desarrollar la política BYOD es la definición de Usos Aceptables dentro del programa. Aunque el dispositivo sea propiedad del empleado, la visualización de contenido inapropiado en el mismo puede ser contrario a las políticas de la organización. Será conveniente por tanto definir qué se considera un uso apropiado del dispositivo en el entorno de trabajo, así como definir qué se considera entorno de trabajo.

Otro tema que también es importante definir claramente son las responsabilidades y derechos de los participantes. Si, por ejemplo, el usuario tiene que comprometerse a reponer el dispositivo en un determinado plazo o a cumplir unas determinadas normas de seguridad, tiene que entender y aceptar explícitamente esas responsabilidades. Del mismo modo, si la organización se compromete a dar determinado nivel de soporte técnico o si va a realizar algún tipo de aporte económico al empleado como parte del programa, es necesario definir claramente las condiciones (quién es elegible, condiciones de participación, cantidades, forma y período de pago, tributación aplicable, etc.).

El área de Recursos Humanos también debería crear un programa de formación y comunicación de los detalles del programa a los usuarios. Si ahora parte de la responsabilidad de protección de la información de la organización va a recaer en los usuarios, es necesario concientizar sobre la importancia de esta protección así como dotarlos de herramientas y conocimientos sobre cómo hacerlo.

Así mismo, trabajando con el área legal y de regulación, también deben establecerse mecanismos para asegurar que los empleados participantes en el programa conocen las condiciones de privacidad y posibles implicaciones legales que puedan derivar del programa, y que estos reconocen la aceptación de la política según requiera la legislación local aplicable.

Soporte al usuario

El soporte al usuario es un elemento crítico del programa. Si no se define adecuadamente puede ser una fuente de insatisfacción para los usuarios y de costes no previstos para la organización. Es conveniente precisar qué pueden esperar los usuarios y a partir de qué punto es responsabilidad suya gestionar el soporte.

Se puede delimitar un tipo y nivel de soporte para cada grupo de usuarios dentro del programa: por ejemplo, usuarios para los que es menos crítico el uso de herramientas móviles se puede ofrecer opciones de autoayuda online a través de wikis y foros, y para el equipo directivo se puede definir un nivel de soporte Premium.

Mobile Device Management

Las herramientas Mobile Device Management (MDM), de uso indispensable para controlar las conexiones a la red organizacional por parte de los dispositivos móviles, ayudarán a las políticas de gestión y seguridad tradicional (firewalls, antivirus, VPN) en su intento por lograr el máximo nivel de seguridad y gestión de los datos de la organización desde dispositivos móviles. Se basan en el control de las aplicaciones y de sus funciones, en el control de los datos y en el comportamiento del usuario.

Estas herramientas permiten asegurar, monitorear y administrar dispositivos móviles de forma que se garantice la seguridad de la información y de la red, ofreciendo, además, otras funciones interesantes para la organización.

Las herramientas de MDM aportan diferentes ventajas al entorno profesional dotando de una base sólida a la organización para la administración de los dispositivos móviles no solo en cuestión de seguridad:

- Permiten realizar un seguimiento de los dispositivos móviles, líneas, usuarios y datos (por ejemplo manteniendo una lista de contactos actualizada de forma centralizada para todos los dispositivos).
- Permiten elaborar informes (por ejemplo, informe de consumo de datos) que permitan tomar mejores decisiones para el futuro de la organización.
- Gestión de la información relacionada con el uso del dispositivo móvil.
- Distribución y administración de aplicaciones organizacionales, tanto organizacionales como de TI.
- Control de las aplicaciones que pueden ser utilizadas evitando que los usuarios ejecuten aplicaciones que no son productivas para las organizaciones.
- Facilitan la administración de los dispositivos.

A nivel de seguridad estos programas permiten asegurar, monitorear y gestionar diversas funciones de forma remota desde un servidor centralizado en el que se definen las políticas o actuaciones a realizar sobre un dispositivo concreto. Como ejemplo, con un sistema MDM, la organización podría establecer la política de que un dispositivo con una aplicación concreta instalada no pueda acceder a la red.

En función de quién sea el propietario del dispositivo se podrán aplicar ciertas funcionalidades o no. Por ejemplo, en caso de que el propietario del dispositivo sea el propio usuario, no se podrá negar al usuario la instalación de aplicaciones no productivas para la organización. En cambio, el departamento TI si podrá controlar que aplicación del dispositivo particular puede acceder a datos organizacionales y cual no.

Una organización debería usar esta tecnología para controlar el uso de los dispositivos en cuanto al acceso que se realiza desde ellos a los datos organizacionales. Esta tecnología le permitiría recuperar un dispositivo perdido o borrar todos los datos que tenga almacenado en caso de que el dispositivo sea robado, evitando así, la extracción de datos del dispositivo.

Políticas como las definidas anteriormente aplicables desde los programas MDM hacen más seguros los accesos a los datos organizacionales dificultando ataques que permitan su

obtención además de permitir el borrado completo de un dispositivo en caso de pérdida (evitando robo de datos o de identidades).

A partir de una aplicación MDM la organización puede controlar diferentes opciones específicas para mitigar los problemas reflejados anteriormente.

Estas herramientas disponen de multitud de opciones que ayudarán a la organización a controlar los riesgos de seguridad existentes con el BYOD.

Se pueden definir los siguientes bloques de seguridad que se puede aplicar a cualquier entorno BYOD:

- Protección antimalware, antiphishing y antispam, usando antivirus u otras tecnologías.
- Controles de aplicaciones, de web y de dispositivos modificados, por ejemplo a través del cumplimiento de políticas.
- Activación de cifrado para la protección de datos, como por ejemplo el uso de VPNs para el envío de datos o de contraseñas para la apertura de archivos.
- Separación de datos organizacionales y personales mediante contenedores (mantienen los datos de organización separados de los personales, permitiendo, entre otras, un borrado selectivo) y restricción de acceso a datos.
- Seguridad en caso de pérdida o robo de dispositivos mediante el rastreo GPS o el bloqueo o borrado remoto.

Podemos diferenciar 5 grandes campos en los que se puede actuar desde una aplicación MDM en cuanto a la seguridad se refiere:

- Gestión de aplicaciones: Gestionando, implementando, instalando, bloqueando las aplicaciones móviles de los dispositivos.
- Gestión de políticas: Controlando identidades, sincronizaciones, integración de cuentas.
- Gestión de seguridad: Aplicando las políticas de seguridad, de autenticación y encriptación definidas, del bloqueo o borrado del dispositivo, de la detección de jailbreak.
- Gestión de inventario: Controlando el estado de los dispositivos y su ubicación.

- Gestión de servicios de telecomunicaciones: Controlando consumos o usos de los servicios de telecomunicaciones.

Estas son algunas opciones/políticas de seguridad de ejemplo aplicables desde un Mobile Device Management a los dispositivos móviles para hacer segura su interacción con la red organizacional:

- Activar cifrado: Mediante esta opción se puede hacer que para acceder a un archivo (ubicado en el dispositivo móvil, enviado por correo) se necesita introducir una clave. Con ello, dificultar el acceso al archivo por parte de personas ajenas a la organización.
- Borrado de los datos de un dispositivo: Permite borrar los datos de un terminal haciéndolos inaccesibles. Esta opción puede usarse en caso de robo o cese de la relación laboral con el trabajador para evitar una fuga o robo de datos.
- Bloqueo del dispositivo: Creando y distribuyendo a los dispositivos móviles reglas de bloqueo del terminal, como por ejemplo el tiempo máximo de inactividad antes de que el terminal se bloquee.
- Requerimiento de PIN: Obligando al usuario del dispositivo a marcar el número PIN para desbloquear el terminal.
- Establecimiento de una contraseña de bloqueo desde el servidor fijando la contraseña a usar.
- Localización y seguimiento de los dispositivos gracias al uso del GPS: permite localizar un terminal perdido o robado.
- Control de las aplicaciones que puedan acceder a los datos organizacionales y cuáles no. Controlando de esta forma qué aplicaciones pueden ser usadas de forma organizacional y descartando aquellas de dudosa fiabilidad (posible malware) o no organizacionales.
- Detectar y restringir los dispositivos con jailbreak o pirateados, pudiendo negarles el uso uso corporativo a sus propietarios o limitados ciertas acciones.

- Control de acciones sobre archivos o correos: Permitiendo, por ejemplo, la visualización de un adjunto a un correo con un programa determinado pero negar su descarga al terminal móvil o su reenvío.
- Instalación, configuración y actualización de un antivirus o firewall a todos los equipos desde el MDM.
- Uso de VPNs en la red organización-dispositivo móvil, creando una conexión segura donde se evite que los datos enviados puedan ser interceptados.
- Establecimiento de políticas para establecer una contraseña.
- Configurar los dispositivos para que conecten a través de VPN en cualquier conexión que realicen con la red organizacional.

Concientización del usuario

Para evitar ataques dirigidos al usuario del dispositivo móvil, sobre todo ataques de ingeniería social, hay que aplicar políticas de seguridad en la organización destinadas a concientizar y educar a los trabajadores para evitar comportamientos que podrían introducir malware o exponer los datos organizacionales a un riesgo deseado.

A través de un conjunto de materiales y acciones formativas la organización deberá de implementar un plan de concientización con el objetivo de concientizar y fomentar hábitos cotidianos de seguridad en sus empleados.

La comunicación es una pieza fundamental del programa BYOD. De nada sirve establecer las mejores políticas, herramientas de seguridad y gestión, así como programas de soporte, si los usuarios no son conscientes de ello.

Colaborando con las áreas adecuadas, como Recursos Humanos, es necesario establecer un marco de comunicación y formación para los usuarios antes del lanzamiento del programa.

Los usuarios deben conocer qué pretenden las políticas BYOD y de seguridad establecidas, los usos aceptados, por qué es importante el cumplimiento de las políticas y qué herramientas va a utilizar el área de TI para implementarlas. Además deben recibir formación sobre las medidas de seguridad que deben implementar en sus dispositivos y el

porqué de ello (por ejemplo, de nada sirve que la organización implemente el más seguro de los sistemas de autenticación, si los usuarios dejan sus credenciales al descubierto).

Los usuarios deben conocer también las consecuencias del incumplimiento de las políticas.

Una vez conocidos los detalles del programa, los usuarios que deseen participar en él deberán firmar explícitamente la aceptación de la política.

Se puede trabajar con Recursos Humanos para que este proceso de formación y aceptación de política se incorpore en el plan de recibimiento para nuevos empleados, y se una al código de conducta y otros documentos organizacionales cuya firma los empleados renuevan periódicamente.

Definición de un piloto

Un programa BYOD es un proyecto muy complejo. Es recomendable empezar definiendo un piloto sencillo, con un grupo limitado de usuarios y pocos dispositivos soportados para, a partir de esa primera experiencia, ir ampliando el proyecto.

En este punto es importante recordar que un programa BYOD no es un proyecto de tecnología, sino un proyecto de gestión del cambio en la organización y hay que tener esto en cuenta a la hora de definir el piloto. Un factor crítico será, por ejemplo, la inclusión de los usuarios finales en el piloto, y el análisis y aceptación del feedback que estos aporten. También será importante la inclusión hábil del equipo directivo puesto que su apoyo será fundamental para la implantación del programa con éxito.

Como se ha comentado anteriormente, antes del arranque del piloto es recomendable que todos los empleados estén informados sobre el proyecto y que los participantes en el piloto hayan recibido la formación adecuada.

Evaluación y seguimiento

El programa BYOD es un proyecto vivo, por lo que deberemos revisar periódicamente la validez de las políticas definidas para asegurarnos que se siguen adaptando a los objetivos y requerimientos de la organización, así como a los avances de la tecnología.

Así mismo, debemos evaluar y monitorear el programa implementado para asegurarnos que el programa funciona según esperábamos y que los requerimientos de negocio y de seguridad se están cumpliendo.

A la hora de definir las métricas a utilizar, además de tener en cuenta el feedback de los usuarios y de las áreas implicadas, debemos identificar aquellas métricas que estén alineadas con los objetivos definidos para el programa. Si, por ejemplo, el objetivo era mejorar la eficiencia del área de ventas, una de las cosas a medir será el incremento en las ventas; si el objetivo era la reducción de costes de TI buscaremos métricas vinculadas a esos costes. Para evaluar la eficiencia del programa, deberíamos incluir también métricas relacionadas con los costes del programa, su impacto en la infraestructura, la satisfacción de los usuarios y los beneficios de negocio logrados.

5.4. Las tendencias del futuro

Según Gartner[45], el movimiento BYOD va a crecer. Para el 2017 la mitad de las organizaciones que sus empleados utilicen sus propios dispositivos para el trabajo, y en el 2020 el BYOD será parte del 85% de las organizaciones. Según sus previsiones, las organizaciones que ofrecerán solo dispositivos organizacionales a los empleados para trabajar serán pronto la excepción.

Figura 17. Previsión de organizaciones que proporcionan dispositivos a los empleados en los próximos años.

Pero además el BYOD no vendrá solo, es y será la era de la Nube Personal. A nivel personal cada vez usaremos más las nubes móviles personales. Nuestro enfoque cambiará hacia los servicios, en vez de hacia el dispositivo que usamos para acceder a esos servicios. Estos nos ayudará a afrontar los tres factores limitantes de la movilidad: vida de la batería, memoria y procesador. Los responsables de TI organizacionales deben tener esta tendencia en cuenta a la hora de plantear las políticas y medidas de seguridad de los programas BYOD.

Otras tendencias que afectarán a que se esté planteando una política BYOD o ya la tengan implantada son:

- Los smartphones y tablets se harán cada vez más inteligentes, incorporarán nuevas funcionalidades y mejorará su capacidad de procesamiento, almacenamiento y ancho de banda. El smartphone ya es y seguirá siendo nuestro ordenador principal. Las organizaciones deben tener en cuenta que veremos las web, y sus servicios, a través de nuestro móvil.
- Crecerá la virtualización del almacenamiento, escritorio, aplicaciones y networking al manejar la seguridad de la virtualización de la capacidad de procesamiento, que permitirá a los dispositivos móviles acceder a los recursos de procesamiento de supercomputadoras y aplicarlos a procesos como compras o logística, por ejemplo.
- La gestión de la identidad digital será cada vez más importante para organizaciones e individuos. Nuevo software permitirá a los usuarios gestionar mejor sus múltiples identidades en redes personales y organizacionales.
- La wearable technology (la tecnología que se viste) estará cada vez más presente. Las principales marcas tecnológicas están lanzando relojes inteligentes, gafas inteligentes y mucho más, creando nuevos problemas y nuevas oportunidades para organizaciones de cualquier tamaño. Si en los últimos años el Bring Your Own Device llegó por sorpresa a las áreas de TI, ahora tienen la oportunidad de

prepararse para una nueva tendencia y empezar a pensar cómo convertirla en una ventaja competitiva, el Wear Your Own Device ya es una realidad.

- Las aplicaciones móviles también para procesos de negocio como compras, cadena de suministro, ventas, mantenimiento, etc. crecerán rápidamente. Cada vez habrá más interés en App Stores organizacionales que permitan a las organizaciones dar acceso a los usuarios a información personalizada. La nueva generación de tecnologías biométricas integradas en nuestros smartphones, jugarán un papel relevante en la gestión de la identidad y la seguridad. Veremos alternativas biométricas, como reconocimiento facial, dactilar, de voz en función de los requerimientos de seguridad necesitados.

Marco Práctico

6. Casos Prácticos Realizados

En este capítulo nos referiremos a 4 (cuatro) casos prácticos realizados en el marco de esta tesina para ayudar a comprender la problemática y a ejemplificar algunos de los desafíos del BYOD, los cuales comprenden una análisis estadístico a adolescentes entre 15 y 18 años, interiorizandonos en sus conocimientos sobre dispositivos móviles y amenazas. Se realizó el análisis de una herramienta de gestión de dispositivos MDM de la empresa Soti, se analizaron sus características y cómo estas herramientas ayudan a las organizaciones a mitigar las amenazas que tienen los dispositivos como blanco de ataque. Se estableció una política de seguridad a modo de ejemplo para una organización con los requerimientos mínimos, para que esta sea de ayuda para definir futuras políticas. Por últimos se creó una Prueba de Concepto que ayude a entender cómo una aplicación maliciosa puede hacerse de información que podría poner en riesgo a un usuario.

