



# MALWARE EN DISPOSITIVOS MÓVILES ANDROID

M. Asunción Vicente Ripoll  
Elche (Alicante)

# MALWARE EN DISPOSITIVOS MÓVILES ANDROID

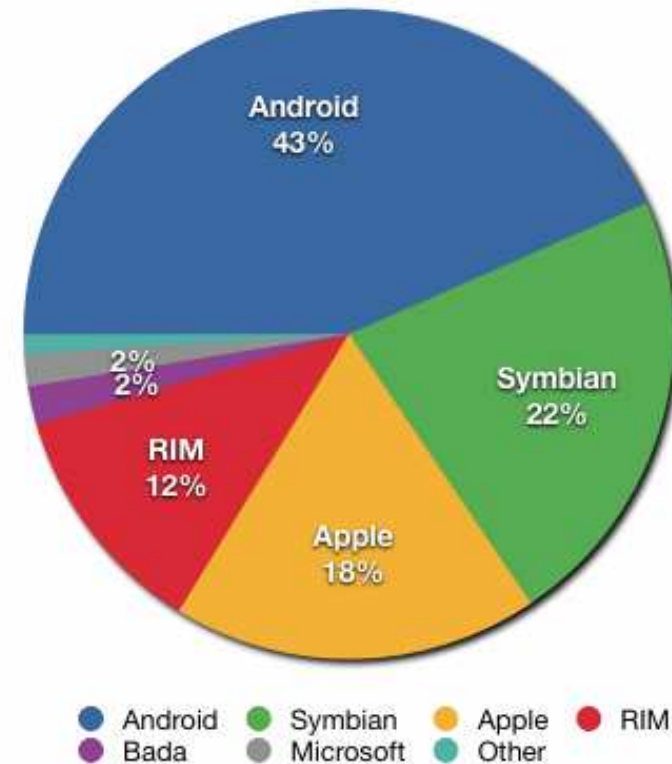
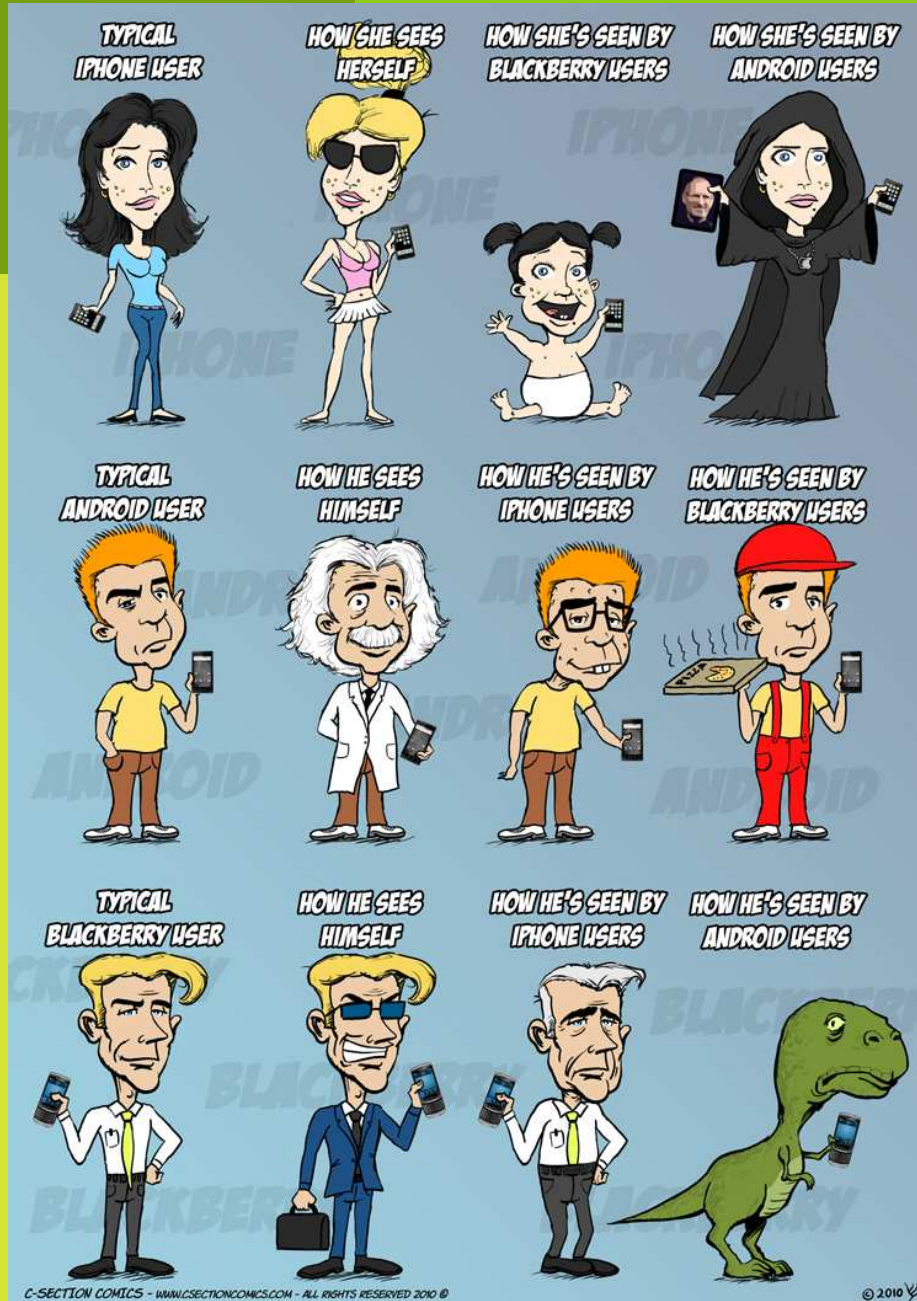
- ① INDICE
  - ① SMARTPHONES
  - ① TIPOS DE AMENAZAS
  - ① MODELO DE SEGURIDAD EN ANDROID
  - ① MALWARE
  - ① SOLUCIONES
  - ① EJEMPLO DE APLICACIÓN CON FLURRY

# SMARTPHONES

- ANDROID
- iOS (*iPhone*)
- Windows Phone
- RIM (*Blackberry*)
- Symbian (*Nokia*)

