RIESGOS Vs FUNCIONALIDAD FRENTE A LOS DISPOSITIVOS MÓVILES

John Alexander Díaz Dimaté
e-mail: alexdiaz10@gmail.com

RESUMEN: *Hace pocos años la aceptación de los dispositivos móviles no tenía la fuerza que hoy día tiene en la sociedad mundial, Colombia no es la excepción. Gente de todas las clases sociales, compañías dedicadas a mercados completamente deferentes, incorporan esta tecnología en sus hábitos tecnológicos, pero de igual forma que sucede con el tradicional portátil existen vulnerabilidades y riesgos implícitos en estos dispositivos, en la actualidad se ve a diario como se ha incrementado el delito informático y en muchos de los casos existe un dispositivo móvil involucrado y todo lo que ello implica. La informática forense no es ajena a esta problemática, entes como la policía judicial ya incorporan en procedimientos investigativos prácticas de informática forense a dispositivos móviles.*

SUMMARY*: A few years ago the acceptance of mobile devices did not have the strength that it now has in the global society, Colombia is no exception. People from all walks of life, companies engaged in completely deferent markets incorporate this technology in their technology habits, but equally the case with the traditional laptop there are vulnerabilities and risks involved in these devices, currently seen daily as has computer crime increased, and in many cases there is a mobile device involved and all that that implies. Computer forensics is not immune to this problem, such as judicial authorities and police investigative procedures incorporated computer forensics practices to mobile devices.*

PALABRAS CLAVE: Dispositivos móviles, análisis forense de dispositivos móviles, herramientas forenses, Smartphone, gestión de riesgos.

1 INTRODUCCIÓN

La evolución de los dispositivos móviles que facilitan actividades diarias, desde el estudiante con sus múltiples aplicaciones sociales, hasta el ejecutivo que lleva la oficina en su Smartphone, ha hecho que estos equipos se masifiquen en diversos tamaños, especificaciones técnicas, sistemas operativos, capacidad de almacenamiento, fabricantes, etc. Se ha convertido en una herramienta de trabajo que acorta distancias, incrementa la productividad de las organizaciones que migran sus aplicaciones a la nube y en general hace la vida más fácil.

Pero tanta dicha no puede ser cierta, toda ventaja trae su desventaja, cada vez que se hace mayor uso de estos dispositivos móviles exponemos más nuestras vulnerabilidades, a los atacantes, puesto que se exponen aspectos tales como: La red, datos personales, claves bancarias, información privada, contactos e incluso hábitos de vida, datos tan personales que ni siquiera nosotros mismos lo tendríamos tan claro.

Habilitando así la capacidad de los ciber-delincuentes para llevar a cabo su ilícito. Los fines delictivos de los atacantes tienen múltiples alcances y modalidades, fraudes se ven a diario contando con la ignorancia del usuario, frente a las múltiples aplicaciones y lo que hacen en nuestros equipos móviles, se

valen para hurtar nuestro bien más preciado, la información y la privacidad.

De la mano de este problema evoluciona la ciencia forense digital, que diariamente debe asumir nuevos retos para enfrentarse a los sofisticados esquemas del delincuente a nivel mundial, Colombia no puede ser la excepción, una de las organizaciones con más experiencia y conocimiento en este caso es la FISCALIA GENERAL DE LA NACION, con procedimientos forenses establecidos y la capacidad de asegurar la evidencia, para ser usada posteriormente como material probatorio en el caso que sea necesario.

2 INFORMÁTICA FORENSE.

2.1 Análisis forense.

Del mismo modo que un médico forense al hacer una necropsia a un cuerpo sin vida buscando la evidencia de su deceso, lo hacen los especialistas en informática forense claro contextualizando el cuerpo inerte se trata de hacer análisis precisos de la información contenida en diferentes medios que puedan contener información relevante que ayude a identificar como sucedieron los eventos que conllevan a confirmar un hecho, los medios a evaluar van desde un computador, un disco duro, una memoria USB, una transacción en internet, una página web, un teléfono celular y así existen una gran cantidad de fuentes tecnológicas que nos darían información acerca de si un incidente informático pueda calificarse como delito o no, de acuerdo con lo estipulado en el código penal Colombiano, la recolección de la evidencia, la custodia y su respectivo análisis en busca de la verdad a grandes rasgos es lo que llamamos Informática Forense.

