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

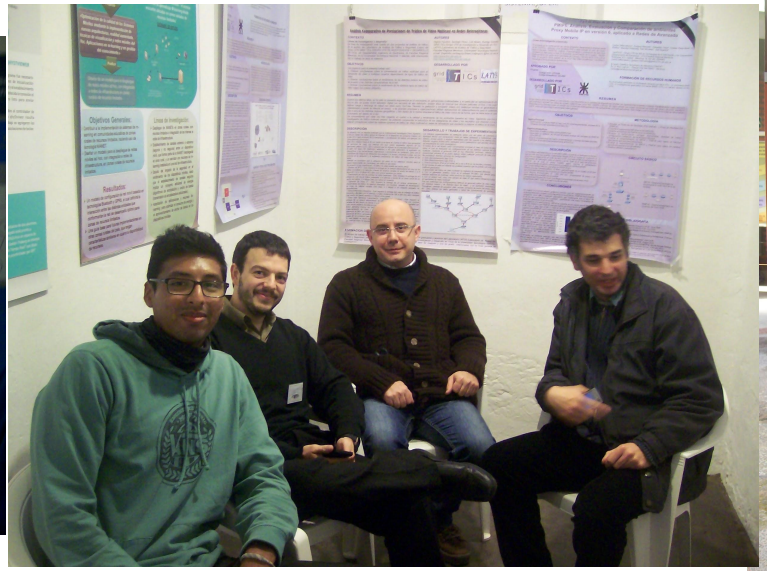
Exposición

Sobre nosotros...

- Sebastian Exequiel Pacheco Veliz
- Carlos Damian Piazza Orlando

Antecedentes en el Tema

Participamos como expositores en WICC 2014 y WICC 2015 con posters acerca de la problemática abordada, dentro del Área Seguridad Informática.



Antecedentes en el Tema

También realizamos la presentación de un paper en CACIC 2016 sobre este tema.

Estimado Colega:
Su artículo 9162 - "Dispositivos móviles y el fenómeno del BYOD. Su impacto en la seguridad de las organizaciones" ha sido aceptado para su exposición y publicación en CACIC 2016 (Argentina).

IMPORTANCIA DEL TEMA

Interés Actual
Relevancia
Aplicabilidad
Bibliografía: **Significativa**

CONTRIBUCION

Originalidad
Claridad del Resumen y Texto
Aporte de las Conclusiones
Calidad del Trabajo Experimental: **Excelente**

SELECCIÓN DE MEJORES TRABAJOS

¿Elegible Para Publicar Entre Los Mejores Trabajos?: **Si**

CALIDAD DE PRESENTACIÓN

Organización
Claridad
Legibilidad
Calidad de Figuras y Tablas
Sintaxis: **Muy Buena**

- Recomendación parcial: **Aceptar (Strong Accept)**
- Calificación global: **8**
- Conocimiento del tema por el evaluador: **8**
- Comentarios: **Muy buen trabajo. Esta presentado con mucha claridad. Puede resultar muy útil en diversos ámbitos.**

Estado actual de la seguridad

Los principios y requisitos comunes en el debate sobre la seguridad de la información son:

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

Lo que determinan es que sólo los usuarios con credenciales adecuadas deben ser capaces de leer, modificar y acceder a los datos privados en cualquier momento.

Motivación: La necesidad de la seguridad

Las amenazas que atentan contra la seguridad de los dispositivos 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.

Primera Etapa - Investigación y Análisis

Lo que se propuso como comienzo, fue conocer las características de las distintas plataformas existentes, así como también los riesgos y amenazas presentes en estas tecnologías y los ataques conocidos que se fueron dando a través del tiempo.

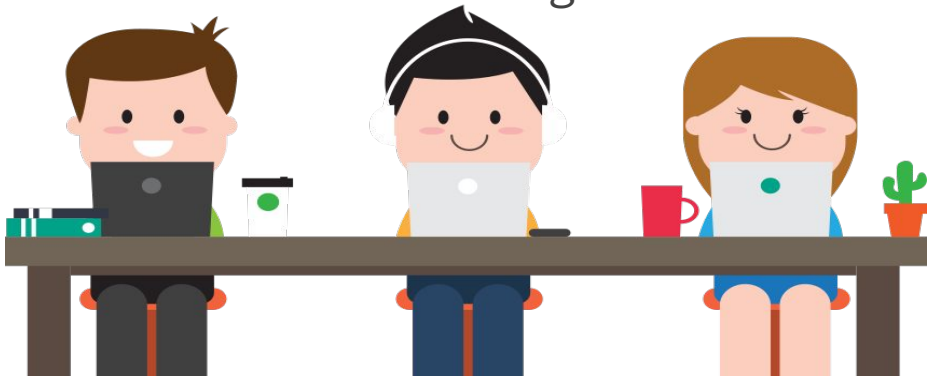
De esta manera se podrían identificar de mejor manera los vectores de ataques comúnmente usados.