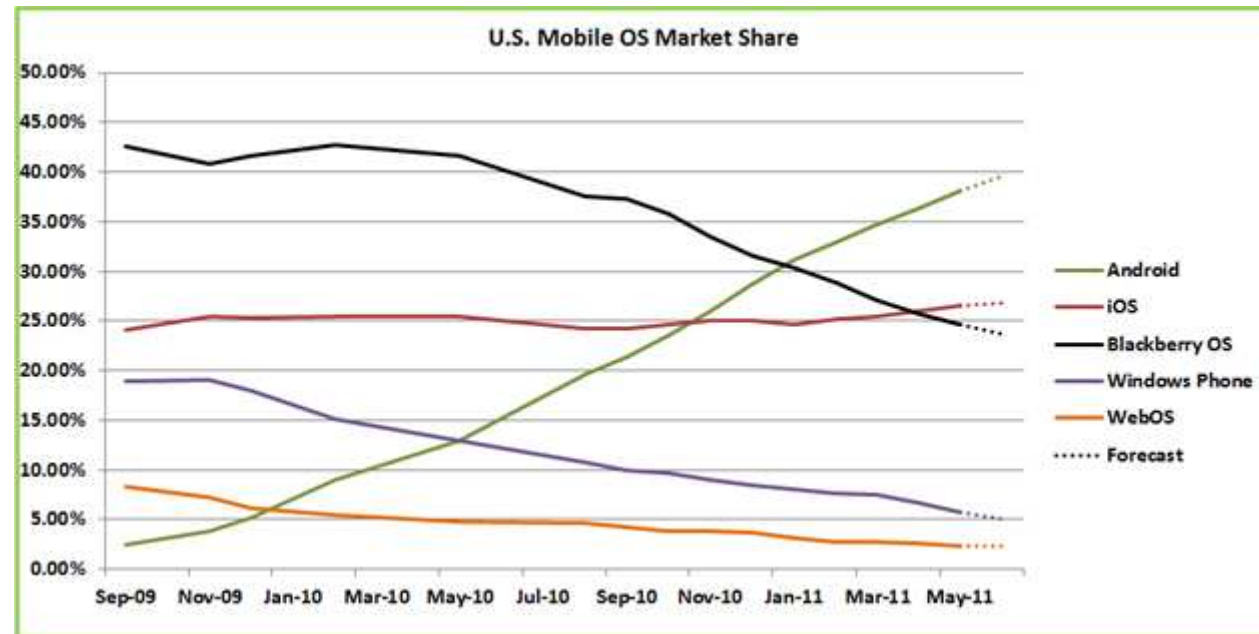


# SMARTPHONES



Datos del 2º cuatrimestre de 2011

# SMARTPHONES



Datos de Mayo 2011

# SMARTPHONES MERCADOS DE APLICACIONES

Plataforma	Tienda	Aplicaciones
Android	Android Market	250. 000 (julio 2011)
iOS (iPhone)	Apple App Store	425.000 (julio 2011)
Windows Phone	Windows Phone Marketplace	32.000 (sept. 2011)
RIM (Blackberry)	Blackberry App World	10.000 (sept. 2011)
Symbian (Nokia)	Ovi Store	50.000 (abril 2011)

# TIPOS DE AMENAZAS

- ⊙ Ataques basados en web
- ⊙ **Malware**
- ⊙ Ataques de ingeniería social
- ⊙ Abusos de la disponibilidad del servicio y de los recursos
- ⊙ Pérdida de datos maliciosa o involuntaria
- ⊙ Ataques a la integridad de los datos del dispositivo

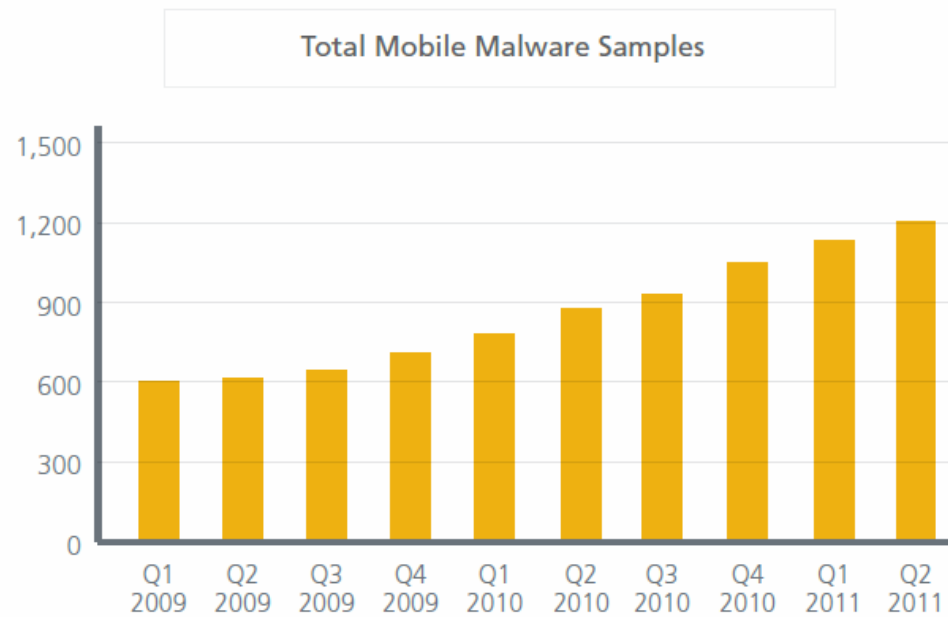
# TIPOS DE AMENAZAS

## © Ejemplos de Malware en Android

- © ***DROID09 (nov 2009)***: pretendía ser una aplicación para la gestión de algunos bancos online, ofreciendo al usuario un listado bastante limitado y solicitando las credenciales posteriormente. Desde la percepción del usuario, no era de extrañar que una aplicación bancaria pidiese tales datos, aunque el destino de sus credenciales no fuera en absoluto legítimo.
- © ***Android.FakePlayer (2010)***: pretendiendo ser una aplicación para reproducir vídeos, es en realidad un código malicioso destinado a enviar mensajes SMS Premium, hasta el momento se han descubierto 3 variantes.
- © ***Android/Jmsonez.A (2011)***: es una aplicación que imita a una aplicación calendario. Siempre muestra el mes de Enero de 2011. Si el usuario trata de cambiar la fecha del calendario, el código malicioso insertado en la aplicación comienza a enviar mensajes SMS a un número de móvil Premium.

# TIPOS DE AMENAZAS

## 📍 Crecimiento del malware en smartphones



# MODELO DE SEGURIDAD PARA MÓVILES

- ⊙ *Control de acceso tradicional*
- ⊙ *Procedencia de la aplicación*
- ⊙ *Cifrado*
- ⊙ *Aislamiento*
- ⊙ *Control de acceso basado en permisos*

# MODELO DE SEGURIDAD DE ANDROID



- ⊙ **Control de acceso tradicional:** proteger los dispositivos utilizando técnicas tradicionales como el uso de contraseñas y otros métodos como el uso del tiempo de inactividad para bloquear automáticamente la pantalla.
- ⊙ **Aislamiento:** limitar la capacidad de una aplicación para acceder a los datos importantes y datos del sistema del dispositivo.
- ⊙ **Control de acceso basado en permisos:** otorga una serie de permisos para cada aplicación y luego, limita a cada aplicación para acceder a los datos y el sistema del dispositivo que están dentro del alcance de esos permisos, bloqueando las aplicaciones si intentan realizar acciones que excedan el ámbito de estos permisos.

