UNIVERSIDAD Ð SEVILLA

Guías de Seguridad

Guía de limpieza de metadatos

Índice

1. Introducción

Los usuarios de la universidad de Sevilla (en adelante, US) al hacer uso de Internet, publican y comparten todo tipo de ficheros con otros usuarios de la US y con el resto de usuarios de Internet. Estos archivos pueden contener información privada o confidencial, por lo tanto sensible, sobre el propio usuario que publica o sobre la US, en forma de metadatos.

Aparentemente no son visibles, pero es fácil acceder a ellos y proporcionan información de gran interés que podría ser usada con fines maliciosos.

Esta guía está pensada para mantener a salvo la privacidad y la seguridad, tanto de los usuarios de la US, como de la propia institución.

2. Qué son los metadatos

Los metadatos son datos que definen o describen otra pieza de información o, dicho de otro modo, son “datos sobre datos”. Por si mismos no son maliciosos pero, aunque pueden ser de gran utilidad, también pueden revelar más información de lo esperado sobre los usuarios, sus dispositivos (ordenador, móvil, etc.) o la propia US.

Muchos dispositivos y aplicaciones insertan automáticamente metadatos en cualquier archivo digital que procesen y dichos metadatos pueden quedar expuestos al publicarlos o difundir los archivos en Internet (en la web, intranet, blogs, etc.) sin conocimiento del propio usuario. Además, la mayoría de los programas de software y los distintos formatos de archivo incluyen marcadores de posición para tipos específicos de metadatos.

Algunos ejemplos de metadatos son:

- Fecha y hora de creación del archivo.
- La dirección o la ubicación geográfica de donde fue creado el archivo.
- El nombre del usuario, el nombre del equipo informático o la 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 en el momento de realizar la foto.
- Tipo de dispositivo de audio o video usado y las configuraciones establecidas al realizar la grabación.
- Marca, modelo y proveedor de servicios del teléfono móvil.

3. Protección para los usuarios

La forma en la que se pueden proteger los usuarios de la US es a través de la concienciación y de la aplicación de ciertas medidas preventivas. La principal recomendación para evitar que se publiquen en Internet documentos o se envíen/divulguen por correo electrónico ficheros con metadatos que no quieren hacerse públicos, es su limpieza previa a la publicación o envío de los ficheros.

En el proceso de limpieza de documentos, se retirará de éstos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.

b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.

c) A la buena imagen de la organización que difunde el documento con metadatos, por cuanto demuestra un descuido en su buen hacer.

3.1. Buenas practicas

A continuación se recogen algunas buenas prácticas para minimizar los efectos perjudiciales de la difusión de información oculta en los archivos:

- Considerar guardar el archivo en un formato que no almacene metadatos, o los tenga muy limitados. Por ejemplo, en lugar de compartir un documento de Word, convertirlo en un archivo con formato pdf, .rtf o .txt previa limpieza de los metadatos. Para imágenes, en vez de usar imágenes JPEG, usar el formato PNG.
- Considerar ejecutar un limpiador de metadatos, como el Inspector de Documentos de Microsoft Office, o herramientas de software especiales para identificar y eliminar los metadatos.
- Revisar las preferencias o configuraciones para cualquier aplicación o dispositivo que se utilice. Se puede limitar la cantidad de metadatos que se almacenan al cambiar las opciones de configuración por defecto. Por ejemplo, deshabilitando el rastreo de geo-localización de la cámara del móvil.
- Antes de enviar o publicar un archivo, considerar el impacto de éste y si contiene metadatos. Esto es especialmente importante al publicar archivos, como fotografías o videos.

