DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

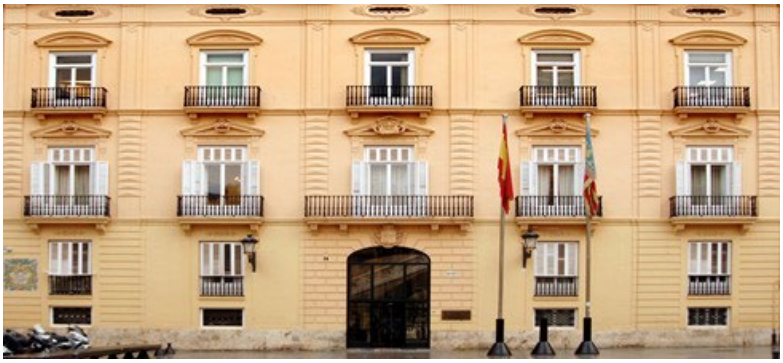
Cuadernos DivalData

Cuadernos dirigidos a delegados, responsables y especialistas en protección de datos personales

Cuaderno nº 24 | Junio 2022

EL BORRADO DE LOS METADATOS

Í N D I C E



EL BORRADO DE LOS METADATOS

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"LOS DOCUMENTOS CON LOS QUE TRABAJAMOS EN EL DÍA A DÍA CONTIENEN INFORMACIÓN ADICIONAL QUE, EN OCASIONES, PUEDE INCLUIR DATOS DE CARÁCTER PERSONAL DE LOS USUARIOS QUE HAN TRABAJADO SOBRE EL DOCUMENTO".

INTRODUCCIÓN

El artículo 32.1.b) del Reglamento General de Protección de Datos exige aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que incluya, entre otros, la capacidad de **garantizar la confidencialidad**.

Los documentos con los que trabajamos en el día a día contienen información adicional que, en ocasiones, puede incluir datos de carácter personal de los usuarios que han trabajado sobre el documento. Es información que no se aprecia a primera vista pero que puede ser accesible a través de las propiedades del documento. Por ello, si enviamos documentos a terceros o los publicamos en la página web, puede verse afectada la confidencialidad de la información si no procedemos previamente al borrado de los metadatos.

En este sentido, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, "ENS") regula el control "Limpieza de documentos [mp.info.5]". En virtud del mismo, se establece la obligación de retirar de los documentos toda 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 un servidor web u otro tipo de repositorio de información.

En el presente Cuaderno analizaremos los principales aspectos a tener en cuenta con el objeto de garantizar un borrado seguro de los metadatos y mitigar el riesgo de fugas de información. En este análisis nos basaremos principalmente en la Guía publicada por el Centro Criptológico Nacional: Guía de Seguridad de las TIC CCN-STIC 835 relativa al Borrado de Metadatos.

"EN EL CASO DE DOCUMENTOS OFIMÁTICOS, LOS METADATOS PUEDEN ALMACENAR INFORMACIÓN DE QUIÉN LO CREÓ, QUIÉN LO MODIFICÓ, QUIÉN REALIZÓ EL ÚLTIMO ACCESO…".

ASPECTOS GENERALES DE LOS METADATOS

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, autentificación, evaluación, preservación y/o interoperabilidad"*.

En el caso de documentos ofimáticos, los metadatos pueden almacenar información de quién lo creó, quién lo modificó, quién 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. Y, por ende, pueden aparecer datos de carácter personal al identificar o hacer identificable a los usuarios que crearon, modificaron o accedieron al documento.

El principal motivo para crear metadatos es facilitar la búsqueda de información relevante utilizando diversos criterios de búsqueda. Los metadatos pueden ayudar a organizar los documentos electrónicos, facilitar la interoperabilidad entre organizaciones, proveer la identificación digital y proporcionar soporte a la gestión del ciclo de vida de los documentos.

En el caso de documentos ofimáticos, también puede existir otro tipo de información oculta en el propio contenido del documento, como por ejemplo texto y objetos formateados como invisibles.

Ejemplo de campos que aparecen en el apartado de propiedades de un documento Word

- Título
- Asunto
- Etiquetas
- Categorías
- Comentarios
- Autores
- Guardado por
- Organización
- Administrador
- Fecha de impresión

RIESGOS Y AMENAZAS

Conforme a lo dispuesto en el considerando 74 del RGPD *"el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas".*

En aplicación del enfoque del riesgo exigido por la normativa vigente en materia de protección de datos, se deben tener en cuenta los riesgos asociados a los metadatos.