# MODELO DE SEGURIDAD DE ANDROID

## ⊙ **Control de acceso basado en permisos**

- ⊙ **Subsistemas de redes:** Las aplicaciones pueden establecer conexiones de red con otros dispositivos de red a través de Wi-Fi o usando la señal de telefonía móvil.
- ⊙ **Identificadores de dispositivo:** Las aplicaciones puede obtener el número de teléfono del dispositivo, el ID de dispositivo (IMEI), el número de serie de la tarjeta SIM, y el número de suscriptor del dispositivo ID (IMSI). Estos códigos pueden ser utilizados por los delincuentes para cometer fraude.
- ⊙ **Sistemas de mensajería:** Las aplicaciones pueden acceder al correo electrónico y a sus archivos adjuntos en la bandeja de entrada del dispositivo, la bandeja de salida, y los sistemas de SMS. Las aplicaciones también puede iniciar la transmisión de correos electrónicos y mensajes SMS salientes sin que el usuario se percate e interceptar correos electrónicos entrantes y los mensajes SMS.
- ⊙ **Agenda y libreta de direcciones:** Las aplicaciones pueden leer, modificar, borrar y añadir nuevas entradas en el calendario y en la libreta de direcciones del sistema.
- ⊙ **Archivos multimedia y de imagen:** Las aplicaciones pueden acceder a archivos multimedia (por ejemplo, archivos MP3) y las fotos almacenadas en la aplicación de fotografía del dispositivo.

# MODELO DE SEGURIDAD DE ANDROID

## ⊙ ***Control de acceso basado en permisos***

- ⊙ ***Acceso a la tarjeta SD externa:*** Las aplicaciones pueden solicitar guardar, modificar o borrar los datos existentes en la tarjeta de memoria externa SD. Una vez concedido este permiso, las aplicaciones tienen acceso ilimitado a todos los datos en la tarjeta SD, que no están cifrados por defecto.
- ⊙ ***Sistema de posicionamiento global:*** Las aplicaciones pueden obtener la ubicación del dispositivo.
- ⊙ ***Sistema de telefonía:*** Las aplicaciones pueden iniciar y potencialmente interrumpir las llamadas telefónicas sin el consentimiento del usuario.
- ⊙ ***Registros e historial de navegación:*** Las aplicaciones pueden acceder a los registros del dispositivo (por ejemplo, el registro de llamadas entrantes y salientes, registro del sistema, errores, etc), así como a la lista de marcadores del navegador web y el historial de exploración.
- ⊙ ***Lista de tareas:*** Una aplicación puede obtener la lista de aplicaciones actualmente en ejecución.

# MODELO DE SEGURIDAD DE ANDROID

## ⊙ *Control de acceso basado en permisos*

### ⊙ Ejemplo:

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

***AndroiManifest.xml***

# MODELO DE SEGURIDAD DE ANDROID

## 📍 *Control de acceso basado en permisos*

INFORMACIÓN GENERAL

VALORACIÓN DE LOS USUARIOS (10)

NOVEDADES

PERMISOS

### Permisos

ESTA APLICACIÓN DISPONE DE ACCESO A LOS SIGUIENTES PERMISOS:

#### TU UBICACIÓN

##### PRECISAR LA UBICACIÓN (GPS)

Permite acceder a las fuentes de ubicación precisas que estén disponibles desde el tablet como, por ejemplo, al sistema de posicionamiento global. Las aplicaciones malintencionadas pueden utilizar este permiso para determinar la ubicación del usuario y pueden consumir batería adicional.

#### COMUNICACIÓN DE RED

##### ACCESO ÍNTEGRO A INTERNET

Permite que una aplicación cree sockets de red.

#### LLAMADAS DE TELÉFONO

##### LEER LA IDENTIDAD Y EL ESTADO DEL TELÉFONO

Permite que la aplicación acceda a las funciones de teléfono del dispositivo. Una aplicación con este permiso puede determinar el número de teléfono y el número de serie de este teléfono, si una llamada está activa, el número al que está vinculada esa llamada, etc.

☑ Mostrar todos

# MODELO DE SEGURIDAD DE ANDROID

## 🎯 *Vulnerabilidades*

- 🎯 Según un informe de Symantec de 2011, los investigadores de seguridad han descubierto hasta 18 vulnerabilidades diferentes en las diferentes versiones del sistema operativo Android. De estas, la mayoría eran de poca gravedad y sólo permitirían a un atacante tomar el control de un proceso solo (por ejemplo, el proceso del navegador Web), pero no permitirían al atacante tomar el control a nivel de administrador del equipo. Las vulnerabilidades restantes son algo más peligrosas, y cuando se explotan, pueden permitir que el atacante tome el control del dispositivo a nivel de *root*, permitiendo el acceso a prácticamente todos los datos en el dispositivo.
- 🎯 Hasta la fecha, todas salvo cuatro de estas vulnerabilidades han sido parcheadas por Google. De las cuatro vulnerabilidades sin resolver, una es más grave. Esta vulnerabilidad ha sido solucionada en la versión 2.3 de Android, pero no ha sido resuelta para las versiones anteriores del sistema operativo.

# SOLUCIONES

## 🎯 Antivirus

Aplicaciones de Android Unos 1.269 resultados



**Antivirus Free**  
CREATIVE APPS / HERRAMIENTAS

★★★★★ (39.548)

INSTALAR

Fast and lightweight malicious app protection for your phone Antivirus Free will detect new applications that are installed on your system, and cross-reference them wi...



**Lookout Security & Antivirus**  
LOOKOUT MOBILE SECURITY / HERRAMIENTAS

★★★★★ (237.649)

INSTALAR

Protege tu teléfono con Lookout, la mejor aplicación de seguridad y antivirus Protege tu teléfono. ¡Consigue Lookout GRATIS: antivirus, localizador de teléfono, backup...



**Dr.Web Anti-virus Light**  
DOCTOR WEB, LTD. / HERRAMIENTAS

★★★★★ (32.380)

INSTALAR

Protect your precious handheld from viruses and malware! Proteja su dispositivo móvil de virus y correos basura con el popular anti-virus del fabricante líder en Rusia...



**Anti-Virus Free**  
AVG MOBILATION / COMUNICACIÓN

★★★★★ (155.220)

INSTALAR

El Antivirus gratis más descargado a nivel mundial - ya disponible para Android™ La solución de seguridad gratuita más descargada a nivel internacional ya se encuentra...



**Zoner AntiVirus Free**  
ZONER, LLC. / HERRAMIENTAS

★★★★★ (1.186)

INSTALAR

Zoner AntiVirus Free - Protege tu Android! Zoner AntiVirus® Free es una solución de seguridad moderna para su dispositivo. Ofrece protección antivirus y para llamadas ...