6.1. Estadísticas sobre uso de dispositivos móviles

En el transcurso del año 2015 y 2016 se realizaron varios encuentros en el marco del proyecto de extensión *"Aprendiendo a estar digitalmente seguros"*. Este taller está destinado a alumnos secundarios y primario de la ciudad de La Plata y alrededores. El taller permitió aprender a partir de demostraciones los riesgos que presentan el uso de las nuevas tecnologías en dispositivos móviles y los servicio de internet, para luego aplicar mecanismos de protección disponibles a través de las opciones de configuración de los dispositivos y herramientas, tanto las buenas prácticas como las malas prácticas que realizan los usuarios. Se experimentó con ejemplos concretos como el uso de dispositivos móviles y redes sociales afectan nuestra vida y nuestra seguridad permitiendo concientizar a los alumnos que tomaron el taller para prevenir prácticas maliciosas a su persona y ellos

mismos puedan difundir estas nuevas amenazas que afectan a los usuarios de estas nuevas tecnologías.

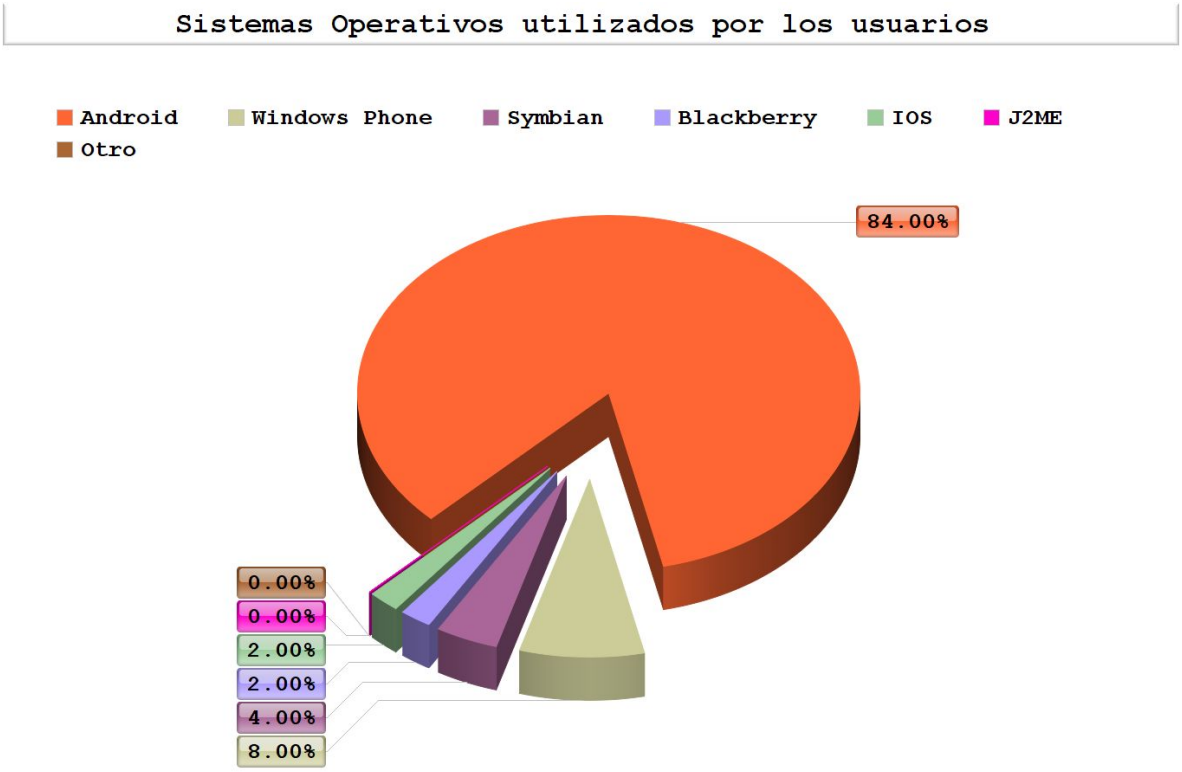
Se les presentó a los alumnos que tomaron el taller un cuestionario para poder generar un informe estadístico que nos permita saber el conocimiento y comportamiento social de los jóvenes entre 15 a 18 años respecto a las nuevas tecnologías y su uso.

Algunos resultados que se pudieron relevar de la encuesta reflejan el comportamiento social de jóvenes entre 15 y 18 años frente a las nuevas tecnologías. Estos jóvenes son parte de una generación en la cual gran parte de estas nuevas tecnologías ya se habían desarrollado masivamente y serán ellos parte de los nuevos avances y paradigmas tecnológicos.

Hay que tener algunas consideraciones antes de analizar los resultados de la encuesta. Muchas de las personas que realizaron la encuesta cuentan con su primer smartphone por lo que ellos mismos están aprendiendo e interiorizando en este mundo de aplicaciones y nuevas tecnologías y los riesgos que conlleva los mismos. Un usuario de más de 24 años fue mutando a la par de la aparición de nuevas tecnologías, en nuestro caso de los inicios de la telefonía analógica, pasando por la telefonía celular y llegando hoy en día a los smartphone 4G, en cambio estos jóvenes se insertaron en esta última etapa sin pasar por las anteriores.

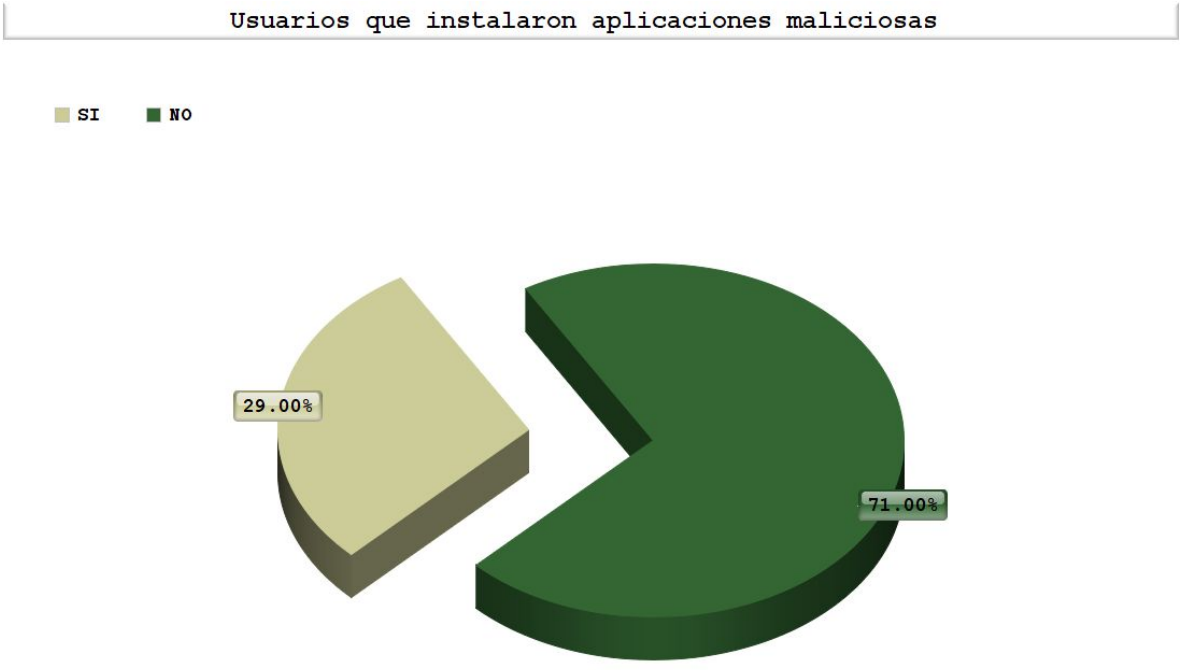
Unas de las primeras preguntas que se les presentó fue si tenían conocimiento de que es un sistema operativo, que función cumple y si tenían conocimiento de cual utiliza su smartphone. Como se visualiza en la siguiente imagen un 84% de los encuestados utilizan alguna versión del sistema operativo Android. Muchos de ellos no tenían noción de que versión es la más actual y cual utiliza su smartphone. Socialmente por lo menos en Argentina, el primer teléfono móvil de un joven es algún teléfono que algún familiar dejó de utilizar o es comprado a un proveedor de telefonía, por lo que la versión del sistema operativo no es la más actual y no fue actualizado, esto conlleva a tener un smartphone con vulnerabilidades que no fueron resueltas.

Después lo sigue el sistema operativo diseñado por windows para competir en el mercado de smartphones. Cabe destacar que los sistemas operativos Blackberry, IOS no son muy populares en el marco de obtención del primer smartphone dado su funcionalidad, disponibilidad y precio.



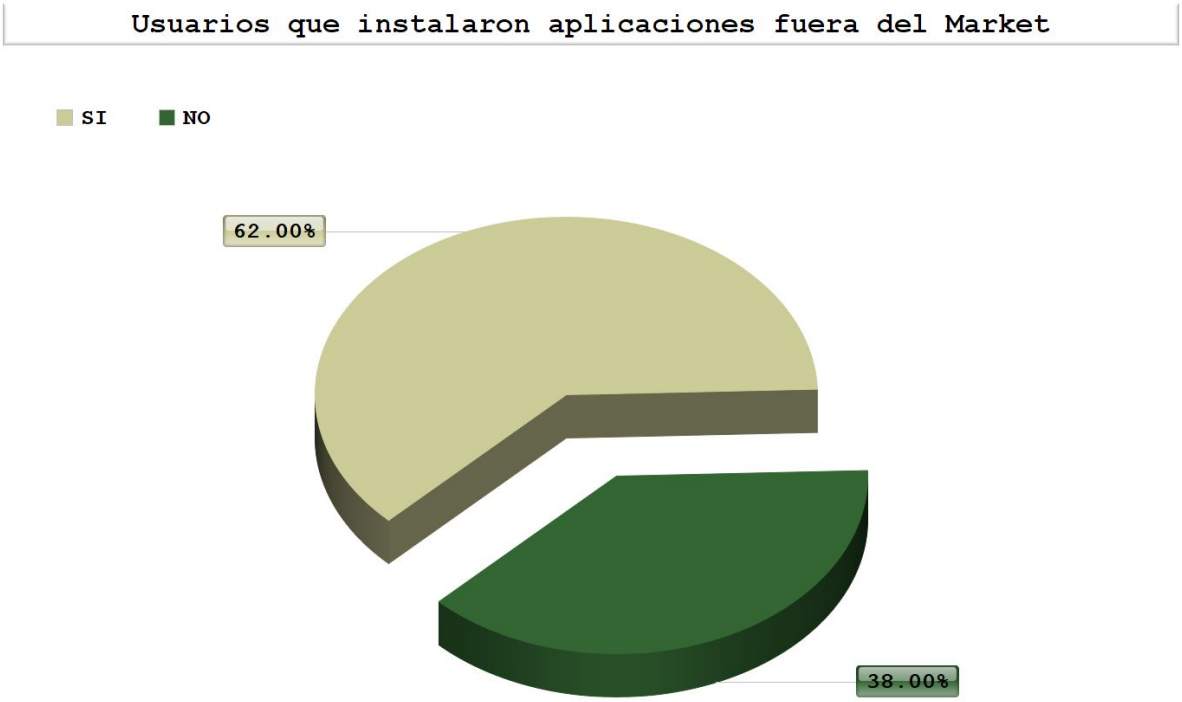
Otra respuesta que se puede destacar es que el 29% de los usuarios reconocieron o pensaron que habían instalado una aplicación maliciosa. Esto es muy común en los usuarios que por primera vez intentan acceder al market de aplicaciones de cada distribución y sin conocimiento pueden llegar a instalar una aplicación que no cumple su función, sino que intenta explotar una vulnerabilidad de la versión del sistema operativo. Los usuarios que por primera vez entran al market, no pueden diferenciar entre una aplicación fake (falsa) o una verdadera. Hoy en día en el market de google hay muchos indicios y parámetros que nos ayudan a diferenciar si una aplicación hace lo que dice en su descripción. Una de las primeras medidas que tomó google fue no repetir las imágenes de las aplicaciones, años anteriores era muy común ver aplicaciones con los mismos

nombres y la misma imagen por lo que el usuario podía entrar en una confusión e instalar una aplicación diseñada por una persona con objetivos maliciosos. Otra forma de diferenciar las aplicaciones es ver el autor o desarrollador de la aplicación, ver si es un proveedor conocido, ver la cantidad de aplicaciones que diseñó y ver la valorización que le dan los usuarios por un sistema de puntuación de estrellas. Una herramienta útil, donde no es necesario conocer aspectos técnicos, son los comentarios que dejan los usuarios que instalaron la aplicación, ahí se podrá visualizar opiniones y satisfacción de los mismos, esto dará un nivel de confianza más. Otra forma de ver si la aplicación hace lo que dice hacer, es ver los permisos necesarios que el usuario le debe dar a la aplicación para que funcione; esto ya entra un poco más en aspectos técnicos, pero no son difíciles de entender ya que el mismo market realiza una breve descripción de los permisos y para qué sirve cada uno.



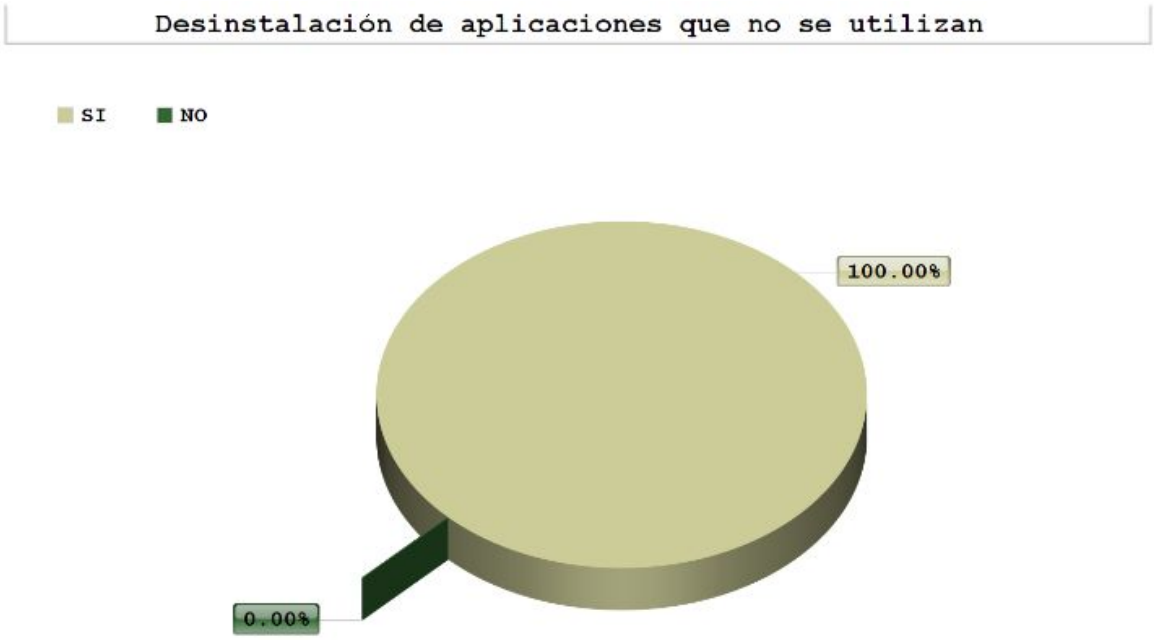
Entre adolescentes es muy común interiorizarse fácilmente en el mundo de las aplicaciones, generalmente las primeras aplicaciones que se instalan son juegos, por lo

que el market está infectado de aplicaciones fake en ese rubro ya que los atacantes buscan los objetivos masivos. Una vez que el usuario pasó la etapa de instalación compulsiva intenta indagar un poco más y quiere aplicaciones que no se encuentran en el market oficial e intentan buscar en otros repositorios de aplicaciones, cayendo en los markets no oficiales, muchos de ellos radicados en Rusia y China (un ejemplo es el market Anzhi[46], repositorio chino). Los usuarios buscan nuevas aplicaciones y descargan estas de markets no oficiales con los peligros que conlleva. Nuestra encuesta refleja que un 62% de los usuarios instalaron una aplicación fuera del market oficial. Esto aumentaría los peligros de instalación de una aplicación maliciosas y comprometería al smartphone y sus vulnerabilidades.

