GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza2
INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía sobre seguridad y privacidad de las herramientas de geolocalización

OBSERVATORIO INTECO

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Marzo 2011

La "Guía sobre seguridad y privacidad de las herramientas de geolocalización" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Eduardo Álvarez Alonso

Susana de la Fuente Rodríguez

Laura García Pérez

El **Instituto Nacional de Tecnologías de la Comunicación** (INTECO), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones en las siguientes líneas: Seguridad Tecnológica, Accesibilidad, Calidad TIC y Formación.

El Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

Índice

1. Introducción

Se denomina “geolocalización” al conjunto de tecnologías que combinan la georreferenciación de elementos del mundo real con la información obtenida a través de una conexión a Internet.

Es una de las manifestaciones más populares del desarrollo actual de las Tecnologías de la Información y las Comunicaciones (TIC), y que está experimentando un auge relevante en los últimos tiempos.

Ilustración 1: Georreferenciación de contenido multimedia en un mapa

En particular, los dispositivos móviles se prestan especialmente a la aplicación de las tecnologías de geolocalización. Por un lado, se han desarrollado múltiples mecanismos que permiten la localización geográfica de un dispositivo (bien mediante la tecnología GPS[1], redes Wi-Fi inalámbricas, o las propias redes de telefonía móvil), mientras que el desarrollo de la banda ancha móvil permite la conexión permanente a Internet para los denominados “teléfonos inteligentes” (smartphones).

Además, es importante reseñar el estrecho vínculo desarrollado entre las tecnologías de geolocalización y las redes sociales, comunidades colaborativas, y otro tipo de servicios ligados a la llamada Web 2.0. Los usuarios tienen la oportunidad de integrar

[1] GPS: *Global Positioning System* o Sistema de Posicionamiento Global.

prácticamente cualquier tipo de información georreferenciada en populares redes sociales como por ejemplo Facebook[2] o Twitter[3] o Tuenti[4], así como utilizar nuevas redes sociales específicamente diseñadas y desarrolladas sobre las tecnologías de geolocalización, como las populares Foursquare[5] y Gowalla[6], entre otras.

Las aplicaciones de geolocalización online permiten, desde cualquier dispositivo conectado a Internet (bien se trate de un dispositivo móvil, ordenador portátil, equipo de sobremesa, etc.), la obtención de todo tipo de información en tiempo real, así como la localización de la misma en el mapa con total precisión.

La combinación de esta tecnología con los sistemas de almacenamiento en la nube[7], además, permite la sincronización automática de información entre dispositivos heterogéneos.

Las funcionalidades de este tipo de aplicaciones van desde algo tan simple como la búsqueda de una estación de servicio cercana, hasta algo tan complejo como la obtención de rutas de navegación en coche, con información del tráfico en tiempo real, y sincronización automática de puntos de interés mediante almacenamiento en la nube; pasando por aplicaciones tan novedosas como la realidad aumentada.

La extensión de estas tecnologías y su demanda, no obstante, lleva asociada la problemática de la naturaleza de la información – frecuentemente privada o sensible – asociada a ellas. Por ello, es importante tomar especial conciencia de los aspectos relacionados con la seguridad y la privacidad, de forma que sea posible ejercer un uso responsable de las herramientas de geolocalización, y asegurar su pleno disfrute.

[2] Disponible en: http://www.facebook.com/places

[3] Disponible en: http://twitter.com/

[4] Disponible en: http://sitios.tuenti.com

[5] Disponible en: http://foursquare.com/

[6] Disponible en: http://gowalla.com/

[7] El término almacenamiento en la nube hace referencia al sistema que permite a los usuarios almacenar toda su información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier sistema con acceso a Internet.

2. ¿Qué es la geolocalización?

2.1 ASPECTOS GENERALES

El término geolocalización comprende la conjunción de una serie de tecnologías que tienen como fin la utilización de información vinculada a una localización geográfica del mundo real.

Se pueden distinguir principalmente **tres componentes** asociados a todo proceso de geolocalización.

1) **Un dispositivo hardware**, que actuará como plataforma en la que se desarrollará el proceso de geolocalización. Puede tratarse de un ordenador de sobremesa, un ordenador portátil, un dispositivo móvil, un navegador GPS, una cámara de fotos, etc. En los casos en que la localización física del dispositivo interviene como un elemento clave del proceso, el dispositivo hardware incorpora los mecanismos necesarios para permitir dicha localización (por ejemplo, un receptor GPS).

2) **Un programa software**, que ejecutará el proceso de geolocalización según su implementación. Este software se ejecutará en la plataforma del dispositivo hardware, y se apoyará en éste para llevar a cabo la búsqueda de información, la determinación de localizaciones geográficas, y la asociación de ambos elementos.

3) **Una conexión a Internet**, que actuará como medio de obtención e intercambio de información y, en ocasiones, como sistema de almacenamiento y procesamiento de la misma (según el modelo en "*la nube*"). Excepcionalmente, pueden ejecutarse procesos de geolocalización sin utilizar una conexión a Internet (modo fuera de línea), cuando los datos necesarios se encuentren cargados con antelación en la memoria del dispositivo.

Se pueden distinguir principalmente **tres categorías de usos comunes** para las tecnologías de geolocalización.

1) La localización física de un objeto o individuo en un sistema de coordenadas (proceso de **georreferenciación**), para posteriormente acceder a información específica. Un ejemplo de esto sería la utilización de un sistema de navegación mediante GPS.

2) La búsqueda de información y su localización física en un sistema de coordenadas (proceso de **geocodificación**). Un ejemplo de esto sería la utilización de un servicio de mapas para buscar museos en una ciudad determinada.

3) La adición de información geográfica a un contenido generado (proceso de **geoetiquetado**), usualmente como paso posterior a un proceso de georreferenciación. Un ejemplo de esto sería la creación de una fotografía, incluyendo en sus metadatos[8] las coordenadas del lugar en que fue tomada.

Dada la importancia del proceso de georreferenciación, y debido a que juega un papel importante en la gran mayoría de las aplicaciones de geolocalización, en ocasiones se utilizan ambos términos indistintamente.

Las tecnologías de georreferenciación más relevantes son las siguientes.

- **GPS**. Mediante la utilización de la red de satélites GPS, es posible georreferenciar un dispositivo con una precisión de entre 1 y 15 metros (en torno a los 3 metros en el 95% de las ocasiones). Es necesario contar con un aparato receptor de GPS, ya que los satélites actúan únicamente como emisores de señal, siendo imposible localizar a un receptor concreto desde la red GPS.

- **Redes Wi-Fi inalámbricas**. Gracias a la utilización de enormes bases de datos es posible georreferenciar un dispositivo con una precisión proporcional al alcance de una red Wi-Fi inalámbrica, típicamente entre 30 y 100 metros. El funcionamiento de este sistema depende de la cobertura del servicio en el área geográfica, así como a la actualización de sus bases de datos. Además, el hecho de consultar dichas bases de datos implica el envío de la información de geolocalización a las mismas.

