Comunidad de Madrid

Grupo de trabajo para la protección de datos personales

RECOMENDACIONES SOBRE LA ANONIMIZACIÓN Y SEUDONIMIZACIÓN DE DATOS PERSONALES

ÍNDICE

1.- CONCEPTO 3

2.- NORMATIVA 4

3.- PRINCIPALES DIFERENCIAS ENTRE ANONIMIZACIÓN Y SEUDONIMIZACIÓN 4

4.- TÉCNICAS DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN 6

5.- SUPUESTOS DE APLICACIÓN 8

5.1.- NOTIFICACIONES POR MEDIO DE ANUNCIOS Y PUBLICACIONES DE ACTOS ADMINISTRATIVOS 8

5.2.- PUBLICACIÓN DE DOCUMENTOS QUE FORMAN PARTE DE PROCEDIMIENTOS Y TRÁMITES ADMINISTRATIVOS 9

5.2.1.- REGLA GENERAL, APLICABLE A LA PUBLICACION EN LA SEDE ELECTRÓNICA DE LA COMUNIDAD DE MADRID (SEDE.COMUNIDAD.MADRID) Y EN OTROS PORTALES DE LA COMUNIDAD DE MADRID. 9

5.2.2.- CONTRATACIÓN PÚBLICA 10

5.2.3.- CONVENIOS ADMINISTRATIVOS 11

5.2.4.- SUBVENCIONES Y AYUDAS PÚBLICAS 11

5.2.5.- HUELLA NORMATIVA 12

5.3.- ACCESO A LA INFORMACIÓN PÚBLICA 12

5.4.- DERECHO DE INFORMACIÓN DE LOS DIPUTADOS 14

5.5.- ÓRGANOS COLEGIADOS 15

5.5.1.- ACTAS DE LAS SESIONES 15

5.5.2.- ACUERDOS ADOPTADOS EN LAS SESIONES 15

5.6.- AVISO INFORMATIVO SOBRE LOS DOCUMENTOS CENSURADOS 16

6.- ENLACES DE INTERÉS 16

ANEXO 17

1.- CONCEPTO

- La **ANONIMIZACIÓN** es un proceso de desvinculación de aquellos datos personales que permiten identificar, directa o indirectamente, a una persona, haciendo imposible que a través de esos datos anonimizados se pueda identificar o reidentificar a la misma.

  Es lo que la Agencia Española de Protección de Datos (AEPD) define como la "ruptura de la cadena de identificación de las personas", siendo su finalidad la de eliminar, de forma irreversible y permanente, cualquier posibilidad de identificación del individuo.

  - ❖ Por ejemplo, la publicación de estadísticas agregadas con los porcentajes de población activa desempleada por municipios de la Comunidad de Madrid.

- La **SEUDONIMIZACIÓN**, por su parte, es definida en el artículo 4.5) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD), como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

  - ❖ Por ejemplo, cambiar el nombre y apellidos del interesado por una clave numérica que no incida ni esté relacionada con esos datos. Solo quien posee la información adicional que establece el vínculo entre los datos personales y el interesado, puede llegar a identificar a la persona.

- Transformar un conjunto de datos personales en información anónima o seudonimizada exige realizar un tratamiento sobre datos personales, que puede afectar a:

  a) Los datos que facilitan la identificación directa de un individuo: DNI/NIF/NIE/Pasaporte, nombre y apellidos, domicilio, teléfono, correo electrónico, etc.

  b) Los datos que pueden contribuir indirectamente a su identificación, bien por separado, o bien agrupados, es decir, identificadores indirectos o cuasi-identificadores, a modo de variables que, en combinación con otra información, permiten la identificación de las personas (sexo, edad, estado civil, código postal u otros datos de localización); fechas significativas (nacimiento, fecha de ingreso hospitalario, etc.), profesiones, raza, pertenencia a grupos sociales minoritarios, ingresos económicos, características antropométricas o físicas, tatuajes o marcas específicas, etc.

  c) Los datos que individualizan a la persona dentro de un conjunto: puesto o cargo en una entidad, como pudiera ser el de presidente, secretario, etc.

2.- NORMATIVA

Hay que tener en cuenta que la anonimización y seudonimización no son exclusivamente técnicas de enmascaramiento, sino que están reguladas, con sus correspondientes obligaciones y efectos a cumplir por el Responsable del tratamiento, en la normativa que se indica a continuación:

- RGPD:
  - Considerando 26
  - Artículo 6.4.e)
  - Artículo 25.1
  - Artículo 32.1.a)

- LOPDGDD:
  - Artículo 28.2.a)
  - Artículo 72. 1.p)
  - Disposición adicional decimoséptima

3.- PRINCIPALES DIFERENCIAS ENTRE ANONIMIZACIÓN Y SEUDONIMIZACIÓN

- Por su **vinculación** con una persona física:

  - La información anónima es un conjunto de datos que no guarda relación con una persona física identificada o identificable.

  - La información seudonimizada es un conjunto de datos que no puede atribuirse a una persona sin utilizar información adicional. Se tratan los datos personales sin los datos identificativos del interesado, pero sin suprimir la vinculación entre los datos que consigan determinar la persona titular de los mismos.

- Por su **posibilidad de reversión**:

  - La anonimización es un procedimiento donde los datos identificativos se disocian totalmente de los datos personales, es un proceso irreversible.

  - La seudonimización desvincula los datos identificativos, pero los datos seudonimizados mantienen datos adicionales que pueden reidentificar a los interesados, por tanto, es un procedimiento reversible.

- Por su **tratamiento normativo**:

  - Los datos anonimizados no están bajo el ámbito de aplicación del RGPD, al no existir una posibilidad razonable de que se pueda identificar a una persona física en un conjunto de datos, en la medida que es posible demostrar objetivamente que no existe capacidad material para asociar los datos anonimizados a una persona física

determinada, directa o indirectamente, ya sea mediante el uso de otros conjuntos de datos, informaciones o medidas técnicas y materiales que pudieran existir a disposición de terceros.

- Los datos seudonimizados sí están bajo el ámbito de aplicación del RGPD, al existir tal posibilidad de reidentificación si no se adoptan las medidas oportunas.

- Por su **resultado**:

  - El tratamiento de anonimización genera un único y nuevo conjunto de datos.

  - El tratamiento de seudonimización genera dos nuevos conjuntos de datos: la información seudonimizada y la información adicional que permite revertir la seudonimización.

- En función de las **garantías técnicas, organizativas o de cualquier otra naturaleza a adoptar,** según se trate de una anonimización o seudonimización, cabe distinguir las siguientes diferencias:

  1. Para datos anonimizados:

     - La robustez del proceso de anonimización contra la posible reidentificación.

     - Es necesario poder demostrar el estudio previo realizado para el tratamiento de anonimización (técnicas empleadas, garantizar la calidad en las mismas, etc.) y determinar cómo evoluciona el riesgo de reidentificación a lo largo del tiempo.

  2. Para datos seudonimizados:

     - Se deben de adoptar las garantías oportunas para que se impida la reidentificación sin disponer de la información adicional, debiendo:

       - No emplear una misma clave de cifrado para diferentes bases de datos.
       - No guardar las claves de cifrado junto a las bases de datos que pueden descifrar.
       - Usar claves distintas o claves rotatorias para cada usuario.

     - Actúan como garantías, entre otras, las limitaciones que se establezcan a las finalidades, el periodo de conservación o la comunicación de los datos seudonimizados.

     - Se podrán asumir garantías adicionales derivadas del riesgo analizado para los derechos y libertades de las personas físicas.

- Las que impidan la materialización de brechas de datos personales, tanto sobre conjunto seudonimizado como de la información adicional.

A la vista de las características señaladas, es importante tener en cuenta que en la anonimización existirá siempre un índice de probabilidad de reidentificación que, además, se incrementa a medida que transcurre el tiempo, como consecuencia de la evolución e incremento de los identificadores indirectos (por ejemplo, la información que el propio interesado haya aportado sobre sí mismo en redes sociales, blogs, etc.), así como debido a la propia evolución y desarrollo de la tecnología.