**MYAndroid Protection Antivirus**  
MYMOBILESECURITY / HERRAMIENTAS

★★★★★ (1.748)

INSTALAR

Descargue ahora e disfrute 30 días GRATIS de la mayor protección para su Android La mejor aplicación de seguridad en el Mercado Android para obtener una máxima protec...



**NetQin Security & Anti-virus**  
NETQIN MOBILE INC. / PRODUCTIVIDAD

★★★★★ (10.184)

INSTALAR

Antivirus móvil, nube escaneado, antipérdida móvil, control de tiempo real NetQin Mobile Security 5.0, una solución completa de seguridad móvil protege su Android de v...



**AegisLab Antivirus gratis**  
AEGISLAB / HERRAMIENTAS

★★★★★ (631)

INSTALAR

Última actualización: 30.09.2011, su apariencia profesional y mejora de funciones. AegisLab Antivirus Free es una herramienta de seguridad antivirus / móvil con las ...

# SOLUCIONES

## ○ MDM (Mobile Device Management)

### Aplicaciones de Android Unos 40 resultados

#### MDM Installer

DIRECTOR JUNG / HERRAMIENTAS

★★★★★ (11)

INSTALAR

B2B 공식 채널(서비스데스크)를 이용하여 문의하시기 바랍니다. 개인 개발자 메일로 받은 문의에 대해서는 별도로 답장하지 않습니다. If you are locked by the security mode that you can't use your mobile phone. Try to run MDM ...



#### AirWatch MDM Agent

AIRWATCH / NEGOCIOS

★★★★★ (16)

INSTALAR

The AirWatch MDM Agent lets you secure, monitor, manage and support your entire fleet of Android devices deployed across your enterprise, when working in conjunction w...



#### MaaS360 MDM for Android

MAAS360 / NEGOCIOS

★★★★★ (25)

INSTALAR

Please contact us directly with any comments or questions. We value your input as we continue to improve your overall experience with MaaS360. Contact us: <http://www...>



#### Tangoe MDM

TANGOE INC / HERRAMIENTAS

★★★★★ (5)

INSTALAR

Tangoe's MDM client provides robust functionality to enterprises for managing their Android devices. Note: The MDM Client requires the use of Tangoe's Mobile Device M...



#### Dell MDM

DELL\_APP / HERRAMIENTAS

★★★★★ (3)

INSTALAR

Dell MDM client enables Android Mobile Devices to be managed in the Enterprise using the Dell Mobile Device Manager. Please contact your Company's IT Department before...



#### Kaseya MDM

KASEYA / HERRAMIENTAS

★★★★★ (6)

INSTALAR

Tap on "Free", then tap "OK". Tap on "Free", then "OK". If you are not doing internal testing, please do not download this, as you will not be able to use it. If you...



#### CLOMO MDM for Android

I3SYSTEMS,INC. / NEGOCIOS

★★★★★ (2)

INSTALAR

組織内の Android / iOS デバイスの管理にお悩みですか? CLOMO MDM では、組織で利用中の複数デバイスを、一つのパネルで統合管理が可能です。 ■ CLOMO MDM 概要 CLOMO MDMは、企業や法人が利用されている iOS / Android デバイスを統合的に管理・運用を実現するクラウドサービスです。管理...



#### MDM Client

FROMDISTANCE / NEGOCIOS

★★★★★ (2)

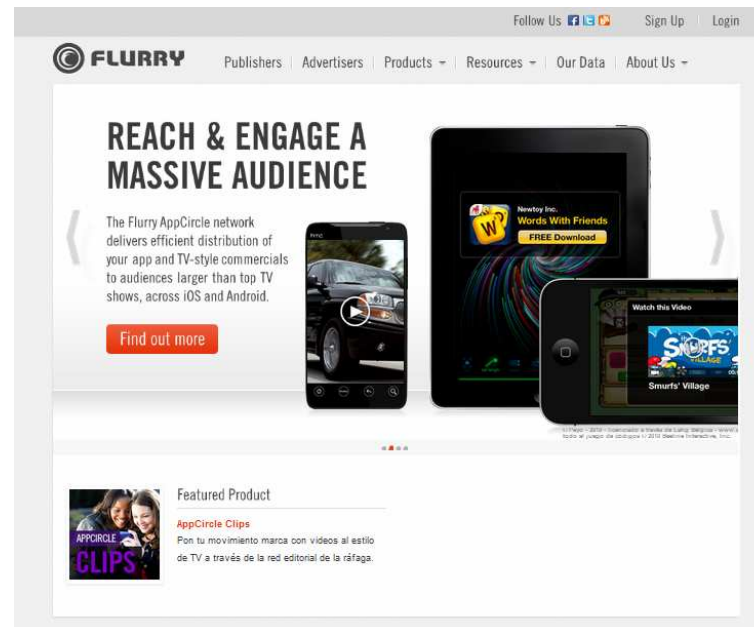
INSTALAR

MDM Client for Android makes possible OTA management of Android devices from an MDM Server (required). The server can be installed on an enterprise's premises or hoste...

# EJEMPLO DE APLICACIÓN CON FLURRY

## 🎯 *Flurry*

- 🎯 *Flurry Analytics* es a algo así como el *Google Analytics* de las aplicaciones móviles, aunque mucho más intrusivo y captador de mucha más información del usuario y su relación con el uso de la aplicación móvil.



The screenshot shows the Flurry website homepage. At the top, there is a navigation bar with the Flurry logo, links for Publishers, Advertisers, Products, Resources, Our Data, and About Us, and a sign-up/login section. The main content area features a large headline: "REACH & ENGAGE A MASSIVE AUDIENCE". Below this, a sub-headline reads: "The Flurry AppCircle network delivers efficient distribution of your app and TV-style commercials to audiences larger than top TV shows, across iOS and Android." A red button labeled "Find out more" is positioned below the sub-headline. To the right of the text, there are three mobile devices (a smartphone and two tablets) displaying various app interfaces, including one for "Words With Friends" and another for "Smurfs' Village". Below the main content, there is a "Featured Product" section for "AppCircle Clips", which includes a small image and a brief description: "Pon tu movimiento marca con videos al estilo de TV a través de la red editorial de la ráfaga."

# EJEMPLO DE APLICACIÓN CON FLURRY

## 🎯 *¿Cómo insertar Flurry en nuestra aplicación?*

1. Descargar Flurry Android SDK
2. Añadir FlurryAgent.jar
3. Configurar el fichero AndroidManifest.xml
4. Añadir las llamadas a la funciones
5. Configurar opciones

# EJEMPLO DE APLICACIÓN CON FLURRY

Para que funcione Flurry correctamente es necesario habilitar un permiso:

**`android.permission.INTERNET`**

con el fin de poder enviar los datos estadísticos a los servidores de Flurry.

