Dispositivos móviles y el fenómeno del BYOD. Su impacto en la seguridad de las organizaciones

Paula Venosa, Nicolás Macia, Carlos Damián Piazza Orlando y Sebastián Exequiel Pacheco Veliz

Facultad de Informática
Universidad Nacional de La Plata
Argentina
{pvenosa,nmacia}@info.unlp.edu.ar
{cpiazza,spacheco}@cespi.unlp.edu.ar

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.
Este artículo 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 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.
fsd

Palabras Claves: Dispositivos móviles, Seguridad, Amenazas, BYOD, (IT) Tecnologías de información, (MDM) Mobile Device Management.

1. Introducción

El uso de dispositivos móviles ha aumentado considerablemente y la diversidad de tecnologías y plataformas conlleva a que aparezca un nuevo desafío en materia de investigación en lo que hace a aspectos relacionados con la seguridad y privacidad de la información.

El fenómeno del BYOD es una tendencia que se expande cada día en las organizaciones cualquiera sea su tamaño: hoy en día es muy común que los integrantes de las mismas hagan uso de sus dispositivos móviles personales para realizar sus labores en la organización. Lo que era antes un dispositivo de uso

personal se convierte en parte de la red de la organización lo cual, es cómodo para el usuario, pero también implica riesgos a la seguridad de la organización. Esta tendencia causa problemas a los administradores de los departamentos de TI (Tecnologías de Información) a la hora de implementar políticas de seguridad. Ahora hay distintos tipos de dispositivos personales sobre los que no se posee ningún control que solicitan acceso a la red de las organizaciones. Por ello se requiere la implementación de políticas MDM (Mobile Device Management), que conlleven a una gestión exitosa de este abanico amplio de dispositivos móviles, en pos de implementar la movilidad organizacional de manera segura. Por lo mencionado, este fenómeno constituye un campo de investigación de interés para aquéllos que estudian problemáticas relacionadas a la seguridad de la información y su aplicación en tecnologías actuales, análisis de protocolos de seguridad y mecanismos de protección disponibles y en desarrollo.

1.1. Amenazas latentes en el uso de dispositivos móviles

Los problemas de seguridad a los que los dispositivos móviles están expuestos son similares a los que está expuesto una computadora[3], pero se ven agravados ya que cuentan con una mayor exposición al ser su comunidad de usuarios más amplia, además de que se 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 relación a las contramedidas que se pueden adoptar. Si eso lo sumamos a con la cantidad de elementos incluidos en los smartphones surgen 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.

A la hora de determinar las distintas amenazas que podrían atacar la integridad del dispositivo y de los datos en él contenidos, podemos armar la siguiente clasificación general:

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. 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. Los autores de malware modernos han comenzado a focalizarse en el desarrollo de malware para dispositivos móviles y Android es una de las plataformas a las que más provecho le sacan.

Robo y Fuga de Datos. La seguridad de la información es esencial para cualquier persona u organización que quiere proteger su información 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. El malware es una de las maneras de lograr el robo y la fuga de información, aunque también puede ser robada por ataques que implican acceso físico al dispositivo.

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.

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 o relacionada a la organización. Las personas que practican la ingeniería social (estafadores) utilizan la interacción social para engañar a sus víctimas logrando que confíen en él. El engaño podría ser 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.

Phishing. Es una forma de ingeniería social, pero por sus características merece ser mencionado de manera particular. Un ataque de phishing es un intento de obtener una parte de la información sensible de los usuarios haciéndoles creer que es por una causa legítima. El ataque se inicia normalmente utilizando el correo electrónico o sitios web maliciosos como herramienta primaria. 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.

Ransomware. Una amenaza con múltiples ataques que se están registrando en estos últimos años es el ransomware. 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 esas restricciones. 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[4], 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, 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.

