

DIPUTACIÓ DE
VALÈNCIA



Protecció de Dades i Seguretat de la Informació



Quaderns DivalData

Quaderns adreçats a delegats, responsables
i especialistes en protecció de dades
personals

Quadern núm. 24 | Juny 2022

L'ESBORRAT DE LES METADADES



Í N D E X



L' ESBORRAT DE LES METADADES

	Pàgina
Introducció	2
Aspectes generals de les metadades	3
Riscos i amenaces	4
Pautes a tenir en compte per al control i esborrat de les metadades	5
Conseqüències de la vulneració del deure de confidencialitat	7
Material complementari i notícies	8



Us convidem a traslladar-nos aquelles temàtiques que resultin del vostre interès per als propers butlletins informatius. Aquestes peticions s'hauran d'adreçar a:

Diputació de València

Departament de Protecció de Dades i
Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedeix al següent

[enllaç](#)



**"ELS DOCUMENTS AMB QUÈ
TREBALLEM EN EL DIA A DIA CONTENEN
INFORMACIÓ ADDICIONAL QUE, EN
OCASIONS, POT INCLOURE DADES DE
CARÀCTER PERSONAL DELS USUARIS
QUE HAN TREBALLAT SOBRE EL
DOCUMENT".**

INTRODUCCIÓ

L'article 32.1.b) del Reglament General de Protecció de Dades exigeix aplicar mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc que inclogui, entre d'altres, la capacitat de **garantir la confidencialitat**.

Els documents amb què treballem en el dia a dia contenen informació addicional que, en ocasions, pot incloure dades de caràcter personal dels usuaris que han treballat sobre el document. És informació que no s'aprecia a primera vista però que pot ser accessible a través de les propietats del document. Per això, si enviem documents a tercers o els publiquem a la pàgina web, es pot veure afectada la confidencialitat de la informació si no procedim prèviament a l'esborrat de les metadades.

En aquest sentit, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en endavant, "ENS") regula el control "Limpieza de documentos [mp.info.5]". En virtut d'aquest, s'estableix l'obligació de retirar dels documents tota informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, llevat quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura és especialment rellevant quan el document es difon àmpliament, com passa quan s'ofereix al públic un servidor web o un altre tipus de repositori d'informació.

En el present Quadern analitzarem els principals aspectes a tenir en compte amb l'objecte de garantir un esborrat segur de les metadades i mitigar el risc de fugues d'informació. En aquesta anàlisi ens basarem principalment en la Guia publicada pel Centre Criptològic Nacional: Guia de Seguretat de les TIC CCN-STIC 835 relativa a l'Esborrat de Metadades.



**"EN EL CAS DE DOCUMENTS
OFIMÀTICS, LES METADADES PODEN
EMMAGATZEMAR INFORMACIÓ DE
QUI EL VA CREAR, QUI EL VA
MODIFICAR, QUI VA REALITZAR
L'ÚLTIM ACCÉS...".**

ASPECTES GENERALS DE LES METADADES

La Societat Espanyola de Documentació i Informació Científica (SEDIC), defineix com *"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 cas de documents ofimàtics, les metadades poden emmagatzemar informació de qui el va crear, qui el va modificar, potserva realitzar l'últim accés al document i les dates corresponents, temps que ha tardat a editar-se el document, dispositiu o programari utilitzat per a la creació del document, o companyia i departament al qual pertany. I, per tant, poden aparèixer dades de caràcter personal en identificar o fer identificable els usuaris que van crear, modificar o accedir al document.

El principal motiu per crear metadades és facilitar la recerca d'informació rellevant utilitzant diversos criteris de recerca. Les metadades poden ajudar a organitzar els documents electrònics, facilitar la interoperabilitat entre organitzacions, proveir la identificació digital i proporcionar suport a la gestió del cicle de vida dels documents.

En el cas de documents ofimàtics, també pot existir un altre tipus d'informació oculta en el propi contingut del document, com per exemple text i objectes com a invisibles.

Exemple de camps que apareixen a l'apartat de propietats d'un document Word

- Títol
- Assumpte
- Etiquetes
- Categories
- Comentaris
- Autors
- Guardat per
- Organització
- Administrador
- Data d'impressió



RISCOS I AMENACES

**"S'HA DE CONSIDERAR QUE LES
METADADES SÓN UNA FONT DE RISC,
JA QUE PODEN CONTENIR
INFORMACIÓ SENSIBLE QUE NO S'HA
DE REVELAR A PERSONAL ALIÈ A
L'ORGANITZACIÓ".**

D'acord amb el que disposa el 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 aplicació de l'enfocament en el risc exigít per la normativa vigent en matèria de protecció de dades, s'han de tenir en compte els riscos associats a les metadades.

