Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Identificación del expediente

Resolución de archivo de las informaciones previas núms. IP 84 y 110/2019, referentes al Consorcio de Administración Abierta de Cataluña ya la Agencia de Residuos de Cataluña.

Antecedentes

1. En fecha 19/03/2019, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba una denuncia referente a la tarjeta T-CAT, con motivo de un presunto incumplimiento de la normativa sobre protección de datos de carácter personal. En concreto, la persona denunciante exponía que, como empleada de la Agència de Residus de Catalunya (en adelante, ARC), disponía de una tarjeta T-CAT. La persona denunciante manifestaba que, desde la última renovación de la tarjeta T-CAT, al firmar electrónicamente documentos o realizar envíos a través de EACAT o e-Notum, constaba su nombre y apellidos y su DNI. En este sentido, el denunciante consideraba que la inclusión del DNI podría vulnerar la legislación de protección de datos personales.

A esta denuncia se le asignó el número IP 84/2019.

2. La Autoridad abrió una fase de información previa, de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad , y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

3. En fecha 25/03/2019, en el seno de esta fase de información previa, se requirió al Consorcio Administración Abierta de Cataluña (en adelante, AOC) para que informara, entre otros, sobre los motivos por los que era necesario que se visualizara el DNI de la persona firmante en la imagen que genera el certificado y en las propiedades de la firma.

4. En fecha 10/04/2019, la AOC respondió a dicho requerimiento a través de un escrito en el que exponía, entre otros, lo siguiente:

- Que la imagen que genera una firma basada en certificado digital es una reproducción gráfica, sin efectos jurídicos, plasmada sobre un documento electrónico que permite evidenciar visualmente que éste ha sido firmado electrónicamente. La falta de efectos jurídicos de la imagen permite que el signatario pueda configurar (si el programa de firma le permite) que aparezca o no una imagen de firma y, en caso afirmativo, el formato y el contenido (como el DNI) que se muestre en el documento firmado.
- Que la determinación de los datos que se muestran en la imagen de una firma electrónica realizada con una tarjeta T-CAT, no depende de este certificado electrónico, sino del

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

programa que utiliza el usuario para firmar y de las posibilidades de configuración que este programa admita y el usuario haya definido.

- Que la AOC informa a los usuarios de la T-CAT sobre cómo se puede modificar un documento PDF para que en la imagen de la firma no aparezca información sobre el DNI del signatario.
- Que, por otra parte, las propiedades de firma son aquellos datos que contiene un documento firmado electrónicamente, correspondientes a los campos que componen un certificado digital (algunos de carácter obligatorio). Estos campos están predefinidos y no son editables por parte de los prestadores de servicios de certificación calificados.
- Que la estandarización de los campos que debe contener un tipo de certificado electrónico permite que las firmas generadas puedan ser reconocidas, interoperables y validadas.
  Las propiedades de firma del certificado y, por tanto, la firma electrónica, es uno de los componentes de los documentos electrónicos, así como requisito de validez de los documentos electrónicos administrativos.
- Que la AOC no tiene potestad como prestamista para decidir si se puede o no visualizar el DNI accediendo a las propiedades de firma de un documento electrónico. Esta cuestión viene condicionada por la normativa que determina de forma estandarizada la estructura (campos y contenidos) de un certificado electrónico, que tiene por objetivo asegurar el reconocimiento e interoperabilidad de los certificados.
- Que de acuerdo con el arte. 2.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante, LSE) un prestador de servicios de certificación es aquella *"persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica" .*
  Por su parte, el artículo 3.20 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, ReIDAS), define a los prestamistas calificado de servicios de certificación de confianza como aquellos que prestan uno o más servicios de confianza cualificados, a los que el organismo de supervisión ha concedido la calificación.
- Que el artículo 11.2.e) de la LSE establece los certificados reconocidos o cualificados deben incluir *"la identificación del firmante, en el caso de personas físicas, por su nombre y apellidos y el número de documento nacional de identidad oa través de un seudónimo que conste como tal de forma inequívoca".*
- Que como indicó la Autoridad en dictamen CNS 15/2013: *"[…] se puede considerar que la utilización del nombre y apellidos de la persona física que firma junto con su número de DNI, en los términos planteados en la consulta , tiene la suficiente cobertura legal en la LSE. El contenido mínimo que deben tener los certificados reconocidos es el que fija el artículo 11.2 de la LSE, que incluye, entre otros, la identificación de la persona física que firma, a través de su nombre y apellidos y de su número de DNI, sin que esto pueda ser considerado como contrario a la Directiva."* En el mismo sentido, se pronunció la Autoridad en el dictamen CNS 17/2017.