- **Redes móviles**. Todo terminal conectado a una red móvil de telefonía y/o datos puede ser georreferenciado, con una precisión que depende directamente del radio de cobertura del dispositivo (entre 50 y 500 metros en núcleos urbanos).

- **Dirección IP**. El método más impreciso, utiliza bases de datos de asignación de direcciones IP a proveedores y su distribución geográfica. En la práctica, no es un mecanismo de localización válido para establecer georreferenciación, excepto en ocasiones muy específicas donde la precisión no es un factor importante.

Las **aplicaciones prácticas** de las tecnologías de geolocalización son muy variadas y, al tratarse de un entorno relativamente novedoso y emergente, las posibilidades de futuro del mismo son muy prometedoras.

- En el **ámbito personal**, existen multitud de aplicaciones relacionadas con el ocio, que van desde las redes sociales (tradicionales como Facebook, o específicas

[8] Los metadatos pueden definirse como un conjunto de datos que definen o caracterizan a una cierta información a la que están asociados.

como Foursquare) hasta las utilidades (navegadores GPS, trazado de rutas en mapas, senderismo, etc.).

- En el **ámbito profesional y empresarial**, se encuentran aplicaciones que van desde la seguridad (localización de vehículos siniestrados, aplicación de georreferenciación a seguros de automóviles para conductores noveles, localización de vehículos robados, etc.) hasta los estudios de mercado (por ejemplo, mediante estadísticas generadas por redes sociales como Foursquare).

2.2 TERMINOLOGÍA SOBRE GEOLOCALIZACIÓN

- **Latitud y longitud.** Coordenadas que miden el ángulo entre un punto cualquiera y su referencia (el ecuador para latitud, el meridiano de Greenwich para la longitud). En la práctica, la combinación de ambos ángulos permiten expresar cualquier posición en la superficie de la Tierra.

- **Georreferenciación.** Proceso de definición de un objeto en un espacio físico, mediante el cálculo de su localización en un sistema de coordenadas. En su aplicación más común, localiza objetos físicos (personas, lugares, etc.) en unas coordenadas geográficas.

- **Geocodificación.** Proceso de asignación de unas coordenadas geográficas (típicamente latitud y longitud) a un punto del mapa (lugares, direcciones, etc.). Esto permite la localización de dicho punto en un sistema de información geográfica.

- **Geocodificación inversa.** Proceso inverso a la geocodificación, y consistente en la obtención, a partir de una coordenada geográfica, de una localización legible por humanos (dirección, nombres de lugares, etc.).

- **Geoetiquetado.** Proceso de adición de información geográfica a los metadatos de un fichero (usualmente de imagen, audio o vídeo), de forma que se permite su posterior georreferenciación.

- **Geomática.** Conjunto de dominios del conocimiento orientados a la captura, procesamiento, almacenamiento, y difusión de información geográfica. Las tecnologías de geolocalización se inscribirían dentro de la Geomática.

- **GPS[9].** Sistema de Posicionamiento Global (*Global Positioning System*). Sistema global de navegación por satélite, que permite la georreferenciación de objetos en la superficie terrestre con gran precisión (metros, centímetros para sistemas diferenciales). Su funcionamiento se basa en una constelación de 32 satélites en órbita geocéntrica media, mantenidos y operados por el Departamento de Defensa de los Estados Unidos.

- **A-GPS.** GPS Asistido (*Assisted GPS*). Mejora del sistema GPS que, sirviéndose de *Servidores de Asistencia* (para el modo en línea) o de información precargada (para el modo fuera de línea), permite acelerar el proceso de conexión a los satélites, así como mejorar el proceso de georreferenciación en condiciones de baja señal.

- **Triangulación.** Método geométrico basado en la trigonometría de triángulos que, usando como referencia la posición de varios puntos conocidos, permite determinar de forma precisa la posición de otro desconocido. En concreto, y en el caso del sistema GPS, se necesitan tres satélites para determinar la posición de un receptor, si bien en la práctica se utiliza un cuatro para la corrección de errores de precisión.

[9] Fuente: CC-BY-SA http://www.flickr.com/photos/aburt/

3. Aplicaciones de geolocalización

Dentro del conjunto de aplicaciones que hacen uso de las tecnologías de la geolocalización, se pueden distinguir principalmente dos grupos, en función de la interacción del usuario con dicha aplicación:

- **Las aplicaciones online** -generalmente aplicaciones Web- utilizadas **desde cualquier tipo de dispositivo**. El usuario solicita una localización y la aplicación responde con información ya existente en la Red.

- **Las aplicaciones diseñadas específicamente para su uso en dispositivos móviles**. En estos casos, la localización del dispositivo móvil se utiliza como una variable más del sistema a la hora de calcular la información solicitada.

A continuación, se analizan ambos conjuntos de aplicaciones, desglosándolos en categorías según su ámbito de actuación, y enunciando algunos ejemplos ilustrativos.

3.1 APLICACIONES ONLINE

Se entiende por “aplicación online” aquella cuya funcionalidad puede ser utilizada mediante una conexión a Internet. Típicamente, se trata de servicios web accesibles mediante un navegador web estándar, si bien en ocasiones se ofrece como una aplicación independiente que debe ser instalada en el sistema operativo anfitrión.

Estas aplicaciones, mediante el uso de las tecnologías de geolocalización, interrelacionan la información existente en la Red, con aquella proporcionada por el usuario.

Típicamente, estas aplicaciones no realizan procesos de georreferenciación, sino que funcionan nutriéndose de información ya existente, y ofreciendo servicios de geocodificación y geocodificación inversa.

3.1.1 Mapas

En este conjunto se engloban aquellas aplicaciones destinadas a la búsqueda de información en mapas.

Entre los servicios típicos de este tipo de aplicaciones se encuentran la búsqueda de información y su geocodificación inversa, la consulta de diversos tipos de mapas (geográficos, físicos o callejeros), el cálculo de rutas (a pie o utilizando vehículos) o la creación de mapas personalizados.