En aquest sentit, s'ha de considerar que les metadades són una font de risc, ja que poden contenir informació sensible que no s'ha de revelar a personal aliè a l'organització.

El procediment a implementar en l'esborrat de metadades dels documents ha de ser coherent amb el principi de mínim privilegi (també conegut com a *"need to know"*), això és, cada persona de l'organització ha d'accedir exclusivament a aquella informació que necessiti per a l'exercici de les seves funcions.

Per això, cal que l'organització i els usuaris siguin conscients del risc que suposa la fuga d'aquesta informació sensible, entre la qual es troba la informació de caràcter personal.

En el millor dels casos, només danyarà la reputació de l'organització. En el pitjor dels casos, podria tenir com a conseqüències la invalidació contractes, plets, sancions o causar seriosos perjudicis a l'organització.

Es planteja a continuació el següent supòsit de fet: a través dels noms d'empleat i complementant amb la recerca en xarxes socials (per exemple, LinkedIn), es pot obtenir tot un llistat d'empleats de l'organització, els seus càrrecs, i fins i tot els seus correus electrònics, la qual cosa pot servir per a atacs de phishing.



**"AQUESTES EINES D'INSPECCIÓ I
ESBORRAT DE METADADES SÓN
AUTOMÀTIQUES [...] PERMETEN
APLICAR UNA CONFIGURACIÓ
ESPECÍFICA DE MANERA UNIFORME".**

PAUTES A TENIR EN COMPTE PER AL CONTROL I ESBORRAT DE METADADES

Hi ha diverses eines d'inspecció esborrat de metadades. Amb caràcter general, aquestes eines i esborrat de metadades són automàtiques, és a dir, permeten aplicar una configuració específica de manera uniforme a tota l'organització, per complir amb els requisits establerts en la **Política de Gestió Documental** sobre la presència de metadades, i no requereixen de la intervenció dels usuaris.

Tanmateix, es poden aplicar diverses pautes per revisar i eliminar les metadades per part dels usuaris. En aquest sentit, alguns sistemes operatius, com per exemple Microsoft Windows, permeten visualitzar determinades metadades contingudes en els documents de forma senzilla, n'hi ha prou amb seleccionar l'arxiu, fer clic amb el botó dret del ratolí i seleccionar Propietats.

MICROSOFT OFFICE

Els documents generats pels programes de Microsoft Office (Word, Excel i PowerPoint) contenen metadades en les Propietats del document que inclouen detalls sobre l'arxiu per descriure'l i identificar-lo, com el títol, nom de l'autor, assumpte i etiquetes per identificar el contingut del document i poder filtrar en les recerques.

Els programes Microsoft Office ofereixen diverses opcions per dur a terme una configuració de seguretat que exerceixi el control sobre les dades personals que s'emmagatzemen en el document.

Són bones pràctiques, les següents:

- Especificar de forma apropiada la informació personal que apareixerà en tots els documents Office que un usuari vagi a crear o modificar.

Aquesta informació es troba en les opcions de configuració d'Office i pot ser editada o eliminada, especificant amb això la informació que es mostrarà en Autor del document, Última persona que ha realitzat modificacions i Autor de comentaris de revisió del document.



**"IGUAL QUE ELS DOCUMENTS OFFICE,
ELS DOCUMENTS PDF DISPOSEN
TAMBÉ DE PROPIETATS DEL
DOCUMENT ON S' EMMAGATZEMEN
METADADES INSERIDES DE FORMA
AUTOMÀTICA".**

Un cop s' actualitza la informació d' una aplicació d'Office, la informació s'actualitza automàticament per a la resta d'aplicacions d'Office.

- Evitar que s'arxivi informació personal quan es guarda un document. Office permet seleccionar aquesta opció, de manera que cada vegada que el document es guardi, no s'emmagatzemarà cap metadada relacionada amb informació personal (Autor, Administrador, Última persona que ha realitzat modificacions en el document, Companyia o Autor de comentaris de revisió del document). Aquesta selecció s' ha de realitzar en cada document.