- Que cualquier prestamista de servicios de certificación de confianza, como la AOC, debe cumplir con las previsiones normativas vigentes en cuanto a la estructura de los certificados electrónicos, que establecen la obligación de incluir el dato del DNI.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

- Que la Administración General del Estado (en adelante, AGE), en cumplimiento del artículo 18 de Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad (en adelante , ENI) y de la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración, aprobó una Política de Firma Electrónica y de Certificados. Esta Política *"servirá de marco general de interoperabilidad para la autenticación y reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. No obstante, dicha política podrá ser utilizada como referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales" (artículo* 18.1 ENI).

- Que el artículo 18.4 del ENI establece que *"Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de modo que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa."*

- Que la mencionada Política es aplicable en aquellos casos en que, como en Cataluña, no se ha desarrollado una política de firma electrónica propia.
- Que en el documento de *"Perfiles de certificados electrónicos"* de abril de 2016 , como parte de su Política de Firma Electrónica y de Certificados, la AGE define cuáles deben ser los campos mínimos de los diferentes certificados digitales, diferenciando entre recomendables o no y fijos u opcionales. Éste es el documento de referencia para los certificados derivados de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público (en adelante, LRJSP).
- Que en lo que se refiere específicamente al certificado de empleado público, el apartado 10.1 *"Criterios de composición del campo CN para un certificado de empleado público"* del documento *"Perfiles de certificados electrónicos"* determina cuáles deben ser los campos y el contenido de los campos que componen el *"Common Name" (en* adelante, CN). Por tanto, los datos del campo *"CN"* no son decisión discrecional del prestador de servicios de certificación, sino que vienen determinados por el propio Ministerio de Hacienda y Administraciones Públicas (en adelante, MHAP).

- Que en cuanto a los certificados de empleado público, este documento determina que el dato relativo al DNI es obligatorio.
- Que de acuerdo con las consideraciones anteriores, los certificados personales reconocidos de trabajador público que emite la AOC, deben incluir obligatoriamente el DNI en el campo *"CN".*
- Que la carencia de inclusión del DNI en la estructura del certificado tendría consecuencias directas sobre la funcionalidad principal del certificado digital, hasta el punto de que dejaría de ser reconocido como de empleado público tanto por parte de la AGE, como de diferentes aplicaciones corporativas.
- Que como reconocía la Autoridad en su dictamen CNS 17/2017, es necesario tener en cuenta las consecuencias que en materia de interoperabilidad podría tener la no inclusión del DNI en la estructura de los certificados calificados de empleado público.
- Que la emisión de certificados sin seguir la estructura predefinida comportaría la pérdida de la condición de prestamista de servicio de certificación calificado, la expulsión de la AOC de la la lista de confianza de prestamistas calificados de servicios electrónicos de certificación *(" Trusted Service*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

List – TSL") y la imposibilidad de continuar expidiendo certificados calificados de trabajador público.

- Que no corresponde a la AOC, como prestador de servicios de certificación calificados, cualquier decisión relativa a la aparición del DNI en las propiedades de firma de un documento electrónico.
- Que el apartado 8º de la Resolución de 19/07/2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico (NTI-DE), que regula el acceso a documentos electrónicos, establece que *"Cuando las administraciones públicas facilitan el acceso a los documentos electrónicos a través de sus sedas electrónicas o de los canales de comunicación que correspondan en cada caso, se mostrará: (...) b) La información básica de cada una de las firmas del documento definida en el anexo III."* Entre esta información básica se incluye la información del signatario del documento que debe incluirse en las propiedades de la firma.
- Que como constató la Autoridad en el dictamen CNS 17/2017, de acuerdo con la normativa de aplicación y el documento *"Perfiles de certificados electrónicos",* el DNI del empleado público en las tarjetas T-CAT aparece en los campos de la estructura del certificado siguientes: *"SerialNumber, SurName y CommonName".*