Otros permisos opcionales que se pueden habilitar son:

**`android.permission.ACCESS_COARSE_LOCATION` o  
`android.permission.ACCESS_FINE_LOCATION`**

Con estos permisos es posible obtener datos locales (ciudad) donde se descarga y utiliza la aplicación. En el caso que no se soliciten estos permisos sólo se obtienen la información del país de descarga.

Esta configuración de permisos se realiza dentro del fichero del proyecto:

***AndroidManifest.xml.***

# EJEMPLO DE APLICACIÓN CON FLURRY

Y luego las llamadas a las funciones

```
// ////////////////////////////////////////  
// / para las estadísticas de la aplicación  
// con Flurry  
public void onStart() {  
    super.onStart();  
    FlurryAgent.onStartSession(this, "Cuentos"); //el id de flurry de Cuentos  
    // your code  
}  
  
public void onStop() {  
    super.onStop();  
    FlurryAgent.onEndSession(this);  
    // your code  
}  
  
// ////////////////////////////////////////
```

---

# EJEMPLO DE APLICACIÓN CON FLURRY

- ① A continuación se mostrarán los resultados proporcionados por Flurry para una aplicación concreta publicada en el Market de Android: **Cuentos**.
- ① La aplicación es muy simple, consiste en una selección de cuentos infantiles en español ubicados en Youtube

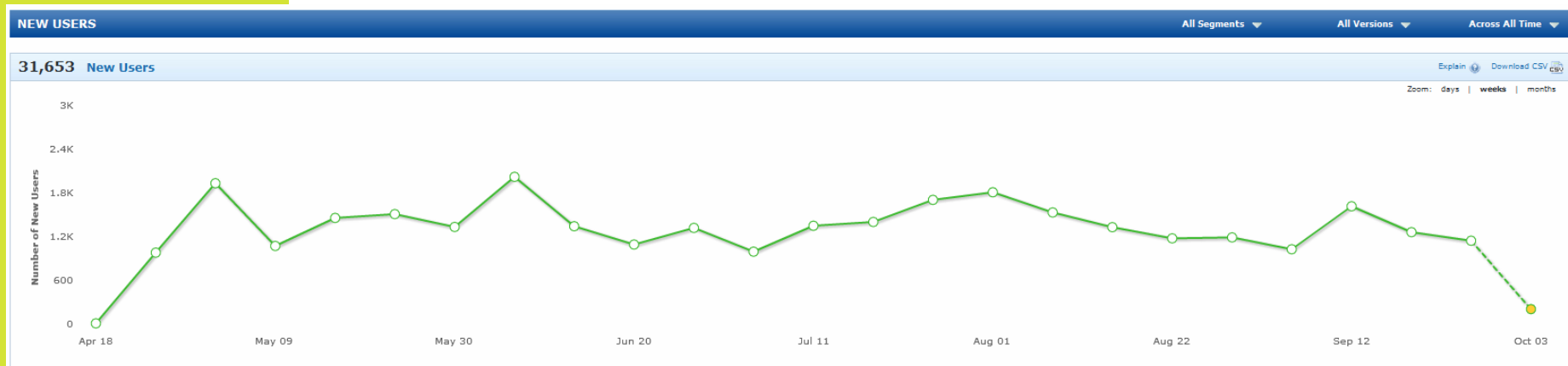
# EJEMPLO DE APLICACIÓN CON FLURRY

The screenshot shows the Android Market interface for the 'Cuentos' application. The page is divided into several sections:

- Header:** 'Android Market' logo and a search bar with the text 'Buscar'.
- Breadcrumbs:** 'Android Market > Educación > Cuentos'.
- Application Card:** Features the app icon (a TV with a rainbow screen), the name 'Cuentos' by 'pekeplay', a 5-star rating from 25 reviews, and an 'INSTALAR' button.
- More from Developer:** A list of other apps by 'PEKEPLAY':
  - Pekephone:** 5 stars (7 reviews), Gratis.
  - Numeros:** 5 stars (4 reviews), Gratis.
  - Abc Pekeplay:** 5 stars (2 reviews), Gratis.
- Other apps consulted:** 'Clan RTVE' by 'RTVE MEDIOS INTERACTIVOS' with a 5-star rating (524 reviews).
- Information Tabs:** 'INFORMACIÓN GENERAL', 'VALORACIÓN DE LOS USUARIOS (11)', 'NOVEDADES', and 'PERMISOS'.
- Description:** 'Cuentos infantiles en español.' with bullet points: '\* Selección de cuentos populares en español', '\* Vídeos cortos de Youtube', '\* Selección manual de los videos para mayor seguridad', and '\* Diversión y aprendizaje'.
- Selected Stories:** '\* Los tres cerditos y el lobo', '\* El patito feo', and '\* Cenicienta'.
- Screen Captures:** Two images showing the app's interface. The first is a menu with options like 'Los 3 cerditos y el lobo', 'El patito feo', 'Cenicienta', etc. The second is a YouTube video player showing a scene from 'Los Tres Cerditos y El Lobo - Cuento Infantil'.
- Right Sidebar:** Social sharing options (+7, 2, Tweet), 'ACERCA DE ESTA APLICACIÓN', 'PUNTAJACIÓN: ★★★★★ (25)', 'ACTUALIZADA EL: mayo 7, 2011', 'VERSIÓN ACTUAL: 1.1', 'REQUIERE ANDROID: 2.2 o superior', 'CATEGORÍA: Educación', 'INSTALACIONES: 10.000 - 50.000', a line graph for 'últimos 30 días', 'TAMAÑO: 158k', 'PRECIO: Gratis', and 'CLASIFICACIÓN DE CONTENIDO: Nivel de madurez bajo'.

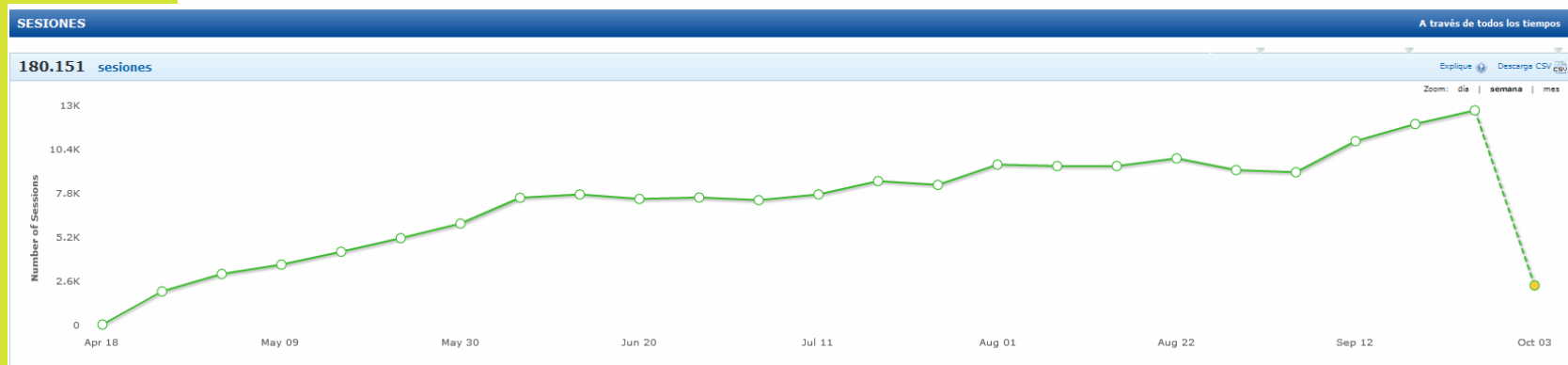
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**USO: Número de nuevos usuarios a la semana**