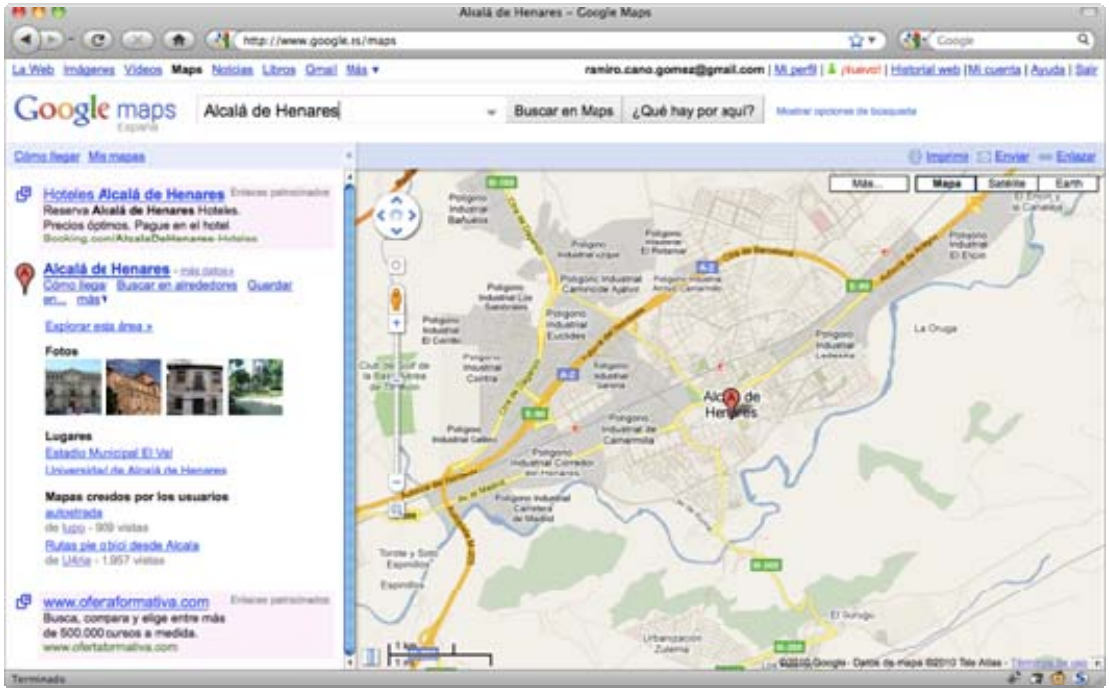


Ilustración 2: Aplicación de mapas Google Maps

Usualmente, la utilización de estos servicios conlleva la asociación de una cuenta de usuario, permitiendo almacenar información como puntos de interés, mapas personalizados, etc.

Algunos ejemplos de aplicaciones de mapas son:

- **Google Maps**[10]. Posiblemente el servicio de mapas más extendido, propiedad de la compañía Google. Integra otras funcionalidades de la compañía e información de diversos servicios mediante el uso de las capas adicionales de Google Labs[11].

- **Google Earth**[12]. Se trata de un Sistema de Información Geográfica (SIG) propiedad de Google, que combina las funcionalidades de diversos servicios con recreaciones en 3D de la superficie del planeta Tierra, de la Luna, e incluso Marte.

- **Bing Maps**[13]**.** Contrapartida de la compañía Microsoft al servicio de Google Maps. Ofrece funcionalidades muy similares, y tecnologías equivalentes a la mayoría de las integradas por Google.

3.1.2 Imágenes y geoetiquetado

Este conjunto de aplicaciones de geolocalización utiliza imágenes como medio de transmisión de la información. Las imágenes son capturadas y geoetiquetadas por algún tipo de dispositivo móvil, para posteriormente incluirse en una base de datos que permita su búsqueda y geocodificación como un servicio online.

Algunos ejemplos de aplicaciones de imágenes y geoetiquetado son:

- **Google Street View**[14]. Característica de Google Maps y Google Earth, que permite la visualización en dichos servicios de panorámicas de las calles. En septiembre de 2010, incluía imágenes de 30 países diferentes, algunos de ellos -como España- con una cobertura casi completa.

- **Street Slide**. Característica de Bing Maps análoga a Google Street View. En octubre de 2010, su cobertura se limitaba a zonas de Estados Unidos y Canadá.

- **Panoramio**[15]. Servicio de compartición de fotografías realizadas, geoetiquetadas y georreferenciadas por los propios usuarios. Pertenece a Google.

- **Flickr Maps**[16]. Servicio que permite la búsqueda de fotografías geoetiquetadas. En octubre de 2010, el servicio contaba con más de 122 millones de fotografías.

[10] Disponible en: http://maps.google.es/maps?hl=es&tab=wl

[11] Disponible en: http://www.googlelabs.com/

[12] Disponible en: http://earth.google.es/

[13] Disponible en: http://www.bing.com/maps/

[14] Disponible en: http://maps.google.com/intl/es/help/maps/streetview/

[15] Disponible en: http://www.panoramio.com/

[16] Disponible en: http://www.flickr.com/map/

3.1.3 Redes sociales

En este conjunto se engloban las aplicaciones de geolocalización relacionadas con redes sociales, la gran mayoría de las cuales se presentan en forma de añadidos a las redes sociales tradicionales, y permiten integrar herramientas de georreferenciación mediante la utilización de dispositivos móviles.

No obstante, existen algunos ejemplos de redes sociales geolocalizadas orientadas al entorno online, y no circunscritas únicamente a los dispositivos móviles:

- **Dopplr**[17]. Red social destinada a la organización de viajes, recorridos y puntos de reunión. Permite definir viajes de placer o de trabajo, compartir dicha información, recibir avisos en las estancias, así como recibir consejos de otros usuarios.

- **Plazes**[18]. Red social destinada a compartir la ubicación y actividad de sus usuarios.

- **Fire Eagle**[19]. Red social propiedad de Yahoo! que actúa como almacén de localizaciones de sus usuarios.

3.2 APLICACIONES PARA DISPOSITIVOS MÓVILES

La mayoría de las aplicaciones de geolocalización se enmarcan dentro del ámbito de las tecnologías móviles. La penetración en el mercado de los denominados "teléfonos inteligentes" (*smartphones*), así como la extensión de las tecnologías de banda ancha móvil, han ayudado al crecimiento de este tipo de aplicaciones, así como de las comunidades de usuarios que las utilizan y respaldan.

Según datos recogidos en marzo de 2010[20], la proporción de terminales inteligentes en España es del 28,3% y la de terminales 3G es la más alta en relación a los principales países europeos (Reino Unido, Francia, Italia y Alemania) con un 53,3%.

Dentro del mercado de los teléfonos inteligentes, se pueden encontrar los siguientes sistemas operativos, ordenados por cuota de mercado[21]: Symbian OS (41,2%), BlackBerry OS de RIM (18,2%), Android de Google (17,2%), iOS de Apple (14,2%), Windows Mobile de Microsoft (5,0%), Linux (2,4%) y otros (1,8%).

[17] Disponible en: http://www.dopplr.com/

[18] Disponible en: http://plazes.com/

[19] Disponible en: http://fireeagle.yahoo.net/

[20] Informe *UK Leads European Countries in Smartphone Adoption with 70% Growth in Past 12 Months*, publicado por comScore. Disponible en: http://www.comscore.com/Press_Events/Press_Releases

[21] Fuente: *Competitive Landscape: Mobile Devices, Worldwide, 2Q10* Disponible en: http://www.gartner.com/it/page.jsp?id=1421013

Las aplicaciones de geolocalización para dispositivos móviles suelen hacer uso típicamente de la georreferenciación del propio dispositivo, bien para geoetiquetar contenido multimedia, o bien para llevar a cabo procesos de geocodificación o geocodificación inversa.

3.2.1 Mapas

En este conjunto se engloban aquellas aplicaciones destinadas a la búsqueda de información en mapas. La posición geográfica del usuario se utiliza como un elemento relevante en el proceso de búsqueda de información. Asimismo, también es habitual que estas aplicaciones se encuentren integradas con algún servicio online (e incluso aplicaciones de escritorio), permitiendo la sincronización de información en la nube.