Amenazas a la seguridad

- Robo y fuga de datos
- Ingeniería Social y Phishing
- Malware y Ransomware
- Vulnerabilidades de software
- Jailbreak y Rooting

Seguridad de la Organización - El Fenómeno BYOD

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 para acceder a los datos.



Seguridad de la Organización - El Fenómeno BYOD

¿Por qué?

La razón por la que ocurre esto es que la tecnología de uso personal es tan buena como la que se usa en la organización, sumando la comodidad del dispositivo propio.

Organizaciones disminuyen costos

+

Miembros trabajan más cómodos

=

Características de un nuevo paradigma

- Uso de dispositivos móviles personales
- Manejo de la información
- Cambios en la gestión de Infraestructura y los recursos
- Teletrabajo (Revista Bit & Byte N°3)
- Gestión de aplicaciones y dispositivos

BYOD

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

Ataques que se 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

BYOD

Todos los **riesgos** del BYOD provienen principalmente del hecho de que es el propio **usuario** quien gestiona sus 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.

Políticas de mitigación

Con las necesidades que surgen hay 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**

Casos Prácticos

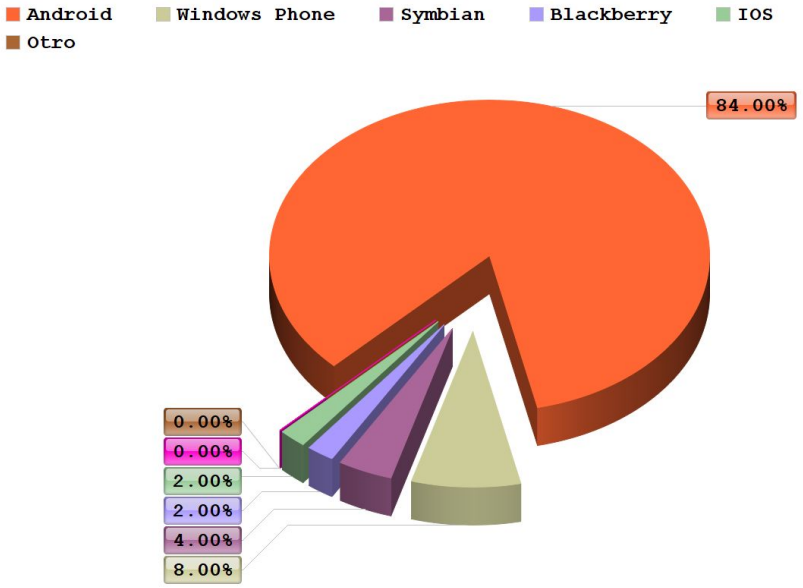
En el marco de esta tesina se realizaron **4 casos prácticos** para ayudar a comprender la problemática de la seguridad móvil y a ejemplificar algunos de los desafíos del BYOD.