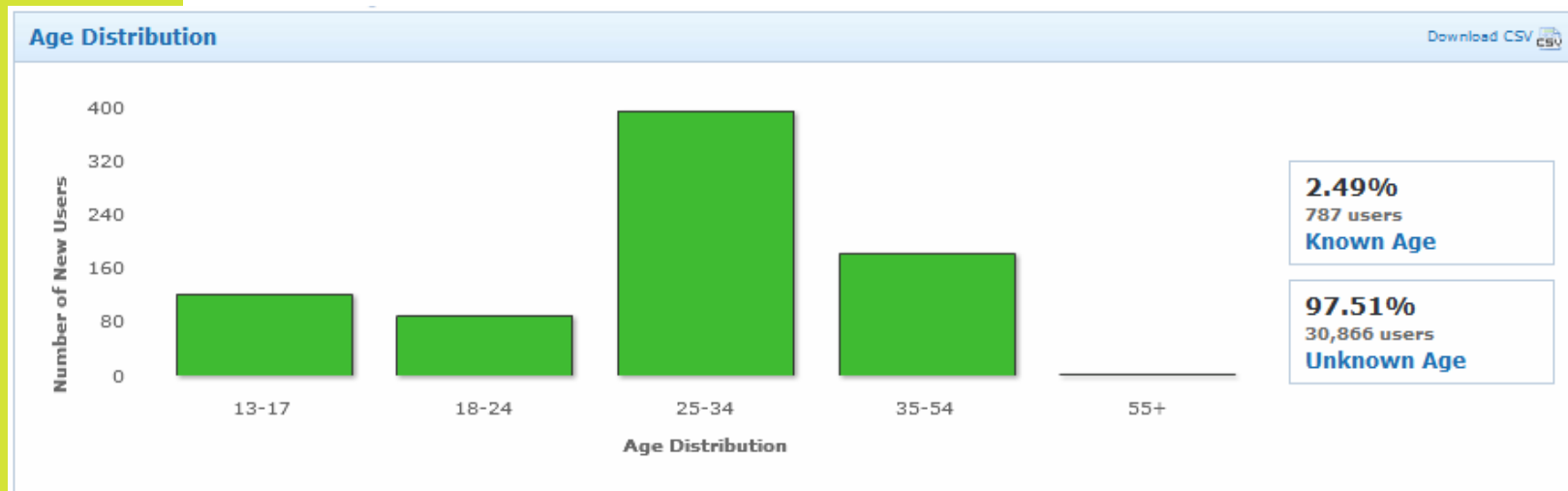
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

USO: Número de sesiones a la semana



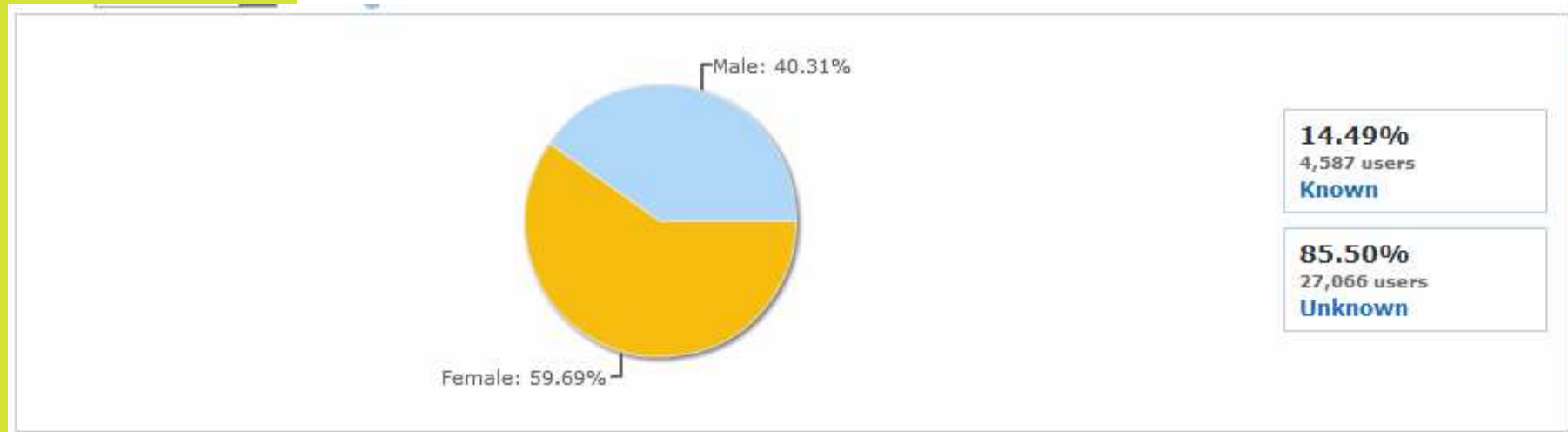
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**AUDIENCIA:** *Distribución de los usuarios por edades*