Por lo tanto, resulta necesario que el Responsable del tratamiento realice un análisis de riesgos tanto de las actuaciones tendentes a la anonimización o seudonimización, con especial atención a la primera en la intención de atenuar al máximo cualquier probabilidad de reidentificación, así como una reevaluación periódica del riesgo residual existente con el fin de introducir parámetros de mejora de la calidad del proceso de anonimización, si fuera preciso.

Para una información más detallada en diferentes aspectos sobre este tema, consultar los "Enlaces de interés" de este documento.

4.- TÉCNICAS DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN

En el Anexo de las presentes recomendaciones se indican, de forma detallada, diversas técnicas de enmascaramiento y los pasos a seguir en cada una de ellas. Es importante tener en cuenta que estas técnicas podrán ser aplicables a la anonimización o seudonimización de datos personales, en función del carácter irreversible o no de su resultado, como se ha visto anteriormente.

Por su parte, la AEPD ha publicado los siguientes documentos, que recogen diversas técnicas de anonimización, y el Responsable del tratamiento podrá asimismo utilizarlas alternativamente o bien pedir su implementación, por ser, en su caso, necesarias para el desarrollo de su trabajo, a Madrid Digital:

- "Orientaciones y garantías en los procedimientos de anonimización de datos personales, en las que se incluyen los términos y técnicas de anonimización de datos personales: https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

- Guía básica de anonimización de la Autoridad de Protección de Datos de Singapur, con importante valor didáctico: https://www.aepd.es/es/documento/guia-basica-anonimizacion.pdf

  En esta última, se facilita una herramienta básica para proceder a la anonimización: https://www.aepd.es/es/descargas/herramienta-anonimizacion-pdpc

- "La adopción de técnicas de seudonimización en el sector sanitario": https://www.aepd.es/es/documento/tecnicas-seudonimizacion-sector-sanitario-enisa.pdf

Por otra parte, la Administración General del Estado ha publicado la Guía "Introducción a la anonimización de datos", que puede consultarse en el siguiente enlace: https://datos.gob.es/sites/default/files/doc/file/informe-anonimizacion-es.pdf

Todas las técnicas que se indican sirven para combatir los riesgos que afectan a la confidencialidad de datos personales y que, generalmente, se agrupan de la forma siguiente:

- Singularización: Es la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.

- Vinculabilidad: Consiste en relacionar, al menos, dos datos referentes al mismo interesado o grupo de interesados, por medio de una o varias fuentes de datos.

- Inferencia: Consiste en deducir, con una alta probabilidad el valor de un atributo, al que no se tiene acceso, a través de otros menos críticos a los que sí se puede acceder en un conjunto de atributos.

En cualquier caso, respecto de las posibles técnicas a utilizar en relación con datos personales que pudieran constar en sistemas de información u otros servicios tecnológicos (cifrado, descomposición en tokens, función hash, etc.[1]), se recomienda consultar con el Encargado del tratamiento, para que informe de las posibilidades existentes a tal efecto y, sin perjuicio de ello, **realizar en todo caso consulta a la Agencia para la Administración Digital de la Comunidad de Madrid (Madrid Digital).**

En particular, respecto de la eliminación de metadatos en los documentos ofimáticos que vayan a ser objeto de publicación o en el caso de envío a terceros, Madrid Digital ha confeccionado una infografía para la limpieza de los mismos, que pueden ser objeto de consulta en el siguiente enlace: http://edicion.comunidad.madrid/sites/default/files/eliminar_metadatos_en_documentos.pdf.

También se considera muy útil la información facilitada por el Instituto Nacional de Ciberseguridad (INCIBE), que se puede consultar en la siguiente página: https://www.incibe.es/protege-tu-empresa/blog/son-los-metadatos-y-eliminarlos.

Sin perjuicio de ello, es muy importante recordar que la eliminación de metadatos no debe aplicarse en modo alguno al documento original, respecto al cual el tratamiento de datos se rige por su normativa específica.

[1] Ver Dictamen 05/2014 del GT 29, sobre técnicas de anonimización: https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf.

Para una información más detallada en diferentes aspectos sobre este tema, consultar los "Enlaces de interés" de este documento.

5.- SUPUESTOS DE APLICACIÓN

5.1.- NOTIFICACIONES POR MEDIO DE ANUNCIOS Y PUBLICACIONES DE ACTOS ADMINISTRATIVOS

Su contenido viene establecido en la Disposición adicional séptima de la LOPDGDD, dedicada a la identificación de los interesados en las publicaciones de actos administrativos y en las notificaciones practicadas mediante anuncios, resultando de aplicación los siguientes extremos:

- En el supuesto de **publicaciones de actos administrativos** que contuvieran datos personales del afectado, se seguirán las recomendaciones de la AEPD en su documento "**Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD"** https://www.aepd.es/sites/default/files/2019-09/orientaciones-da7.pdf:

  - Dado un DNI con formato 12345678X, se publicarán los dígitos que en el formato ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.
  - Dado un NIE con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, evitando el primer carácter alfabético, cuarta, quinta, sexta y séptima. En el ejemplo: ****4567*.
  - Dado un pasaporte con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: *****3456.
  - Dado otro tipo de identificación, siempre que esa identificación contenga al menos 7 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima. Por ejemplo, en el caso de la identificación como: XY12345678AB, la publicación sería: *****4567***.
  - Si ese tipo de identificación es distinto de un pasaporte y tiene menos de 7 dígitos numéricos, se numerarán todos los caracteres, alfabéticos incluidos, con el mismo procedimiento anterior y se seleccionarán aquellos que ocupen las cuatro últimas posiciones. Por ejemplo, en el caso de una identificación como: ABCD123XY, la publicación sería: *****23XY.

    Los caracteres alfabéticos, y aquellos numéricos no seleccionados para su publicación, se sustituirán por asteriscos por cada posición.

Cuando se trate de la **notificación por medio de anuncios**, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad,

número de identidad de extranjero, pasaporte o documento equivalente; salvo las personas físicas que se encuentren en situación de especial vulnerabilidad, como es el caso de víctimas de violencia de género, cuando esta publicación pudiera incidir sobre esta situación.

- Cuando **el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores**, se identificará al afectado únicamente mediante su nombre y apellidos.

- En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

5.2.- PUBLICACIÓN DE DOCUMENTOS QUE FORMAN PARTE DE PROCEDIMIENTOS Y TRÁMITES ADMINISTRATIVOS

5.2.1.- REGLA GENERAL, APLICABLE A LA PUBLICACION EN LA SEDE ELECTRÓNICA DE LA COMUNIDAD DE MADRID (SEDE.COMUNIDAD.MADRID) Y EN OTROS PORTALES DE LA COMUNIDAD DE MADRID.

- Los actos administrativos que se publiquen en la sede electrónica de la Comunidad de Madrid lo serán conforme a lo dispuesto en el apartado anterior.

- Respecto de la publicación de documentos en esta sede que no se refieran a las publicaciones mencionadas en el apartado 5.1, y salvo que pudiera haber legislación sectorial que dispusiera otra medida, se indican, con carácter general, las siguientes recomendaciones:

  - En el caso de que el documento contenga firmas electrónicas deberá ocultarse el DNI/NIE/Pasaporte cuando este sea visible en el recuadro de firma.

  - Igualmente deberán ocultarse, en su caso, las firmas manuscritas y rúbricas o "*visé*".

  - Se ocultará el CSV (Código Seguro de Verificación) de todas las páginas de los documentos firmados electrónicamente, que posibilita obtener el documento electrónico original. Si aparecen códigos de barras, estos también deberán ser ocultados en todas las páginas.

- Estas recomendaciones son aplicables, con carácter general, a los documentos que se publiquen en otros portales o páginas web de la Comunidad de Madrid salvo que su publicación venga regulada por normativa específica o estén recogidos en otros apartados de esta guía.

