

## PROCEDIMIENTO PARA LA LIMPIEZA DE METADATOS

### Versión 1

#### 1.- Objeto

El objeto del presente documento es la definición del procedimiento para la limpieza de metadatos.

Al hacer uso de Internet, se publican y comparten todo tipo de ficheros. Estos ficheros pueden contener información privada o confidencial 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.

#### 2.- Ámbito de aplicación

Este procedimiento es de aplicación a todo el ámbito de actuación de la Universidad de Alicante, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información y en las Normas de Seguridad de la misma.

El presente procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Universidad de Alicante, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la misma.

En el ámbito del presente procedimiento, se entiende por usuario cualquier empleado público perteneciente o ajeno a la Universidad de Alicante, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Universidad y que utilice o posea acceso a los Sistemas de Información de la misma.

#### 3.- Vigencia

El presente procedimiento ha sido aprobado por la Comisión TI de la Universidad de Alicante, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la misma pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la Universidad de Alicante.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este procedimiento.

#### **4.- Revisión y evaluación**

La gestión de este Procedimiento corresponde al Responsable de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Responsable de Seguridad revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación de la Comisión TI de la Universidad de Alicante.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

#### **5.- Procedimiento para la limpieza de metadatos**

##### **5.1- Definiciones**

La Sociedad Española de Documentación e Información Científica (SEDIC), define metadato como “toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso u objeto de información que tiene la finalidad de facilitar su recuperación, autenticación, evaluación, preservación y/o interoperabilidad”.

En el caso de fotografías digitales, por ejemplo, la propia cámara a la vez que captura las imágenes puede ir guardando en forma de metadatos, información de cómo fue tomada la fotografía: fecha, hora, diafragma, velocidad, uso de flash, modo de captura o localización.

En el caso de documentos ofimáticos, los metadatos pueden almacenar información de quién lo creó, quién lo modificó, quien realizó el último acceso al documento y las fechas correspondientes, tiempo que ha tardado en editarse el documento, dispositivo o software utilizado para la creación del documento, o compañía y departamento al que pertenece.

##### **5.2- Medidas de protección**

La principal medida de protección para evitar que se publiquen en Internet documentos o se envíen 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.

Un conjunto de buenas prácticas sería:

- 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.
- 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 geolocalización de la cámara del móvil.

## 6.- Referencias

Guía de seguridad de las TIC (CCN-STIC-835): [BORRADO DE METADATOS](#).

¿Qué información contienen nuestros ficheros? 24 septiembre 2012, Blog del Servicio de Informática de la Universidad de Alicante. <https://blogs.ua.es/si/2012/09/24/que-informacion-contienen-nuestros-ficheros/>