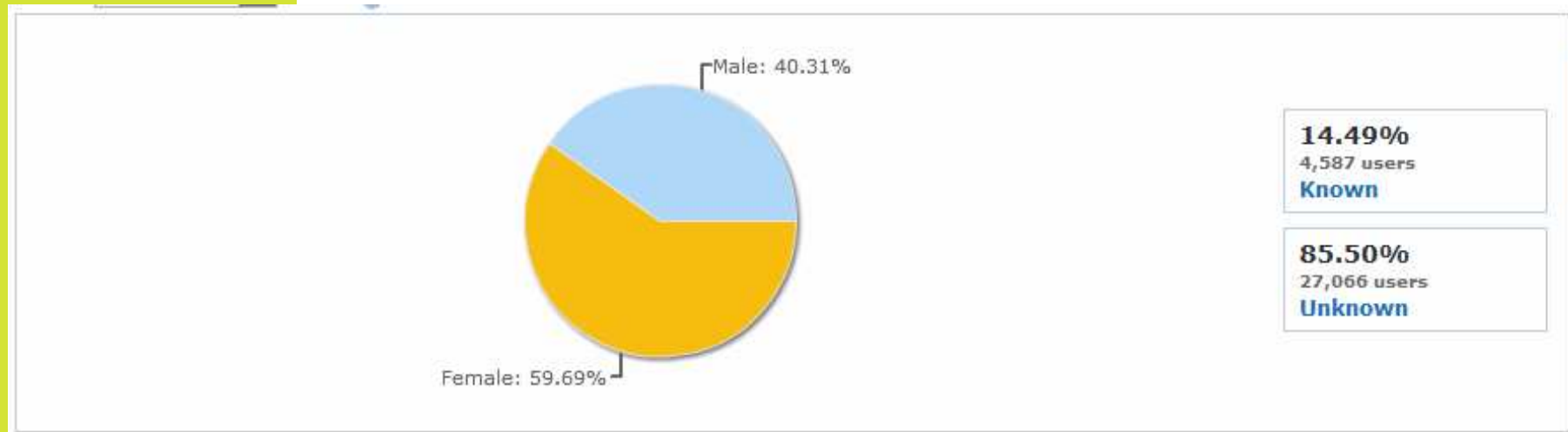
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**AUDIENCIA:** *Distribución de los usuarios por sexo*



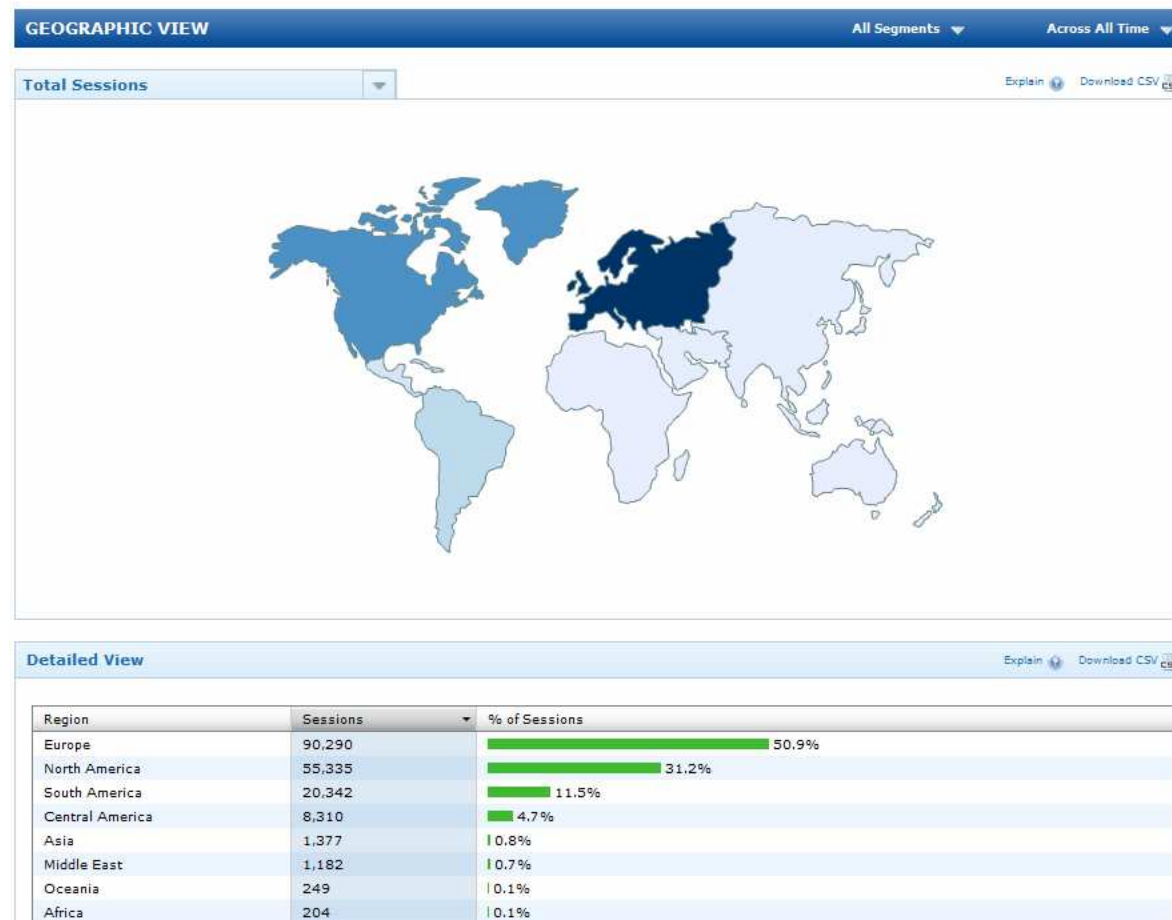
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**AUDIENCIA:** *Distribución de los usuarios por sexo*



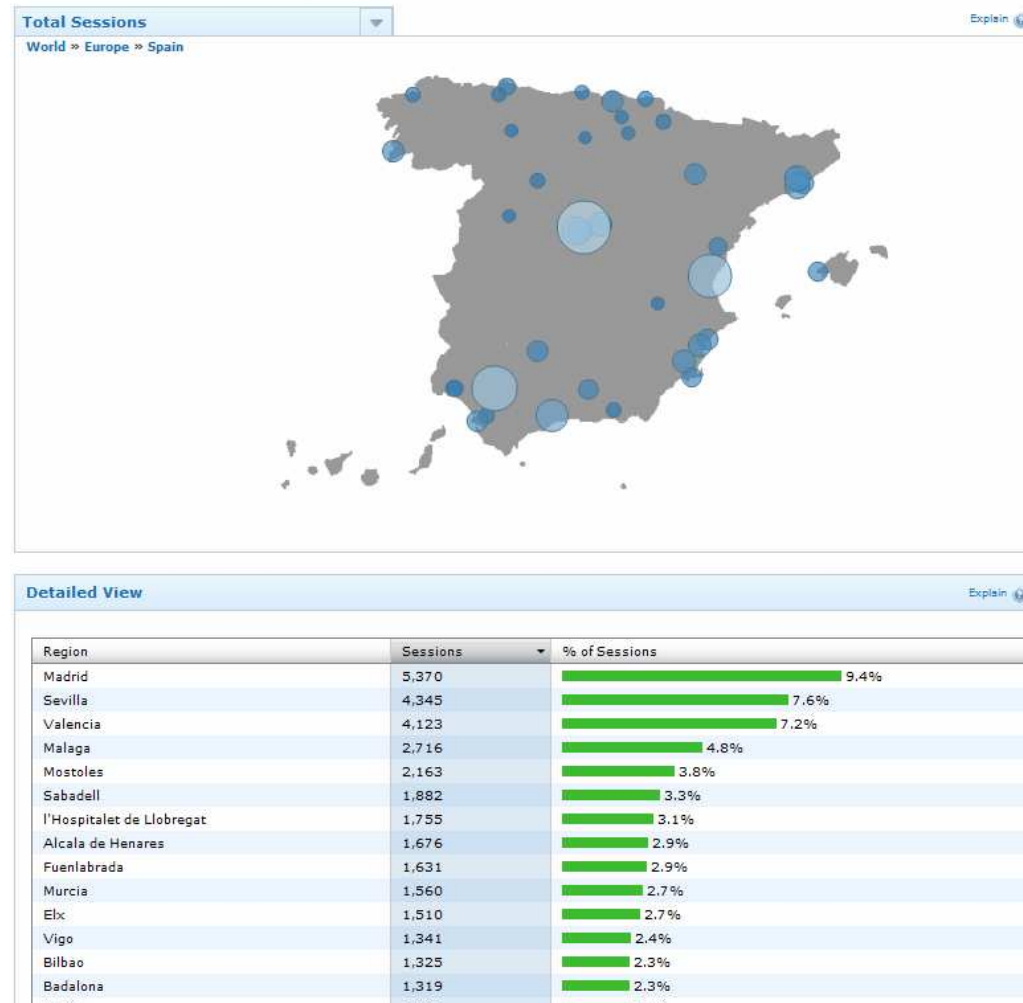
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**AUDIENCIA:** *Distribución de los descargas por continentes*