Jailbreak 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. El jailbreak es el término genérico que se le ha puesto a los métodos que hay para saltarse las medidas de seguridad impuestas por Apple en su sistema iOS y poder instalar, modificar y cambiar cualquier aspecto del sistema. Un dispositivo con jailbreak[5] ofrece a los usuarios y desarrolladores el acceso a los recursos que se le fueron prohibidos. Sus principales usos son modificación del sistema, personalizar más el sistema con fuentes de letra diferentes, animaciones, nuevas funciones que no están en iOS. Descarga de aplicaciones que no han sido aceptadas en la App Store o aplicaciones de pago gratuitas. Los usuarios ya no se limitan a sólo usar App Store para obtener más aplicaciones y por lo tanto podrían utilizar copias de contrabando de aplicaciones legítimas (de sitios de terceros) que podrían ser maliciosas.

Android Rooting. Root, Rooting o Rutear(Rootear) se le conoce al método utilizado para darle al usuario los privilegios de Administrador o Super Usuario(SuperUser) del sistema operativo Android. Este concepto proviene del OS Linux y hace referencia al mismo comportamiento en Android ya que este también es un tipo de Linux. 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). 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 o modificarlo a niveles avanzados, como cambiar la velocidad del microprocesador. En este punto es donde nos detendremos y prestaremos 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"[6]. Las restricciones impuestas por Android a nivel de permisos de aplicación están pensados 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 móvil 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.

Como se puede ver, existe un amplio espectro de amenazas que pueden atentar contra la seguridad de un dispositivo móvil. Además, gracias al fenómeno del BYOD estas amenazas también atentarán contra la seguridad de la organización. Debido a esto, resulta necesario para las organizaciones que acepten el BYOD tener en cuenta los problemas mencionados con la finalidad de poder mantener un ambiente organizacional seguro. Para ello, será necesario que las

organizaciones desarrollen y apliquen políticas de uso, uso de software de gestión para dispositivos móviles (MDM) y capaciten a sus usuarios, entre otras cosas.

2. El fenómeno BYOD y la seguridad

2.1. ¿Qué es BYOD?

Bring Your Own Device[7] es un fenómeno cultural y tecnológico que incentiva a los miembros de una organización a utilizar sus propios dispositivos móviles personales en las actividades laborales de la organización donde trabajan.

El fenómeno del BYOD 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. La razón por la que esto ocurre es la premisa de que quien trabaja cómodo trabaja mejor. Además, 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.

Debido a todo esto, a partir del BYOD, lo que era un dispositivo personal se convierte en parte de la red organizacional con los problemas que esto podría acarrear en lo que a seguridad se refiere.

2.2. BYOD y buenas prácticas de seguridad en la organización

A partir del fenómeno del BYOD anteriormente descrito, surgen líneas claras en las que las organizaciones deben trabajar para mantener la seguridad de la red de la organización. Entre estas líneas podemos mencionar:

- Definición de política de seguridad en el uso y la gestión de dispositivos móviles.
- Uso de aplicaciones para el Mobile Device Management (MDM).
- Concientización y capacitación del usuario.

Definición de políticas de seguridad en el uso y la gestión de dispositivos móviles

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.

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 de la organizacion en cualquier momento, en cualquier lugar y desde

cualquier dispositivo. Las iniciativas de movilidad deben contribuir a facilitar la continuidad del trabajo, mejorar la colaboración, simplificar el teletrabajo y mejorar la satisfacción de los miembros. 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 complicado 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 la misma. Cuando los miembros de la organización saben qué se espera de ellos, cuáles son los comportamientos aceptables y las consecuencias del incumplimiento, es menos probable que rompan las reglas.

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.

Mobile Device Management

Las herramientas Mobile Device Management (MDM) permiten la gestión de los dispositivos móviles de una organización. Las herramientas tipo MDM sirven para asegurar, monitorear y administrar dispositivos móviles de forma centralizada. La gestión se realiza desde un servidor centralizado en el que se pueden definir políticas, actuaciones o incluso localizar o realizar un borrado remoto de la información contenida en un dispositivo móvil perdido evitando así por ejemplo, la extracción de datos de su memoria.

Como ejemplo, con un sistema MDM, la organización podría establecer la política de que un dispositivo que tiene determinada aplicación 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 IT si podrá controlar qué aplicación del dispositivo particular puede acceder a datos corporativos y cual no.