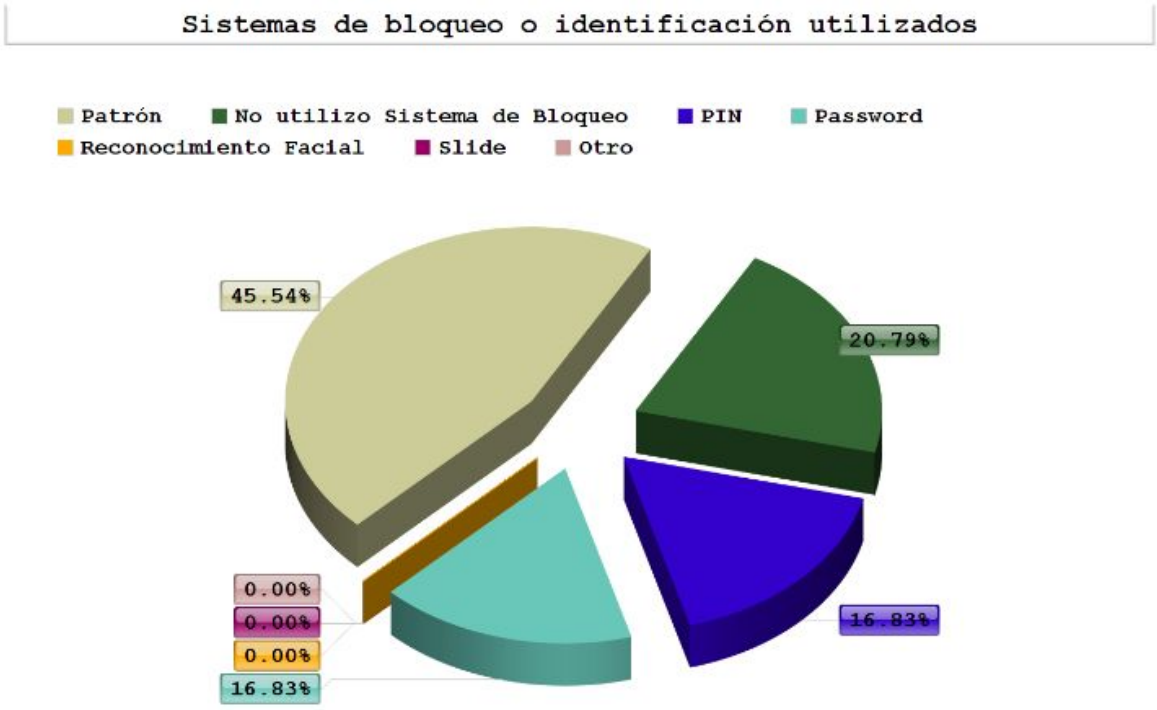


Una de las respuestas que nos sorprendió fue si los usuarios una vez que instalaban una aplicación y la dejaban de utilizar ellos mismos se encargaban de desinstalar. Se sabe que al cargar de aplicaciones un smartphone, y más si esa aplicación utiliza muchos recursos y necesita gran cantidad de privilegios, puede hacer bajar el rendimiento y durabilidad de la

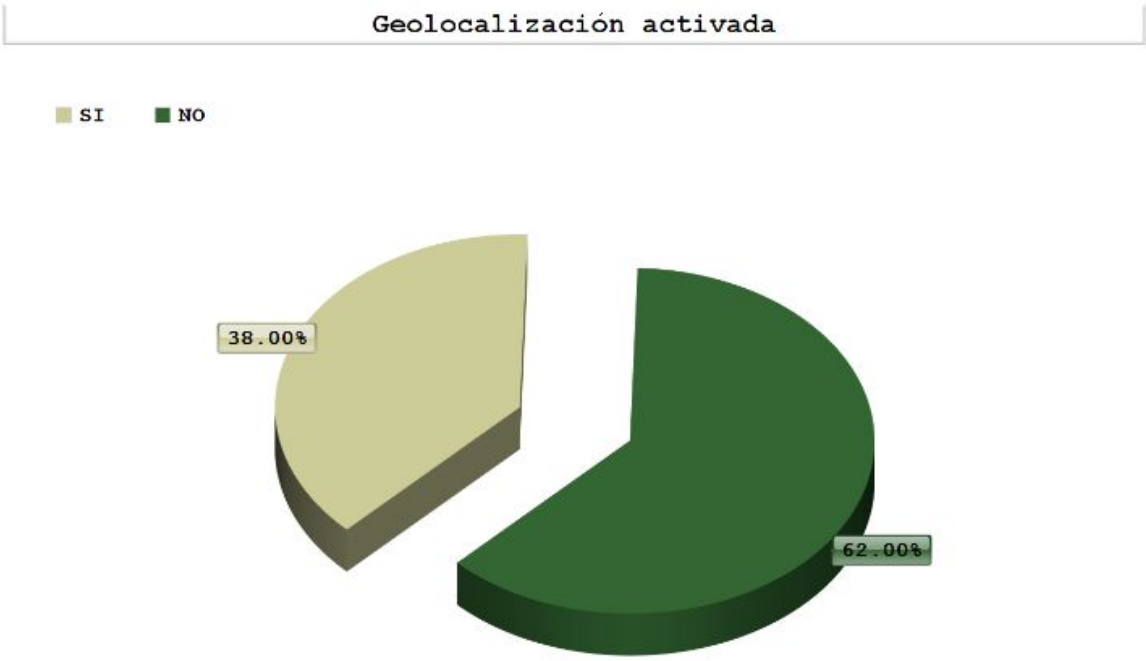
batería del dispositivo. El resultado dio que un 100% no desinstala aplicaciones que no utiliza, por lo que aplicaciones maliciosas pueden convivir en el dispositivo y realizar su trabajo para el cual fueron creadas.



Una de las formas de protección de la información que contiene nuestro smartphone, ya sea fotos, videos, contactos, cuentas de correos y redes sociales es el uso de sistemas de bloqueos que impedirían a una persona intrusa poder acceder al contenido del dispositivo. La encuesta reflejó que el sistema de bloqueo de pantalla más utilizado es el patrón con un 45%, ello se debe a que es fácil y rápido de utilizar, pero a su vez puede comprometer al teléfono ya que existieron casos que se puede adivinar el patrón a simple vista si no se limpia la pantalla apropiadamente. La encuesta también reflejó que un 20% no utiliza ningún sistema de bloqueo de pantalla dejando vulnerable el acceso de algún intruso por pérdida o robo del mismo. Después lo sigue el pin y la password como sistemas de protección más utilizados.



Una de las herramientas que nos provee los smartphone es el uso del sistema de geolocalización que nos permite interactuar con el ambiente, saber que transporte tomar, sus recorridos, conocer edificios, calles, obtener información de restaurant y saber nuestra ubicación en el mapa. Pero esta funcionalidad es un arma de doble filo ya que dependiendo del sistema operativo que utilicemos se guardará toda información de nuestra ubicación y recorridos realizados con fecha y hora. Esta información que, por ejemplo en android es vinculada a la cuenta de gmail, se utilizará para poder registrarte en el market oficial, si esa cuenta queda comprometida, cualquier persona que tenga acceso podrá ver nuestros contactos y recorridos habituales pudiendo diagramar alguna situación ilícita (secuestros a personas, secuestros virtuales, etc). También esta funcionalidad es muy utilizada en casos de menores, esto permitiría a los padres controlar a sus hijos, saber donde están y cuánto tiempo llevan a ahí.



Conclusiones

Esta encuesta fortalece la idea de seguir fomentando y divulgando las buenas prácticas en seguridad móvil en la sociedad. Hoy en dia los jovenes son el futuro y la nueva camada de usuarios que serán parte del cambio cultural y laboral en las organizaciones, llevando al BYOD no solo a ser un fenómeno temporal sino a instalarse definitivamente en el concepto laboral, por lo que es necesario que estén preparados para estos cambios y sepan afrontar las amenazas y problemáticas que aparezcan en su camino.

La encuesta también refleja el índice dado por IDC donde más del 80% de la población mundial utiliza el sistema operativo Android, este índice se comprobó en cada charla impartida, fortaleciendo los conceptos y dando un panorama más acertado de donde esta parada la sociedad y qué tecnologías utiliza.

6.2. Software de gestión organizacional de MDM - Soti Mobicontrol

Dentro del marco del presente trabajo, se decidió realizar un análisis de una herramienta de manejo de dispositivos móviles (MDM). La herramienta seleccionada fue SOTI Mobicontrol[47] y a continuación se presenta el estudio realizado.

SOTI Mobicontrol es una herramienta comercial para el manejo de dispositivos organizacionales (Enterprise Mobility Management - EMM). Entre las funcionalidades que provee se encuentra el manejo de aplicaciones, contenido, información, servicios de localización, filtros web, filtros de llamada, control de malware y hasta control del plan de tarifas de los dispositivos que se registren en la herramienta. Actualmente posee soporte para dispositivos Android, IPhone, Windows Phone permitiendo definir un repositorio de aplicaciones propio para que los dispositivos puedan seleccionar las aplicaciones a instalar de un listado brindado por el administrador del sistema y luego descargarlas ya sea desde el store de aplicaciones o desde el servidor donde Mobicontrol esté corriendo, permitiendo tener un mayor control de las aplicaciones que los dispositivos de la organización pueden o deben tener instaladas.
La herramienta funciona sobre la arquitectura Windows, tanto en versiones Desktop (Windows 7 en adelante, versiones de 64 bits) como Server. Para el almacenamiento de la información utiliza una base de datos de tipo SQLServer (2008 en adelante) que puede instalarse por separado si se prefiere. También se presenta la posibilidad de contratar un servicio de Cloud que Soti ofrece, pero esta versión quedó fuera del alcance de este análisis.

Para este estudio de la herramienta se utilizó una licencia por 30 días que un contacto de Soti nos administró para poder conocer la herramienta. La infraestructura utilizada para el servidor de Mobicontrol fue: una máquina virtual en VirtualBox con Windows 7 y SQLServer 2008 R2 instalado de manera independiente ya que el instalador de

SQLServer que provee la herramienta presentaba problemas. Las pruebas se realizaron principalmente para la tecnología Android. Los dispositivos utilizados para las pruebas fueron:

1. Movil Sony Xperia U con Android Ice Cream Sandwich 4.0.4
2. Movil Motorola MotoG con Android KitKat 4.4

Una vez instalada, la herramienta provee un panel de control desde donde se pueden administrar aspectos relacionados a certificados para la conexión https, hostname del servidor, estado de los servicios, etc.

El acceso al sistema de administración de dispositivos se realiza mediante un WebBrowser(se utilizo Mozilla Firefox 42.0), donde se solicita usuario y contraseña para autenticarse (Fig. 1) y una vez autenticado se ingresa a la pantalla principal donde se muestran los dispositivos suscriptos (Fig. 2). Los mismos se encuentran divididos en grupos de dispositivos para tener una mejor organización y un agrupamiento en base a algún criterio.

Figura 1. Pantalla de Login.

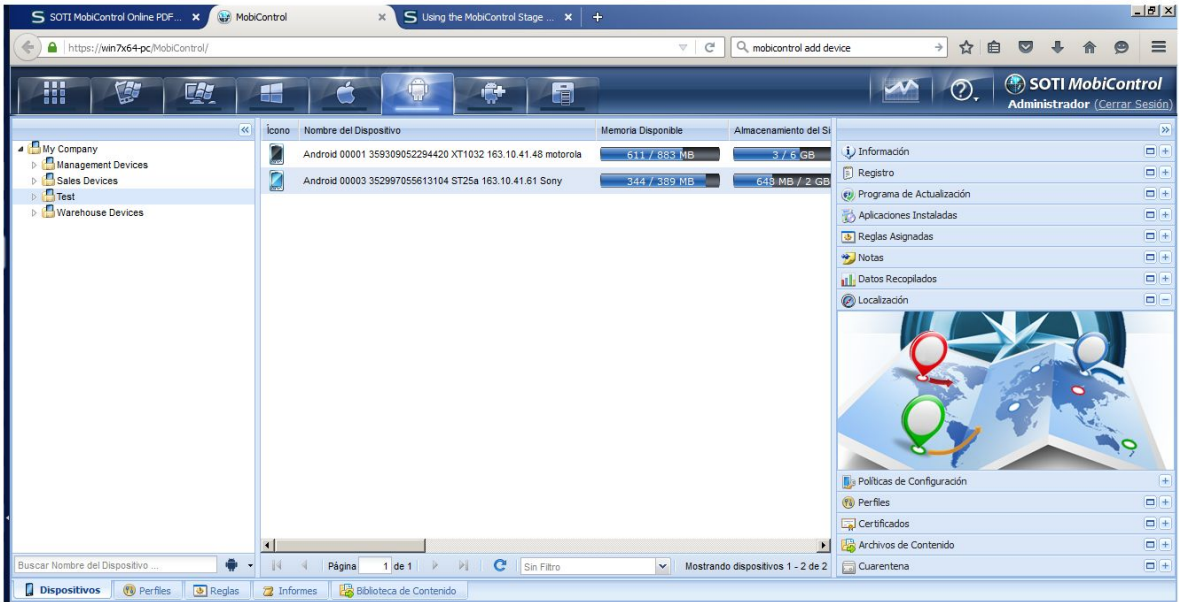


Figura 2. Pantalla Principal de Dispositivos. El dispositivo con pantalla oscura no está registrado actualmente.

La herramienta funciona mediante la instalación de un Agente que se encuentra en los repositorios de aplicaciones de las distintas arquitecturas (Google Play - Android 2.2 en adelante, Apple Store, etc). Cuando un dispositivo instala el Agente Mobicontrol, este solicita la dirección del servidor al que debe conectarse para poder realizar las configuraciones correspondientes y suscribir el dispositivo.

En el menú de dispositivos, presionando botón derecho del mouse sobre un dispositivo, se despliega un menú de opciones para aplicar directamente sobre el dispositivo de manera individual que permite realizar distintas acciones (Fig. 3) entre las que se incluyen: bloquear el dispositivo, borrar todos los datos, localizarlo (Fig. 4 y 5), enviar un mensaje (Fig. 6,7 y 8), etc.

Figura 3. Opciones de Dispositivo, Accion.