DOCUMENTS PDF

El present apartat es refereix als documents generats pels programes Acrobat (en endavant, "documents PDF")

Igual que els documents Office, els documents PDF disposen també de propietats del document on s'emmagatzemen metadades inserides de forma automàtica per l'aplicació o metadades estàndard i personalitzades inserides per l usuari o l'organització.

A aquestes metadades s'hi accedeix des de l'opció de menú Arxiu, seleccionant Propietats.



**"GARANTIR L'ESBORRAT DE
METADADES ABANS D'ENVIAR ELS
DOCUMENTS A TERCERS QUE NO HAN
DE CONÈIXER AQUESTA INFORMACIÓ,
AIXÍ COM DOCUMENTS QUE ES
PUBLICARAN A LA PÀGINA WEB,
FORMA PART DEL DEURE DE
CONFIDENCIALITAT"**

CONSEQÜÈNCIES DE LA VULNERACIÓ DEL DEURE DE CONFIDENCIALITAT

D'acord amb el que estableix l'article 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD") estableix que totes les persones que intervinguin en qualsevol fase del tractament estaran subjectes al deure de confidencialitat.

Garantir l'esborrat de metadades abans d'enviar els documents a tercers que no han de conèixer aquesta informació, així com documents que es publicaran a la pàgina web, forma part del deure de confidencialitat.

La vulneració del deure de confidencialitat establert a l'esmentat article constitueix una **infracció molt greu**, en aplicació del que disposa l'article 72.1.i LOPDGDD.

Actuar amb diligència en la gestió de les dades personals constitueix un deure de tot el personal. Les dades personals han de ser protegides en totes les fases del seu tractament.

Aquesta obligació s'estén a les entitats externes que hi participen i/o gestionen el tractament de dades personals.

Per això, és important garantir que es formalitza amb els proveïdors el corresponent contracte d'encàrrec que inclogui el contingut mínim exigít per l'article 28 RGPD.

Entre altres aspectes, es requereix que l'encarregat del tractament garanteixi 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."



MATERIAL COMPLEMENTARI

- Guía de Seguridad de las TIC CCN-STIC 835. Esquema Nacional de Seguridad. Borrado de Metadatos. Consulta [aquest enllaç](#).
- Guía sobre borrado seguro de la información. Instituto Nacional de Ciberseguridad (INCIBE). Consulta [aquest enllaç](#).
- Guía: "Protección de datos por defecto" Agència Espanyola de Protecció de Dades (AEPD). Consulta [aquest enllaç](#).
- Guía: "Gestión del riesgo y evaluación de impacto en tratamiento de datos personales" Agència Espanyola de Protecció de Dades (AEPD). Consulta [aquest enllaç](#).
- Dictamen 05/2014 sobre tècniques d'anonimització. Consulta [aquest enllaç](#).

NOTÍCIES

- **L'AEPD imposa una sanció d'advocament a una Associació per una infracció de l'article 5.1.f) del RGPD (principi d'integritat i confidencialitat) i de l'article 32 RGPD (seguretat del tractament).** En el present cas, els fets consitutius d'infracció consisteixen en la publicació de forma oberta una resolució amb les dades personals del reclamant ja que, tot i que es col·locava un rectangle negre damunt del seu nom i cognoms, aquest text no era eliminat, i apareixia al pdf, per la qual cosa era possible accedir-hi. El reclamant al·legava que es realitza una anàlisi dels arxius indexats en cercadors fent servir un programari específic que s'utilitza principalment per trobar metadades i informació oculta en els documents que examina i que es publiquen a la pàgina web. Tanmateix, no s'analitza el contingut dels documents, sinó només les metadades associades. Tant el contingut del document com les metadades associades a aquest han de ser revisades per evitar que es publiquen de forma indeguda dades personals. Consulta la resolució en [aquest enllaç](#).
- **L'AEPD imposa una sanció d'advertir a una Associació per una infracció de l'article 5.1.f) del RGPD (principi d'integritat i confidencialitat), en relació amb l'article 5 LOPDGDD (deure de confidencialitat).** Sense entrar en el fons de l'assumpte, cal destacar que l'Ajuntament reclamant al·lega, entre altres qüestions, que ha comprovat si en el seu portal de transparència existien metadades en l'arxiu susceptibles de ser objecte d'indexació pels motors de cerca a internet, no localitzant-se que el contingut del mateix haja sigut objecte d'indexació per part de cercadors d'internet. Consulta en [aquest enllaç](#).