Concientización del usuario

Para evitar que los usuarios de una organización sean el destino de las distintas amenazas mencionadas, las organizaciones deberían implementar acciones de concientización y capacitación de sus usuarios. Estas acciones se realizan en el marco de la política de seguridad intenta reducir, por ejemplo, la posibilidad de que un usuario introduzca algún malware y exponga datos sensibles de la organización a terceros.

Es bueno que una organización implemente un plan de concientización con el objetivo de concientizar y fomentar hábitos cotidianos de seguridad en sus

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

3. Experiencias

A partir de la experiencia de nuestro grupo en el área de seguridad tanto en el marco de CERTUNLP[8][10][11][12][13][14][15] como en el de distintos proyectos de extensión relacionados a Concientización en Seguridad de la Información[1][2][9], los autores de este artículo venimos trabajando hace un tiempo en cuestiones relacionadas a seguridad en dispositivos móviles. En el ámbito de la UNLP, teniendo en cuenta las líneas de trabajo descritas en la sección anterior, se han desarrollado diversas tareas que se describen a continuación.

En primer lugar, se investigó sobre la temática y se realizaron recomendaciones de seguridad respecto a cuestiones de BYOD. Estas recomendaciones se realizaron teniendo en cuenta estándares de referencia como lo es la ISO 27000[16], y fueron aplicadas en nuestro ámbito de trabajo. La metodología utilizada ha sido la de construir una matriz de criticidad, que permita identificar fácilmente cuáles son los dispositivos más críticos para la organización. Esto puede estimarse en base a la criticidad de la información que dicho dispositivo almacena y además teniendo en cuenta el grado de exposición que el mismo tiene.

Luego, en base a la criticidad de la información y al grado de exposición, se ha armado una matriz que determina la forma de aplicar las recomendaciones de seguridad, definiendo básicamente prioridad en cuanto a aplicar controles a los dispositivos móviles. También como parte de este marco, se han definido recomendaciones, que incluyen buenas prácticas, para los distintos tipos de dispositivos móviles con los que cuenta la organización, así como un procedimiento a seguir en caso de pérdida o robo.

Por otro lado, dado que se hace imprescindible contar con alguna herramienta de MDM nos introdujimos en el tema a través del testeo de la herramienta SOTI Mobicontrol[17], ya que tuvimos la oportunidad de contar con una una licencia por 30 días que se nos suministró para poder conocer la herramienta, ver sus características y entender mejor el funcionamiento de una herramienta de MDM desde una visión práctica.

SOTI Mobicontrol es una herramienta comercial para el manejo de dispositivos organizacionales (Enterprise Mobility Management - EMM)[18]. 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 este 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.

La infraestructura utilizada en las pruebas 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:

- Movil Sony Xperia U con Android Ice Cream Sandwich 4.0.4
- Movil Motorola MotoG con Android KitKat 4.4

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; y el acceso al sistema de administración de dispositivos se realiza mediante un navegador.

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. Las pruebas realizadas nos han posibilitado entender el funcionamiento de este tipo de servicios. Una desventaja que presenta es que sólo 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 que se instala en los dispositivos el código se encuentra ofuscado para quedar ilegible.

Por último, en sintonía con las líneas descritas, en el marco de la semana de la seguridad de la información de noviembre pasado, se ha realizado una jornada denominada "Concientización sobre seguridad de la información. Redes sociales y smartphones: principios, riesgos y cuidados"[19], destinada a usuarios de la UNLP de direcciones de enseñanza de Facultades, Colegios (SIPECU) y postgrados. En la misma se abordaron riesgos en el uso de dispositivos móviles personales en el ámbito de nuestra organización: la Universidad Nacional de La Plata.

4. Conclusiones

De la misma manera que con las PC, los dispositivos móviles son un blanco de los ataques contra la seguridad de la información. Los problemas de seguridad

a los que están expuestos son similares. Al contar los dispositivos móviles con GPS, cámara y micrófono hacen que estos sean un objetivo valioso.

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 como la nuestra, 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 la 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.