5.2.2.- CONTRATACIÓN PÚBLICA

- A efectos de su publicación en el Perfil del Contratante, en su apartado dedicado a la Publicidad de las contrataciones del Portal de Contratación de la Comunidad de Madrid (artículos 63, 154.1 y 346.3 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en adelante, LCSP):

    1. Los **datos identificativos** de personas físicas contenidos en los documentos de los expedientes de contratación pública, o en las firmas electrónicas de estos documentos, que han de ser objeto de publicación, habrían de constar en los siguientes términos:

        - Licitadores, adjudicatarios o contratistas: nombre y apellidos, sin acompañarlo de los datos del DNI/NIE o cualquier otro documento identificativo (por ejemplo, pasaporte).
        - Empleados públicos que intervienen en el procedimiento de contratación en razón de su cargo o funciones: nombre, y apellidos, completando esta información con la indicación de su cargo o puesto de trabajo.
        - La identificación de la denominación y NIF de las personas jurídicas no se ve afectada, al no resultar de aplicación la normativa en materia de protección de datos personales.

        Para estos casos:

        - Deberán ocultarse todas las firmas, sean manuscritas o electrónicas, así como, en su caso, el Código Seguro de Verificación (CSV).
        - A tal efecto, se pueden seguir las recomendaciones técnicas incluidas en el Anexo del presente documento.
        - En el caso de los datos personales de empleados públicos que hubieran comunicado que se encuentran en circunstancias singulares de especial vulnerabilidad (por ejemplo, víctima de violencia de género), se adoptarán las medidas de ocultación de la identidad de los mismos.

    2. Respecto de **otros datos personales que puedan ser objeto de publicidad** (a título de ejemplo, correos electrónicos no genéricos, dirección de protocolo de internet, datos de terceros, etc.), y que no sean los expresados en el apartado anterior, también debe procederse a su ocultación en los términos expresados anteriormente, cuando se refieren a firmas o referencias a otros empleados públicos.

- Comunicación de la información a unidades u organismos de la Administración General del Estado, a fin de posibilitar el ejercicio de sus competencias de supervisión y control:

- Con carácter general, no serán necesarias medidas de anonimización de los datos personales, puesto que dicha labor exige disponer de la totalidad de la información que los documentos contienen.

5.2.3.- CONVENIOS ADMINISTRATIVOS

- A efectos de su publicación en el **Registro de Convenios**:

  - Deberán ocultarse todas las firmas, sean manuscritas o electrónicas, así como, en su caso, el Código Seguro de Verificación (CSV).

  - La publicación del número de DNI, NIE, NIF o documento identificativo equivalente resulta innecesaria y, por lo tanto, contraria al principio de minimización, al no aportar ningún elemento adicional a la hora de identificar a los firmantes del convenio.

  - Por el contrario, sí deben constar el nombre, apellidos y cargos de las personas firmantes y entidad a la que pertenecen, como datos personales de necesaria publicidad activa.

- En el Anexo del presente documento se incluyen recomendaciones técnicas para materializar este tipo de actuaciones antes de proceder a la publicación/acceso.

5.2.4.- SUBVENCIONES Y AYUDAS PÚBLICAS

- El artículo 8.1.c) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIBG), ordena la publicación de la información sobre las subvenciones y ayudas públicas concedidas, indicando la persona beneficiaria, lo que en principio obliga a su identificación.

- No obstante, no debe efectuarse la identificación de la persona en el caso de subvenciones o ayudas que revelen categorías especiales de datos, como por ejemplo si el motivo de la ayuda está relacionado con la salud de la persona beneficiaria.

- Además, debe tenerse en cuenta la limitación prevista en el artículo 20.8.b) de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, en el que se regula la Base de Datos Nacional de Subvenciones (BDNS) y que dispone que no se identificará a la persona beneficiaria cuando en razón del objeto de la subvención, tal publicación pueda ser contraria al respeto y salvaguarda del honor, a la intimidad personal o familiar de las personas físicas.

- De forma complementaria, el artículo 7.5.b del Real Decreto 130/2019, de 8 de marzo, por el que se regula la BDNS y la publicidad de las subvenciones y demás ayudas públicas, dispone que no se publicarán las subvenciones recibidas por personas físicas cuando estas se encuentren en una situación de protección especial que pueda verse agravada con la

cesión o publicación de sus datos personales, en particular, cuando sean víctimas de violencia de género o de otras formas de violencia contra la mujer.

- A efectos de eliminar la identidad de los beneficiarios de convocatorias de subvenciones públicas, cuando se trata de personas en estas situaciones de especial protección, consultar el punto 1.4 del documento "FAQ BDNS y SNPSAP. Respuestas a preguntas frecuentes", elaborado por la Intervención General de la Administración del Estado (IGAE).

- En el Anexo del presente documento se incluyen recomendaciones técnicas para materializar este tipo de actuaciones antes de proceder a la publicación.

5.2.5.- HUELLA NORMATIVA

- Los documentos a publicar en el apartado "HUELLA NORMATIVA" del Portal de Transparencia habrán de ajustarse a lo recogido en el artículo 14 del Decreto 52/2021, de 24 de marzo, por el que se regula y simplifica el procedimiento de elaboración de las disposiciones normativas de carácter general en la Comunidad de Madrid:

  "*1. La huella normativa está constituida por los documentos que deben publicarse, conforme a la legislación de transparencia, en un apartado específico del Portal de Transparencia de la Comunidad de Madrid con esa misma denominación.*

  2. Los documentos y contenidos disponibles en la huella normativa lo estarán en formato accesible, sin firmas ni rúbricas y siendo válido el documento pdf generado a partir del texto de que se trate previo a su firma".

- Se recuerda que en las Memorias de análisis de impacto normativo (MAIN), la identificación de las personas físicas que hubieran participado durante los trámites de "Consulta pública" y/o "Audiencia e información pública", deberá efectuarse tan solo con su nombre y apellidos, sin que estos vayan acompañados de otros datos identificativos, como por ejemplo: DNI/NIE/Pasaporte, dirección, correo electrónico, etc.

5.3.- ACCESO A LA INFORMACIÓN PÚBLICA

- La normativa principal a tomar en consideración es la LTAIBG, con especial consideración a sus artículos 14 y 15.

- Respecto de la aplicación de ambos preceptos, resulta de especial relevancia el criterio interpretativo conjunto CI/002/2015, de 24 de junio, del Consejo de Transparencia y Buen Gobierno (CTBG) y la Agencia Española de Protección de Datos Personales (AEPD), sobre la aplicación de los límites al derecho de acceso a la información: https://www.consejodetransparencia.es/dam/jcr:77d11404-2f9a-45e6-be70-d6c96409acd5/C2_2015_limites_derecho_de_informacion.pdf, y cuyas conclusiones son las siguientes:

a) *Los artículos 14 y 15 de la LTAIBG regulan los límites del derecho de acceso a la información que no operan de forma automática, sino que habrán de ser aplicados de acuerdo con las reglas de aplicación y los elementos de ponderación que establecen la citada Ley y la LOPD* (en la actualidad, LOPDGDD).
b) *El orden de ponderación opera desde el artículo 15 al 14 con valoración de los elementos que modulan la toma de decisiones.*
c) *El artículo 14 no supondrá, en ningún caso una exclusión automática del derecho a la información, antes al contrario, deberá justificar el test del daño y el del interés público para ser aplicado.*
d) *Del mismo modo, su aplicación deberá justificar y motivar la denegación.*
e) *En cualquier caso, si no cupiera el otorgamiento del acceso a la totalidad de la información una vez hechas las valoraciones anunciadas, se concederá acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida.*
f) *Todas las resoluciones denegatorias, total o parcialmente, del acceso en aplicación de los límites previstos en el artículo 14 de la LTAIBG serán objeto de publicidad en los términos establecidos en el art. 14.3 de la misma.*

- Para aquellos casos en los que, fruto de la referida ponderación, se hiciera precisa la anonimización de datos personales, en el Anexo del presente documento se incluyen recomendaciones técnicas para materializar la misma antes de facilitar al solicitante la información de su interés.