"SE HA DE CONSIDERAR QUE LOS METADATOS SON UNA FUENTE DE RIESGO, YA QUE PUEDEN CONTENER INFORMACIÓN SENSIBLE QUE NO DEBE REVELARSE A PERSONAL AJENO A LA ORGANIZACIÓN".

En este sentido, se ha de considerar que los metadatos son una fuente de riesgo, ya que pueden contener información sensible que no debe revelarse a personal ajeno a la organización.

El procedimiento a implementar en el borrado de metadatos de los documentos debe ser coherente con el principio de mínimo privilegio (también conocido como *"need to know"),* esto es, cada persona de la organización debe acceder exclusivamente a aquella información que necesite para el ejercicio de sus funciones.

Por ello, es necesario que la organización y los usuarios sean conscientes del riesgo que supone la fuga de esta información sensible, entre la se que se encuentra la información de carácter personal.

En el mejor de los casos, sólo dañará la reputación de la organización. En el peor de los casos, podría tener como consecuencias la invalidación contratos, pleitos, sanciones o causar serios perjuicios a la organización.

Se plantea a continuación el siguiente supuesto de hecho: través de los nombres de empleado y complementando con la búsqueda en redes sociales (por ejemplo, LinkedIn), se puede obtener todo un listado de empleados de la organización, sus cargos, e incluso sus correos electrónicos, lo cual puede servir para ataques de phishing.

PAUTAS A TENER EN CUENTA PARA EL CONTROL Y BORRADO DE METADATOS

Existen diversas herramientas de inspección y borrado de metadatos. Con carácter general, estas herramientas inspección y borrado de metadatos son automáticas, es decir, permiten aplicar una configuración específica de manera uniforme a toda la organización, para cumplir con los requisitos establecidos en la **Política de Gestión Documental** sobre la presencia de metadatos, y no requieren de la intervención de los usuarios.

Sin embargo, se pueden aplicar diversas pautas para revisar y eliminar los metadatos por parte de los usuarios. En este sentido, algunos sistemas operativos, como por ejemplo Microsoft Windows, permiten visualizar determinados metadatos contenidos en los documentos de forma sencilla, basta con seleccionar el archivo, hacer clic con el botón derecho del ratón y seleccionar Propiedades.

“ESTAS HERRAMIENTAS DE INSPECCIÓN Y BORRADO DE METADATOS SON AUTOMÁTICAS […] PERMITEN APLICAR UNA CONFIGURACIÓN ESPECÍFICA DE MANERA UNIFORME”.

MICROSOFT OFFICE

Los documentos generados por los programas de Microsoft Office (Word, Excel y PowerPoint) contienen metadatos en las Propiedades del documento que incluyen detalles sobre el archivo para describirlo e identificarlo, como el título, nombre del autor, asunto y etiquetas para identificar el contenido del documento y poder filtrar en las búsquedas.

Los programas Microsoft Office ofrecen varias opciones para llevar a cabo una configuración de seguridad que ejerza el control sobre los datos personales que se almacenan en el documento.

Son buenas prácticas, las siguientes:

- Especificar de forma apropiada la información personal que aparecerá en todos los documentos Office que un usuario vaya a crear o modificar.

  Esta información se encuentra en las opciones de configuración de Office y puede ser editada o eliminada, especificando con ello la información que se mostrará en Autor del documento, Última

persona que ha realizado modificaciones y Autor de comentarios de revisión del documento.

Una vez que se actualiza la información de una aplicación de Office, la información se actualiza automáticamente para el resto de aplicaciones de Office.

- Evitar que se archive información personal cuando se guarda un documento. Office permite seleccionar esta opción , de forma que cada vez que el documento se guarde, no se almacenará ningún metadato relacionado con información personal (Autor, Administrador, Última persona que ha realizado modificaciones en el documento, Compañía o Autor de comentarios de revisión del documento). Esta selección debe realizarse en cada documento.

"AL IGUAL QUE LOS DOCUMENTOS OFFICE, LOS DOCUMENTOS PDF DISPONEN TAMBIÉN DE PROPIEDADES DEL DOCUMENTO DONDE SE ALMACENAN METADATOS INSERTADOS DE FORMA AUTOMÁTICA".