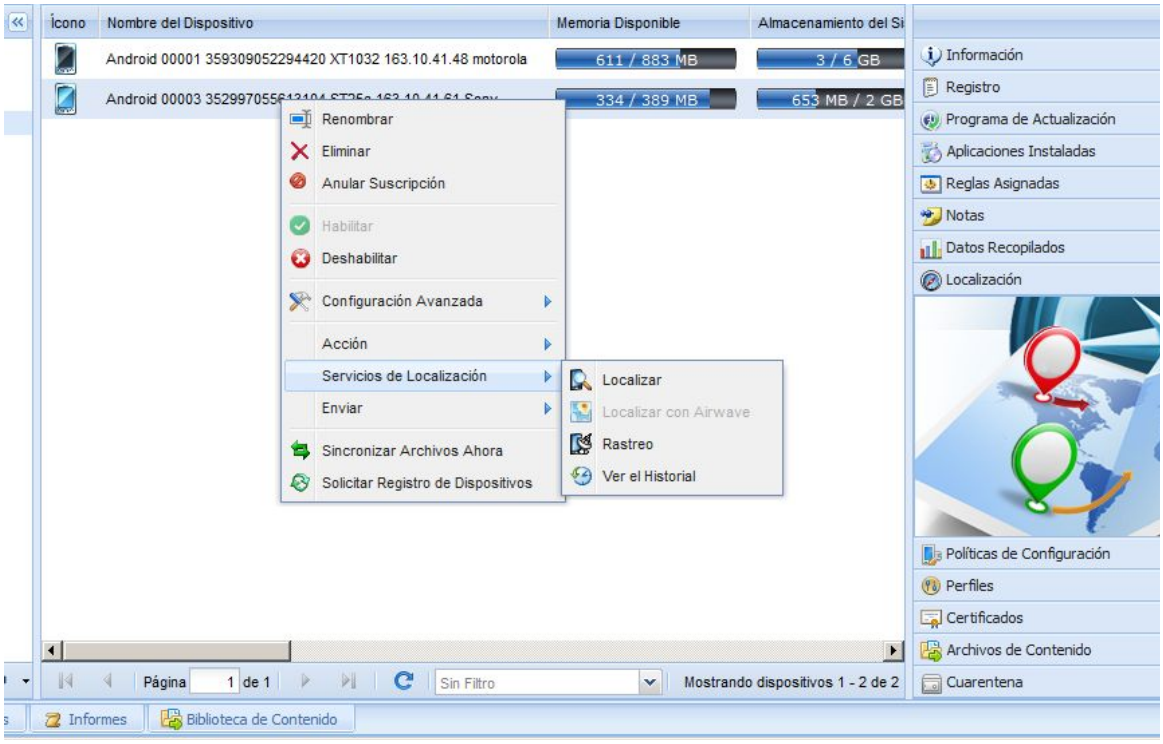


Figura 4. Servicios de Localización.

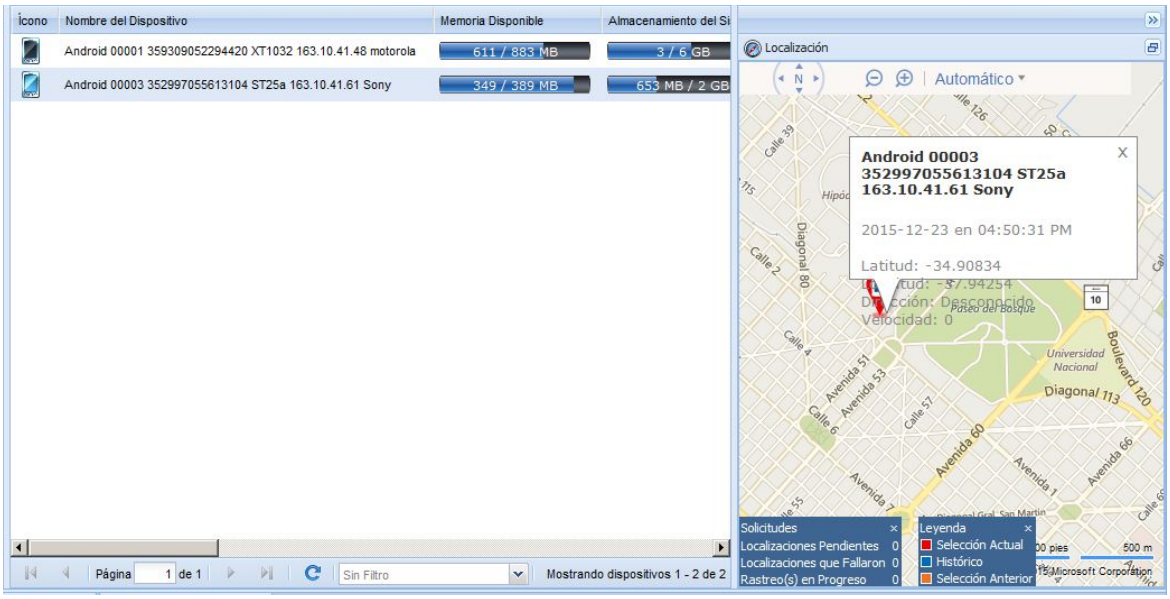


Figura 5. Servicios de Localización, dispositivo Localizado.

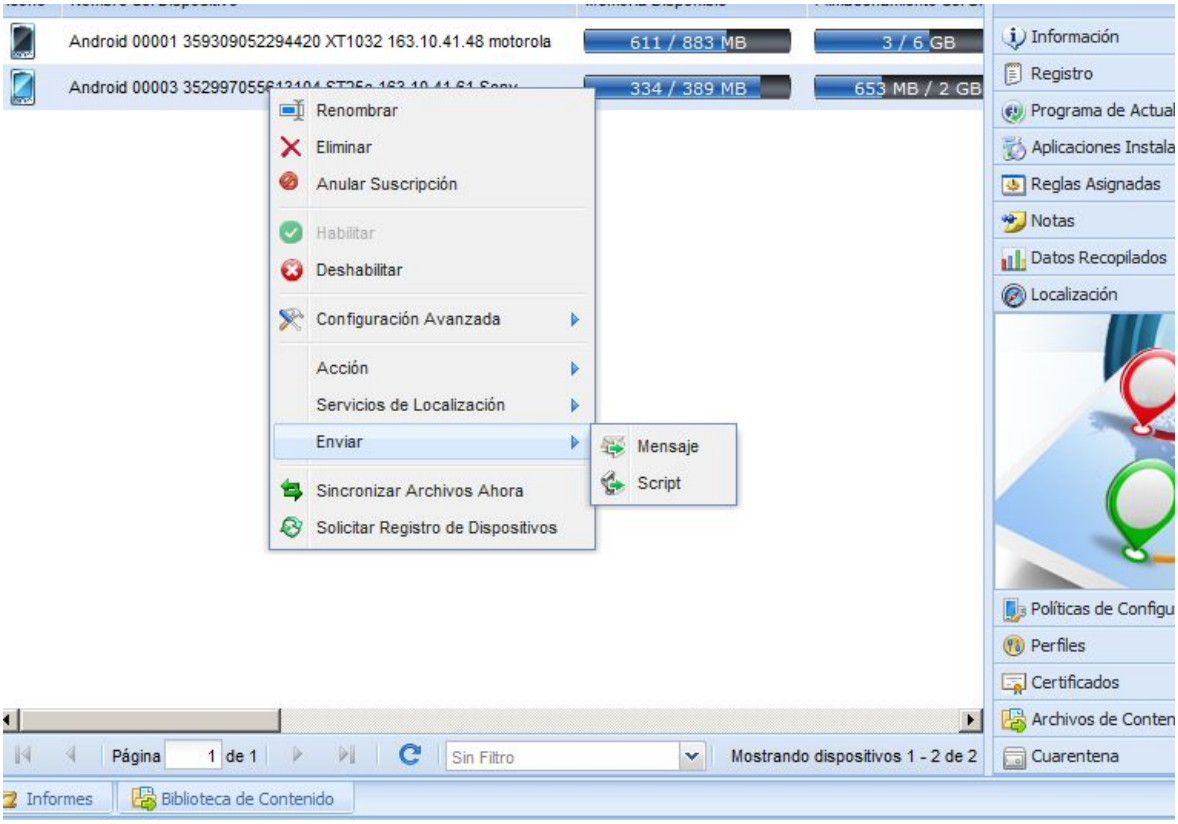


Figura 6. Envío de Mensaje.

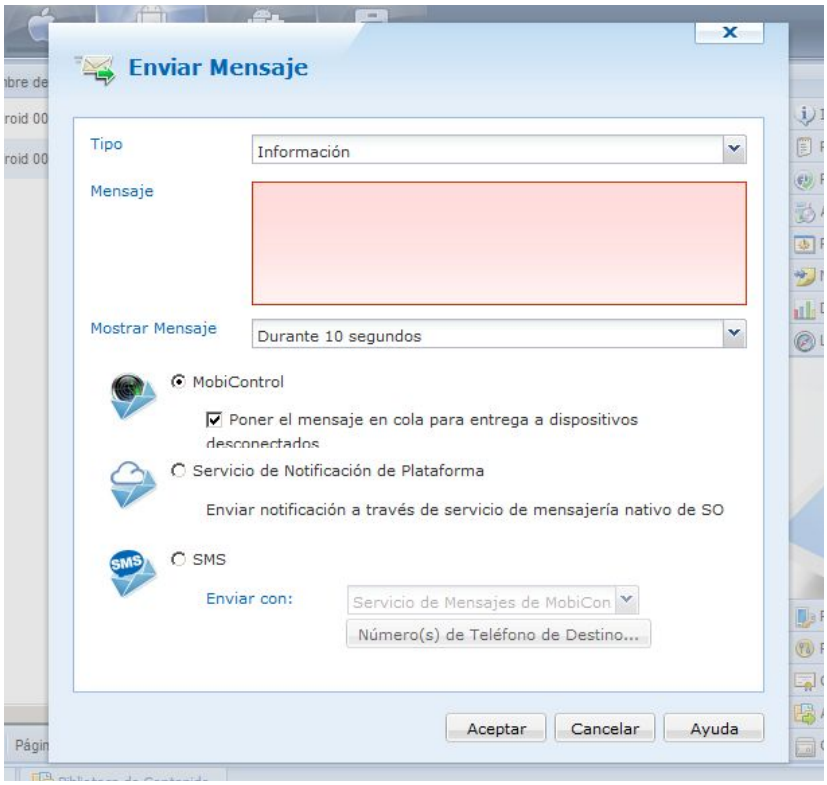


Figura 7. Envío de Mensaje, creación del mensaje

Figura 8. Recepción en el Móvil.

NOTA: Desde aquí nos centraremos exclusivamente en el comportamiento bajo la Arquitectura Android.

El Agente Mobicontrol se suscribe al servidor (Fig. 9) y mediante la utilización de la api Device Manager provista por Android, instala un manejador de dispositivo en el móvil encargado de realizar las tareas que desde el servidor se indican mediante los perfiles a los que los dispositivos sean asignados.

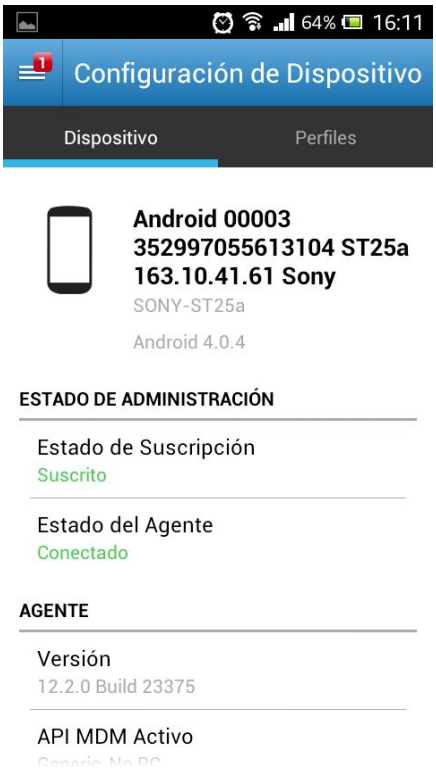


Figura 9. Imagen del Agente en el Móvil.

Los Perfiles deben ser creados para luego poder asignarlos (Fig. 10), la asignación se realiza sobre los grupos de dispositivos y no sobre los dispositivos individuales. Cuando se asocia un dispositivo entra en juego el/los perfiles que tiene asignado según el grupo al que el dispositivo se adhiera (Fig. 11).

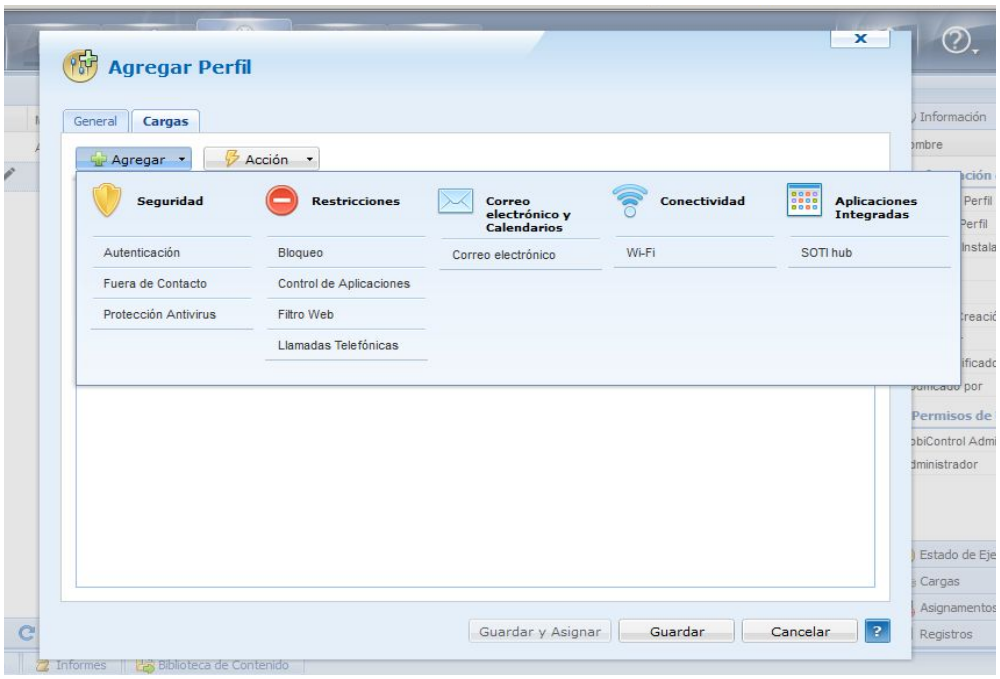


Figura 10. Pantalla de Creación de Perfiles.

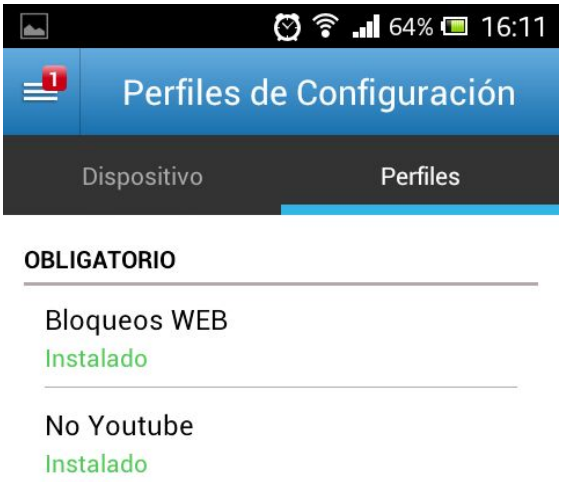


Figura 11. Perfiles descargados en el Móvil.

Entre los distintos tipos de perfiles que pueden ser creados, a modo de ejemplo, se presentan imágenes de perfiles para control antivirus (Fig. 12), control de llamadas (Fig. 13 y Fig. 14) y fuera de contacto (Fig. 15 y Fig. 16).