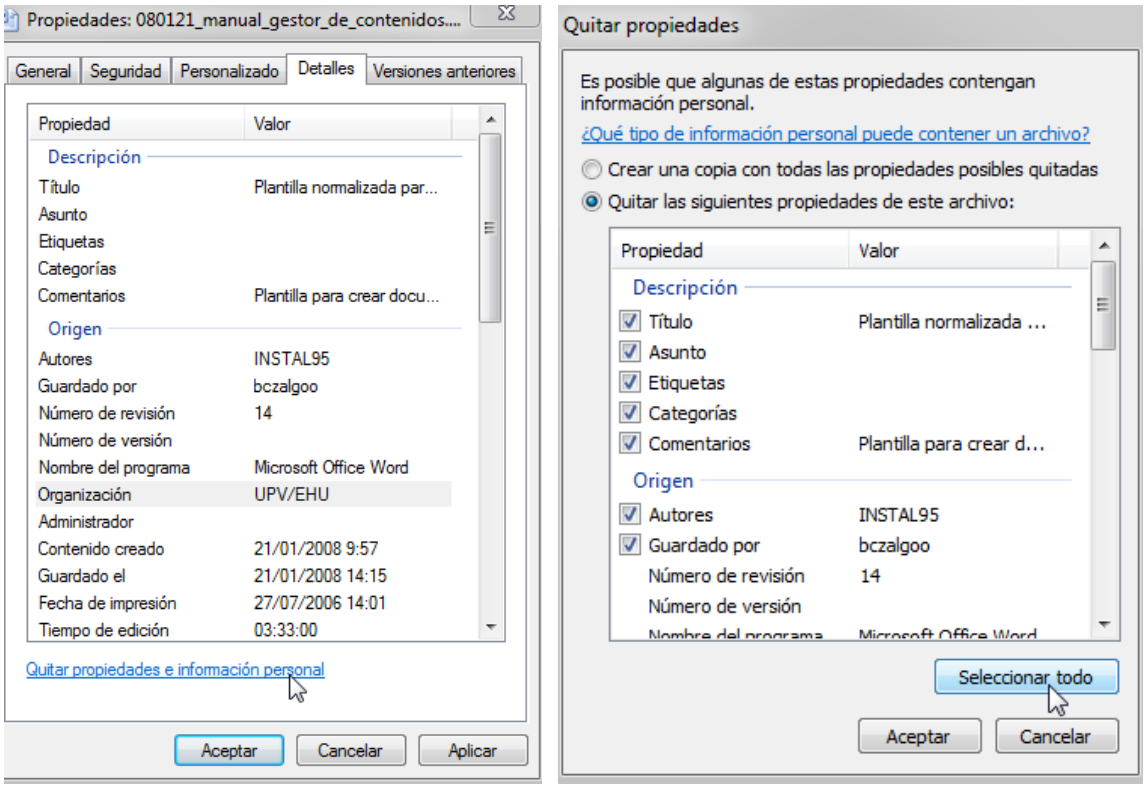
Siguiendo estas buenas prácticas se asegura que solo la información que se desea comunicar a otros sea realmente la compartida.

3.2. Identificar y eliminar metadatos en nuestro sistema

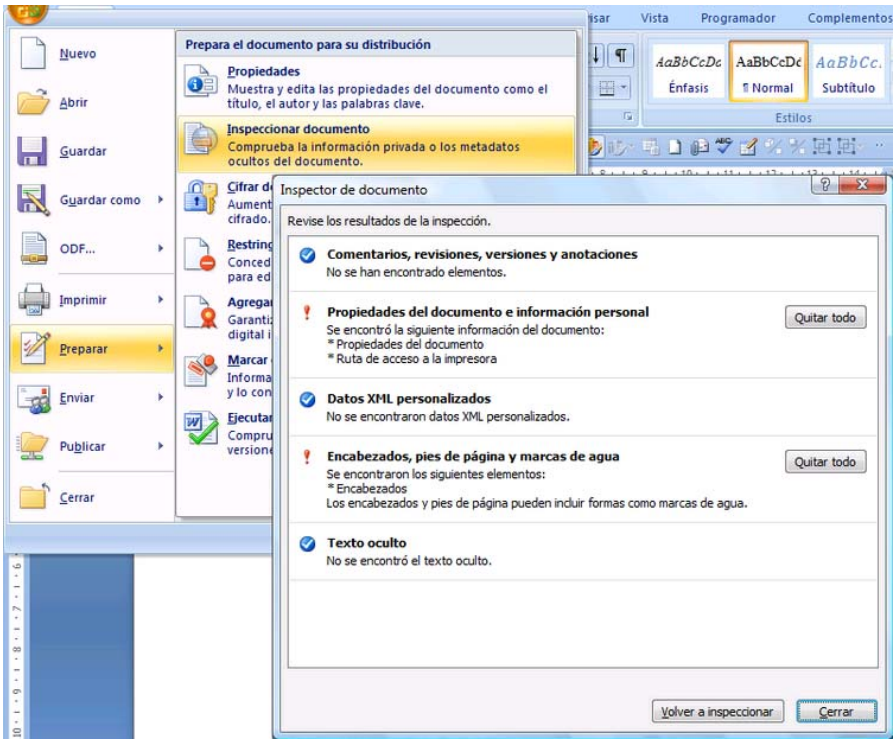
Al ser las fuentes de metadatos tan diversas, es difícil buscar una solución única para la limpieza de los metadatos. Según sea la herramienta de creación de documentos y el sistema operativo en el que se trabaje, los metadatos se identificarán y eliminarán de forma diferente.

