

## Geoetiquetación: Los riesgos de hacer pública tu ubicación

Por *Carmina Cecilia Espinosa Madrigal, Israel Andrade Canales*

[numero-11](#)<sup>[1]</sup>

[Tweet](#)<sup>[2]</sup>

Compartir ideas y experiencias por medio de imágenes, videos, texto y sonidos de manera ágil a través de las redes sociales es un tarea cada vez más difundida. Este mecanismo de socialización requiere que sus usuarios aprendan también sobre ciertas medidas y consecuencias al publicar esta información, sobre todo en las relacionadas con geotiquetación.

Hoy en día, el fácil acceso a la tecnología nos permite compartir ideas y experiencias por medio de imágenes, videos, texto y sonidos de manera ágil a través de las redes sociales. Además nos permite enriquecer nuestras formas de comunicación al combinar diferentes contenidos entre sí y con otras tecnologías.

La Geoetiquetación es una tecnología con la que podemos vincular datos de localización

Ejemplos de lo anterior es la fotografía digital y los mensajes de texto. La fotografía digital al integrarse con tecnologías GPS (Global Position System) permite conocer la ubicación geográfica de las fotografías; mientras que en el caso de mensajes de texto, se puede llegar a conocer el origen del mensaje. Redes sociales como Flickr, Twitter y Facebook han popularizado y facilitado el consumo de esta tecnología y cada vez son más los usuarios que aprovechan los beneficios de estos servicios (*Figura 1 y Figura 2*).



Figura 1. *Flickr* permite ubicar en un mapa las fotografías que contengan datos GPS incrustados. En la figura se observa el “Amoxcalli” dentro de Ciudad Universitaria en la Ciudad de México.



Figura 2. *Twitter* permite vincular un mensaje de texto con la ubicación geográfica del autor en el momento de la publicación.

Es importante enfatizar que cualquier tipo de dato que haga referencia a nuestra ubicación debe ser considerado “privado”, por la simple razón de brindar información relacionada con lugares que frecuentamos o con actividades que realizamos cotidianamente. Por ejemplo, las fotografías geoetiquetadas podrían generar un mapa ilustrando de nuestras actividades diarias (Figura 3), los lugares de convivencia con nuestra familia y amigos, así como la ubicación de nuestras pertenencias.

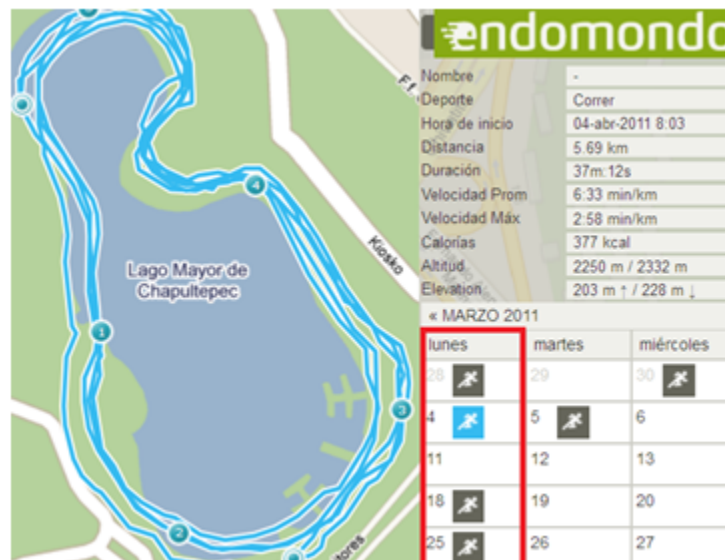


Figura 3. El servicio de “endomondo” permite llevar un registro de actividades deportivas referenciadas con datos GPS. En la figura se ilustra un ejemplo de información de actividades cotidianas.