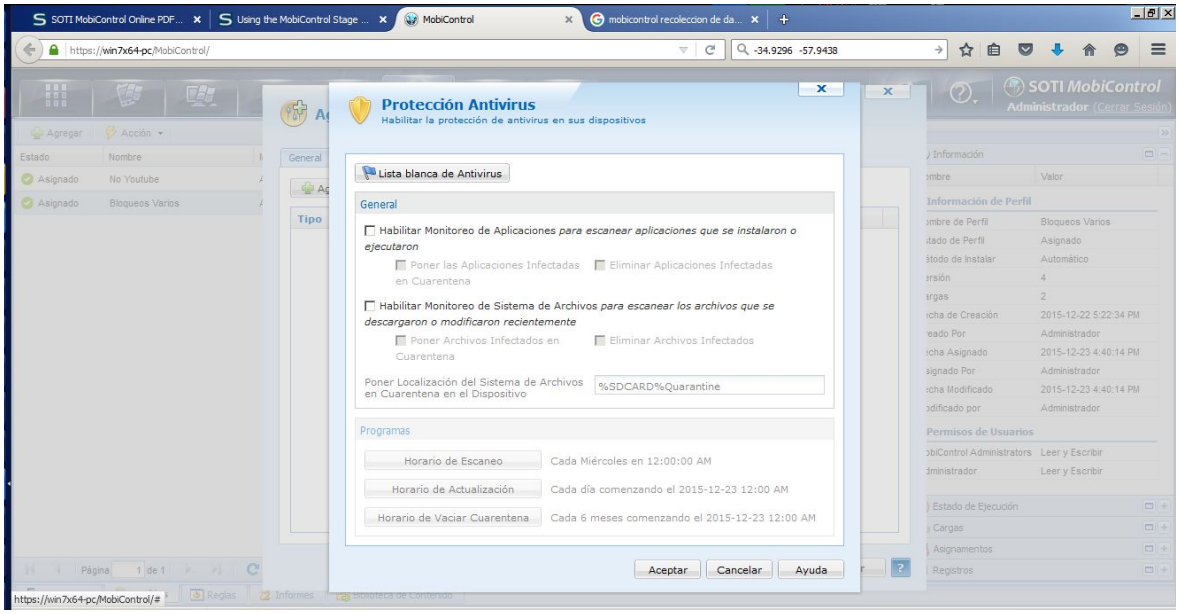


Figura 12. Definición del comportamiento del Antivirus que provee la Aplicación.

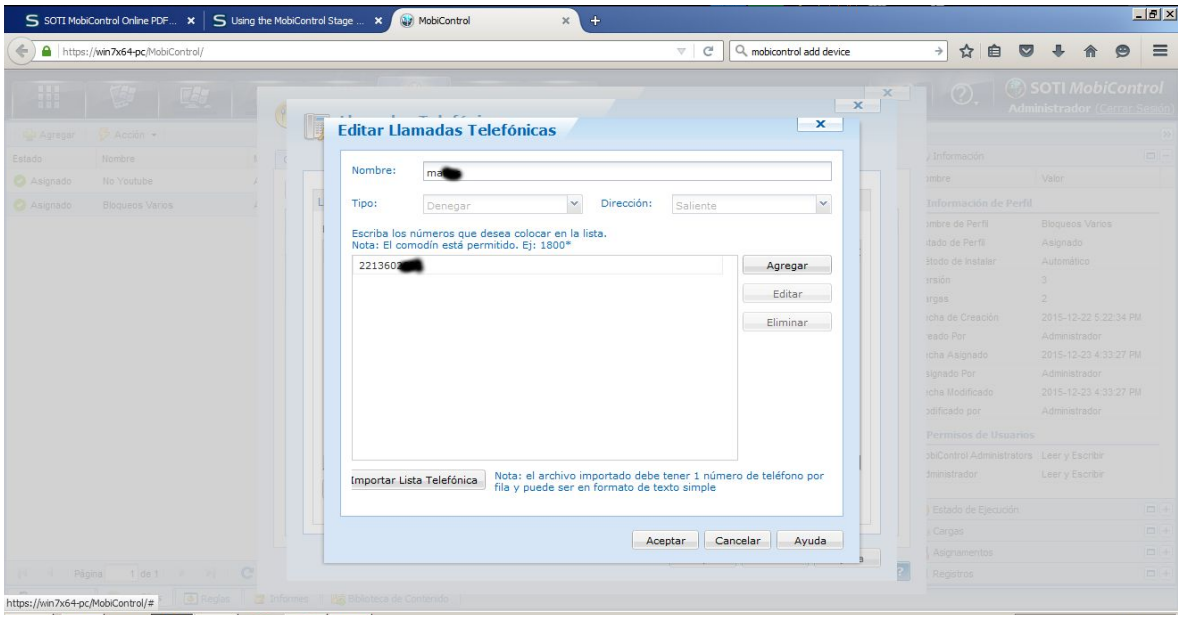


Figura 13. Definición de filtrado de números para llamadas.

Figura 14. Llamada Saliente Bloqueada en Móvil.

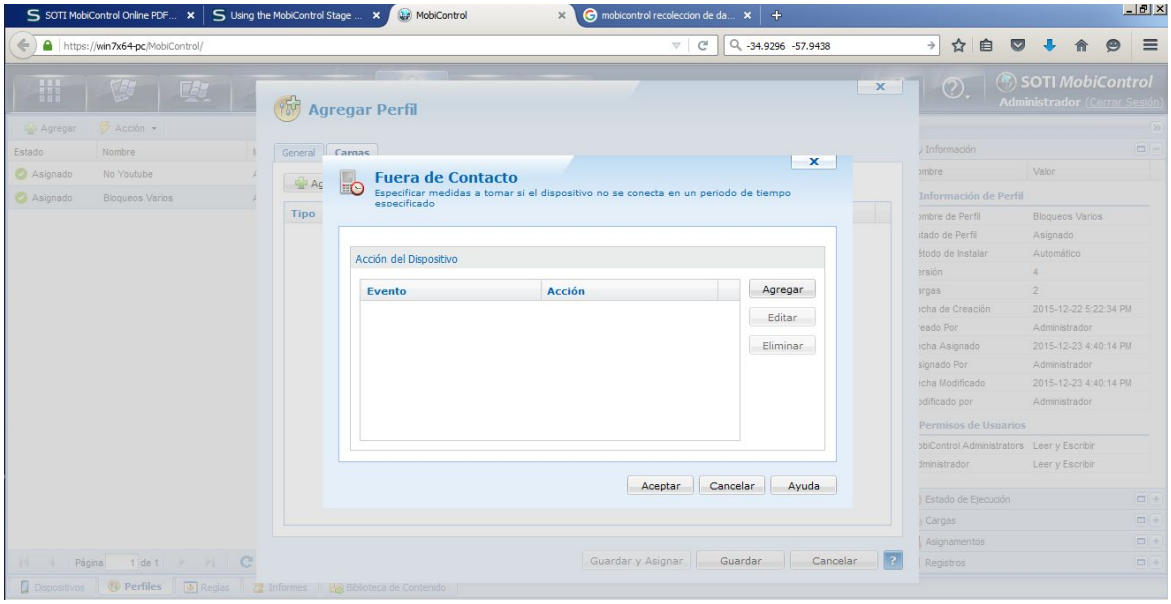


FIgura 15. Creación de Perfil por Larga desconexión de un Dispositivo.

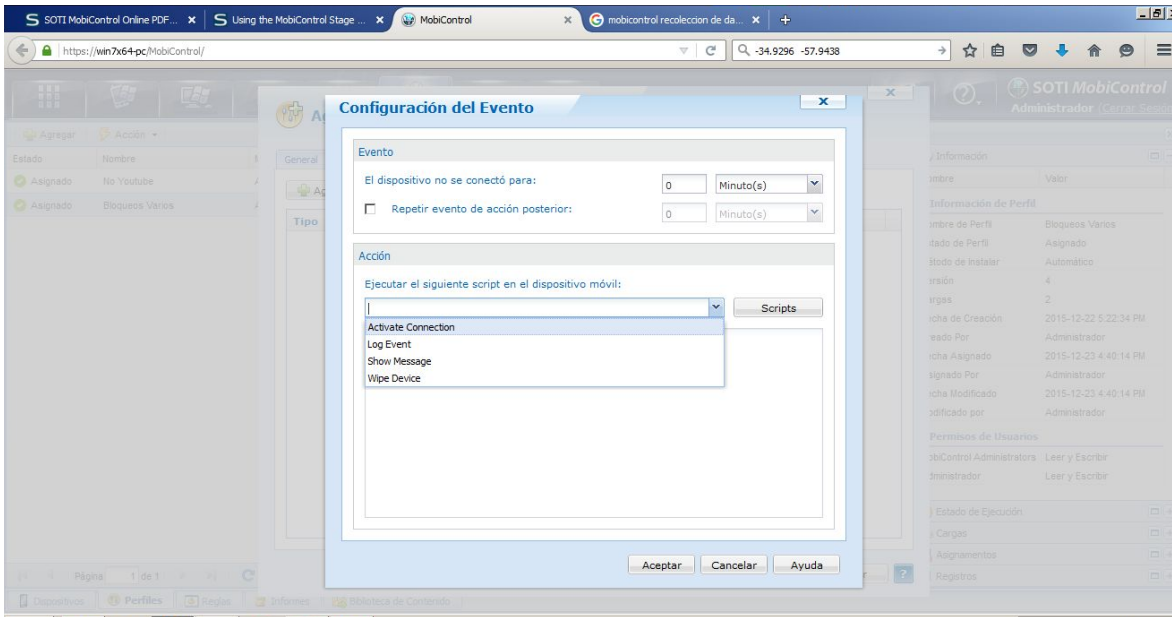


Figura 16. Creación de Perfil por Larga desconexión de un Dispositivo, configuración del evento a generar.

Sumado a los perfiles asignables, se pueden definir conjuntos de reglas para ser aplicadas a los dispositivos para definirles distintos tipos de directivas (mediante reglas se definen qué perfiles se asignan a qué grupo). Entre las reglas que pueden aplicarse se presentan a modo de ejemplos reglas referentes a: aplicaciones a tener instaladas, recopilación de datos (ubicación del dispositivo, llamadas, direcciones IP, etc), sincronización de archivos, alertas frente a eventos.

1) Regla sobre Aplicaciones: En el servidor se presenta la funcionalidad de tener un catálogo de aplicaciones (Fig. 17) que la herramienta luego presenta al Móvil. Esto puede ser utilizado para tener definido bajo la política organizacional que aplicaciones están permitidas de una manera centralizada y clara. El Agente presenta en el móvil una pantalla con las aplicaciones que se agregan al catálogo del servidor de Mobicontrol (Fig. 19). En el catálogo puede definirse si las aplicaciones son de carácter opcional u obligatorio, si deben descargarse desde el App store (Fig. 18) o del servidor en caso de ser aplicaciones propias de la organización.

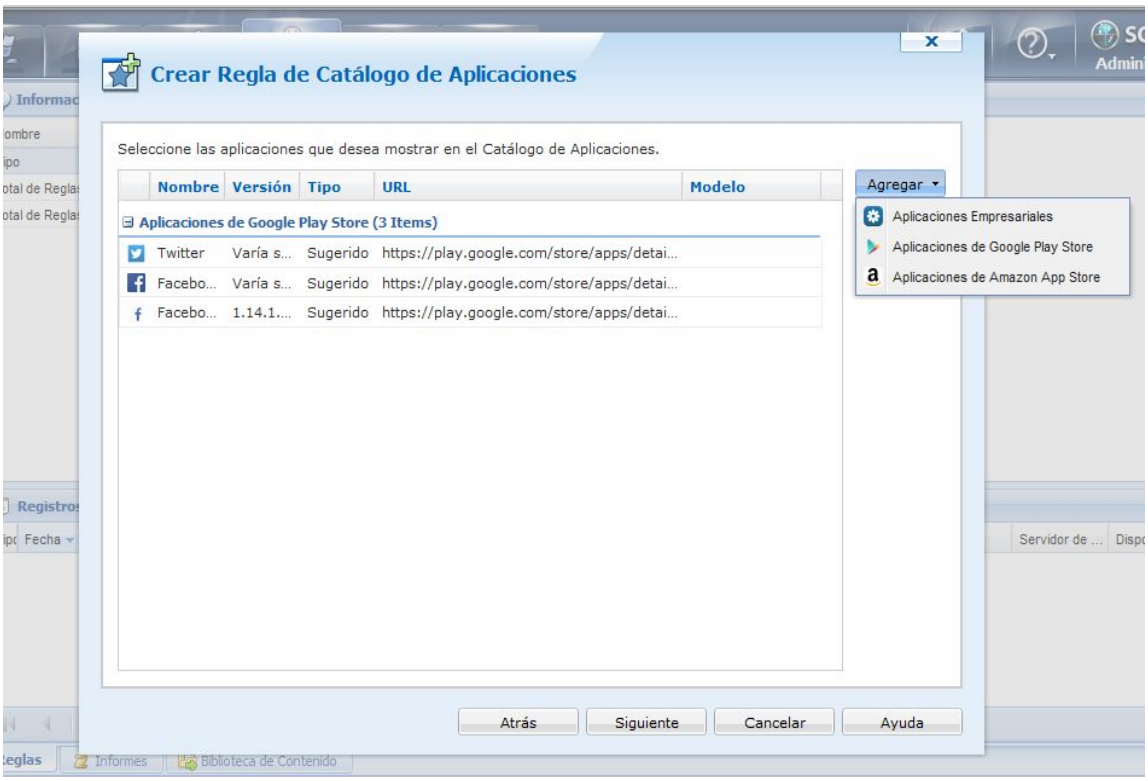


Figura 17. Creación del Catálogo de Apps.

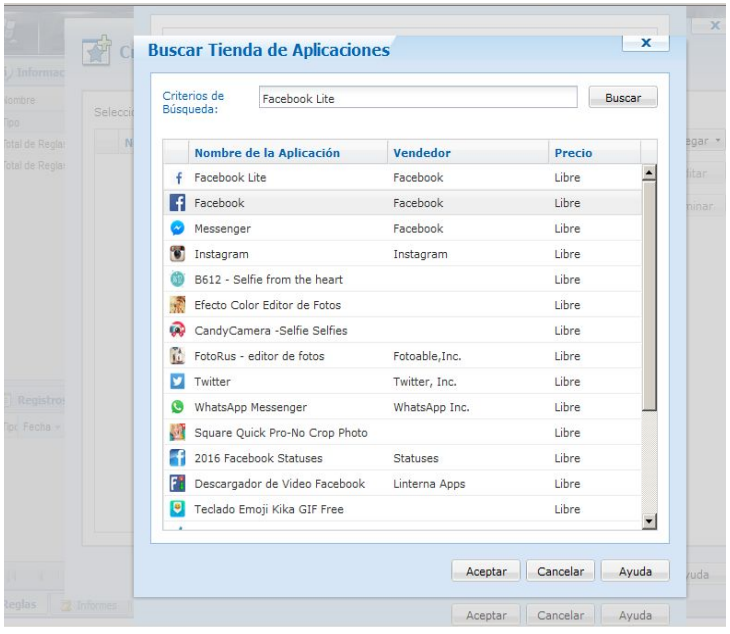


Figura 18. Seleccionando Apps del Play Store.

Figura 19. Catálogo de Apps en el móvil.

2) Regla de Recopilación de datos: Se permiten definir reglas para recolectar información de los dispositivos suscriptos a la herramienta (Fig. 20). Los tipos de información a recolectar vienen predefinidos, solo se puede elegir de un listado que la herramienta presenta. El intervalo de tiempo para cada recolección también debe ser configurado, aumentando la carga en el móvil a medida que el intervalo configurado es más corto. Una vez configurada la regla, el servidor va almacenando la información para que pueda ser consultada (Fig. 21,22,23).