DOCUMENTOS PDF

El presente apartado se refiere a los documentos generados por los programas Acrobat (en adelante, "documentos PDF")

Al igual que los documentos Office, los documentos PDF disponen también de propiedades del documento donde se almacenan metadatos insertados de forma automática por la aplicación o metadatos estándar y personalizados insertados por el usuario o la organización.

A estos metadatos se accede desde la opción de menú Archivo, seleccionando Propiedades.

CONSECUENCIAS DE LA VULNERACIÓN DEL DEBER DE CONFIDENCIALIDAD

Conforme a lo establecido en el artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD") establece que todas las personas que intervengan en cualquier fase del tratamiento estarán sujetas al deber de confidencialidad.

Garantizar el borrado de metadatos antes de enviar los documentos a terceros que no deben conocer esa información, así como documentos que se van a publicar en la página web, forma parte del deber de confidencialidad.

La vulneración del deber de confidencialidad establecido en el citado artículo constituye una **infracción muy grave**, en aplicación de lo dispuesto en el artículo 72.1.i LOPDGDD.

Actuar con diligencia en la gestión de los datos personales constituye un deber de todo el personal. Los datos personales deben ser protegidos en todas las fases de su tratamiento.

Dicha obligación se extiende a las entidades externas que participan y/o gestionan el tratamiento de datos personales.

Por ello, es importante garantizar que se formaliza con los proveedores el correspondiente contrato de encargo que incluya el contenido mínimo exigido por el artículo 28 RGPD.

Entre otros aspectos, se requiere que el encargado del tratamiento garantice que:

> "*las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria*.

"GARANTIZAR EL BORRADO DE METADATOS ANTES DE ENVIAR LOS DOCUMENTOS A TERCEROS QUE NO DEBEN CONOCER ESA INFORMACIÓN, ASÍ COMO DOCUMENTOS QUE SE VAN A PUBLICAR EN LA PÁGINA WEB, FORMA PARTE DEL DEBER DE CONFIDENCIALIDAD"

MATERIAL COMPLEMENTARIO

- Guía de Seguridad de las TIC CCN-STIC 835. Esquema Nacional de Seguridad. Borrado de Metadatos. Consulta este enlace.
- Guía sobre borrado seguro de la información. Instituto Nacional de Ciberseguridad (INCIBE). Consulta este enlace.
- Guía: "Protección de datos por defecto" Agencia Española de Protección de Datos (AEPD). Consulta este enlace.
- Guía: "Gestión del riesgo y evaluación de impacto en tratamiento de datos personales" Agencia Española de Protección de Datos (AEPD). Consulta este enlace.
- Dictamen 05/2014 sobre técnicas de anonimización. Consulta este enlace.

NOTICIAS

- **La AEPD impone una sanción de apercibimiento a una Asociación por una infracción del artículo 5.1.f) del RGPD (principio de integridad y confidencialidad) y del artículo 32 RGPD (seguridad del tratamiento).** En el presente caso, los hechos consitutivos de infracción consisten en la publicación de forma abierta una resolución con los datos personales del reclamante ya que, aunque se colocaba un rectángulo negro encima de su nombre y apellidos, este texto no era eliminado, y aparecía en el pdf, por lo que era posible acceder a él. El reclamado alegaba que se realiza un análisis de los archivos indexados en buscadores usando un software específico que se utiliza principalmente para encontrar metadatos e información oculta en los documentos que examina y que se publican en la página web. Sin embargo, no se analiza el contenido de los documentos, sino solamente los metadatos asociados. Tanto el contenido del documento como los metadatos asociados al mismo deben ser revisados para evitar que se publiquen de forma indebida datos personales. Consulta la resolución en este enlace.

- **La AEPD impone una sanción de apercibimiento a una Asociación por una infracción del artículo 5.1.f) del RGPD (principio de integridad y confidencialidad), en relación con el artículo 5 LOPDGDD (deber de confidencialidad).** Sin entrar en el fondo del asunto, cabe destacar que el Ayuntamiento reclamado alega, entre otras cuestiones, que ha comprobado si en su portal de transparencia existían metadatos en el archivo susceptibles de ser objeto de indexación por los motores de búsqueda en internet, no localizándose que el contenido del mismo hubiera sido objeto de indexación por parte de buscadores de internet. Consulta en este enlace.