2.2 Delito informático.

Hoy día ya podemos hablar de delito informático con alguna tranquilidad de que serán judicializados quienes llegaren a cometer este tipo de delitos, en Colombia ya se habla de la tipificación de delitos informáticos y existen las leyes que como ciudadanos colombianos nos protegen, por ejemplo la Ley 1273 de 2009 que hable de la protección de la información y los datos, preservando integralmente los sistemas usados para la información y las comunicaciones, posteriormente la Ley 1581 de 2012 y su decreto 1377 de 2013, que hablan de la protección de los datos personales y su tratamiento, leyes que van regulando las conductas tecnológicas de la sociedad actual, tomando cuerpo y forma y muy aterrizadas al contexto nacional.

"La Estafa WhatsApp: Funciona de forma muy parecida a la estafa de la llamada perdida solo que por medio de la famosa aplicación WhatsApp. Llega la notificación que alguien está hablando pero sin embargo el mensaje no llega y dice que para acceder a este se debe enviar un mensaje a un número determinado. Una vez enviado queda suscrito a un servicio de SMS Premium de costo muy alto." [1]

Así como este delito hace unos años no existía porque tampoco existía la famosa aplicación ***WhatsApp*** se puede iniciar un proceso judicial que compromete en este caso un dispositivo móvil y una víctima de estafa y un victimario que puede ser una sola persona o una organización detrás de esta estafa, pero lo importante es que hay leyes que van siendo muy bien estructuradas y aunque falte bastante camino por recorrer, tipificar muchos más delitos y aterrizar los nuevos delitos informáticos, Colombia no se está quedando atrás frente a la evolución delincuencial informática.

3. POLICÍAS Y LADRONES.

3.1 Fiscalía General de la Nación.

"Es un organismo independiente adscrito a la rama judicial del Poder Público en Colombia. La Fiscalía General nació en 1991 con la promulgación de la nueva Constitución Política y empezó a operar el 1 de julio de 1992.

Esta institución retoma las tareas que se realizaban en la extinta Dirección Nacional de Instrucción Criminal, y su principal función es investigar y acusar a los presuntos responsables de haber cometido un delito a partir del sistema penal oral acusatorio implementado con la ley 906 de 2004." [2]

Por ende este organismo se encuentra habilitado para las investigaciones judiciales y también está facultado para ejercer la informática forense, con especialistas que siguen un protocolo con herramientas esterilizadas informáticamente hablando, aseguramiento de escena obtención de evidencia digital (*Información relevante encontrada en un sistema, recolección de evidencias. Ejemplo: fechas de archivos, metadatos, registros de navegación, restos de software instalado, archivos temporales, procesos en ejecución, dispositivos físicos*), etiquetado y custodia de la evidencia, análisis forense, elaboración de informes y al final obtener una evidencia con fundamento veraz y repetible, para ser utilizada frente a un juez, demostrando la culpabilidad o inocencia frente a un hecho, este organismo cuenta con herramientas de avanzada tecnología capaces de hacer informática forense a múltiples dispositivos dentro de los cuales se encuentran los dispositivos móviles y Smartphone, una herramienta llamada "*UFED Physical Analyzer es la aplicación más avanzada de análisis, decodificación y generación de informes en la industria del análisis forense para dispositivos móviles. Esta aplicación incluye detección de programas maliciosos, funciones de decodificación y generación de informes mejoradas, gráfico de línea de tiempo, capacidades de exportación de datos y mucho más.* [3]

La implementación de una herramienta como esta en organismos de investigación forense como la Fiscalía General de la Nación da cuenta del incremento delictivo a través de los dispositivos móviles, por ser una información tan volátil la que se almacena en estos equipos, se debe contar con una herramienta capaz de mantener la información integral, como uno de los principios de la información, para que pueda ser presentada de manera transparente e irrefutable en la demostración del echo investigado, existen desarrollos muy especializados para hacer investigación forense digital y aunque herramientas como esta que están en la actualidad en capacidad de intervenir sistemas operativos como IOS, Android, BlackBerry, GPS y en algunos sistemas operativos extraer más información que en otros nunca podrán disuadir la delincuencia mientras exista la oportunidad generada por los usuarios también existirá el depredador a la caza de la presa desprevenida, para hurtarle o hacerle daño de algún modo.

3.2 Delincuente cibernético.

Una Tablet o un Smartphone ofrecen innumerables ventajas tales como su versatilidad, conectividad, grandes capacidades computacionales en dispositivos cada vez más pequeños y tan fácil de camuflar y trasladar, dan a los delincuentes un arma que no dispara balas pero si hace grandes daños, por otro lado también a favor de la delincuencia cibernética, está el uso desproporcionado y libertad de acceso de nuestros equipos a las aplicaciones instaladas en los teléfonos inteligentes tabletas celulares y en general dispositivos móviles.