Algunos ejemplos de aplicaciones de mapas para dispositivos móviles son:

- **Google Maps**[22]. Disponible para sistemas Android, Blackberry, iOS, Symbian y Windows Mobile (si bien las funcionalidades difieren), esta aplicación integra el servicio Google Maps y la mayoría de sus funcionalidades en el dispositivo móvil.

Ilustración 3: Aplicación de Google Maps 4.5.1 en Android 2.2

- **Google Earth**. Disponible para algunos sistemas Android e iPhone, esta aplicación integra el servicio Google Earth y ciertas de las funcionalidades presentes en la aplicación de escritorio.

- **MyTracks**[23] (Android), **Map My Tracks**[24] (iPhone, Symbian, Blackberry, Windows Mobile). Aplicaciones que permiten grabar recorridos geolocalizados, así como integrarlos en otros servicios y redes sociales.

[22] Disponible en: http://www.google.es/mobile/maps/

[23] Disponible en: http://mytracks.appspot.com/

[24] Disponible en: http://www.mapmytracks.com/

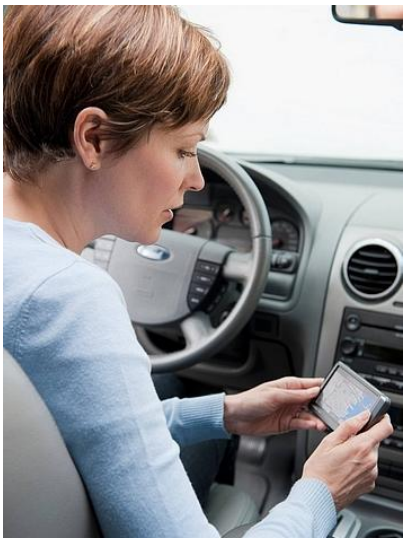
3.2.2 Navegación GPS

En este conjunto se engloban aquellas aplicaciones destinadas a la navegación paso a paso -a pie o en vehículos- haciendo uso de un dispositivo GPS. Su principal aplicación se encuentra en el mundo de la automoción.

Algunos ejemplos de aplicaciones de navegación GPS para dispositivos móviles son:

- **Tom Tom Navigator**[25]. Posiblemente el navegador GPS más extendido y utilizado, funciona sobre plataformas hardware propias (dispositivos embebidos), así como en iOS, Windows Mobile, Symbian (versión descontinuada). Soporta varios idiomas, mapas para distintas zonas geográficas, puntos de interés personalizados, e información del tráfico en tiempo real (con suscripción).

- **Google Maps Navigator**[26]. Navegador GPS de Google, integrado con los mapas y funcionalidades del servicio Google Maps, y que facilita información del tráfico en tiempo real. Requiere de una conexión de datos para el uso de mapas, y en octubre de 2010 se encontraba disponible únicamente para la plataforma Android.



- **CoPilot Live**[27]. Sistema de navegación GPS que funciona sobre plataformas hardware propias, siendo también compatible con iOS, Android y Windows Mobile.

- **Nokia OviMapas**[28]. Navegador GPS de Nokia, compatible únicamente con algunos dispositivos con sistema operativo Symbian del fabricante finlandés.

- **Waze**[29]. Sistema de navegación GPS con información colaborativa sobre el estado del tráfico e incidencias en la carretera. Está disponible para iOs, Android, Windows Mobile y Symbian.

[25] Disponible en: http://www.tomtom.com/

[26] Disponible en: http://www.google.es/intl/es_ALL/mobile/navigation/

[27] Disponible en: http://www.alk.com/copilot/

[28] Disponible en: http://www.nokia.es/ovi/mapas

[29] Disponible en: http://world.waze.com/

3.2.3 Redes sociales

En este conjunto se engloban aquellas aplicaciones cuya finalidad principal consiste en la integración de información en redes sociales, bien tradicionales (como Facebook o Twitter) o bien específicas para aplicaciones móviles. Estas aplicaciones son las que mayor difusión presentan dentro del ámbito de la geolocalización en dispositivos móviles.

Algunos ejemplos son:

- **Facebook Places**[30]. Aplicación de la red social Facebook que, haciendo uso de la georreferenciación de dispositivos móviles, permite compartir la posición del usuario con sus amigos.

- **Twitter Places**[31]. Funcionalidad de la red social Twitter que permite a los usuarios, mediante georreferenciación o especificación explícita, definir el lugar exacto asociado a un mensaje concreto. Incluye integración con las redes sociales Foursquare y Gowalla.

- **Foursquare**[32]. Red geosocial basada en la georreferenciación de sus usuarios, que pueden hacer "*check-in*" en diversos lugares. Con dicha información se puede participar en juegos sociales, promociones y eventos especiales. Su aplicación está disponible para iOS, Android, Blackberry, Windows Phone 7 y webOS.

- **Google Latitude**[33]. Servicio de geolocalización para dispositivos móviles de Google. El servicio se encuentra integrado con la mayoría de los servicios de Google, y es compatible con Android, iOS, Blackberry, Windows Mobile y Symbian.

- **Gowalla**[34]. Red geosocial basada en la georreferenciación de usuarios, y con un funcionamiento básico muy similar a Foursquare. Está disponible para Android, iOS, webOS y BlackBerry, así como a través de su página web.

[30] Disponible en: http://www.facebook.com/places/

[31] Disponible en: http://support.twitter.com/entries/194473-twitter-places-and-how-to-use-them

[32] Disponible en: http://foursquare.com/

[33] Disponible en: http://m.google.com/latitude

[34] Disponible en: http://gowalla.com/

3.2.4 Puntos de interés

En este conjunto se engloban las aplicaciones que permiten al usuario localizar lugares de interés cercanos (restaurantes, tiendas, etc.) a partir de su posición geográfica.

Algunos ejemplos de aplicaciones de puntos de interés para dispositivos móviles son:

- **Bliquo**[35]. Servicio que se define como un "buscador de ocio urbano", y que permite consultar directorios especializados de restaurantes, bares, discotecas, etc. Incorpora un componente social, al permitir la creación y consulta de comentarios y evaluaciones. Está disponible para iOS y Android.

- **AroundMe**[36]. Servicio de búsqueda de puntos de interés para iOS.

- **Buzzd**[37]. Red geosocial de búsqueda de puntos de interés. Está disponible para Android, iOS, Blackberry, y como servicio de red social a través de su página web.

- **Google Places Directory**[38]. Servicio de búsqueda de puntos de interés de Google. Permite su integración en Google Maps, así como la definición de categorías personalizadas. Está disponible para Android.

Ilustración 4: Google Places Directory 1.0.24 en Android 2.2

3.2.5 Realidad aumentada

En este conjunto se engloban aquellas aplicaciones que, haciendo uso de la georreferenciación, así como de otras tecnologías de detección (sensores de movimiento y orientación, brújula, etc.), permiten al usuario enriquecer la visión del mundo real, combinándola con la información virtual extraída de Internet.

Gracias a la georreferenciación, es posible determinar la posición del usuario, y gracias a los sensores de orientación, es posible determinar hacia dónde está mirando. En cuanto a lo que observa, la aplicación captura la imagen del mundo real obtenida a través de una cámara y añade en la pantalla la información obtenida a través de Internet.