Desafortunadamente, en muchos dispositivos y programas es difícil eliminar los metadatos de los archivos creados o editados. Se muestran a continuación algunos ejemplos.

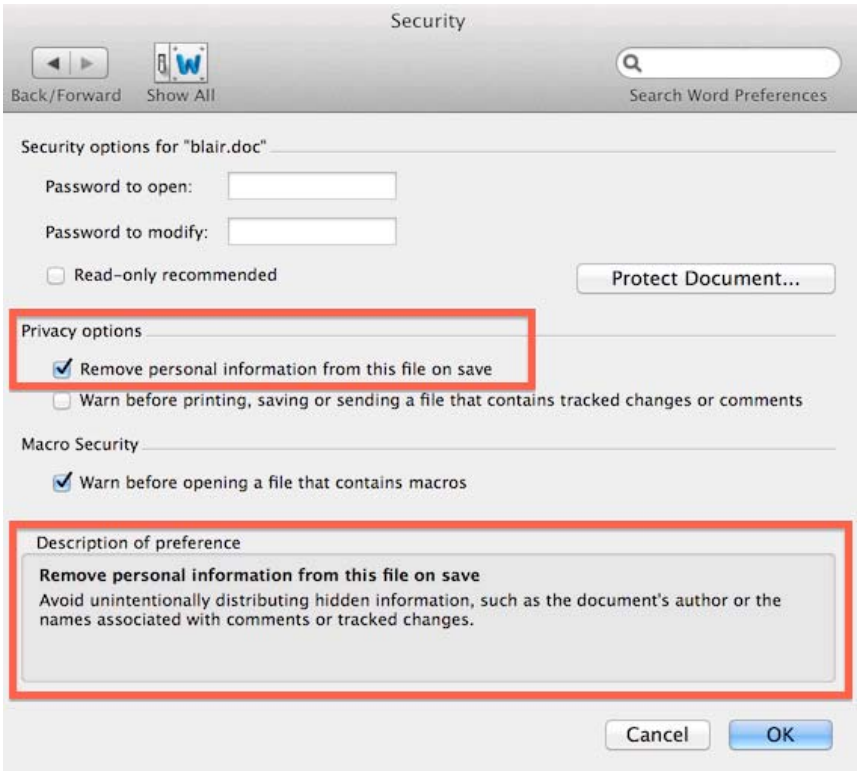
En Windows 7, existe la posibilidad de eliminar los metadatos, individualmente, accediendo a las Propiedades del Archivo (*click* con botón derecho del ratón), seleccionando la pestaña “Detalles” y pinchando en el enlace “Quitar propiedades e Información Personal”. Al seleccionar “Quitar las siguientes propiedades de este archivo”, pulsar botón “Seleccionar todo”, o bien, las propiedades que deseen eliminar y al pulsar “Aceptar” se eliminan los metadatos seleccionados del archivo.