- Resta advertir de la importancia de no confundir las medidas de anonimización que vengan exigidas por este acceso a la información pública en el ejercicio del derecho contemplado en la normativa de transparencia, donde el solicitante no ostenta la condición de interesado, con aquellas otras que pudieran obedecer al ejercicio del derecho que trae causa de los artículos 53.1.a) y e) y 82 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el que el solicitante sí ostenta tal condición, como sucede, por ejemplo, con los participantes en procesos de concurrencia competitiva[2].

  En este último caso, la anonimización de los datos personales, suele tener carácter excepcional, aplicándose cuando deba prevalecer la intimidad de los restantes interesados en el procedimiento (por ejemplo, si el tercero es una víctima de violencia de género[3]; un testigo protegido, etc.).

[2] De especial interés la información contenida en la FAQ de la AEPD https://www.aepd.es/es/preguntas-frecuentes/11-transparencia-y-pd/FAQ-1106-puedo-acceder-a-la-documentacion-del-resto-de-candidatos-de-un-concurso-oposicion.

[3] Ver https://www.aepd.es/es/documento/2019-0149.pdf.

5.4.- DERECHO DE INFORMACIÓN DE LOS DIPUTADOS

- El derecho a la información pública de los diputados es un derecho fundamental que se inserta en el artículo 23 de la Constitución española y que ha sido ampliamente analizado por la jurisprudencia constitucional al ir definiendo sus características básicas, según los recursos de amparo que se han presentado[4]. Este derecho a la información se integra dentro de las funciones parlamentarias de impulso y control del gobierno y del sector público y es un derecho de configuración legal, cuya norma de referencia son los reglamentos parlamentarios, que delimitan su ámbito material.

- En el caso de la Comunidad de Madrid, se ha de destacar, a este respecto, las determinaciones contenidas en el artículo 18 y artículo 192 del Reglamento de Madrid[5], que se refieren, respectivamente, al derecho de información sobre datos, informes y documentos y a las preguntas que se presenten por escrito a la Mesa de la Asamblea, cuyas respuestas, en su literal, están accesibles a través del buscador de iniciativas parlamentarias de la página web de la Asamblea de Madrid, así como en el propio Boletín Oficial de la Asamblea de Madrid respecto a las preguntas escritas de conformidad con el art. 97 Reglamento de la Asamblea de Madrid.

- En el supuesto de existencia de datos personales en la documentación requerida al Responsable del tratamiento, y partiendo de que el derecho a la información de los diputados no puede ser de peor condición que el de los ciudadanos[6], habrá que estar a lo dispuesto en la LTAIBG, complementada por la Ley 10/2019 de 10 de abril, de transparencia y participación de la Comunidad de Madrid (en adelante LTPC). Esto es debido a la coordinación entre el derecho fundamental a la información con las previsiones contendidas en el artículo 15 LTIBG, y todo ello en relación con el artículo 86 RGPD[7] y la Disposición adicional segunda LOPDGGD[8].

  En orden a saber cuándo es posible la anonimización prevista en el artículo 15.4 LTIBG y artículo 9 y 35.4 LTPC, el Centro directivo tendrá que hacer un estudio, caso por caso, teniendo en cuenta previamente el resto de las determinaciones de los artículos mencionados anteriormente (en especial la ponderación prevista para los supuestos de que la información solicitada no contuviera datos especialmente protegidos) y en concordancia entre la conexión entre la petición y el interés público de los datos personales que se solicitan.

---

[4] Por ejemplo: SSTC 45/1990,196/1990 o 220/1991.

[5] Reglamento de la Asamblea de Madrid aprobado por acuerdo de Pleno de 17 febrero de 2019 (BOCM 22 febrero de 2019)

[6] STS 15 de junio de 2015.

[7] Art. 86 RGPD: Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

[8] Disposición adicional segunda LOPDGDD: La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

- Ahora bien, si del resultado de la aplicación normativa antedicha se ofreciere una respuesta positiva, es decir, que permitiera el acceso a los datos personales, se deben facilitar dichos datos personales, aunque fuera de manera limitada, de conformidad con el principio de minimización de datos.

- Por último, debe señalarse el artículo 18.4 del Reglamento de la Asamblea, conforme al cual, cuando los datos, informes o documentos solicitados afecten al **contenido esencial**[9] **de derechos fundamentales o libertades públicas constitucionalmente reconocidas**, entre los que se encuentra incluido el de la protección de datos personales del art 18.4 de la Constitución Española, la Mesa de la Asamblea, previa petición del Gobierno, puede declarar secreta la información solicitada por el diputado. A tal efecto, el diputado tiene acceso directo a toda la documentación en dependencias administrativa, sin necesidad de censurar firmas, ni datos confidenciales de ningún documento. Como garantía solo puede tomar notas, no pudiendo hacer copias, ni reproducciones de ningún tipo; así como no poder ir acompañado de otra persona.

5.5.- ÓRGANOS COLEGIADOS[10]

5.5.1.- ACTAS DE LAS SESIONES

- Los sujetos obligados a cumplir con las normas de transparencia publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública (artículo 5.1 LTAIBG).

- Con carácter general, se ocultarán los datos personales de personas físicas que no sean pertinentes, sin que afecte a los datos personales que se limiten estrictamente a identificar a los miembros que conforman el órgano colegiado, ya que estos estarían incluidos en el artículo 15.2 LTAIBG, salvo que:

  - sea de aplicación alguno de los límites contenidos en el artículo 14.1 LTAIBG

  - a la vista de las circunstancias concurrentes y realizado el juicio de ponderación del artículo 15 LTAIBG, deba prevalecer el derecho a la protección de datos de carácter personal.

5.5.2.- ACUERDOS ADOPTADOS EN LAS SESIONES

- Si bien debe prevalecer el acceso a estos acuerdos, por ser de interés público, aquellos datos personales que no sean relevantes, o que su conocimiento resulte desproporcionado, han de omitirse/anonimizarse en atención al principio de minimización.

[9] Sentencia TC 76/2019, de 22 de mayo https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25942

[10] Análisis basado en la STS 17 de noviembre de 2022 (rec.1837/2021) https://delajusticia.com/wp-content/uploads/2022/11/STSactas.pdf.

Se ocultarán los datos personales que no sean meramente identificativos de los miembros del órgano personal.

- Por reelaboración debe entenderse *«volver a elaborar algo»*, sin que integre tal concepto un mínimo tratamiento de datos y que, en todo caso, en el supuesto de que la información contenga datos de carácter personal, su anonimización no debe entenderse como reelaboración (STS 25 de marzo de 2021, rec.2578/2020).

5.6.- AVISO INFORMATIVO SOBRE LOS DOCUMENTOS CENSURADOS

En los documentos ya censurados que resulten de los distintos supuestos contemplados en los diferentes apartados del punto 5 ya referidos, excepto en el apartado 5.2.5 al tener su tratamiento específico, se recomienda que, al menos en la primera página, se inserte un aviso indicando que el documento se ha obtenido directamente del original que contiene la firma auténtica. A estos efectos, se recoge el siguiente texto orientativo: ***Este documento es copia del original firmado. Se han ocultado datos personales en aplicación de la normativa vigente.***

6.- ENLACES DE INTERÉS

- 10 malentendidos relacionados con la anonimización (AEPD):

  https://www.aepd.es/es/documento/10-malentendidos-anonimizacion.pdf

- La K-anonimidad como medida de privacidad (AEPD):

  https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

- Dictamen 05/2014, sobre técnicas de anonimización (GT 29):

  https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

- Orientaciones sobre la protección de datos en la reutilización de la información del sector público:

  Orientaciones sobre la protección de datos en la reutilización de la información del sector público | datos.gob.es

- Introducción al hash como técnica de seudonimización de datos personales (AEPD):

  Introducción al hash como técnica de seudonimización de datos personales. (aepd.es)

- Cifrado Homomórfico:

  Cifrado y Privacidad III: Cifrado Homomórfico | AEPD

ANEXO

ENMASCARAMIENTO DE UN DOCUMENTO PDF PARA ELIMINAR DATOS PERSONALES ANTES DE SU PUBLICACIÓN O COMUNICACIÓN

Para enmascarar u ocultar los datos personales en un documento PDF podemos actuar de diferentes modos en función de las herramientas disponibles:

- En el caso de tener herramientas avanzadas de edición que incorporen una funcionalidad para **censurar** podremos utilizar directamente dichas herramientas.