[35] Disponible en: http://www.bliquo.es/

[36] Disponible en: http://www.tweakersoft.com/mobile/aroundme.html

[37] Disponible en: http://www.buzzd.com/

[38] Disponible en: http://sites.google.com/site/placesdirectory/

Ilustración 5: Realidad aumentada con Layar 4.0.1 en Android 2.2

Algunos ejemplos de aplicaciones de realidad aumentada para dispositivos móviles son:

- **Layar**[39]. Esta aplicación funciona cargando desde Internet "capas" de información, que van desde transportes públicos hasta juegos sociales, y pasando por información de Wikipedia, etc. Está disponible para terminales iOS y Android, y se espera una versión para Symbian que está en desarrollo.

- **Wikitude**[40]. Explorador de realidad aumentada centrado especialmente en el ámbito del turismo, incluyendo guías de viaje y navegación paso a paso. Está disponible para dispositivos iOS, Android y Symbian.

[39] Disponible en: http://www.layar.com/

[40] Disponible en: http://www.wikitude.org/

4. Riesgos relacionados con la geolocalización

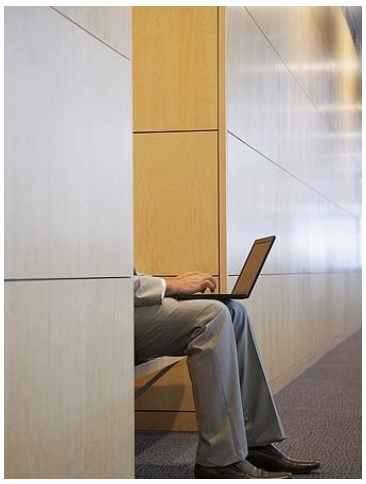
La propia naturaleza de los datos que manejan las aplicaciones de geolocalización, relativa a la posición georreferenciada de los usuarios, hace que se consideren aplicaciones especialmente sensibles desde el punto de vista de la seguridad.

Por otro lado, el hecho de que esta información se integre en ocasiones dentro de redes sociales, aumenta las posibles consecuencias de los fallos de seguridad y privacidad asociados, al conjugar la información de geolocalización con toda clase de datos personales. En este sentido, sitios como Please Rob Me[41] tratan – en este caso, en clave de humor – de concienciar a la población acerca de la importancia de la seguridad en las aplicaciones de geolocalización. Al transmitir información sensible asociada a su georreferenciación, los riesgos para el ciudadano no se limitan a posibles robos de información o datos a través de Internet, sino que pueden llegar incluso a suponer un peligro para su integridad física y personal.

A continuación, se describen los principales elementos existentes en todo proceso de geolocalización, para analizar los riesgos y amenazas asociados de forma independiente.

4.1 RIESGOS PARA LA PRIVACIDAD

Posiblemente, el aspecto más importante relacionado con los riesgos de las aplicaciones de geolocalización sea el de la privacidad. La naturaleza de los datos manejados por las aplicaciones de geolocalización resulta especialmente sensible, y su integración en las redes sociales agrava aún más el problema.



De esta forma, resulta peligroso que no exista una restricción en el ámbito en el que los datos estarán disponibles. El hecho de que cualquier persona pueda conocer la localización de un ciudadano conlleva riesgos que van desde el robo de datos, el hurto o robo físico, a la agresión contra su persona.

Asimismo, el hecho de que pueda conocerse la posición de un usuario en todo momento, puede derivar en la creación de un perfil del mismo, y a ser utilizado sin autorización en estudios de mercado, envío de publicidad, etc.

También conviene ser conscientes del riesgo que representa la ingeniería social en el caso de las redes geosociales. Un usuario podría hacerse pasar por otra persona o entablar amistad o contacto con alguna excusa, ocultando algún interés malicioso.

[41] Disponible en: http://pleaserobme.com/

Otro aspecto importante relacionado con la privacidad y la geolocalización, es la revelación involuntaria de información privada. Se encuentran ejemplos de personas que han comunicado a través de redes geosociales su posición, encontrándose después con problemas al conocerse dicha información en su círculo laboral o personal.

El mayor problema relacionado con la privacidad y la geolocalización, en la mayoría de las ocasiones, recae en el tratamiento irresponsable de los datos llevado a cabo por las empresas: cesión de datos de usuarios sin su consentimiento, utilización indebida de datos para estudios de mercado fuera de las cláusulas de privacidad, vulneración de la configuración de privacidad de los usuarios.

Es conocido el caso de una red geosocial[42] que, en su página, mostraba información aleatoria sobre un cierto número de usuarios y su última localización anunciada. El problema radicaba en que los usuarios seleccionados y anunciados públicamente, lo eran a pesar de que hubieran configurado su cuenta de forma privada, y sólo quisieran que su información fuera conocida por sus contactos. Tras hacerse público el fallo, la red geosocial en cuestión cambió la configuración de su política de privacidad.

4.2 RIESGOS PARA LA SEGURIDAD

4.2.1 Riesgos para la seguridad del sistema operativo

Todo dispositivo, para poder desempeñar sus funciones, ejecuta un tipo especial de software que se encarga de gestionar los recursos del sistema. Este software se conoce como “sistema operativo”, y juega un papel fundamental en la seguridad.

En el ámbito de los **ordenadores personales** (sobremesa o portátiles), los sistemas operativos más utilizados son Microsoft Windows, Mac OS X y GNU/Linux. Todos ellos ofrecen al usuario servicios muy similares, permitiendo manejar los recursos del sistema.

En el ámbito de los **dispositivos móviles**, y obviando sistemas embebidos propios (como dispositivos de navegación GPS), los sistemas operativos más utilizados son Android de Google, iOS de Apple, Windows Mobile y Windows Phone de Microsoft, Symbian OS de Symbian Foundation, Blackberry de RIM y webOS de Palm. Nuevamente, todos ellos ofrecen servicios similares al usuario, y permiten el acceso a los recursos del sistema.

Al actuar el sistema operativo como instrumento de gestión de recursos, se convierte en el punto central de gestión de la información almacenada y procesada por el dispositivo.

[42] Fuente: *White Hat Uses Foursquare Privacy Hole to Capture 875K Check-Ins, Wired, 29 de junio de 2010.* Disponible en: http://www.wired.com/threatlevel/2010/06/foursquare-privacy/

Es, por tanto, uno de los elementos más sensibles desde el punto de vista de la seguridad.

- Una de las amenazas más evidentes es el **código malicioso o malware**, que usualmente se presenta en forma de virus, troyanos o programas espía. Este tipo de programas infectan el sistema operativo anfitrión con el fin de dañar el sistema o la información contenida en él.

- En el caso de virus no específicos, el daño puede ir desde la inutilización del sistema operativo (posible denegación de servicio) hasta el robo de información.

- En el caso de virus o troyanos específicos, se pueden encontrar herramientas desarrolladas a medida. En esta clasificación se encuentran troyanos como Zeus[43], que tienen por objetivo la creación de botnets o redes de ordenadores infectados, controlados de forma remota para la realización de operaciones conjuntas. Investigaciones en seguridad[44] han demostrado que el modelo de generación de botnets por infección de troyanos resulta extrapolable a teléfonos inteligentes, por lo que el peligro de este tipo de ataques no se limita únicamente a ordenadores personales.