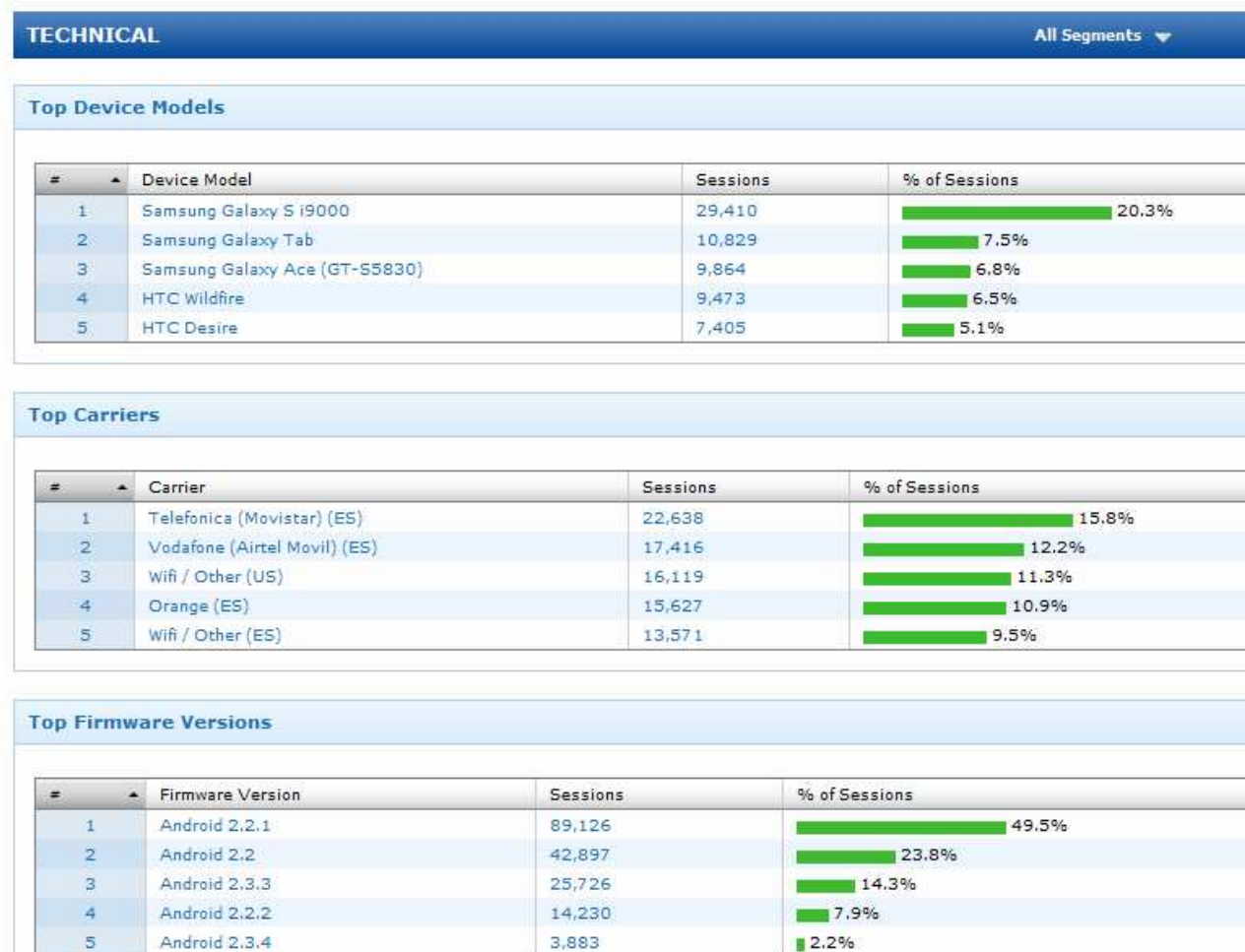
# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

**AUDIENCIA:** *Distribución de las descargas por ciudades españolas*



# EJEMPLO DE APLICACION CON FLURRY - RESULTADOS

## DATOS TÉCNICOS



# CONCLUSIONES

- ① Cada día se venden más smartphones y se lanzan al mercado cientos de nuevas aplicaciones de todo tipo. Este crecimiento ha hecho surgir también problemas en la seguridad de estos dispositivos.
- ② En este trabajo se enumeran los principales casos de malware que han surgido. Y también se proponen las principales soluciones para luchar contra ellos (el uso de antivirus, principalmente).
- ③ A modo de ejemplo, se ha mostrado cómo realizar una aplicación con un código de recopilación de datos intrusivo que revela datos sorprendentes de la distribución de una aplicación entre los usuarios. Es una pequeña muestra del control al que nos someten los desarrolladores de aplicaciones.

# CONCLUSIONES

- © La evolución del mercado de los terminales en el futuro inmediato y las nuevas aplicaciones decidirán el contexto de la seguridad de estos dispositivos que actualmente parece muy relajada. La mayoría de los usuarios de smartphones creemos que son unos dispositivos más individuales y protegidos que los típicos ordenadores de sobremesa, nada más lejos de la realidad. El malware para smartphones ya es una realidad y hay que aceptar esta amenaza y aprender a defenderse de ella.



# MALWARE EN DISPOSITIVOS MÓVILES ANDROID

Máster en Administración, Comunicaciones y Seguridad Informática