1. Estadísticas sobre usos de dispositivos móviles

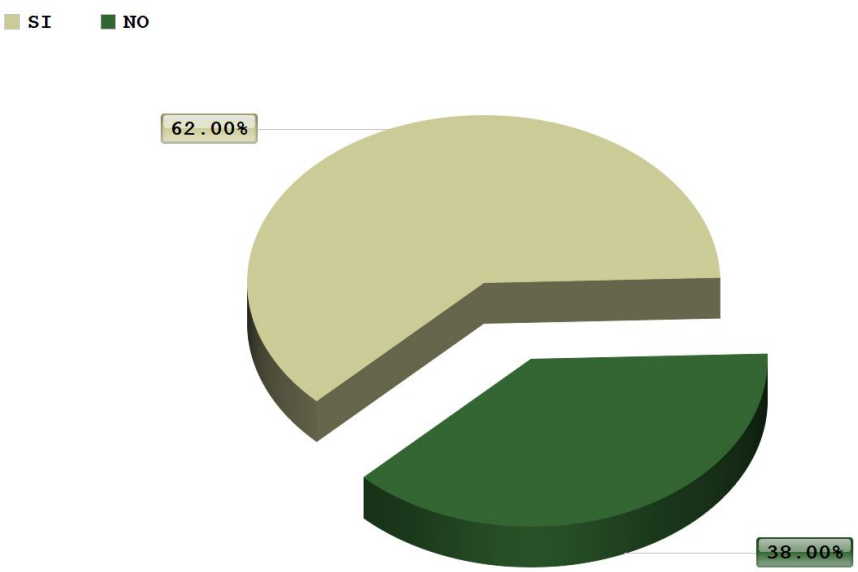
Integramos el taller "Aprendiendo a estar digitalmente seguros" del Proyecto "Extensión en vínculo con la escuela secundaria" desde el año 2015 y participamos con el equipo CERTUNLP en la "Jornada de seguridad de la información" en el CeSPI en al año 2015