- En segundo lugar, el sistema operativo, como cualquier software, no está exento de **fallos de seguridad** ("*bugs*") que permitan la intrusión de un hipotético atacante.

- Los fallos de seguridad más peligrosos en un sistema operativo son aquellos que permiten su explotación de forma remota, a través de una red de intercomunicación. En el caso de los dispositivos portátiles, el hecho de contar con múltiples interfaces de comunicación de red (redes de telefonía, redes Wi-Fi inalámbricas, Bluetooth, infrarrojos…), aumenta los posibles vectores de ataque en caso de fallo de seguridad.

- Además, en el caso concreto de los teléfonos inteligentes y dispositivos portátiles, es habitual la **modificación no autorizada del sistema operativo**, con el fin de acceder a funciones que se encuentran bloqueadas por el fabricante. Un ejemplo de este tipo de modificaciones sería el *jailbreak* en dispositivos iOS, o el *rooteo* en dispositivos Android.

- El hecho de habilitar la instalación de programas no firmados puede provocar la entrada de software malicioso que, bien suplantando a uno original o no, llegue a infectar el sistema operativo y los programas y aplicaciones en él instalados.

[43] Disponible en: http://cert.inteco.es/cert/Notas_Actualidad/Aclaraciones_sobre_la_BotNet_Zeus

[44] Disponible en: http://www.slideshare.net/rootedcon/david-barroso-iphone-botnets-fun-rootedcon-2010

4.2.2 Riesgos asociados al software de geolocalización

Todo software de geolocalización, y al igual que ocurre en el caso del sistema operativo, es susceptible de contener fallos de seguridad. Aún cuando el sistema operativo se encuentre funcionando perfectamente y libre de fallos (en una situación ideal), un fallo en el software encargado de gestionar el proceso de geolocalización puede suponer un potencial vector de ataque, siendo posible incluso la escalada del fallo hasta llegar al propio sistema operativo.

- En el caso de **aplicaciones específicas**, estos fallos de seguridad tienen una gravedad directamente proporcional a la clase de privilegios del usuario que las ejecuta, limitando de esta forma el posible daño al sistema operativo.

- En el caso concreto de **dispositivos móviles**, estos suelen funcionar sobre algún sistema de *sandboxing*[45] mediante máquinas virtuales, que permita aislar el entorno de ejecución de la aplicación.

- No obstante, y en caso de un fallo de estas características, la información gestionada por la propia aplicación siempre se encontrará comprometida, pudiendo ocasionar fallos de privacidad.

- En el caso de **servicios online**, el rango de los posibles fallos de seguridad aumenta. Algunas de las amenazas[46] existentes son:

    - Inyección de código en sitios cruzados *o cross-site scripting.*
    - Falsificación de petición en sitios cruzados o *cross-site request forgery.*
    - Ataques de inyección de código SQL o *SQL injection,*
    - Secuestro de *clic* o *clickjacking.*
    - Falsificación de información en formularios o *form tampering.*

4.2.3 Riesgos en la comunicación de red

Dejando a un lado el hecho de que una conexión a Internet supone un posible vector de ataque, el principal problema asociado a una conexión de red es la **intercepción de las comunicaciones** (*eavesdropping*).

Debido a la propia arquitectura de Internet, la información, en su camino entre el origen y el destino de la comunicación, viaja por un número indeterminado de máquinas. Así, toda

[45] El *sandboxing* o aislamiento de procesos consiste en la ejecución separada de ciertas aplicaciones, controlando y aislando los recursos del sistema a los que éstas acceden.

[46] Más información: http://cert.inteco.es/cert/INTECOCERT

comunicación que no se encuentre protegida por métodos criptográficos, es susceptible de ser intervenida por personas no autorizadas.

En el caso de las aplicaciones específicas sobre geolocalización (tanto para dispositivos móviles como de escritorio), no siempre es posible conocer los mecanismos de comunicación utilizados, y si estos funcionan sobre una conexión segura -cifrada- o no.

Por otro lado, cabe destacar el **factor de la seguridad de la propia red de interconexión**.

- Desde el punto de vista lógico de la conexión, existen diversos ataques de tipo "hombre en el medio" (*man-in-the-middle*) que permiten interponerse en una comunicación e interceptar la información no cifrada que viaje por la Red. Un ejemplo de este tipo de ataques sería el clásico envenenamiento de caché ARP[47] (*ARP poisoning*).

- Desde el punto de vista físico, la posible intercepción de la comunicación depende fuertemente del tipo de red utilizada.

    - En el caso de las redes cableadas físicas, típicas del entorno doméstico y laboral, el riesgo de una intercepción física es bajo.

    - Este riesgo aumenta enormemente en el caso de las redes inalámbricas, al estar exponiendo el medio físico de la red de forma abierta.

    - En el caso de redes abiertas (sin contraseña), no existe ningún tipo de protección física, y los datos se encuentran, en consecuencia, expuestos. A cambio, se utilizan algoritmos de cifrado, como WPA y WPA2, con los que la protección física aumenta al tratarse de algoritmos robustos. No obstante, no resulta infalible, pues la efectividad del algoritmo está también ligada al tipo de contraseña utilizada como clave de protección.

    - En el caso de las redes móviles la situación es similar. Las redes móviles de tercera generación (3G) se consideran bastante robustas, en cuanto a la seguridad de sus algoritmos de cifrado y protección. Por otro lado, la seguridad de las redes de segunda generación (2G y 2.5G) se ha puesto

[47] El envenenamiento ARP es una técnica usada por atacantes en redes internas cuyo fin es obtener el tráfico de red circundante, aunque no esté destinado al sistema del propio intruso. Más información: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/articulo_envenenamiento_ARP

en entredicho en diversos estudios[48], por lo que actualmente no se considera segura.

Por último, es posible adquirir en Internet dispositivos distorsionadores ("*jammer*") que impidan la utilización de determinadas bandas de frecuencia utilizadas por las tecnologías móviles. Usando un dispositivo de estas características, se impide la conexión de un dispositivo a las redes de telefonía móvil, forzándolo a conectarse a una red inalámbrica maliciosa; o impide la conexión a las redes 3G, para forzar su conexión mediante tecnologías 2.5G (como GPRS y EDGE).

4.2.4 Riesgos para la seguridad física

Se entiende por seguridad física aquella que está relacionada con los dispositivos hardware, en este caso aquellos en los que tiene lugar algún proceso de geolocalización. El riesgo más evidente supone la pérdida o sustracción de un dispositivo hardware, en el que podrían estar almacenados datos personales, contraseñas de acceso a servicios de geolocalización, etc.

Este riesgo, en el caso de los ordenadores de sobremesa, es bajo, si bien en los ordenadores portátiles y especialmente en el caso de dispositivos móviles y teléfonos inteligentes resulta bastante elevado.

Por otro lado, debe considerarse también el riesgo de una modificación no autorizada en el hardware, cuyas consecuencias pueden ir desde el funcionamiento defectuoso del mismo (posible denegación de servicio), hasta la captura de contraseñas de acceso mediante dispositivos físicos (denominados "*keyloggers hardware*").