- Que en aquellas herramientas que dependen de la AOC, se está trabajando para adecuarlas con el objetivo de que no muestren el DNI en la visualización de la firma realizada, dando así cumplimiento tanto al principio de minimización de datos, como a la privacidad por defecto.
  Éste es el caso, por ejemplo, de la aplicación signasuite y el portafirmas de la AOC.
- Que la AOC se ha dirigido en varias ocasiones a la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública para trasladar la inquietud generada por el hecho de que los certificados calificados de trabajador público contengan el DNI en el campo *"CN ".*
- Que la AOC ofrece como alternativa a la T-CAT, la posibilidad de solicitar certificados de empleado público con seudónimo. Este tipo de certificados preservan de forma anónima la identidad del firmante, en lo que se refiere a la información sobre su DNI, información que queda sustituida en el *"CN"* del certificado digital por un seudónimo. Esta alternativa ya fue reconocida por la Autoridad, entre otros, en su dictamen CNS 15/2013.
- Que la solicitud y expedición de este tipo de certificados queda condicionada al cumplimiento de la normativa de aplicación, debiendo tratarse de seudónimos que consten como tal de forma inequívoca y para unos colectivos reglados de trabajadores públicos.

5. En fecha 09/04/2019, tuvo entrada en la Autoridad un escrito de otra persona que indicaba que era funcionaria de un ente local (el cual no concretaba), por el que formulaba una denuncia también referente a la tarjeta T-CAT. En concreto, la persona denunciante exponía que, cuando firmaba cualquier documento electrónico dirigido a los administrados, la imagen que se generaba contenía su DNI. A su vez, añadía que su DNI también contaba en las propiedades de la firma. Por último, la persona denunciante manifestaba que su número de DNI *"es un dato personal que no debería salir en la asignatura digital como funcionario público."*

A esta denuncia se le asignó el número IP 110/2019.

Fundamentos de derecho

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

1. De acuerdo con lo que prevén los artículos 90.1 de la LPAC y 2 del Decreto 278/1993, en relación con el artículo 5 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y el artículo 15 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, es competente para dictar esta resolución la directora de la 'Autoridad Catalana de Protección de Datos.

2. A partir del relato de hechos que se ha expuesto en el apartado de antecedentes, es necesario analizar los hechos denunciados que son objeto de la presente resolución de archivo, referente a la tarjeta T-CAT que disponen los empleados públicos de la Generalidad de Cataluña y las administraciones locales, la cual contiene un certificado digital reconocido o calificado.

2.1. Sobre la imagen que se genera al firmar electrónicamente un documento.

En este sentido, la Autoridad se ha pronunciado en los dictámenes CNS 17/2017, 23/2017, 58/2018 y 1/2019, en los siguientes términos:

> *"(...) el aspecto o la imagen de una firma basada en un certificado es algo que a priori se puede definir previamente mediante las opciones que, en este sentido, ofrece el programa empleado para firmar electrónicamente (por ejemplo, Adobe Acrobat), por lo que los datos del trabajador público que están incorporados al certificado electrónico no necesariamente deben ser visibles una vez se ha firmado electrónicamente el documento. La visibilidad o no de estos datos personales dependerá, por tanto, de la forma en que se haya preestablecido el formato de dicha firma. Y esto con independencia del tipo de certificado electrónico de que disponga el trabajador."*

Así las cosas, el aspecto o imagen que se genera al firmar un documento electrónico mediante el certificado digital o reconocido (T-CAT), y en particular, los datos que se muestran pueden configurarse mediante el programa a través del cual se firma .

Esta circunstancia, tal y como se expondrá más adelante, comporta que se requieran medidas correctoras al respecto.