1. Estadísticas sobre el uso de dispositivos móviles

Sistemas Operativos utilizados por los usuarios

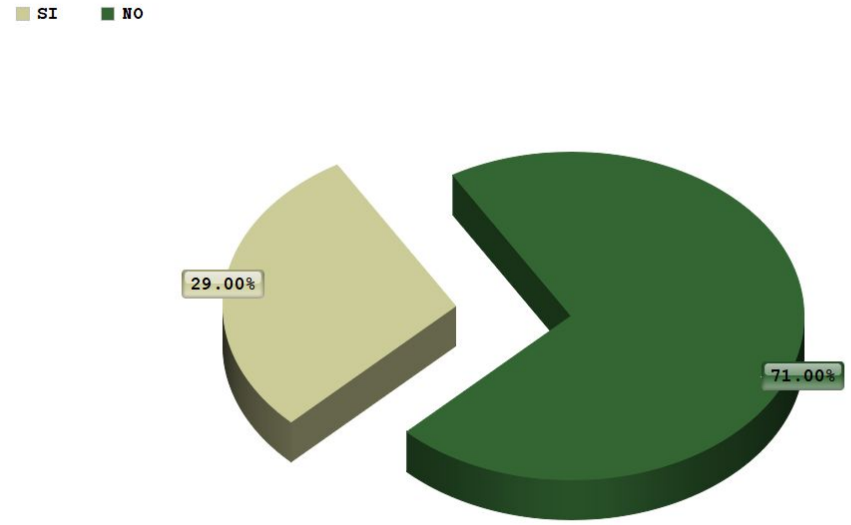


Usuarios que instalaron aplicaciones fuera del Market

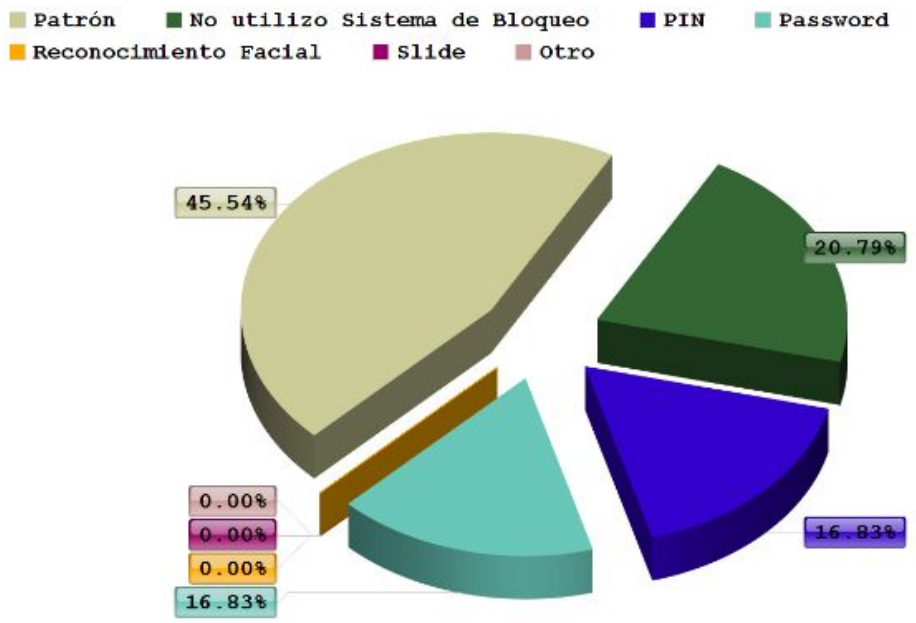


1. Estadísticas sobre el uso de dispositivos móviles

Usuarios que instalaron aplicaciones maliciosas



Sistemas de bloqueo o identificación utilizados



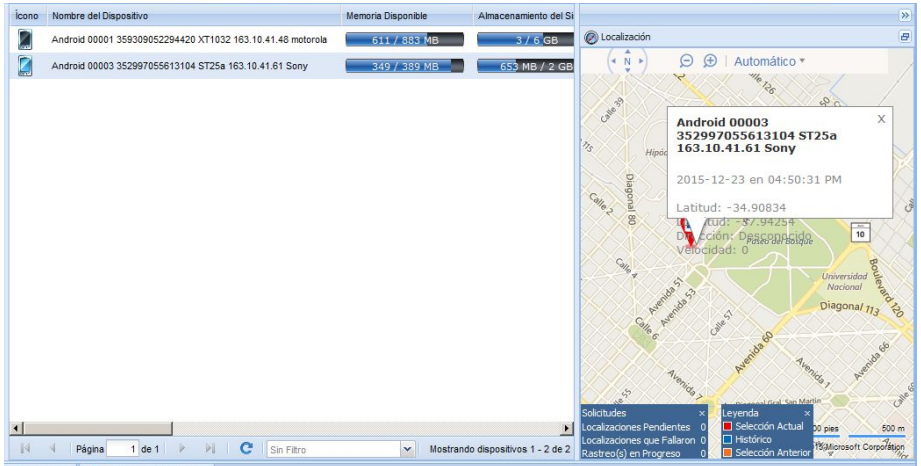
1. Estadísticas sobre el uso de dispositivos móviles

La encuesta refleja datos similares a los del índice dado por IDC donde más del **80%** de la población mundial utiliza el sistema operativo **Android**.

Esta encuesta reafirma la idea de **seguir fomentando y divulgando buenas prácticas en seguridad móvil en la sociedad**, principalmente en los jóvenes que son parte del cambio cultural, y laboral en las organizaciones.

2. Análisis de herramienta para MDM - Soti Mobicontrol

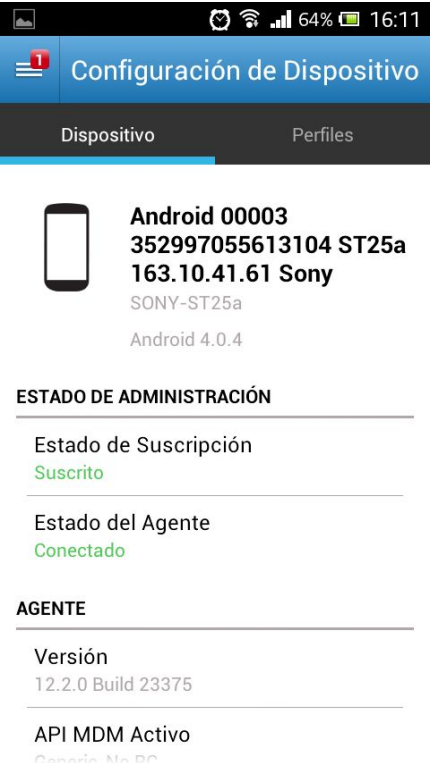
SOTI Mobicontrol es una herramienta **paga** para manejo de dispositivos organizacionales (Enterprise Mobility Management - EMM). Provee el manejo de aplicaciones, filtros de contenido, información, servicios de localización, etc.