[48] Disponible en: http://cryptome.org/gsm-crack-bbk.pdf

5. Recomendaciones de privacidad para el uso de la geolocalización

Se recomienda:

- Leer con detenimiento y comprender las cláusulas de privacidad de los servicios de geolocalización y las redes geosociales.
- En general, restringir al máximo la información que se ofrece de forma pública.
- Desconfiar, como norma general, de toda persona que no sea conocida.
- Adecuar la precisión de las publicaciones sobre georreferenciación. Por ejemplo, en una red social orientada al turismo podría ser suficiente con anunciar la ciudad de estancia, siendo innecesario anunciar también el hotel concreto.
- Elegir con cuidado el grupo de usuarios que podrán ver la información de geolocalización generada por las aplicaciones o redes geosociales. La mayoría de las redes sociales permiten configurar este aspecto, restringiendo las publicaciones a grupos privados.
- Configurar correctamente los vínculos entre aplicaciones de georreferenciación y redes sociales, evitando a toda costa el envío indiscriminado de información.
- No aportar información que pueda conducir a deducir el lugar en que se encuentra un usuario en un momento dado. Para ello, conviene evitar anunciar los desplazamientos habituales (por ejemplo, al entorno laboral) y los períodos de vacaciones.

En el ámbito de la geolocalización, el marco legal de referencia abarca diferentes aspectos de la privacidad de los datos personales.

La **Constitución Española** establece, en su artículo 18.1, que *se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*. En este sentido, la **Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen** establece, en su artículo primero, que dicho derecho *será protegido civilmente frente a todo género de intromisiones ilegítimas*, de acuerdo con lo establecido en dicha ley. La propia Constitución también establece, en su artículo 18.3, que *se garantiza el secreto de las comunicaciones* y en su artículo 18.4, que *la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*.

En la legislación española, la principal ley dedicada a garantizar el cumplimiento del artículo 18.4 de la Constitución, es la **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)**, junto con el **Real Decreto 1720/2007 de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD)**.

El RLOPD define en su artículo 81 tres niveles de protección, atendiendo al tipo de datos considerados y su papel en la privacidad del individuo: básico, medio y alto[49].

- Nivel alto: tratamientos con datos relacionados con la ideología, creencias, religión, raza, vida sexual, salud, aquellos recabados para fines policiales sin el consentimiento de los afectados (ficheros de las Fuerzas de Seguridad del Estado) y derivados de actos de violencia de género.

- Nivel medio: tratamientos con datos relativos a información laboral, fiscal, financiera, de solvencia, infracciones penales y administrativas, que ofrezcan una definición de la personalidad y de los operadores de comunicaciones electrónicas, respecto a los datos de tráfico y localización.

- Nivel básico: tratamientos con datos de carácter personal. También datos sobre ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando se utilicen en el marco de una transferencia dineraria, son accesorios en la realización de una operación o se refieran a la condición de discapacidad o invalidez (este último caso relativo a los datos de salud).

Partiendo de esta clasificación, en el caso concreto de la utilización de servicios de geolocalización destaca que:

- Con carácter general, los datos de geolocalización, y siempre que dichos datos se refieran a una persona identificada o identificable, se considerarían datos de nivel básico.

- Por otro lado la LOPD, de acuerdo al artículo 81.2 apartado f), también contempla la posibilidad de que datos de nivel básico lleguen a ser considerados de nivel medio, mediante la combinación con otros datos que, bien de manera directa o por inferencia, ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos. Esto resulta especialmente importante en el caso de las redes geosociales como Foursquare, que combinan información de geolocalización con otros datos privados de sus usuarios.

[49] Información extraída de la Guía de Seguridad de Datos–2010 de la Agencia Española de Protección de Datos, disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

- Asimismo la LOPD presenta una excepción para los datos de localización de los que sean responsables operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas, en cuyo caso se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 del reglamento, relativas al registro de accesos.

Para toda aplicación o servicio de geolocalización que haga uso de sus datos, todo ciudadano deberá ser informado de modo preciso, previo e inequívoco de los siguientes aspectos:

- La existencia de un **fichero o proceso de tratamiento de datos**.
- **La finalidad en la recogida de los datos**, exponiendo la finalidad legítima con absoluta sinceridad.
- **Carácter obligatorio u optativo** de las preguntas planteadas.
- **Consecuencias de la negativa a suministrar ciertos datos**.
- La posibilidad de ejercer **los derechos de Acceso, Rectificación, Cancelación y Oposición**, definidos en el Título III de la LOPD.
- **Identidad y dirección del responsable del tratamiento de los datos**.

Es importante reseñar que, salvo por razones de seguridad pública, como se establece en el artículo 25 LOPD, todo ciudadano podrá ejercer sus derechos de acceso (consulta de la información existente sobre sí mismo), rectificación (modificación de datos incorrectos), cancelación (eliminación de los datos de un fichero) y oposición (impedir la inclusión de sus datos en un fichero) sobre los datos que cualquier fichero almacene sobre éste.

El organismo encargado de velar por el cumplimiento de la LOPD es la **Agencia Española de Protección de Datos (AEPD)**. Todo fichero adscrito a la LOPD deberá ser puesto en conocimiento de dicha agencia; en el caso de ficheros de titularidad pública, mediante su publicación en el Boletín Oficial del Estado o Diario Oficial; y en el caso de ficheros de titularidad privada, mediante notificación explícita a la AEPD por parte del responsable.

La falta de atención de los derechos de los ciudadanos establecidos por la legislación, la violación de los mismos, la ausencia de colaboración con las autoridades y la AEPD, así como la falta de notificaciones en las circunstancias establecidas por la Ley, son causas que derivan en la pertinente investigación por parte de la AEPD, pudiendo imponerse las medidas y sanciones oportunas previstas en la LOPD.

Cualquier ciudadano que acredite el incumplimiento de la LOPD puede dirigir una denuncia a la AEPD, utilizando el modelo de denuncia que facilita dicho organismo en su página web. Para más información:

https://www.agpd.es/portalwebAGPD/canalciudadano/denunciasciudadano

La intervención de la AEPD no sólo tiene lugar cuando se presenta una denuncia, sino que la Agencia también puede actuar de oficio, cuando se considera que los derechos de los ciudadanos, en materia de privacidad y protección de datos, han podido ser violados. Un ejemplo en este sentido sería la investigación abierta en 2010 a Google[50], debido a la captura de información en redes Wi-Fi inalámbricas desprotegidas, a través de su flota de vehículos para la toma de fotografías de Google Street View.

En conclusión, todos los ciudadanos están amparados por la Ley en cuanto a la protección de sus datos personales, según establece la legislación vigente y la propia Constitución. Precisamente por esto, el uso responsable y seguro de estas tecnologías es fundamental para poder disfrutar de sus servicios sin poner en peligro el aspecto íntimo y personal de los ciudadanos. También para que puedan evolucionar y aportar más funcionalidades al usuario.