- Otra posibilidad consiste, utilizando herramientas de edición de documentos que no tengan la opción de censurar, en ocultar los datos personales mediante elementos gráficos (tipo rectángulo o similar) y **posteriormente imprimir el documento a PDF** para convertirlo en un PDF puramente gráfico o de imagen.

A continuación, podemos ver cómo realizar la censura de datos personales utilizando diferentes herramientas.

I. Adobe Acrobat DC Professional.
II. Adobe Acrobat Standard o Adobe Reader.
III. ABBYY PDF Transformer.

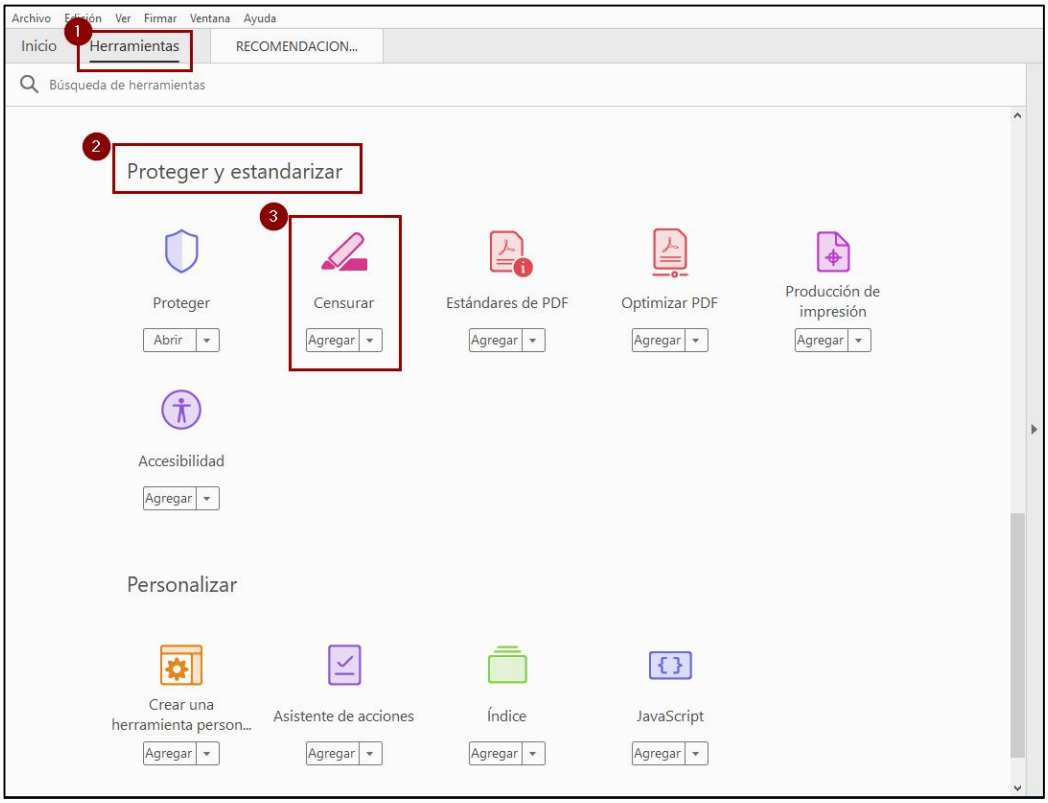
I. Editando un documento mediante Adobe Acrobat DC Professional[11], usando la herramienta avanzada "Censura"

La censura es el proceso de quitar permanentemente texto y gráficos visibles de un documento. La herramienta **Censurar** sirve para ocultar contenido de manera irreversible. Los pasos a realizar son los siguientes:

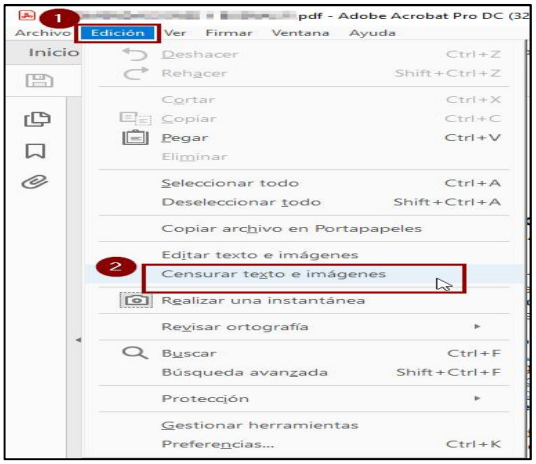
1) Una vez que hemos abierto el archivo pdf en Acrobat podemos acceder a la herramienta **Censurar** de dos maneras:

   - Desde la pestaña **Herramientas,** buscamos la sección **Proteger y estandarizar** y hacemos clic sobre **Censurar**.

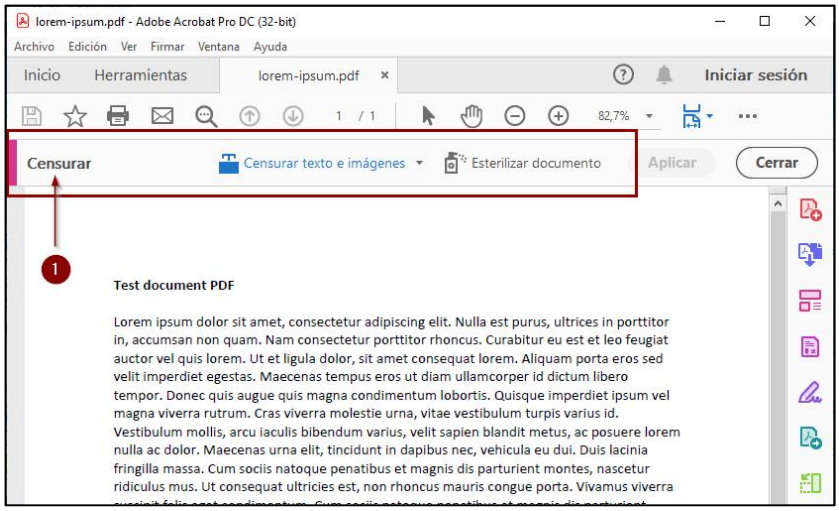
[11] Fuente: https://helpx.adobe.com/es/acrobat/using/removing-sensitive-content-pdfs.html.



- Accediendo al menú **Edición** y seleccionando **Censurar texto e imágenes**.

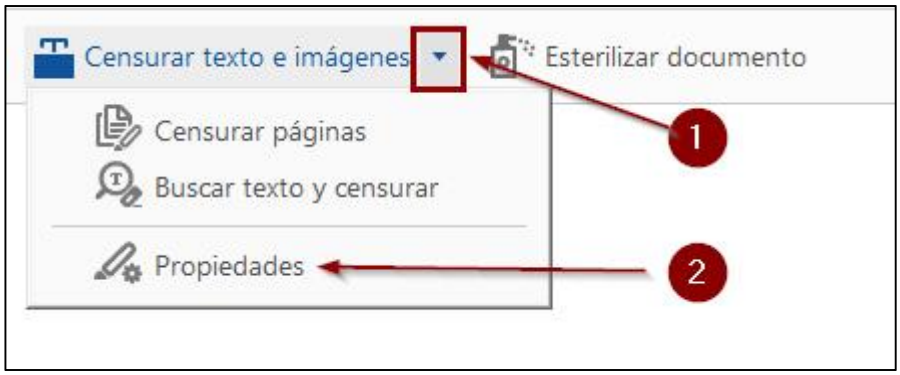


2) Observaremos que aparece la barra de herramientas de **Censurar** en la parte superior de la pantalla.