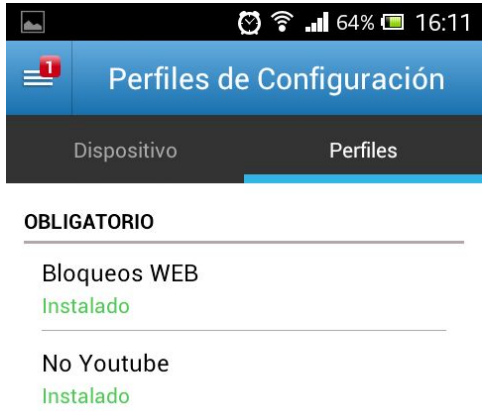


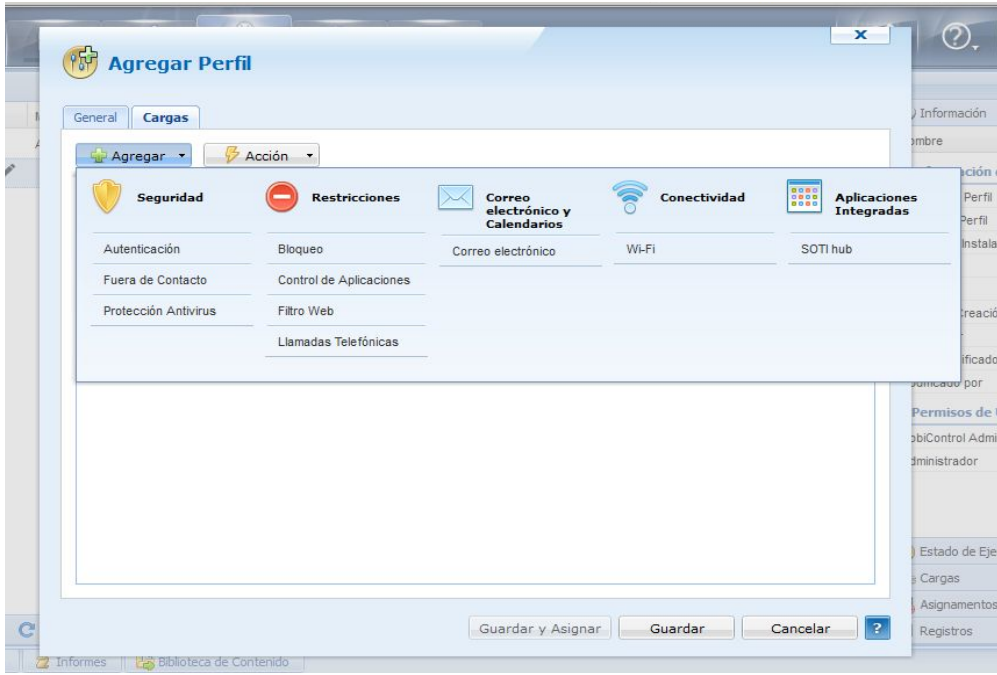
2. Software de gestión organizacional MDM Soti Mobicontrol

La herramienta funciona mediante la instalación de un **Agente** disponible 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.

2. Software de gestión organizacional MDM Soti Mobicontrol







2. Software de gestión organizacional MDM Soti Mobicontrol

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.

Hoy en el mercado se pueden encontrar múltiples herramientas de MDM tanto pagas como gratuitas, pero lo importante de estas herramientas es que **se adecuen a las necesidades de cada organización**.

3. Establecimiento de un marco de seguridad aplicable a una organización

---

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 propuso una política modelo para ser usada como base por las organizaciones que quieran crear la propia.

3. Establecimiento de un marco de seguridad aplicable a una organización

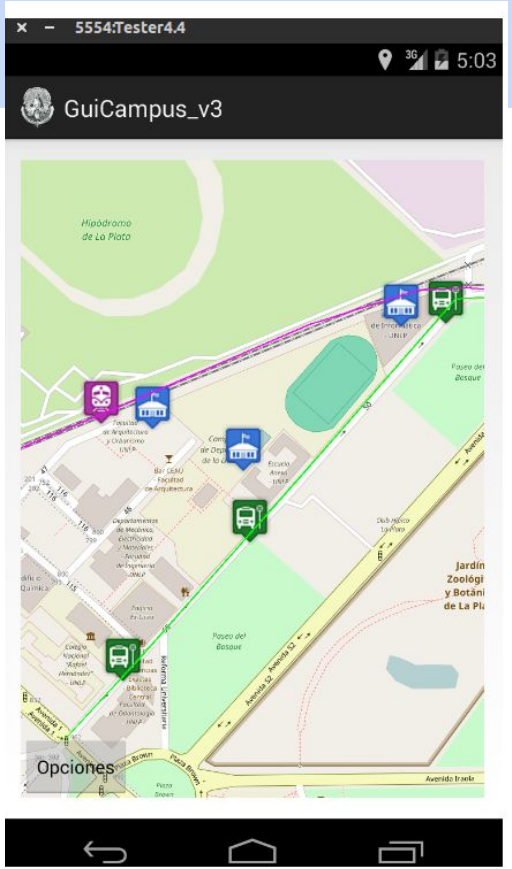
---

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 trabajo, mejorar la colaboración, simplificar el teletrabajo y mejorar la satisfacción de los miembros de la organización.