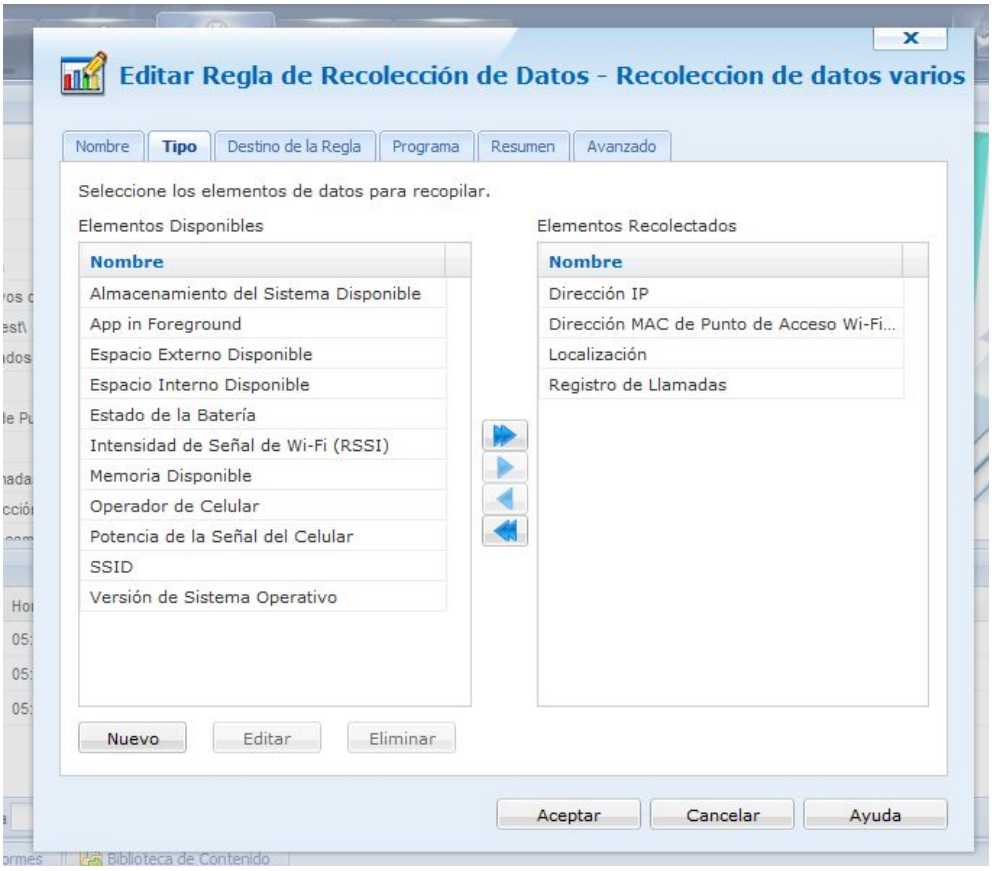


Figura 20. Definición de una regla para recolección de datos.

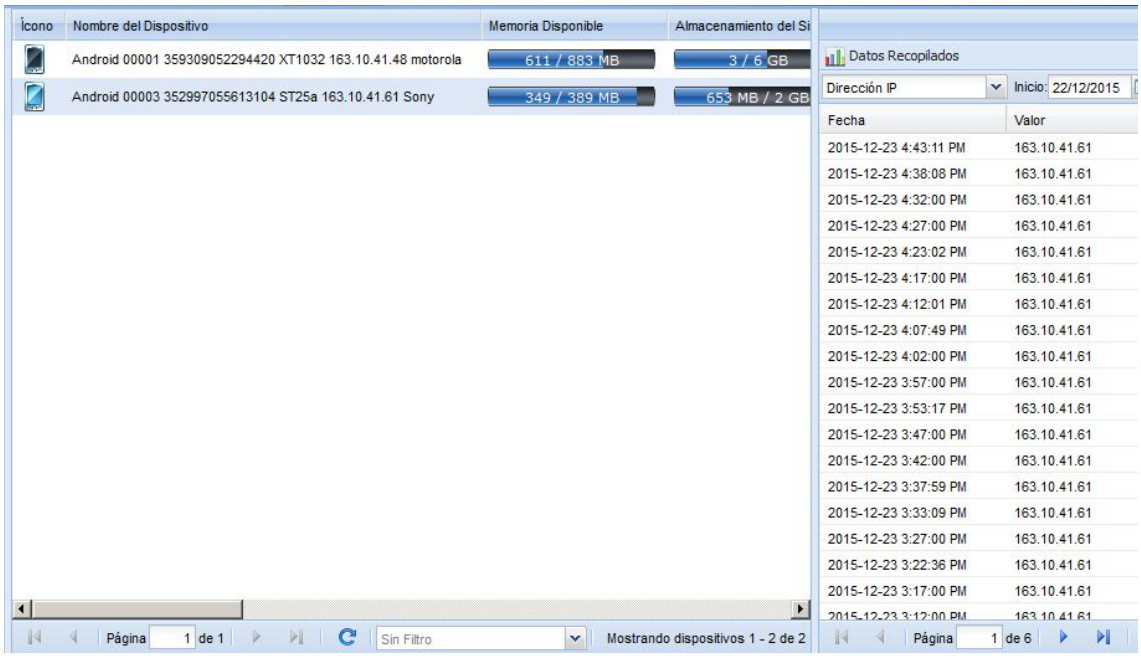


Figura 21. Datos Recopilados, direcciones IP.

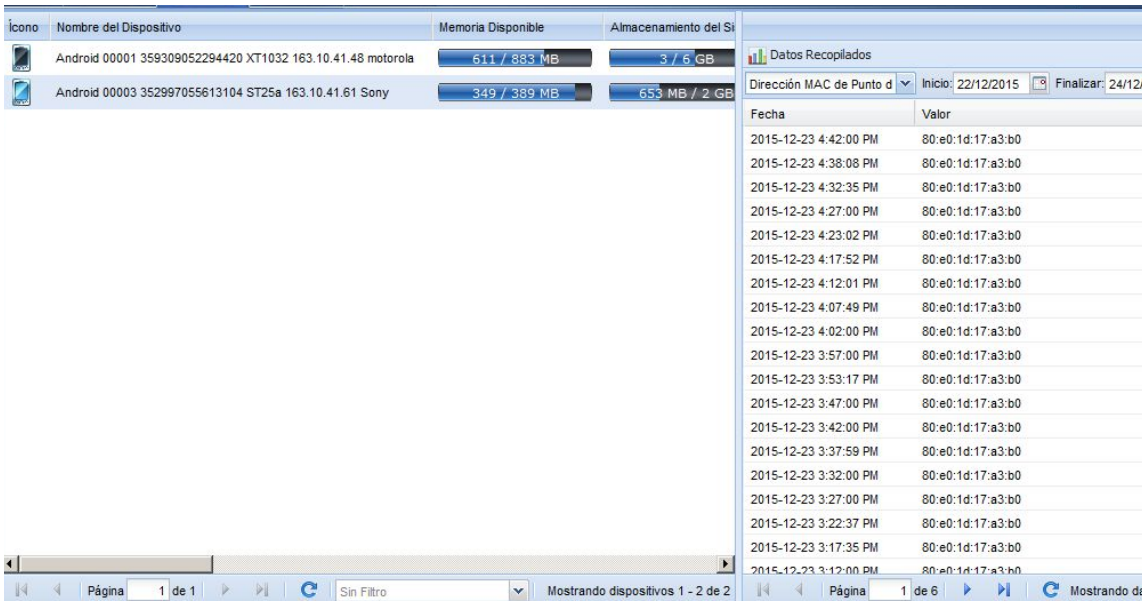


Figura 22. Datos Recopilados, dirección mac del AP utilizado para conexión Wifi.

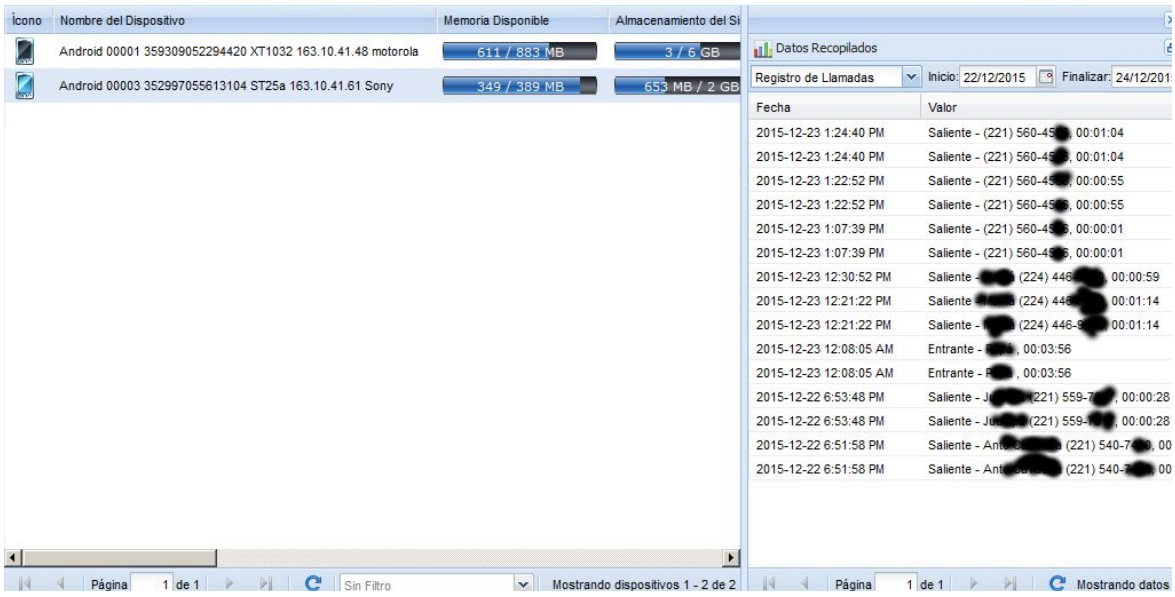


Figura 23. Datos Recopilados, historial de llamadas

3) Regla para Sincronización de archivos: Se brinda la funcionalidad para sincronizar archivos entre los dispositivos y el servidor, cargando archivos desde el servidor a los clientes o descargando desde el cliente al servidor(Fig. 24).

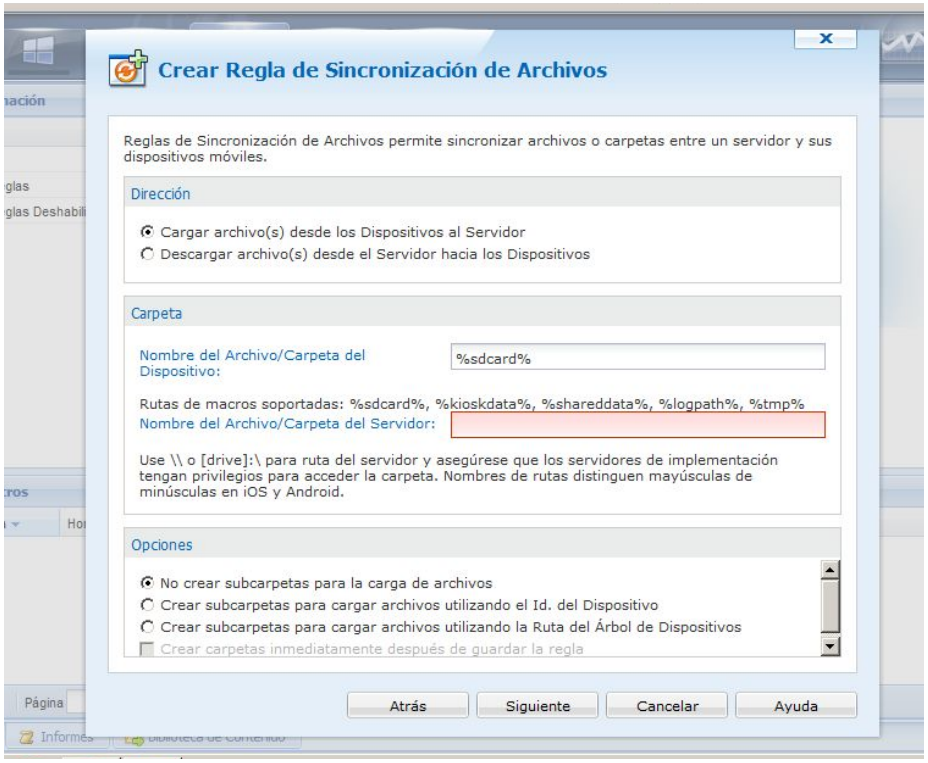


Figura 24. Definición de regla para sincronización de archivos.

4) Regla para Alertas frente a eventos: Se pueden crear reglas que funcionen para generar alertas en el servidor frente a eventos predefinidos en el sistema que ocurran en el móvil como una conexión wifi establecida, un malware detectado, un archivo sincronizado, etc (Fig. 25).

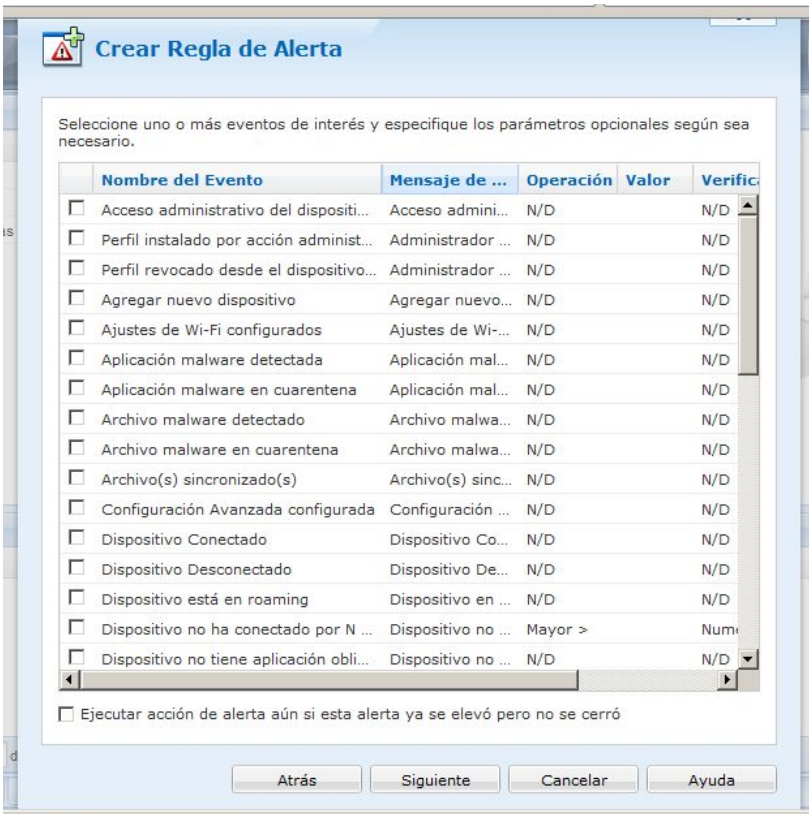


Figura 25. Creación Regla de Alerta, selección de evento.

Conclusiones

Soti Mobicontrol resulta una herramienta de MDM muy completa que abarca muchos de los conceptos necesarios para la administración de dispositivos organizacionales de manera centralizada. Una contra que presenta es que solo existe una versión para sistemas operativos Windows y que no pertenece a la familia de software Open Source, decompilando el .apk de la aplicación agente el código se encuentra ofuscado para quedar ilegible.

Hoy en el mercado se pueden encontrar múltiples herramientas de MDM que sean pagas y gratuitas, pero lo importante de estas herramientas es que se adecuen a las necesidades de cada organización. Hay que tener en cuenta en el momento de elección de una de estas herramientas las características de los dispositivos de las personas que son parte de la organización, de nada sirve si la población de dispositivos es obsoleta, entiéndase por obsoletas dispositivos sin sistemas operativos actuales o versiones de SO muy antiguas, debería quedar claro en una política que dispositivos se podrán utilizar en la organización.
Para definir una política de mitigación es una primordial la elección de una herramienta MDM, es uno de los 3 pilares:

- Definición de política de uso y gestión.
- Uso de aplicaciones Mobile Device Management (MDM).
- Concientización del usuario

6.3. Establecimiento de un marco de seguridad aplicable a una Organización - Ejemplo de política BYOD

Una política BYOD es específica de cada organización, pero establecer un marco general para ejemplificar que podría contener y los puntos que deben considerarse, puede ayudar a dar los primeros pasos a la hora de definir la propia. Por este motivo, se propone la presente a modo de facilitar la creación posterior en organizaciones.

Introducción

La presente Política pretende asegurar la confidencialidad, disponibilidad e integridad de la información organizacional que se acceda desde dispositivos móviles personales. Los miembros de la organización deben aceptar las condiciones establecidas para poder hacer uso de sus dispositivos dentro de la organización.

Dispositivos: ¿Que tipos de dispositivos se consideran?