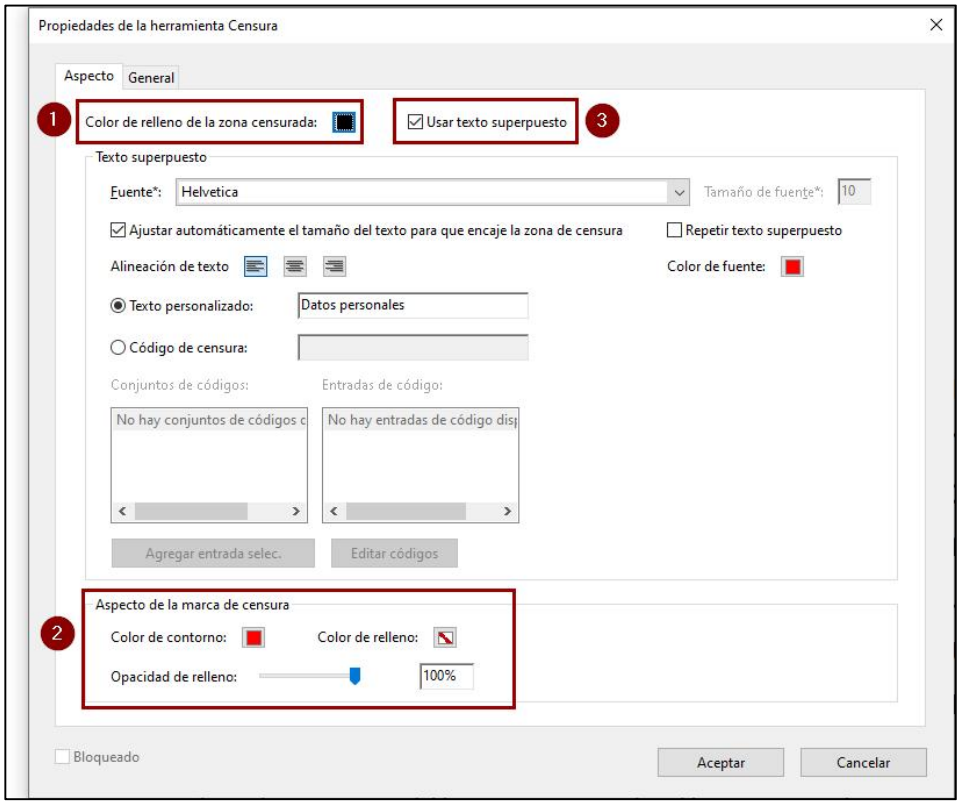


3) A partir de este momento podemos censurar los elementos que queramos simplemente seleccionándolos con el ratón directamente en el documento, para ello mantendremos pulsado el botón izquierdo del ratón mientras pasamos por encima de ellos. También podemos seleccionar una palabra o imagen haciendo doble clic sobre ella.

   Dependiendo de cómo tengamos configurado el aspecto de la marca de censura esta se verá de una u otra manera en el documento. Podemos editar la apariencia haciendo clic en desplegable del menú **Censurar texto e imágenes (1)** y posteriormente seleccionando **Propiedades (2)** en las opciones del menú que aparece.

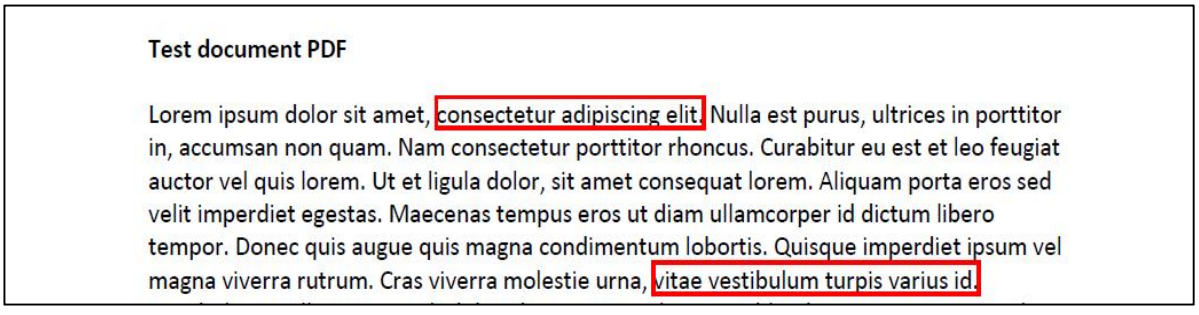


   El sistema abre una ventana denominada **Propiedades de la herramienta Censura**. Aquí, dentro de la pestaña **Aspecto**, podemos configurar:

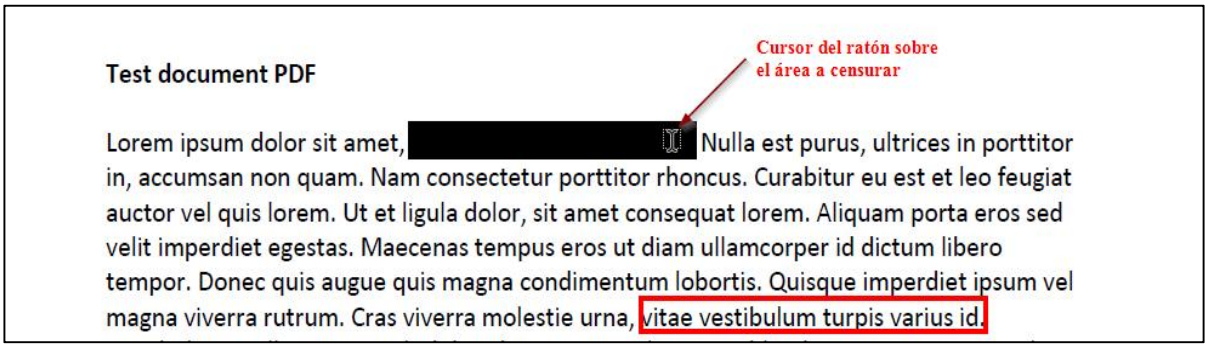


- El **color de relleno de la zona censurada (1)**. Que será el color con el que finalmente se verá la zona censurada cuando se apliquen los cambios y se guarde el documento.
- El **aspecto de la marca de censura (2)**. Nos permite especificar cómo vamos a ver nosotros, mientras censuramos el documento, las marcas de censura. De este modo por ejemplo podemos establecer un color de relleno transparente que nos permita ver el contenido del texto que hemos censurado.
- La opción **Usar Texto Superpuesto (3)** permite establecer las características del texto que se mostrará, si así lo deseamos, sobre la zona censurada. Al activarla podemos configurar cómo será dicho texto.

Por ejemplo, si configuramos el color de relleno de la zona censurada a negro y el aspecto de la marca de censura con un borde rojo y relleno transparente, nosotros veremos el documento así:

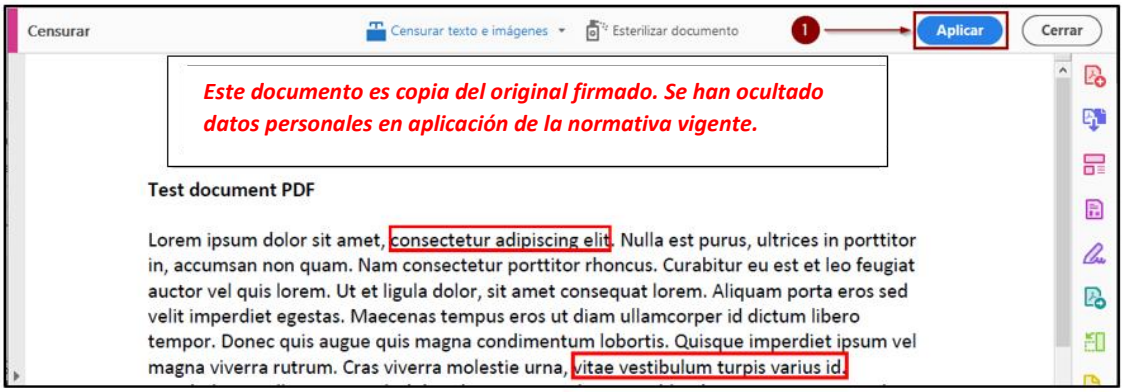


Si queremos ver cómo quedará aplicada la marca de censura simplemente debemos dejar el cursor del ratón sobre el área marcada.