1. **Riesgos de seguridad Fuga de datos.** El primer y principal riesgo de seguridad a la que nos enfrentamos con el uso de la geoetiquetación, es la fuga inconsciente de datos de ubicación a través de las redes sociales. Esto ocurre por desconocimiento sobre el funcionamiento de estas tecnologías en nuestros dispositivos móviles, ya que algunos de ellos están configurados para incrustar geoetiquetas de forma automática (Figura 4). En agosto del 2010, Adam Savage, conductor del programa Cazadores de Mitos

(MythBusters), publicó en Twitter una fotografía de un automóvil estacionado fuera de su casa, la imagen contenía una geotiqueta con información exacta del lugar en el que se tomó la foto, revelando la dirección de su casa. Además el mensaje de la imagen decía “Voy al trabajo”. Con toda esta información publicada inconscientemente, el famoso conductor proporcionó datos muy valiosos que pudieron ser aprovechados por ladrones.

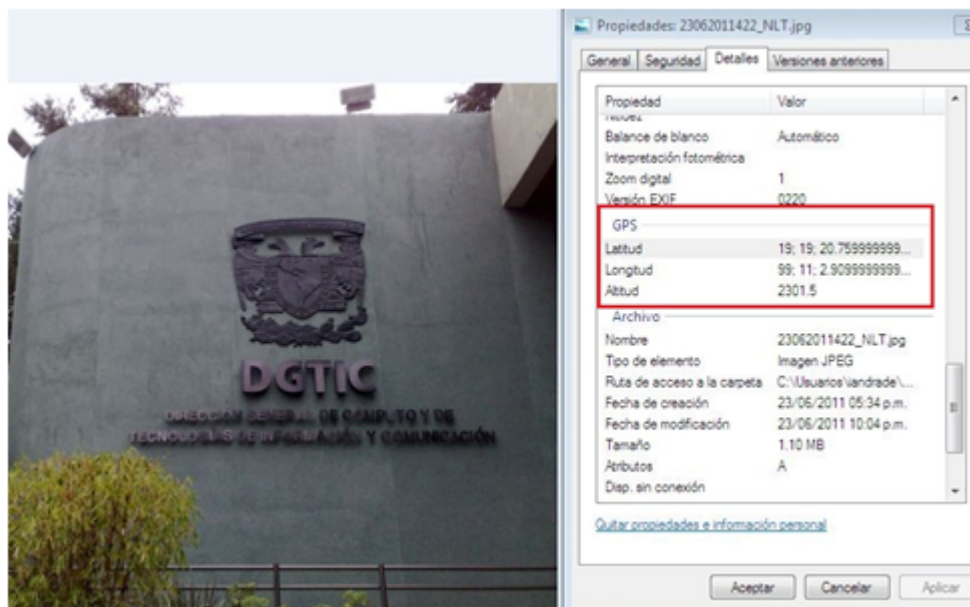


Figura 4. Datos de ubicación (georreferencia) incrustados automáticamente por la cámara digital.

- 2. **Configuraciones deficientes.** El segundo riesgo, es la deficiencia en las configuraciones de privacidad específicamente con los servicios y aplicaciones de redes sociales donde compartimos información georreferenciada. Una configuración deficiente (Figura 5) podría permitir que personas mal intencionadas tengan acceso a datos de nuestra ubicación, aprovechándose de esto para realizar acciones criminales. Por ejemplo, a través de mensajes o imágenes georreferenciadas se puede conocer el comportamiento y rutinas de una persona, datos suficientes para realizar un secuestro.

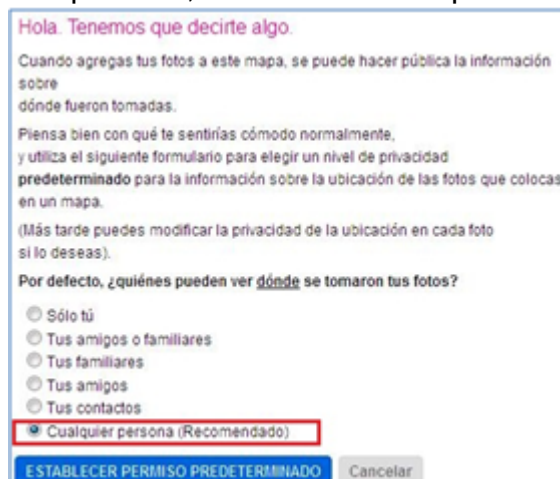


Figura 5. Ejemplo del panel de configuración predeterminada de Geotiquetación. En la

figura se resalta una mala práctica de privacidad, la cual permite que cualquier persona tenga acceso a nuestros datos de ubicación.