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 las consecuencias de no hacerlo, por lo que la **capacitación** y la **divulgación** de estas políticas es fundamental para su correcta ejecución.

4. Prueba de Concepto

GuiCampus_v3 es una aplicación diseñada para servir de guía a la hora de hacer una visita al campus universitario de la Universidad Nacional de La Plata, ayudando y ubicando al usuario en este entorno educativo.



Permite al usuario visualizar las diferentes características y opciones que presenta el campus en materia de facultades, transporte inter-facultades y sectores de interés dentro del campus.

4. Prueba de Concepto

Al mismo tiempo que realiza las legítimas tareas mencionadas, de forma **“silenciosa”** envía ilegítimamente 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.

4. Prueba de Concepto

LISTADO DE DISPOSITIVOS Y PUNTOS REGISTRADOS


```
{
    "devices": [
        {
            "Identity": "000000000000000",
            "Descrip": "cd.tato@gmail.com,",
            "LastSeen": "2016-11-02 18:44:56",
            "CreatedAt": "2016-11-01 12:31:54",
            "UpdatedAt": "2016-11-02 18:44:56"
        },
        {
            "Identity": "352997055613104",
            "Descrip": "",
            "LastSeen": "2016-11-02 19:11:55",
            "CreatedAt": "2016-11-02 17:44:19",
            "UpdatedAt": "2016-11-02 19:11:55"
        },
        {
            "Identity": "359309052294420",
            "Descrip": "celu1.cert@gmail.com,pv.sebas@gmail.com,pv.sebas@gmail.com,WhatsApp,sebaspev@hotmail.com,Messenger,Hu
            "LastSeen": "2016-11-02 18:04:57",
            "CreatedAt": "2016-11-02 18:04:29",
            "UpdatedAt": "2016-11-02 18:04:57"
        },
        {
            "Identity": "aaaa-aaaa-aaaa",
            "Descrip": "TESTEO POSTMAN",
            "LastSeen": "2016-11-02 20:00:51",
            "CreatedAt": "2016-11-02 20:00:51",
            "UpdatedAt": "0000-00-00 00:00:00"
        }
    ],
    "points": [
        {
            "owner": "000000000000000",
            "lat": "-34.907440",
            "lng": "-57.945908",
            "time": "2016-11-01 12:31:54"
        },
            "lat": "-34.908150",
            "lng": "-57.942459",
            "time": "2016-11-02 17:44:21"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908119",
            "lng": "-57.942448",
            "time": "2016-11-02 17:44:22"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908134",
            "lng": "-57.942463",
            "time": "2016-11-02 17:44:23"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908146",
            "lng": "-57.942455",
            "time": "2016-11-02 17:44:24"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908092",
            "lng": "-57.942459",
            "time": "2016-11-02 17:44:26"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908070",
            "lng": "-57.942497",
            "time": "2016-11-02 17:44:27"
        },
        {
            "owner": "352997055613104",
            "lat": "-34.908047",
            "lng": "-57.942535",
            "time": "2016-11-02 17:44:28"
        },
        {
            "owner": "352997055613104",
```

4. Prueba de Concepto

DEMO

Conclusiones

¿Qué buscabamos con esta tesina?

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, y atractiva para atacantes.
- La concientización del usuario es y seguirá siendo un factor determinante para reducir daños y exposición al malware.
- El BYOD llegó para quedarse. A la hora de diseñar e implementar soluciones y gestionar la seguridad bajo el BYOD, se debe abordar la problemática en forma integral como se describe en este trabajo.

Trabajo a futuro

- Realizar un relevamiento de herramientas MDM actuales, libres y pagas, comparando características y analizando cuales se adecuan más a una tipo de organización.

- Desarrollar una aplicación MDM que sea útil para organizaciones pequeñas y medianas como las PYMES.

- Seguridad en Dispositivos IoT, conformar un grupo de trabajo que se encargue de analizar la problemática, comparando características de seguridad de empresas que desarrollan nuevos dispositivos IoT.

GRACIAS

Muchas GRACIAS al Jurado

FELICES FIESTAS !!!