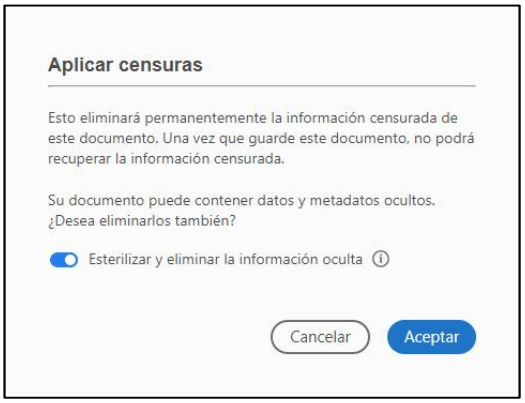


4) Una vez que hemos marcado todos los elementos a censurar, y antes de guardar el documento, será necesario insertar un cuadro de texto, adaptado a la casuística del documento, advirtiendo que se trata de una copia del original custodiado por el responsable, que contiene todas las firmas, DNI, rúbricas, CSV, etc.

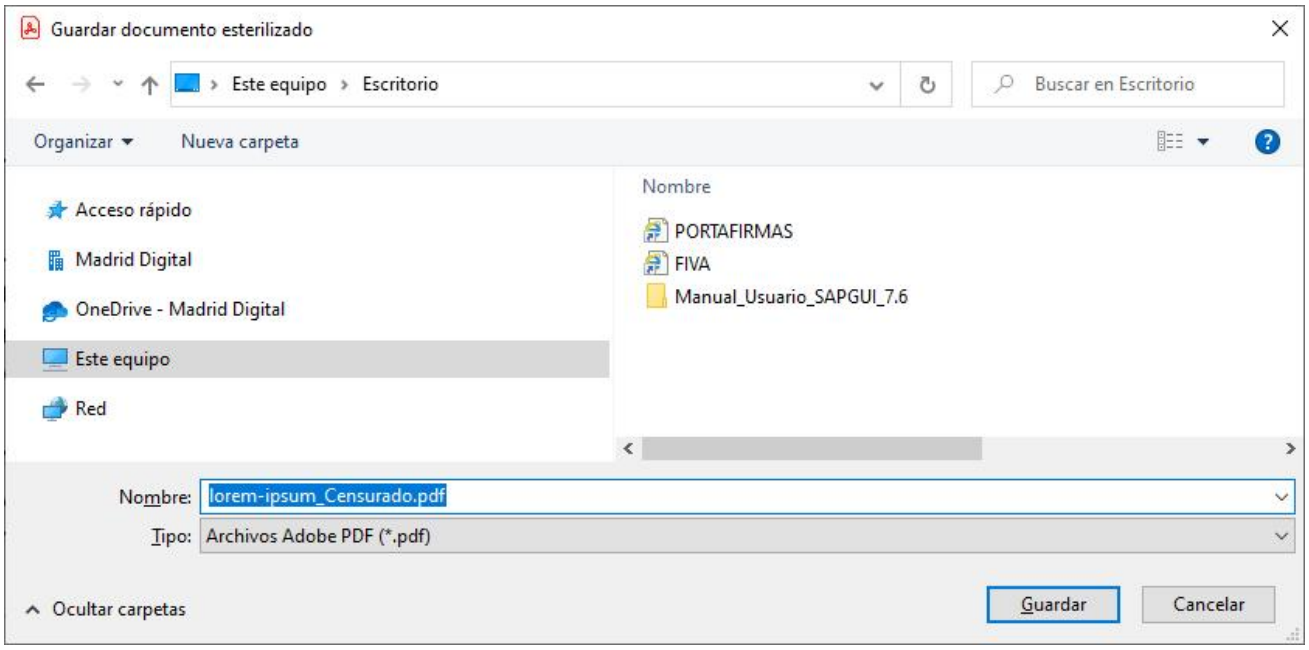
5) Finalmente, para hacer que las marcas de censura queden permanentemente en el documento debemos hacer clic en el botón **Aplicar** de la parte superior de la pantalla:



6) El sistema mostrará una ventana que indica que esta acción eliminará permanentemente la información censurada de este documento. Igualmente, la misma ventana, nos ofrece la posibilidad de **Esterilizar y eliminar la información oculta** del documento, que aparece marcada por defecto y que debemos dejar activada.



7) Una vez que hacemos clic en **Aceptar** el sistema nos muestra una nueva pantalla donde podemos indicar el lugar en el que vamos a guardar el documento. El texto "*Censurado*" se añade automáticamente al final del nombre del archivo sugerido para el documento.

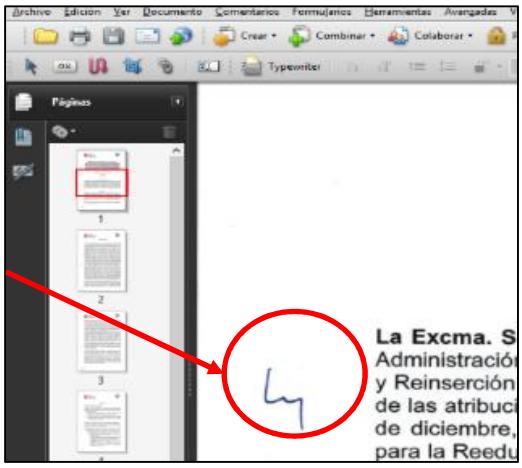


Una vez guardado ya tendremos nuestro documento censurado y limpio de metadatos.

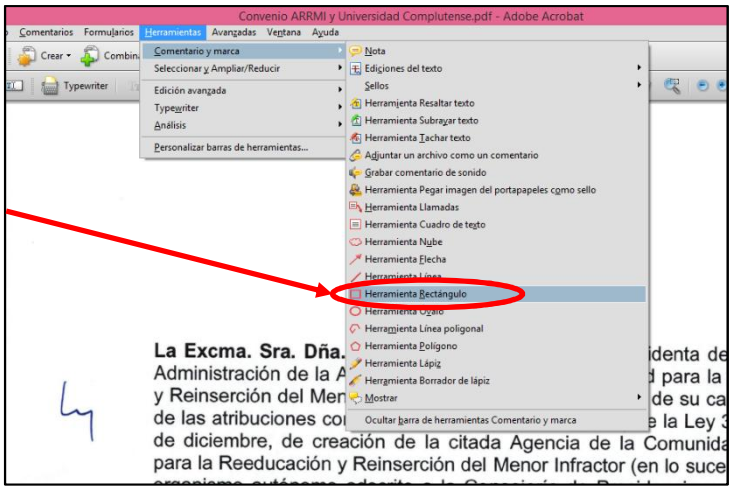
II. Si disponemos de **Adobe Acrobat Standard o Adobe Reader** (o de un programa de edición equivalente):

a) Documentos en formato PDF elaborados a partir de documentos **firmados de forma manuscrita:**

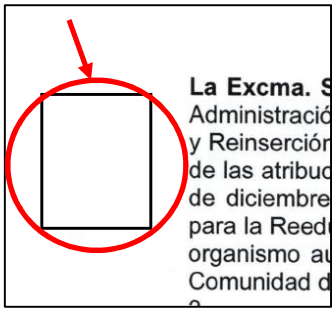
Abrimos el PDF y nos trasladamos al primer elemento que queramos ocultar (por ejemplo, una rúbrica en un convenio):



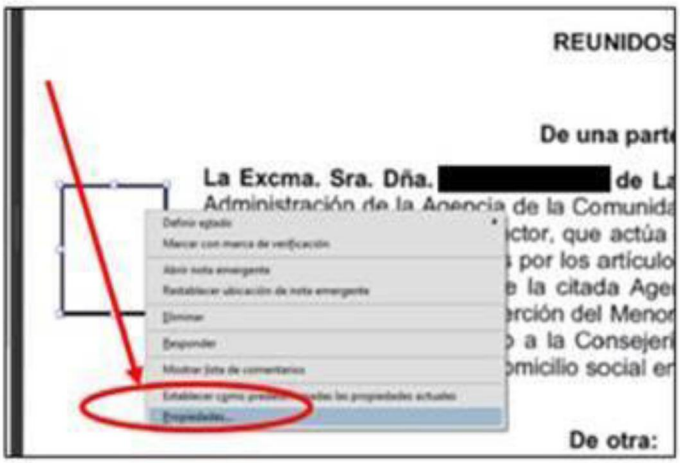
Dentro del Menú "Herramientas", elegimos "Comentario y marca" y, después, "Herramienta rectángulo":