3. **Pérdida o robo de dispositivos móviles.** Muchos dispositivos móviles integran sistemas GPS que pueden almacenar la ubicación geográfica, sitios de interés, números telefónicos y fotografías de contactos, si estos dispositivos son robados o extraviados y no están protegidos mediante contraseña, toda esta información se verá seriamente comprometida y podría ser usada para extorsiones y secuestros, (Figura 6).



Figura 6. Ejemplo de datos privados geoetiquetados que pueden ser encontrados en un dispositivo móvil.

## Prevenir el mal uso de tu información

A continuación, te exponemos algunas sugerencias que pueden ayudar a aprovechar al máximo los beneficios de esta tecnología minimizando los riesgos:

- Lee el instructivo de tu cámara digital o teléfono móvil para que conozcas su funcionamiento y puedas configurar adecuadamente el GPS. Desactiva la funcionalidad del GPS y sólo actívala cuando vayas a utilizarla.
- Si vas a publicar un contenido digital que contenga datos de tu ubicación, asegúrate que sólo esté disponible para personas de confianza, esto lo puedes realizar al restringir el acceso a tu información visitando la sección de configuración de tus redes sociales.
- Recuerda que una fotografía puede decir más que mil palabras, ésta puede dar información de los sitios que más frecuentas, horarios de visita y ubicación geográfica. Piensa dos veces antes publicarla.
- Muchos dispositivos móviles o GPS tienen la capacidad de almacenar ubicaciones para acceder a ellas rápidamente, evita poner nombres que den información extra como:
- Asegura con contraseña el acceso a tu dispositivo móvil, ya que existe el riesgo de extravío o robo del mismo y por lo tanto de tu información.

El empleo de tecnologías innovadoras o emergentes siempre debe ir acompañado de medidas básicas de seguridad, sé consciente del tipo de información que generas, transformas, almacenas o comunicas, sin olvidar los riesgos que implica. Contribuye a mantener una cultura de seguridad de la información que propiciará un ambiente en el que se confíe en las nuevas tecnologías y sus aplicaciones.

## Referencias:

- <http://es.wikipedia.org/wiki/Geoetiquetado> [3]
- <http://icanstalku.com/how.php#disable> [4]
- <https://support.twitter.com/articles/20169204-sobre-los-tweets-con-ubicacion> [5]
- <http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> [6]
- <https://support.twitter.com/articles/20169204-sobre-los-tweets-con-ubicacion> [5]
- <http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf> [7]

[Carmina Cecilia Espinosa Madrigal](#) [8]

[Israel Andrade Canales](#) [9]

[numero-11](#)

[Universidad Nacional Autónoma de México](#)

[Universidad Nacional Autónoma de México](#)  
[Directorio](#)

[Dirección General de Cómputo y de Tecnologías de Información y Comunicación](#)

[Dirección General de Cómputo y de](#)  
[Tecnologías de Información y Comunicación](#)

[SSI / UNAMCERT](#)

[SSI / UNAMCERT](#)

[ [CONTACTO](#) ]

Se prohíbe la reproducción total o parcial  
de los artículos sin la autorización por escrito de los autores

---

**URL del envío:** <http://revista.seguridad.unam.mx/numero-11/geoetiquetaci%C3%B3n-los-riesgos-de-hacer-p%C3%BAblica-tu-ubicaci%C3%B3n>

## Enlaces:

[1] <http://revista.seguridad.unam.mx/category/revistas/numero-11-1>

[2] <http://twitter.com/share>

[3] <http://es.wikipedia.org/wiki/Geoetiquetado>

[4] <http://icanstalku.com/how.php#disable>

[5] <https://support.twitter.com/articles/20169204-sobre-los-tweets-con-ubicacion>

[6] <http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf>

[7] <http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf>

[8] <http://revista.seguridad.unam.mx/autores/carmina-cecilia-espinosa-madrigal>

[9] <http://revista.seguridad.unam.mx/autores/israel-andrade-canales>