Dispositivos: Podemos suponer que entre los dispositivos existentes a proteger hay:

1. Smartphones:
    a. Diferentes modelos de Iphone
    b. Android (diferentes Versiones del SO)
2. Tablets:
    a. Android
    b. Apple Ipad
3. Notebooks (sin GPS ni 3G):
    a. Windows
    b. Linux

Establecimiento de la Criticidad:

A la hora de decidir y aplicar medidas de seguridad, es necesario saber el grado de importancia que un dispositivo representa para la organización. Esto puede estimarse en

base a la criticidad de la información que dicho dispositivo accede y/o almacena y además teniendo en cuenta el grado de exposición que el mismo tiene.

En base a esto, es posible armar una tabla que permita identificar fácilmente cuáles son los dispositivos más críticos para la organización.

Por ejemplo, considerando que:

1. Respecto a la criticidad de la información, podrían establecerse 3 niveles:
    a. Baja: El dispositivo es un soporte de trabajo en el cual no se guarda/accede a información sensible
    b. Media: El dispositivo es para uso personal, con información sensible, pero en el contexto de la información personal del que lo usa. Dependiendo de la persona, podría considerarse la criticidad MEDIA o ALTA
    c. Alta: El dispositivo se usa para realizar una tarea propia del área por lo que aloja información sensible.
2. Respecto al grado de exposición, también podrían definirse 3 niveles:
    a. Bajo: el dispositivo siempre se usa en las instalaciones de la organización
    b. Medio: el dispositivo se usa ocasionalmente fuera de la organización
    c. Alto: el dispositivo se usa habitualmente dentro y fuera de la organización

Se podría establecer la siguiente matriz de criticidad:

Dispositivo	Criticidad de la información que transporta	Grado de exposicion	Comentarios
Dispositivo 1	ALTA	ALTA	La usa el grupo X para las salidas Y
Dispositivo 2	ALTA	BAJO	Uso en la oficina X
Dispositivo 3	MEDIO	MEDIO	La usa la persona X que tiene funciones administrativas para realizar sus tareas dentro de la organización y ocasionalmente se lo lleva a su casa para armar alguna presentación.

Orden de aplicación de las recomendaciones

Sería adecuado aplicar las recomendaciones de seguridad en función del nivel de criticidad de los dispositivos, utilizando un orden de aplicación:

Orden de Aplicación	Criticidad de la información que transporta	Grado de exposicion
1	ALTA	ALTA
2	MEDIO	ALTA
3	ALTA	MEDIO
4	MEDIO	MEDIO

Este orden de aplicación determina a qué dispositivos deberá darse mayor relevancia a la hora de aplicar las recomendaciones.

Recomendaciones Generales para Notebooks

1. Utilizar contraseñas fuertes para el acceso.
2. Exigir el uso de aplicaciones antivirus/antimalware.
3. Tener copias de seguridad de la información que deba resguardarse.
4. Encriptar el disco, la partición o el área de trabajo de modo que no se pueda comprometer la confidencialidad de la información almacenada bajo ninguna circunstancia.
5. Instalar un medio de borrado remoto de la información y de tracking del dispositivo.

Recomendaciones Generales para Smartphones y Tablets

1. Configurar un código de desbloqueo robusto con opción de auto-borrado luego de una serie de intentos fallidos.
2. En caso de que no esté provisto por la plataforma, instalar un medio de borrado remoto de la información y de tracking del dispositivo.

3. Para dispositivos Android, no permitir la instalación de aplicaciones de fuentes externas al Google Play Store.
4. Exigir el uso de aplicaciones antivirus/antimalware.
5. Para dispositivos que pertenezcan al orden de aplicación 1 o 2, permitir realizar un análisis del dispositivo por parte del departamento de TI/Seguridad.
6. Realizar el cifrado de la memoria interna y externa
    a. En caso de no poderse cifrar la memoria interna o externa, este dispositivo no debería ser usado para almacenar información con CRITICIDAD MEDIA o ALTA.
7. No permitir realizar ningún jailbreak o rooteo o equivalente sobre dispositivos móviles usados para almacenar información con CRITICIDAD MEDIA o ALTA.
8. Mantener versiones actualizadas del SO del dispositivo y de las herramientas que contenga
    a. En caso de no poderse actualizar a versiones superiores este dispositivo no debería ser usado para almacenar información con CRITICIDAD MEDIA o ALTA.
9. Los dispositivos utilizados para realizar conexión remota deben contar con las aprobaciones requeridas previa auditación del dispositivo por el departamento de TI/Seguridad y se deben acatar las condiciones de uso establecidas para dichas conexiones.

Recomendaciones a llevar a cabo ante la pérdida o robo

En caso de pérdida de un dispositivo móvil utilizado dentro de la organización, se recomienda que el usuario del mismo lleve a cabo el siguiente procedimiento a fin de minimizar los riesgos de seguridad:

1. Dar aviso a la organización del hecho (coordinador).
2. Realizar un borrado remoto de la información del dispositivo.
3. Cambiar las contraseñas de acceso tanto a los servicios de la organización como de las cuentas personales que se usaban desde el dispositivo, como ser:
    a. Contraseñas de correo electrónico:

i. Organizacionales → aviso a departamento de TI/Seguridad
ii. Personales

b. Contraseñas de mensajería instantánea:
   i. Organizacionales → aviso a departamento de TI/Seguridad
   ii. Personales
c. Contraseñas de acceso a las redes a las que se conectaban con el dispositivo en forma automática:
   i. VPNs organizacionales → aviso a departamento de TI/Seguridad
   ii. WiFi organizacionales, En este caso dar aviso a departamento de TI/Seguridad para que se evalúe puntualmente el caso.
   iii. (Opcional) WiFi personales
d. Contraseñas de administración general:
   i. Usuario Gmail (Dispositivos Android)
   ii. Usuario Itunes (Dispositivos IOS)

4. En caso de usar certificados digitales PKI o PGP, revocarlos.

Conclusiones

Tener una política coherente y segura tiene que ser el primer paso para implementar BYOD. Una política BYOD tiene que contribuir a facilitar la continuidad del negocio, mejorar la colaboración, simplificar el teletrabajo y mejorar la satisfacción de los empleados.

Hay que asegurarse de que se estén cumpliendo las políticas de la organización. No tiene mucho sentido ponerse a crear una estrategia, planear y desplegarla para después no utilizarla.

Los usuarios deben conocer que pretenden las políticas BYOD y de seguridad establecidas, los usos aceptados, por qué es importante el cumplimiento de las políticas y qué herramientas va a utilizar el área de TI para implementarlas, por lo que la capacitación y la divulgación de estas políticas es fundamental para su correcta ejecución.

6.4. Prueba de Concepto - Explicación del “POC” Realizado

Dentro del marco práctico de la tesina, se propuso crear una prueba de concepto que permita ejemplificar cómo una aplicación maliciosa puede hacerse de información que podría poner en riesgo a un usuario. El POC resultante es una aplicación para la plataforma Android que hace uso del GPS del dispositivo para servir como guía dentro del campus universitario de la UNLP, al mismo tiempo que de forma “silenciosa” envía la información de geolocalización del usuario a un servidor donde es almacenada.
La finalidad del POC reside en demostrar cómo se explota la confianza del usuario al hacerle creer que la aplicación se trata de algo que resulta útil y que presenta una funcionalidad llamativa, pero que en realidad realiza, sin informar al usuario, una tarea de espionaje enviando la información de geolocalización a un servidor remoto.

La intención a la hora de desarrollar la POC fue la de utilizar la menor cantidad de permisos extras que los que cualquier aplicación que utiliza el geoposicionamiento necesita, con el fin de hacerla pasar desapercibida también desde el enfoque de los permisos. Una aplicación cualquiera que utiliza el GPS y muestra mapas al usuario (en este caso utilizando la librería osmdroid que es libre) necesita mínimamente los siguientes permisos:

```
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

Con estos permisos, la aplicación ya puede utilizar el GPS, utilizar la conexión de RED y acceder a la Memoria SD. El POC utiliza de manera adicional algunos permisos para obtener información acerca del dispositivo con la finalidad de demostrar cómo podría extraerse información del usuario de manera oculta, en este caso las cuentas de usuario

configuradas en el dispositivo, y para obtener el número de IMEI[48] del dispositivo para usarlo como identificador único. Los permisos usados entonces son:

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
```

Vale la pena recordar que si la aplicación estuviera diseñada para usar permisos de superusuario en el caso de estar corriendo en un dispositivo rooteado, no sería necesario solicitar estos permisos al usuario de manera explícita, haciendo la tarea de espionaje aún más oculta.

A la hora de instalar la aplicación, por los permisos declarados más arriba se le presenta la siguiente pantalla informativa:

Figuras 26 y 27. Permisos solicitados al usuario al instalar..

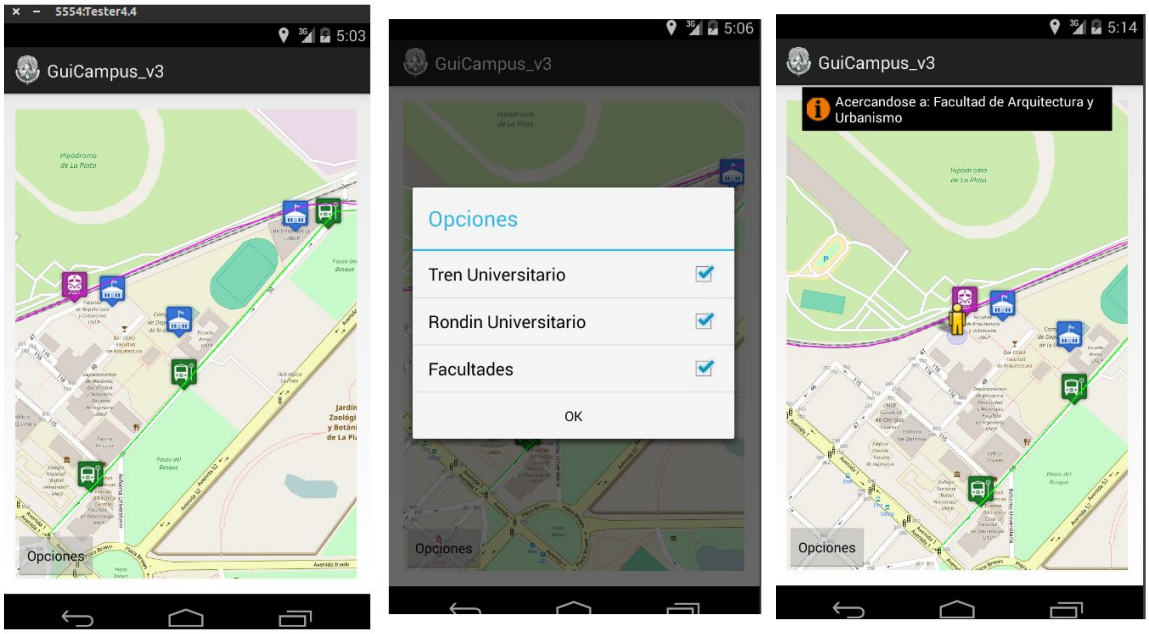
La realización del POC se llevó a cabo utilizando los SDKs de Android disponibles libremente para desarrolladores. El POC se realizó para que sea compatible con Android 4.4.2 en adelante (API Versión 19), para funcionar con la mayor cantidad de dispositivos posibles[49].

La POC tiene las siguientes componentes:

- por un lado consta de una aplicación para android
- y por el otro consta de un pequeño web service RESTful que recibe mensajes desde la aplicación y almacena en una base de datos mysql los datos acerca de los dispositivos y la información de geolocalización.

El webservice no presenta demasiados puntos interesantes para explicar en relación a esta tesina, es simplemente un webservice escrito en lenguaje php que almacena datos en una base de datos mysql. Cuando un mensaje HTTP enviado mediante POST llega al puerto 80 del servidor a la uri donde corre el web service, este atiende la petición y comprueba si la información necesaria existe en el mensaje, de ser así realiza las tareas de almacenamiento de la información en la BD.

La aplicación android, denominada “GuiCampus_v3”, es una aplicación que presenta la funcionalidad de ser un guía para el usuario dentro del campus de la UNLP, utilizando el gps. Presenta información acerca de las facultades y los servicios de transporte que se encuentran en las inmediaciones de las dependencias, que el usuario puede consultar. Aunque no se trata de una aplicación 100% funcional, ya que solamente contiene cargada información de la zona comprendida entre las calles 1-122 y 47-53 aproximadamente, alcanza para demostrar la idea de la aplicación.



Figuras 28,29 y 30. Mapa e informacion desplegada por la App.

Para el usuario, la única información acerca de la aplicación es la que se muestra en pantalla, aunque cada vez que el usuario se mueve y el gps registra un cambio en la posición del usuario, además de mostrar el cambio en la pantalla y si se está acercando a algún punto de interés envía un mensaje HTTP al webservice con información acerca del geo-posicionamiento del usuario. Esto se realiza mediante el llamado a un método de una clase que se encarga de realizar la tarea de enviar de manera asíncrona la información para no bloquear la interfaz de usuario.

Para también ejemplificar el comportamiento de una aplicación con fines maliciosos, a la hora de generar el .apk de la aplicación para su distribución este se hace aplicando un proceso de ofuscamiento para que si se realiza una descompilación del .apk para poder ver su código fuente, este sea más difícil de interpretar y de hacer un reversing (ver fig. 29 y 30).

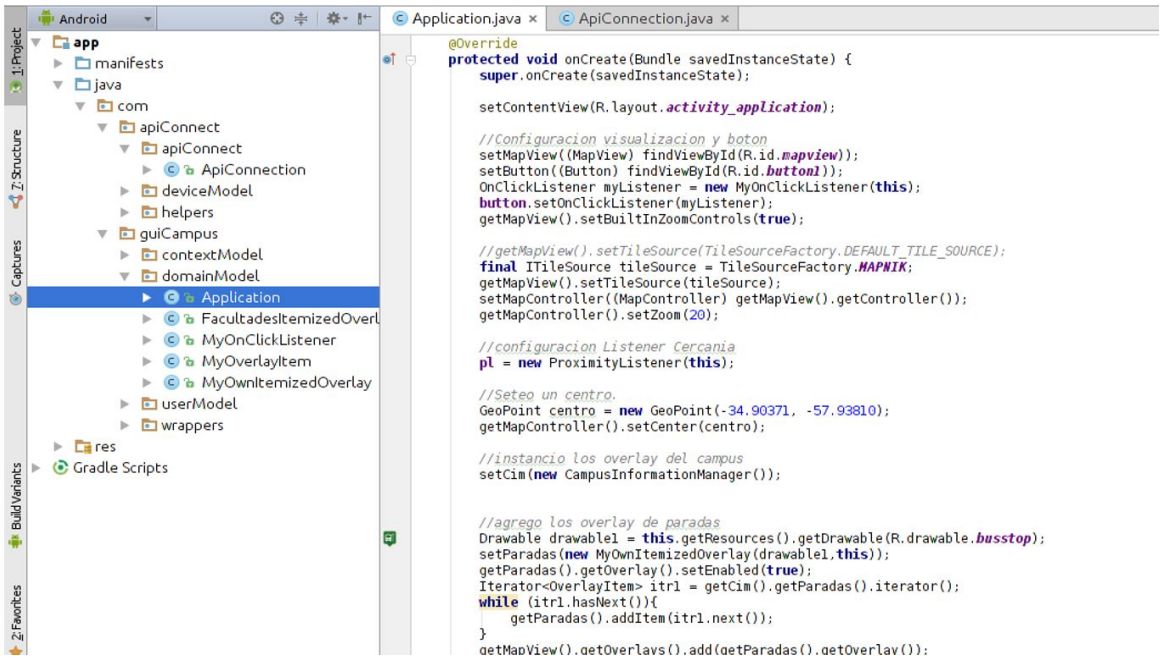


Figura 29. Código no ofuscado.