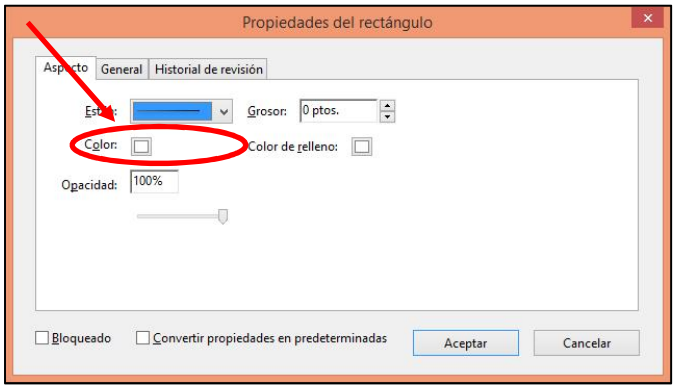
Veremos que el cursor se ha convertido en un aspa. Haremos "clic" con el botón izquierdo del ratón y, sin soltar, dibujaremos un cuadrado que tape lo que queremos ocultar:



En el caso de que, como se ve en la imagen, el cuadrado aparezca con un borde visible, haremos clic sobre él con el botón derecho y seleccionaremos “Propiedades” con el botón izquierdo.



Aparecerá un cuadro de diálogo, “Propiedades del rectángulo”, en el que escogeremos, como color de línea, el blanco. Así, el cuadro “desaparecerá”:

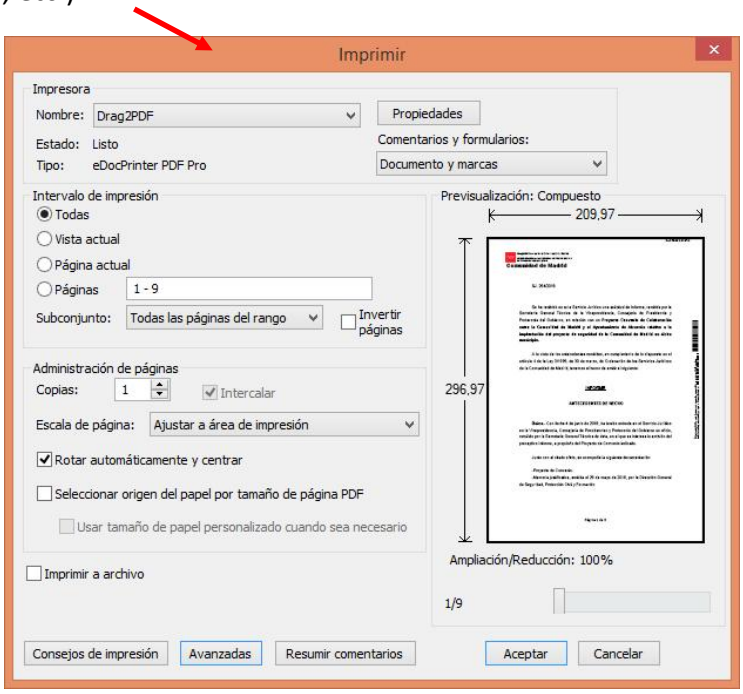


Se recuerda que, una vez editado el documento en estos términos, **ha de imprimirse a PDF para convertirlo en un PDF puramente gráfico o de imagen**, que impedirá que se pueda revertir el proceso (Archivo” → “Imprimir” y escogeremos cualquiera de las opciones disponibles para hacer un “pdf”).

b) Documentos en formato PDF elaborados a partir de un documento **firmado electrónicamente:**

Primero tendremos que hacer un nuevo PDF del documento.

Con el documento abierto, haremos clic en "Archivo" → "Imprimir" y escogeremos cualquiera de las opciones disponibles para hacer un "pdf" (eDocPrinter, PDF Pro, drag2PDF, etc.):



Este nuevo PDF podremos manipularlo tal y como se ha explicado en el apartado a).

En ambos casos, una vez que disponemos de una copia del documento en formato PDF, y tras realizar en ella el enmascaramiento o censura de los datos personales el resultado obtenido deberá tener la siguiente forma:

1) Una imagen con un formato PDF puramente gráfico sin la información a ocultar,

2) o bien un documento PDF desprovisto de los datos y metadatos a ocultar.

Es necesario, en este último caso, incidir en la importancia de eliminar del documento todos los metadatos que, aunque sean información no visible, pueden contener restos de la información personal que se deseaba ocultar.

Para eliminar metadatos que se encuentran en las Propiedades de documento de forma manual en Adobe Acrobat es necesario acceder a "Propiedades de documento" y modificar o borrar su contenido.

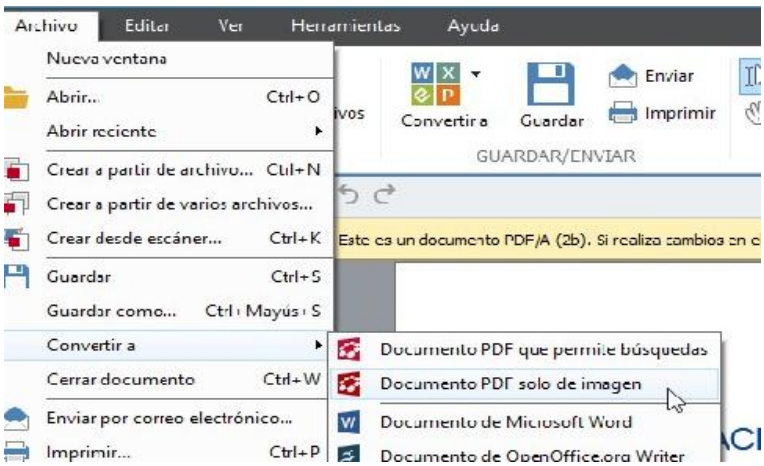
Adobe Acrobat 9.0 dispone de una utilidad para inspeccionar y eliminar todos los metadatos e información oculta de un documento, "**Examinar Documento**".
En el documento generado, una vez enmascarados todos los datos personales, deberá constar expresamente la advertencia de que el original contiene todas las firmas auténticas. Se aconseja que dicha advertencia figure al menos en la primera página en lugar destacado y resaltado en negrita o en un color llamativo. A continuación, se recomienda incluir la siguiente sugerencia o modelo de aviso a este respecto:

Este documento es copia del original firmado. Se han ocultado datos personales en aplicación de la normativa vigente.

Una vez grabado el documento, la copia censurada puede ser publicada o comunicada a quien corresponda.

III. Editarlo con el programa **ABBYY PDF Transformer+**[12], proporcionado por Madrid Digital, que permite editar documentos PDF.

Una vez enmascarados los datos personales hay que guardar el archivo: en el menú "Archivo" elegir "Convertir a", y pulsar en "Documento PDF sólo de imagen", como se indica en la siguiente captura de pantalla:



Antes de guardar el archivo, se debe incorporar, previamente, un cuadro de texto con una advertencia similar a la que ahora se propone:

Este documento es copia del original firmado. Se han ocultado datos personales en aplicación de la normativa vigente.

[12] Se trata de un programa proporcionado por Madrid Digital que, aunque ya no puede solicitarse, se sigue utilizando en algunos puestos de trabajo.

OBSERVACIÓN GENERAL: Sin perjuicio de lo expuesto en el presente Anexo, se recuerda que cualquier imagen que identifique o haga identificable a una persona física, que pudiera constar y acompañar a los textos en estos documentos, habría de ser pixelada o censurada en términos suficientes que no permitan su identificación.

Documento aprobado por el Grupo de Trabajo para la protección de datos personales de la Comunidad de Madrid en su reunión celebrada el 26 de enero de 2023. Modificaciones aprobadas en reunión de 18 de mayo de 2023.