Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- ¿Qué son los Metadatos?
- Identifica y Elimina los Metadatos
- Protégete

# Metadatos

## EDITOR INVITADO

James Tarala es el editor invitado para esta edición. Instructor sénior del SANS Institute y director de consultoría en Enclave Security (www.enclavesecurity.com), es además, autor de numerosos cursos de entrenamiento del SANS, incluyendo *SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls* y SANS Audit 407: *Foundations of Auditing Information Systems*.

## RESUMEN

Todos los días, los usuarios de computadoras comparten fotografías, documentos, hojas de cálculo, presentaciones, clips de audio y otros archivos digitales con gente alrededor del mundo. De lo que no te das cuenta, es que estos archivos pueden incluir inadvertidamente información privada o confidencial sobre ti o tu organización, en forma de metadatos. Para ayudarte a mantener a salvo tanto tu privacidad como tu seguridad, explicaremos qué son los metadatos, cómo encontrarlos y eliminarlos, así como algunos pasos que debes considerar para protegerte.

## ¿QUÉ SON LOS METADATOS?

Los metadatos son datos que definen o describen otra pieza de información. Por sí mismos no son maliciosos, pero pueden revelar más de lo que piensas sobre ti, tu organización o tus dispositivos. Muchos dispositivos, como las computadoras, las cámaras o los *smartphones*, incrustan automáticamente metadatos en cualquier archivo digital que produzcan. Además, la mayoría de los programas de software o formatos de archivo incluyen marcadores de posición para tipos específicos de metadatos. Un ejemplo muy común es Microsoft Word, el cual por *default* incluye información acerca del autor, la fecha de creación del documento y cualquier comentario o revisión incrustada. Algunos ejemplos de metadatos son:

- Fecha y hora de creación del archivo
- La dirección o la ubicación geográfica de dónde fue creado el archivo
- Tu nombre, el nombre de tu organización, el nombre de tu máquina o dirección IP
- Los nombres de cualquier persona que haya contribuido con el documento o los comentarios que insertaron
- El tipo de cámara utilizada y sus configuraciones al momento de tomar la foto.
- Tipo de dispositivo de audio o video usado y las configuraciones establecidas al realizar una grabación
- Marca, modelo y proveedor de servicios de tu teléfono inteligente.

© The SANS Institute 2012

# Metadatos

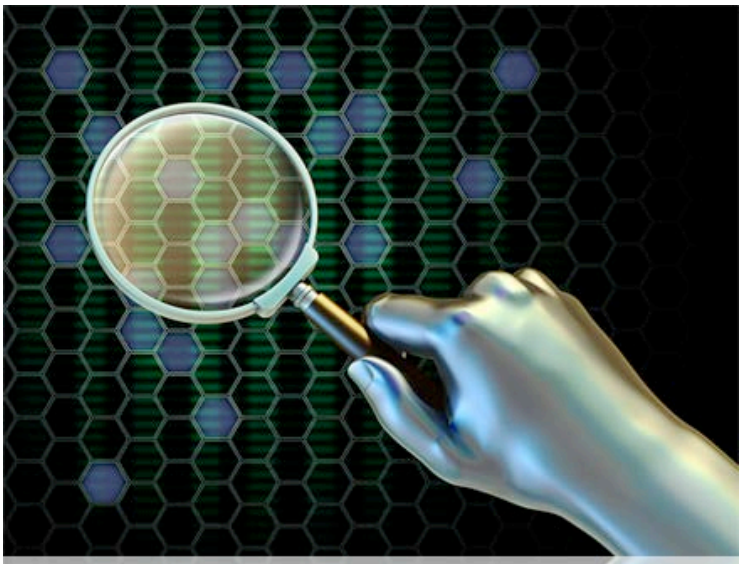
## IDENTIFICA Y ELIMINA LOS METADATOS

Desafortunadamente, en muchos dispositivos y programas es difícil eliminar los metadatos de los archivos creados o editados. Generalmente, los metadatos se insertan en lugares recónditos para los usuarios ordinarios de computadoras. Una forma común de visualizar y eliminar los metadatos de cualquier archivo con el que trabajes en una máquina que ejecuta Windows, es haciendo clic-derecho y posteriormente ver sus "*Propiedades*". Desde ahí, podrás eliminar los metadatos seleccionando la pestaña "*Detalles*", después haz clic en "*Quitar propiedades e información personal*". Otra forma para ver los metadatos, es abrir el archivo en aplicaciones especiales. Por ejemplo, la aplicación "*Preview*" de Mac OS X puede mostrarte los metadatos de cualquier fotografía que abras.