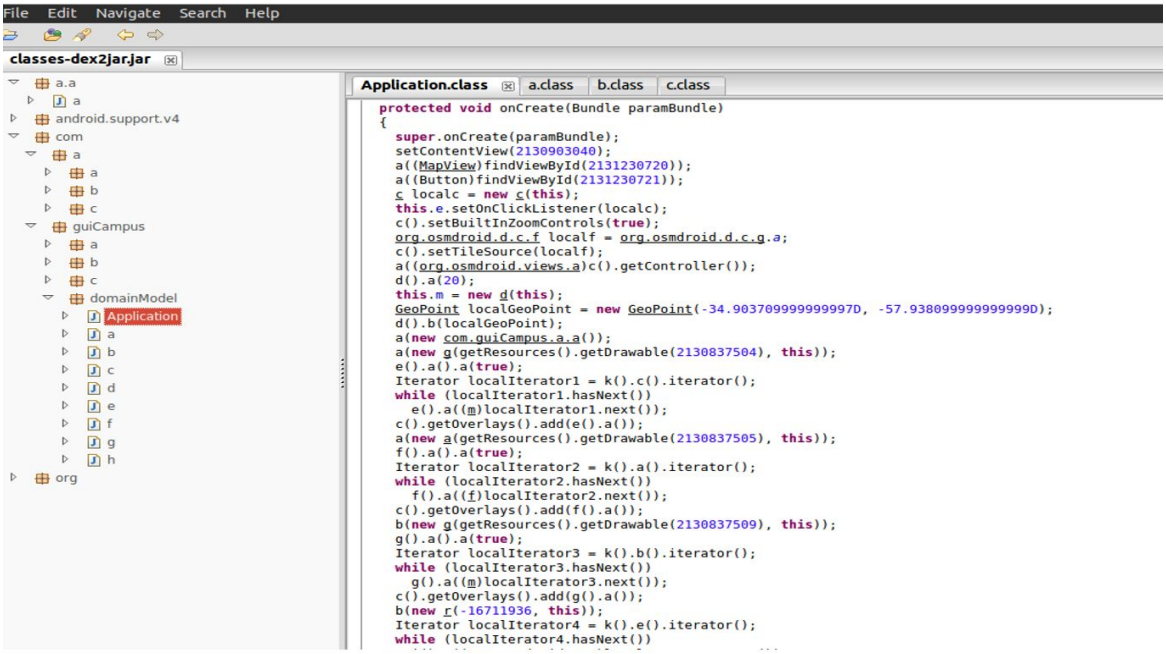


Figura 30. Código ofuscado.

En este casos se usó el ofuscador de código que viene como parte de la herramienta de desarrollo “Android Studio”, ya que el resultado es suficiente para ejemplificar lo que se menciona.

Conclusiones

La implementación de esta POC estuvo centrada en reflejar la facilidad con la cual, con algunos conocimientos de desarrollo de aplicaciones en android, una persona puede crear una aplicación que realice más acciones de las que dice hacer, por ejemplo una tarea de espionaje o el de robar información sensible, ocultándola mediante alguna funcionalidad que resulte atractiva.

Conocer qué realizan y el nivel de información que manejan los permisos de android es clave a la hora de implementar una aplicación.

7. Trabajo a futuro

Cuando se habla de BYOD se hace referencia a una tendencia consolidada y ante la cual las organizaciones deben hacer un análisis de riesgos para tomar una posición al respecto. La adopción del fenómeno puede traer grandes beneficios relacionados con la disminución de gastos en infraestructura, la comodidad de los miembros de la organización para el manejo de la información y por tanto el incremento de la productividad. No obstante, la organización enfrenta nuevas amenazas que deben ser gestionadas, siendo las principales y quizás más preocupantes la fuga de datos y el acceso no autorizado a la información sensible. Un trabajo futuro podría enfocarse en buscar hoy en día qué herramientas tienen las organizaciones que ayudan a mitigar estas amenazas, definir en la política de mitigación que acciones tomar ante estas situaciones y que no solo quede en un simple párrafo. Un estudio que podría realizarse sobre la fuente de conectividad de los dispositivos propios de los usuarios, es decir las redes a las cuales se conectan, es un análisis de tráfico para ver que tipo y volúmenes de datos se manejan en las distintas redes inalámbricas para estudiar cuál debe ser la distribución de estas y el uso que debe dárseles, buscando formas de mantener seguras redes en las cuales esos dispositivos no deberían tener acceso o a los datos que no se deberían acceder utilizando esas conexiones.

Como se ha visto en la sección de “Estadísticas sobre usos de dispositivos móviles” es muy importante y crítico que las organizaciones tengan como prioridad la educación de sus miembros para que conozcan sus políticas, los riesgos y sepan cómo enfrentarlos, por los que la capacitación debe ser constante y emprender esta tarea de brindar capacitación resulta un interesante punto de trabajo futuro.

Como trabajo a futuro se podría realizar un relevamiento de herramientas MDM que se encuentran en el mercado y comparar las herramientas de software libre contra las herramientas pagas, comparando características y analizando cuáles se adecuan más a una organización. De aquí se puede desprender desarrollar una aplicación MDM que sea útil para organizaciones pequeñas y medianas como son las PyMES.

Con la aparición de nuevas tecnologías y tendencias que hoy en día están impulsando la interconexión de todos los dispositivos hogareños, el IoT empieza a fortalecerse y cada vez son más los nuevos desafíos de seguridad que hay que afrontar. Ataques como el explicado por Cloudflare en el articulo *"Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras"*[50] se harán cada vez más frecuentes. Una de las líneas de trabajo a futuro que resultan interesantes para este enfoque son la evolución del IoT de la mano de la seguridad, armando un registro acerca de que se está haciendo en materia de seguridad, cómo va evolucionando y las alternativas que el mercado propone para mitigar las amenazas, como así también conformar un grupo de trabajo que se encargue de analizar la problemática, comparando protocolos de seguridad de empresas que desarrollan nuevos dispositivos IoT y poder determinar qué factores son importantes a la hora de, por ejemplo, la elección del protocolo de conexión.

8. Conclusiones

De la misma manera que con las PC, los dispositivos móviles son un blanco de los ataques contra la seguridad de la información y los problemas de seguridad a los que están expuestos son similares. Al contar los dispositivos móviles con GPS, cámara, micrófono, etc. hacen que estos sean un objetivo valioso a la hora de realizar tareas como las de espionaje. El uso tan extendido de dispositivos móviles ha hecho que se conviertan de manera activa en una herramienta más de nuestro trabajo, alojando en muchas ocasiones información organizacional crítica o valiosa que en caso de ser interceptada, conllevaría grandes problemas de seguridad. Dicho uso tan extendido de estos dispositivos ha hecho que los ciberdelincuentes lo vean como un mercado a explotar, y al día de hoy, los dispositivos móviles se han convertido en uno de los focos principales ante ataques informáticos. El "malware móvil" es muy variado y tiene un espectro de ataque muy amplio, pasando desde el comportamiento enteramente destructivo hasta el robo de información y el chantaje, siendo los malwares más abundantes aquellos que buscan algún rédito financiero. La exposición al malware queda altamente reducida si los usuarios solo se manejan por los canales seguros de distribución de aplicaciones implementados por los fabricantes y desarrolladores de las plataformas, pero ni así están completamente a salvo. Los problemas inherentes a las plataformas así como los ataques "de día cero" y las vulnerabilidades descubiertas seguirán existiendo, siendo la única solución el mantenerse actualizado, por más que a veces resulte dificultoso. La concienciación del usuario es y seguirá siendo siempre un factor determinante a la hora de reducir los daños y la exposición al malware.

La seguridad de los dispositivos móviles constituye una problemática actual de gran interés para las organizaciones cualquiera sea su tamaño, y en particular también para las del ámbito académico donde el fenómeno del BYOD se presenta como una realidad difícil de restringir. A la hora de diseñar e implementar soluciones y gestionar la seguridad de los dispositivos de una organización, se debe abordar la problemática en forma integral, teniendo en cuenta como se describe en este trabajo: la implementación de políticas,

normas y procedimientos (establecimiento un marco de seguridad aplicable a la organización), herramientas que faciliten la administración de la seguridad en los activos de la organización y concientizando a los empleados de la organización a través de actividades específicas para fomentar buenas prácticas en el marco del BYOD.

Hoy día la movilidad es algo inevitable en las organizaciones, pero el BYOD sí lo es. En los últimos años la movilidad ha pasado de ser una ventaja competitiva a ser un requerimiento necesario para cualquier organización. Sin embargo, el BYOD es sólo un modelo de implementación de la movilidad. Existen otras opciones. Las organizaciones deberían evaluar qué modelos encajan mejor dadas sus circunstancias concretas y, en cualquier caso, tomar una decisión respecto al BYOD. Puede optarse, por ejemplo, por modelos híbridos que combinan dispositivos organizacionales y dispositivos personales en función del perfil del usuario. O puede optarse por modelos como el CYOD (Choose Your Own Device), en los que las opciones de dispositivos y aplicaciones están mucho más limitadas que en el BYOD y el dispositivo puede pertenecer a la organización o al empleado, o por modelos COPE (Corporate-owned, Personally-Enabled), en los que el dispositivo pertenece a la organización pero el empleado puede usarlo como personal. Para obtener el máximo beneficio del BYOD las organizaciones deberían afrontarlo desde un enfoque estratégico, definiendo unas metas globales y resultados deseados de la implementación del programa BYOD, identificando cómo impactará el programa BYOD en las diversas unidades de negocio, así como los procesos de negocio que deben ser modificados, y definiendo un marco temporal para alcanzar los beneficios acordados del programa BYOD. Hemos visto que estos fenómenos tienen sus ventajas e inconvenientes. Pueden decidir adoptarlos o prohibirlos, pero en ningún caso las organizaciones pueden permitirse ignorar el BYOD, puesto que las implicaciones para la seguridad de la información organizacional son demasiado importantes, y pueden derivar en incidentes con un impacto negativo para la organización (a nivel económico, legal o reputacional).

9. Referencias

[1] Enhanced Network Security for Seamless Service Provisioning
in the Smart Mobile Ecosystem
http://www.nemesys-project.eu/nemesys/files/document/deliverables/NEMESYS_Deliverable_1.1_v4_rev_final.pdf

[2] Taxonomy: Mobile Malware Threats and Detection Techniques
http://airccj.org/CSCP/vol4/csit42222.pdf

[3] Android Malware Detection System Classification
http://www.scialert.net/fulltext/?doi=rjit.2014.325.341&org=10

[4] Reporte de malware 2014 por F-secure,
https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf

[5] Android el sistema operativo móvil mas utilizado,
http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[6] Dashboard Platforms versions,
http://developer.android.com/about/dashboards/index.html#Platform

[7] MDM Mobile Device Management,
http://es.wikipedia.org/wiki/Mobile_device_management

[8] Android mantendra su amplio dominio en los proximos cinco años, segun IDC,
http://www.redusers.com/noticias/android-mantendra-su-amplio-dominio-en-los-proximos-cinco-anos-segun-idc/

[9] Open Handset Alliance,
http://www.openhandsetalliance.com/

[10] Entendiendo el impacto de ART, la nueva maquina virtual de android,
http://www.elandroidelibre.com/2014/08/entendiendo-el-impacto-de-art-la-nueva-maquina-virtual-de-android.html

[11] Is your application ready for Android Lollipop?
https://fastest.cognizant.com/webapps/views/images/casestudy/fastest_Android%20L%20report.pdf

[12] Android Security 2015 Year In Review
http://static.googleusercontent.com/media/source.android.com/es//security/reports/Google_Android_Security_2015_Report_Final.pdf
[13] Seguridad de IOS
https://www.apple.com/es/business/docs/iOS_Security_Guide_es_Oct14.pdf
[14] Apple Developer Enterprise Program
https://developer.apple.com/programs/enterprise/
[15] Unified Extensible Firmware Interface
https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface
[16] Publish Windows apps
https://dev.windows.com/en-us/publish
[17] How to create your first app for Windows Phone 8
https://msdn.microsoft.com/en-us/library/windows/apps/ff402526(v=vs.105).aspx
[18] OWASP Mobile Security Project
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
[19] ¿Por qué tienen éxito los Advanced Persistent Threat (APT)?
http://www.redseguridad.com/opinion/articulos/por-que-tienen-exito-los-advanced-persistent-threat-apt
[20] Android Trojan Used in APT Attacks
http://www.securityweek.com/android-trojan-used-apt-attacks
[21] Dissecting the Android Bouncer
https://jon.oberheide.org/files/summercon12-bouncer.pdf
[22] Near field communication
https://es.wikipedia.org/wiki/Near_field_communication
[23] OWASP Mobile Security Project Top 10 Mobile Risks
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

[24] Analysis and Exploitation of a Linux Kernel Vulnerability (CVE-2016-0728)
http://perception-point.io/2016/01/14/analysis-and-exploitation-of-a-linux-kernel-vulnerability-cve-2016-0728/
[25] Nueva vulnerabilidad de Android susceptible a ataques de phishing por SMS
http://www.tuexperto.com/2012/11/05/nueva-vulnerabilidad-de-android-susceptible-a-ataques-de-phising-por-sms
[26] SMS phishing attackers continue to pursue Apple users
http://www.welivesecurity.com/2016/04/23/sms-phishing-attackers-continue-pursue-apple-users/
[27] El auge del ransomware para Android: criptográfico y de bloqueo de pantalla
http://www.welivesecurity.com/la-es/2016/02/18/auge-ransomware-para-android/?utm_source=newsletter&utm_medium=email&utm_campaign=wls-newsletter-190216
[28] Un agresivo ransomware para Android puede cambiar el código PIN del equipo
http://www.welivesecurity.com/la-es/2015/09/11/ransomware-para-android-cambiar-pin/
[29] Laboratorio de seguridad informática Hispasec
http://hispasec.com/
[30] iOS se hunde en arenas movedizas
http://unaaldia.hispasec.com/2015/08/ios-se-hunde-en-arenas-movedizas.html
[31] Palo Alto Networks - YiSpecter
http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/
[32] WireLurker, nuevo malware para iOS y OS X
http://unaaldia.hispasec.com/2014/11/wirelurker-nuevo-malware-para-ios-y-os-x.html
[33] Apple’s official statement on the YiSpecter iOS malware
http://www.loopinsight.com/2015/10/05/apples-official-statement-on-the-yispecter-ios-malware/
[34] AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device

http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

http://unaaldia.hispasec.com/2016/03/nuevo-malware-para-ios-puede-infectar.html

[35] SU (Substitute User)

http://man7.org/linux/man-pages/man1/su.1.html

[36] Smudge Attacks on Smartphone Touch Screens

https://www.usenix.org/legacy/events/woot10/tech/full_papers/Aviv.pdf

[37] Tiny Flashlight app

https://play.google.com/store/apps/details?id=com.devuni.flashlight

[38] Mobile Security Review 2015

http://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf.

[39] Multi-Factor Authentication (MFA)

https://en.wikipedia.org/wiki/Multi-factor_authentication

[40] BYOD Retos de la seguridad

http://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_byod_W.pdf

[41] Info volumen de datos 2020

http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

[42] Back Office

https://es.wikipedia.org/wiki/Back_office

[43] BYOD Libertad de eleccion de los dispositivos sin sacrificar la red de TI

http://www.cisco.com/c/dam/global/es_es/assets/pdf/byod_cisco_device-freedom_white-paper_es-eu.pdf

[44] Reporte de Fortinet BYOD

http://www.fortinet.com/press_releases/120619.html

[45] Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes

http://www.gartner.com/newsroom/id/2466615

[46] Anzhi Repositorio Chino

http://www.anzhi.com/

[47] SOTI Mobicontrol

https://www.soti.net/products/mobicontrol/overview/

[48] IMEI

https://es.wikipedia.org/wiki/IMEI

[49] Android Platform Versions Distribution

https://developer.android.com/about/dashboards/index.html

[50] Cloudflare - Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras.

https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/