2.2. Sobre la normativa española respecto al contenido de los certificados electrónicos.

En este sentido, la AOC invoca en su escrito de respuesta al requerimiento que se le formuló, que esta Autoridad exponía en el dictamen CNS 15/2013 que *"se puede considerar que la utilización del nombre y apellidos de la persona física que firma junto con su número de DNI, en los términos planteados en la consulta, tiene la suficiente cobertura legal en la LSE. El contenido mínimo que deben tener los certificados reconocidos es el que fija el artículo 11.2 de la LSE, que incluye, entre otros, la identificación de la persona física que firma, a través de su nombre y*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

apellidos y de su número de DNI, sin que esto pueda ser considerado como contrario a la Directiva."

Al respecto, cabe destacar que este dictamen es anterior al ReIDAS, que fue aplicable a partir del 01/07/2016 (artículo 52.2 del ReIDAS), por lo que en cuanto al contenido de los certificados calificados o reconocidos debe tener en cuenta lo dispuesto en este reglamento europeo.

Efectuada esta puntualización, debe tenerse en cuenta que el DNI también resulta accesible por cualquier persona receptora del documento firmado electrónicamente por un empleado público, consultando las propiedades de la firma donde se pueden ver todos los campos de información que forman parte de la estructura del certificado (entre ellos, se incluye el DNI del empleado público). Cabe decir que, tal y como exponía esta Autoridad en el dictamen CNS 17/2017, esta configuración no puede ser modificada ni por el trabajador público, ni tampoco por la Administración pública a la que pertenece.

Asentado lo anterior, procede dirimir si la inclusión del dato referente al DNI de la persona empleada pública en dicho certificado electrónico, es necesaria.

En primer lugar, los apartados 1 y 2.e) del artículo 11 de la LSE, que se refieren al concepto y contenido de los certificados reconocidos, disponen que:

> *"1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y otras circunstancias de los solicitantes ya la fiabilidad y garantías de los servicios de certificación que presten.*
> *2. Los certificados reconocidos deben incluir, al menos, los siguientes datos: (...)*
> *e) La identificación del firmante, en el caso de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad oa través de un seudónimo que conste como tal de forma inequívoca y, en el caso de personas jurídicas, por su denominación o razón social y su código de identificación fiscal."*

Tal y como se apuntaba en el dictamen CNS 17/2017, de conformidad con el precepto transcrito, la identificación de la persona firmante en la configuración del certificado reconocido por parte del prestador de servicios de certificación tanto puede llevarse a cabo *"indicando el nombre , apellidos y DNI como un seudónimo, en sustitución de estos datos".*

Por su parte, los apartados 1 y 4 del artículo 18.1 del ENI, establecen que:

> *"1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para la autenticación y reconocimiento mutuo de firmas electrónicas dentro del ámbito de actuación. Sin embargo, dicha política podrá ser utilizada como*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

referencia por otras Administraciones públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales. (...)
4. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de modo que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa. Dichos certificados serán los definidos en la Ley 11/2007, de 22 de junio, la Ley 59/2003, de 19 de diciembre, de firma electrónica y sus desarrollos normativos."

Tal y como informó la AOC por medio de escrito de 09/04/2019, la política de firma electrónica y de certificados aprobada por la Administración General del Estado (en adelante, AGE), resulta aplicable en la medida en que en Cataluña no se ha desarrollado una propia.

Por su parte, en el documento *"Perfiles de certificados electrónicos"* elaborado por el MHAP en 2016, se establece el contenido de los campos para los certificados electrónicos de empleados públicos (apartados 5.3 y 10.1) y para los certificados electrónicos de empleados públicos con seudónimo (apartados 5.4 y 11.1).

En relación con los primeros (apartado 10.1), los criterios de composición del campo *"CN"* del certificado prevén, entre otros:

"• Incluir obligatoriamente el número de DNI/ NIE, junto con la letra de control, de acuerdo con lo indicado en el DNI/ NIE.
• Incluir obligatoriamente un SÍMBOLO o CARÁCTER que separe el número y apellidos del número de DNI."

A su vez, el apartado 10.2 del citado documento también contempla la inclusión del número de DNI como obligatoria en el campo *"Surname"* del certificado (campo 1.5.9) y como recomendable en el campo *"SerialNumber" (campo* 1.5 .8).