Referencias

1. Lic. Nicolás Macia - Lic. Einar Lanfranco - Lic. Paula Venosa - Lic. Alejandro Sabolansky A.P.U. Carlos Damián Piazza Orlando - A.P.U. Sebastian Exequiel Pacheco Veliz: Uso de dispositivos móviles y BYOD: Su impacto en la seguridad. XVII Workshop de Investigadores en Ciencias de la Computación (Salta, 2015).
2. Lic. Nicolás Macia - Lic. Einar Lanfranco - Lic. Paula Venosa - Lic. Alejandro Sabolansky A.P.U. Carlos Damián Piazza Orlando - A.P.U. Sebastian Exequiel Pacheco Veliz: Seguridad en dispositivos móviles: un enfoque práctico.XVI Workshop de Investigadores en Ciencias de la Computación (Usuahia, 2014).
3. Reporte de malware por F-secure - `https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2014.pdf`
4. 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`
5. Malware attacks Jaibroken IOS devices `http://researchcenter.paloaltonetworks.com/2015/08/keyraider-ios-malware-steals-over-225000-apple-accounts-to-create-free-app-utopia/`
6. The risks of rooting your Android phone `http://www.bullguard.com/bullguard-security-center/mobile-security/mobile-threats/android-rooting-risks.aspx`
7. BYOD Retos de la seguridad - `http://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_byod_W.pdf`
8. Díaz, Francisco Javier; Venosa, Paula; Macia, Nicolás; Lanfranco, Einar Felipe; Sabolansky, Alejandro Javier; Rubio, Damián: Análisis digital forense utilizando herramientas de software libre. XVIII Workshop de Investigadores en Ciencias de la Computación (WICC 2016, Entre Ríos, Argentina)
9. Çompromiso social y calidad educativa: desafíos de la extensión Proyecto Caperucita y el lobo en el ciberespacio. Concientización en seguridad informática para jóvenes y tercera edad. IV Congreso Nacional de Extensión Universitaria y a las IX Jornadas Nacionales

10. Lanfranco, Einar Felipe; Benencia, Raúl; Macia, Nicolás; Venosa, Paula: Automatizando la gestión de configuraciones en pos de la seguridad.XVII Workshop de Investigadores en Ciencias de la Computación (Salta, 2015).
11. Javier Díaz, Alejandra Osorio, Paola Amadeo, Nicolás Macia, Paula Venosa: Seguridad Proactiva en los Sistemas de Gestión e Información académica: el caso de la UNLP. TICAL (Chile, 2015)
12. Traberg, Gastón; Molinari, Lía; Venosa, Paula; Macia, Nicolás; Lanfranco, Einar Felipe. Automatizando el descubrimiento de portales de autenticación y evaluación de la seguridad mediante ataques de fuerza bruta en el marco de una auditoría de seguridad. XXI Congreso Argentino de Ciencias de la Computación (Junín, 2015).
13. Santiago Alessandri, Matias Fontanini, Nicolás Macia. Service-Knocking Communication. 41JAIIO. Año 2012.
14. Lanfranco, Einar Felipe; Macia, Nicolás; Venosa, Paula; Molinari, Lía; Díaz, Francisco Javier: Tendencias en incidentes de seguridad atendidos por el CERT académico Cert-UNLP. XII Workshop de Investigadores en Ciencias de la Computación (2010)
15. Díaz, Francisco Javier; Foster, Pablo Mauricio; Lanfranco, Einar Felipe; Macia, Nicolás; Molinari, Lía; Venosa, Paula: Definición e Implementación de un Centro de Atención de Incidentes (CERT) para un ámbito Universitario. XV Congreso Argentino de Ciencias de la Computación (2009)
16. ISO 27000 - http://www.iso27000.es/download/doc_iso27000_all.pdf
17. Mobicontrol - https://www.soti.net/products/mobicontrol/overview/
18. Enterprise mobility management (EMM) - http://searchmobilecomputing.techtarget.com/definition/enterprise-mobility-management-EMM
19. Concientización sobre seguridad de la información. Redes sociales y smartphones: principios, riesgos y cuidados - http://www.cespi.unlp.edu.ar/articulo/2015/11/25/el_cespi_realizara_el_evento__equipo_certunlp__jornada_de_seguridad_de_la_informacion_