Algunas aplicaciones incluyen herramientas específicas para eliminar metadatos. Por ejemplo, Microsoft Office 2007 y 2010 incorporan una herramienta llamada "*Inspector de Documentos*", la cual identificará los metadatos en un archivo de Office, y te proporcionará las opciones para eliminar, selectivamente, algunos o todos los metadatos. Aunque Microsoft Office para Mac no tiene esta herramienta, sí te permitirá eliminar los metadatos de un documento de Office dirigiéndote a *Preferencias/Seguridad/Privacidad* y seleccionando "*Eliminar información personal al guardar este archivo*". Finalmente, existen diversas aplicaciones de código abierto y comerciales diseñadas para identificar, editar o eliminar metadatos en los archivos.

## PROTÉGETE

La mayoría de los metadatos por sí solos no son dañinos.



**Los metadatos no son malos, pero pueden revelar más de lo que imaginas. Revisa tus archivos digitales antes de compartirlos.**

De hecho, puedes hacer que, deliberadamente, los metadatos estén disponibles, como agregar tu nombre en una imagen para propósitos de derechos de autor. Sin embargo, cuando se trata específicamente de archivos con información confidencial o sensible, debes tomar en cuenta los metadatos que estás revelando a otros. Cuando creas un archivo que incluye metadatos, no sabes dónde podría terminar esta información en el futuro. Por lo tanto, algunas buenas prácticas para lidiar con metadatos son:

1. Considera guardar el archivo en un formato que no almacene metadatos, o los tenga muy limitados. Por ejemplo, en lugar de compartir un documento de

# Metadatos

Word, conviértelo en un archivo con formato .rtf o .txt. Para imágenes, en vez de usar imágenes JPEG, usa el formato PNG.

2. Considera ejecutar un limpiador de metadatos, como el *Inspector de Documentos* de Microsoft Office, o herramientas de software especiales para identificar y eliminar los metadatos.
3. Revisa las preferencias o configuraciones para cualquier aplicación o dispositivo que utilices. Podrías limitar la cantidad de metadatos que almacenas al cambiar las opciones de configuración por default; por ejemplo, deshabilita el rastreo de *geo-localización* de la cámara de tu *smartphone*.
4. Antes de enviar o publicar un archivo, considera el impacto de éste si contiene metadatos. Esto es especialmente importante al publicar archivos, como fotografías o videos, en sitios de redes sociales como Flickr, Twitter o Facebook.

Al considerar estos simples pasos, ayudas asegurar que sólo la información que deseas comunicar con otros sea realmente la compartida, pues los datos privados deben permanecer privados.

## RECURSOS

Algunos de los enlaces mostrados a continuación, se redujeron para mejorar la legibilidad a través del servicio de TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino solicitando permiso antes de abrirlo.

Inspector de documentos:
http://preview.tinyurl.com/7caymly

Explicación Metadatos EXIF:
http://preview.tinyurl.com/7wpnc6y

Herramienta gratuita para extracción de metadatos:
http://meta-extractor.sourceforge.net
o http://preview.tinyurl.com/aueb4

Deshabilitar la *geo-localización* en *smartphones*:
http://preview.tinyurl.com/83ft4no

Geoetiquetación: Los riesgos de hacer pública tu ubicación:
http://preview.tinyurl.com/7b559s9

Glosario de seguridad informática:
http://preview.tinyurl.com/7rkkkcx

## MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

## VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

***OUCH! es publicado bajo el programa Securing The Human de SANS y es distribuido bajo la licencia Creative Commons BY-NC-ND 3.0. Se concede el permiso para distribuir este boletín siempre y cuando se referencie la fuente, la distribución no sea modificada ni usada con fines comerciales. Para traducción o más información, por favor contacte a: ouch@securingthehuman.org.***

*Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner*
*Versión en español a cargo de UNAM-CERT: Iván Alvarado, Pablo Lorenzana, Andrés Hernández, Galvy Cruz*