Algunas aplicaciones incluyen herramientas específicas para eliminar metadatos. Por ejemplo, Microsoft Office 2007, 2010 y 2013, incorporan la opción “Inspeccionar documento” dentro del menú “Preparar”, que identifica los metadatos en un archivo Office, proporcionando las opciones para eliminar, selectivamente, algunos o todos los metadatos.



Aunque Microsoft Office para Mac no tiene esta herramienta, sí permite eliminar los metadatos de un documento Office accediendo en Preferencias/Seguridad/Privacidad y seleccionando “Eliminar información personal al guardar este archivo”.



La aplicación “Preview” de Mac OS X puede mostrar los metadatos de cualquier fotografía que se abra.

Existen numerosas herramientas que permiten inspeccionar documentos en busca de metadatos, y eliminarlos para evitar problemas de seguridad. Algunas son aplicaciones de código abierto y otras comerciales y están diseñadas para identificar, editar o eliminar metadatos en los archivos.

3.3. Revisión para publicación Web

Por la amplia difusión de los documentos publicados en las páginas Web, es recomendable dedicar especial atención a la tarea de limpieza de metadatos en documentos que van a ser publicados o ya lo están. Para ello es conveniente:

1. Usar herramientas de identificación y eliminación de metadatos por parte de los administradores de páginas Web en la US.
2. Usar herramientas de seguridad como *firewalls* o IDS/IPS bien configuradas, para detectar y frenar escaneos que buscan metadatos en documentos publicados en las Webs de la US.

4. Algunos recursos

Se adjunta documentación útil sobre metadatos y herramientas para tratarlos.

Documentación:

- *Guía de seguridad de las TIC (CCN-STIC-835): BORRADO DE METADATOS.* Guía del CCN-Cert para la inspección y borrado de los metadatos y otros datos ocultos existentes en los documentos electrónicos, incorporados de forma automática por los programas de generación y tratamiento de estos documentos, o por los propios usuarios de la organización.
- *Guía de seguridad (CCN-STIC-818): HERRAMIENTAS DE SEGURIDAD EN EL ENS.* Guía del CCN-Cert que incluye en su Anexo A, apartado “Limpieza de metadatos” algunas herramientas gratuitas y comerciales diseñadas para inspeccionar, editar y eliminar metadatos en diversos formatos para multitud de tipos de documentos.

Herramientas:

- *FOCA* (*Fingerprinting Organizations with Collected Archives*) es una herramienta utilizada para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en el disco local o en una página web.

- *GNU Libextractor* es una librería de software libre para extraer metadatos de cualquier tipo de archivo.
- *Exif Viewer* visualiza metadatos de imágenes y fotografías *online*.
- *Doc Scrubber* borra metadatos en documentos de Word generando una nueva versión del fichero.
- *BeCyPDFMetaEdit* es una herramienta de software libre que permite editar los metadatos de documentos PDF.
- *Metadata Analyzer* analiza y elimina metadatos de documentos Microsoft Office y Adobe PDF.
- *BatchPurifier* es una utilidad que detecta y elimina información oculta en documentos. La versión gratuita solo limpia ficheros JPEG.
- *MetaStripper* es una herramienta que se encarga de eliminar los metadatos EXIF, IPTC y COM de cualquier fotografía en formato JPEG.
- *OOMetaExtractor* extrae y limpia metadatos de documentos OpenOffice o LibreOffice.
- *Microsoft Remove Hidden Data* elimina metadatos de documentos creados con Microsoft Office.
- *MetaShield Protector* protege los entornos documentales mediante el análisis, filtrado y tratamiento de metadatos.
- *Metadata Extraction Tool* es una herramienta de software libre para limpieza de metadatos.
- *SnapsCleaner* es una herramienta de limpieza de metadatos para ordenadores MAC de Apple.

Apéndice: Lenguaje de género

Esta guía ha sido redactada con género masculino como género gramatical no marcado. Cuando proceda, será válido el uso del género femenino.