Para un delincuente cometer delitos con la certeza que su rostro no quedará grabado en las cámaras de vigilancia cuando se está cometiendo un hurto, es como miel para las abejas, no exponerse a una persecución policial o a la reacción de la víctima le hacen más fácil el trabajo al atacante cibernético y en muchos de los casos tienen éxito, sin ser detectados hasta un buen tiempo después de que el incidente sucedió.

4. ENTORNO EMPRESARIAL.

4.1 Evolución digital de las empresas colombianas.

La globalización implícitamente involucra la humanidad en general, al ritmo

vertiginoso de la tecnología, las comunicaciones, transferencias de grandes volúmenes de información en tiempos muy cortos, negocios que se firman al otro lado del mundo es esta necesidad la que hace que la infraestructura tecnología también evolucione para facilitar las necesidades industriales y comerciales, es por ello que cada vez más las industrias de diferentes mercados hacen uso de las nuevas tecnologías y es allí cuando empezamos hablar de los dispositivos móviles, aplicaciones en la nube, desarrollos a la medida funciones preinstaladas que se incorporan a las herramientas de trabajo (***WhatsApp, Skype, Facebook, Line, etc.***) definitivamente facilitan las comunicaciones y el trabajo, pero ¿Quién en las organizaciones está controlando y revisando el uso adecuado de estos equipos y aplicaciones? Cada vez es un reto más complejo el control y resguardo de la información que a través de estos equipos se transmite, así mismo surge la pregunta en cuanto al desarrollo de software, ¿Están mis aplicaciones desarrolladas pensando en la funcionalidad y la seguridad, capaz de blindar la información que proceso para mi empresa en dispositivos móviles?

Un artículo del periódico EL ESPECTADOR publicado el 5 marzo de 2012 revela que la firma de seguridad informática SYMANTEC realiza una encuesta en la que declaran.

"Estamos impresionados con el ritmo que la adopción de dispositivos y aplicaciones móviles está teniendo en las organizaciones. *Este cambio cultural de rechazar los dispositivos móviles en un inicio y ahora distribuirlos, soportarlos y desarrollar aplicaciones móviles, trae consigo un nuevo conjunto de retos y complejidades para los encargados de TI. También es importante comentar que, desde la perspectiva de seguridad, hoy son muchas las organizaciones que están pensando más allá de la pérdida y robo de teléfonos móviles", comentó CJ Desai, vicepresidente senior del Grupo de Endpoint y Movilidad en Symantec.*
La Encuesta sobre Movilidad 2012 de Symantec evaluó cómo la adopción de tecnologías móviles está redefiniendo el cómputo empresarial e introduciendo cambios masivos dentro de las organizaciones. [4]

En las organizaciones que aún no son conscientes de la inminencia de un incidente informático, se observa como el descuido incluso por profesionales de tecnología se presta para poder cometer fácilmente un ilícito en la organización desde un ataque de denegación de servicios, inserción de código malicioso, virus, gusanos, hurto de información, acceso no autorizado de servicios, desfalcos, estafas entre muchos más que inicialmente se desencadenan por una falta de control en seguridad de la información, clasificación de los riesgos, evaluación de los activos y un efectivo plan de gestión de la seguridad de la información, un ejemplo clásico, cuando llega un invitado a la compañía y solicita la clave del WIFI, desde el mismo gerente, pasando por el director financiero y lo que es peor por el profesional de tecnología, le dan acceso a la red sin premeditar las implicaciones que esto podría tener y no solo porque el invitado quisiera afectar de algún modo la compañía, que si fuera ese el objetivo, al conseguir la clave de la red inalámbrica ya tendría gran parte del ataque logrado, sino que también es posible que sin saber esta persona que en su teléfono celular o en su tableta cuanta con software malicioso que podría atacar cualquiera de los recursos de la compañía, pero entonces como se debería proceder para decirle al invitado del gerente que no podemos darle la clave del WIFI porque tenemos miedo de sufrir un ataque cibernético.