[50] Fuente: *La Agencia de Protección de Datos abre investigación a Google, El País, 19 de mayo de 2010*. Disponible en: http://www.elpais.com/articulo/tecnologia/Agencia/Proteccion/Datos/abre/investigacion/Google/elpeputec/20100519elpeputec_5/Tes

6. Recomendaciones de seguridad para el uso de la geolocalización

Una vez conocidos los riesgos y amenazas asociados a las tecnologías de geolocalización, es necesario definir unas configuraciones y prácticas de seguridad que permitan, mediante su aplicación, la utilización segura de estas aplicaciones.

6.1 SEGURIDAD DEL SISTEMA OPERATIVO

Se recomienda:

- Mantener siempre actualizado el sistema operativo y los programas instalados, aplicando las actualizaciones periódicas que el fabricante suministra.
- Utilizar, cuando esté disponible y sea necesario, un sistema de protección de Red de tipo cortafuegos para proteger el sistema de conexiones peligrosas.
- Utilizar, cuando esté disponible y sea necesario, un sistema antivirus. La base de datos de definiciones de virus, así como el propio software, deberán mantenerse siempre actualizadas.
- Utilizar software original, cuya procedencia sea conocida y pueda ser certificada.
- Evitar las modificaciones no autorizadas del software o el hardware, pues pueden ocasionar problemas de seguridad no contemplados por el fabricante.
- Utilizar usuarios con privilegios bajos en el sistema, reservando el uso del usuario privilegiado (administrador, *root*) para las ocasiones en que sea estrictamente necesario.
- En los dispositivos móviles, configurar las opciones de localización de forma adecuada a las necesidades de la aplicación a utilizar. No todas las aplicaciones requieren de la precisión del GPS, o no siempre es conveniente que esté habilitada la georreferenciación mediante redes Wi-Fi inalámbricas.

Ilustración 6: Configuración de seguridad y ubicación en Android 2.2

6.2 SOFTWARE DE GEOLOCALIZACIÓN

Se recomienda:

- Utilizar únicamente aplicaciones de confianza, obtenidas a través de los canales de distribución pertinentes. Entre ellos se incluyen las páginas web oficiales de los proyectos y las tiendas de aplicaciones.

- Mantener siempre actualizadas las aplicaciones de geolocalización.

- Tener en cuenta los permisos que solicita una aplicación para su instalación en el sistema. No tiene sentido, por ejemplo, que un juego solicite acceso al hardware de georreferenciación y a la red de comunicaciones, pues podría tratarse de un software destinado a espiar al usuario.

Ilustración 7: Solicitud de permisos en instalación

- Vigilar, en las actualizaciones de las aplicaciones, los posibles cambios en los permisos requeridos del sistema.

- Establecer, en la configuración de la aplicación, en qué momento se permite la utilización de funciones de geolocalización, y con quién se va a compartir dicha información.

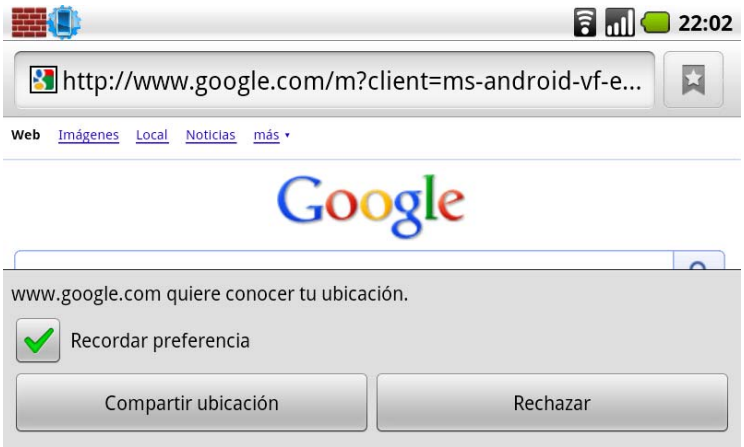


Ilustración 8: Configuración de compartición de ubicación

- Tener en consideración la vinculación de datos que establecen ciertas aplicaciones de geolocalización con las redes sociales.

- En el caso de aplicaciones online, utilizar una versión actualizada del navegador web, además de mantener actualizados todos sus complementos y *plugins*.

- En aplicaciones online, utilizar algún complemento destinado a la prevención de ataques web y explotación de vulnerabilidades[51].

6.3 COMUNICACIÓN DE RED

Se recomienda:

- No enviar nunca información o documentos sensibles a través de una conexión sin cifrar. Asegurarse de que los credenciales de conexión (nombre de usuario y contraseña) viajan cifrados a través de SSL.

- Conectarse, en la medida de lo posible, a redes de confianza. Es preferible utilizar la red doméstica o laboral, antes que otro tipo de redes.

- En redes locales, comprobar que la conexión con la puerta de enlace es directa y el equipo no está sufriendo un ataque de hombre en el medio. Para ello, se puede acudir a herramientas de trazado de conexiones (como *tracert* en Microsoft Windows o *traceroute* en sistemas GNU/Linux y Mac OS X) o consultar la tabla de correspondencias ARP.

- No utilizar en ningún caso redes Wi-Fi inalámbricas abiertas, cuyo origen resulta desconocido y desconfiar de redes Wi-Fi inalámbricas gratuitas, como las ofrecidas en locales.

- Configurar la propia red Wi-Fi inalámbrica doméstica con seguridad WPA2.

- En redes móviles, preferir el uso de redes de tercera generación (3G) frente a las de segunda generación (2G, GPRS y EDGE).

6.4 SEGURIDAD FÍSICA

Se recomienda:

- Instalar programas de borrado remoto, que en caso de sustracción o pérdida, y si fuera imposible su recuperación, permitan eliminar toda información privada del dispositivo.

- Instalar programas que impidan la utilización de los mismos en caso de que cambie la tarjeta SIM instalada.

[51] Por ejemplo, NoScript para Mozilla Firefox. Disponible en: http://noscript.net/

- En caso de pérdida o sustracción de un teléfono móvil, solicitar al operador de red su bloqueo mediante IMEI, tras establecer la correspondiente denuncia en las dependencias policiales.

- En el caso de ordenadores portátiles, utilizar un cable de seguridad para anclarlo a una estructura fija, cuando se utilicen en lugares públicos.

- Establecer contraseñas de acceso para todos los dispositivos, incluyendo ordenadores de sobremesa, portátiles y dispositivos móviles.

- Asegurarse de que, tras activar un dispositivo suspendido, se solicita nuevamente la contraseña de acceso o una diferente.

- Utilizar contraseñas fuertes, combinando números, letras mayúsculas y minúsculas, y símbolos; con una longitud mínima de 8 caracteres. Asimismo, se deben cambiar las contraseñas con cierta periodicidad.

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

OBSERVATORIO
INTECO

Web http://observatorio.inteco.es

Perfil en Scribd del Observatorio de la Seguridad de la Información:
http://www.scribd.com/ObservaINTECO

Canal Twitter del Observatorio de la Seguridad de la Información:
http://twitter.com/ObservaINTECO

BLOG Blog del Observatorio de la Seguridad de la Información:
http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/

observatorio@inteco.es