4.2 Mejor prevenir que lamentar.

¿En general como se deberían hacer las cosas para evitar reaccionar con forense lo que se puede prevenir con gestión? Una planeación estratégica comprometida con la seguridad de la información, implementar un estándar de aseguramiento y gestión de la información, existen algunos más complejos y de mayor alcance que otros "ISO 27001 y sus derivados, COBIT 4.1, entre otros" pero lo más importante es comprometer desde la alta dirección hasta el más humilde colaborador de la organización con una idea clara de los

riesgos que se corren en temas de seguridad informática, políticas orientadas a la culturización del buen uso y la responsabilidad de los activos de la compañía hacen menos vulnerable y riesgoso la implementación de nuevas tecnologías y mantenerse a la vanguardia de las comunicaciones, no siempre debe ser la planeación más costosa y complicada la que asegura los tres principios de la información (*Confidencialidad, Integridad, Disponibilidad*), todo esto va más allá de las normas y los controles, su base fundamental es la conciencia del riesgo y las implicaciones que tiene estar en la onda tecnológica y en esto es en lo que más coinciden los estándares de gestión de la seguridad de la información.

4.3 Hacer seguro su dispositivo móvil.

Lo primero a tener en cuenta es que al usar estos equipos ya se está exponiendo al riesgo, lo que no implica que deba ser inseguro, poder disfrutar de los beneficios si se mantiene un estricto control del uso y lo que comparte, llevar en la mano su información de manera segura es posible, inicialmente al igual que un computador es recomendable el antivirus para dispositivos móviles, preferiblemente que no sean los gratuitos, pero en general un sistema de seguridad, mantener claves seguras que no sean fáciles de romper, las redes sociales traen uno de los mayores focos de ataque sobre todo por lo que se comparte en ellas, cuando instale una aplicación tenga en cuenta cuales son los privilegios que requiere dicha aplicación del dispositivo y hasta donde va a publicar sus datos, tales como posicionamiento, datos contenidos en el dispositivo, información de comportamiento y gustos, existen aplicaciones que analizan desde sus hábitos alimenticios búsquedas más frecuentes, gustos musicales y en general más información de la que usted pueda creer, redes inalámbricas a las que vincula su equipo, información que descarga de correos o mensajes masivos que llegan a través de las redes sociales, en general lo que no conozca como seguro investíguelo para determinar su alcance.

"*Las siguientes tablas resumen nuestras conclusiones acerca de las diversas fortalezas y debilidades de las plataformas Móviles iOS y Android.*" *[5]*

Tabla 1. Resistencia frente a tipos de ataques.

Table 1

Resistencia frente a tipos de ataques

Resistencia a:	iOS Apple	Android Google
Ataques basados en la Web		
Ataques malware		
Ataques ingeniería social		
Ataques de abuso y recursos de servicio		
Pérdida de datos (mal-ciosa y accidental)		
Ataque integridad de datos		

[5]

Tabla 2. Implementación de funciones de seguridad.

Table 2

Implementación de funciones de seguridad

Pilares de seguridad	iOS Apple	Android Google
Control de acesso		
Procedencia de aplicación		
Encriptación		
Aislamiento		
Control de acceso basado en permisos		

[5]

[5]

5. **CONCLUSIONES.**

Los dispositivos móviles y sus funcionalidades, indudablemente ofrecen ventajas que agilizan el diario vivir y además entretienen en momentos de ocio, sin embargo y como he mencionado a lo largo de este articulo el uso implica exposición a los riesgos propios de esta tecnología, implícitamente dependiendo del sistema operativo de preferencia y el ámbito en el que se desarrolla, entre otros aspectos siempre seremos vulnerables, por ello es importante mantener un esquema de seguridad que nos de la confianza de no exponer datos personales o de nuestras organizaciones para que puedan ser aprovechadas por un delincuente, del mismo modo las organizaciones deben blindarse frente a este auge exponencial del uso de los dispositivos móviles, hasta donde permiten el acceso de equipos móviles en sus organizaciones, políticas de uso de las cuentas de correo corporativas, la sincronización de información con drives en la nube, así mismo el manejo de incidentes, la pérdida o robo de estos equipos, los desarrollos empresariales para móviles basados en seguridad de la información y en general un esquema de control en el presente, para evitar un dolor de cabeza en el futuro.

6. REFERENCIAS

[1] http://www.delitosinformaticos.com/08/2014/delitos/fraudes-y-estafas/las-principales-estafas-telefonicas -ADALID Corp Colombia

[2] http://es.wikipedia.org/wiki/Fiscal%C3%ADa_General_de_la_Naci%C3%B3n_(Colombia) ci%C3%B3n_(Colombia)

[3] http://www.cellebrite.com/es/mobile-forensics/products/applications/ufed-physical-analyzer

[4] http://www.elespectador.com/tecnologia/dispositivos-moviles-son-claves-empresas-articulo-330538

[5] http://www.sadvisor.com/downloads/InformeSymantecSET.pdf