De acuerdo con lo anterior, en los campos *"CN"* y *"Surname"* que forman parte de la estructura del certificado electrónico de los empleados públicos, se prevé como obligatoria la inclusión del número de DNI. Y en el campo *"SerialNumber",* la inclusión de este dato es opcional.

Y en lo que se refiere a los certificados electrónicos de empleados público con seudónimo (apartado 11.1), se dispone expresamente que en el campo *"CN" "No se podrá incluir el número de DNI/ NIE".* Cabe decir, que el citado documento también restringe el uso de estos certificados con seudónimos por parte de los empleados públicos a los supuestos contemplados en el RD 1671/2009.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

En definitiva, de acuerdo con la normativa expuesta en este apartado (y en particular el artículo 11.2 de la LSE), el contenido mínimo de los certificados reconocidos o calificados podría incluir el dato en lo referente al DNI.

2.3. Sobre la norma *"ETSI EN 319 412-2".*

Asentado lo anterior, cabe mencionar la norma *"ETSI EN 319 412-2" "Certificate profile for certificates issued to natural persons"* que, precisamente, apoya los requisitos de los certificados calificados exigidos en el ReIDAS, ya los que también hace referencia l citado documento del MHAP para concretar la información que debe incluirse en los certificados calificados de trabajador público. Al respecto, en el dictamen CNS 17/2017 se señalaba lo siguiente:

> *"De conformidad con esta norma, en el campo relativo a la persona firmante (Subject) del certificado deben incluirse los atributos: país (CountryName), nombre y apellidos o seudónimo de la persona firmante (GivenName and Surname or Pseudonym), y CN.*
>
> *La inclusión en el certificado del atributo relativo a un número o código de identificación de la persona firmante (SerialNumber), como sería el caso del DNI, se considera pertinente sólo en aquellos casos en los que del establecimiento de los atributos anteriores (CountryName, GivenName y Surname or Pseudonym, y CN) no se puede identificar inequívocamente a la persona firmante. Añade la norma que este campo SerialNumber no tiene una semántica definida (no concreta qué información podría incluirse), de tal modo que podría ser un número o código asignado por la entidad de certificación (el Consorci AOC) o un número de identificación asignado por el Estado nacional (el DNI o el código de identificación profesional del trabajador, por ejemplo).*
>
> *Asimismo, la norma dispone que el campo CN debe contener un nombre de la persona firmante y que está permitido hacerlo en diferentes formatos o incluso la utilización de seudónimos y alias, dado que, a diferencia del campo GivenName and SurName or Pseudonym , se trata de un campo que se emplea para dar información sobre la identidad de la persona firmante de forma informal."*

De conformidad con esta norma, la inclusión del dato DNI en el campo *"CN"* de los certificados cualificados de trabajadores públicos no sería pertinente ni necesaria, a efectos de identificar a la persona firmante, dado que esta identificación se alcanzaría con el nombre y apellidos del empleado público, tal y como sucede en los documentos firmados de forma manuscrita.

Asimismo, debe tenerse en cuenta que el eventual riesgo de que dos personas tengan el mismo nombre y apellidos, se evita con otra información que también contiene el certificado cualificado, como el nombre de la entidad donde el empleado presta servicios - campo *"Organization"-;* así como la previsible inclusión del cargo en el pie de firma.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

También en relación a la identificación de la persona firmante, el artículo 24.1 del ReIDAS establece que los prestadores calificados de servicios de confianza (como la AOC) deben cumplir con los siguientes requisitos:

> *"1. Al expedir un certificado calificado para un servicio de confianza, un prestador calificado de servicios de confianza verificará, por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide un certificado calificado.*
>
> *La información a que se refiere el párrafo primero será verificada por el prestador de servicios de confianza bien directamente o bien mediante tercero de conformidad con el Derecho nacional: a) en presencia de la persona física o de un representante autorizado de la persona jurídica, ob) a distancia, utilizando medios de identificación electrónica, para los que se haya garantizado la presencia de la persona física o de un representante autorizado de la persona jurídica previamente a la expedición del certificado calificado, y que cumplan los requisitos establecidos con el artículo 8 respecto a los niveles de seguridad «sustancial» o «alto», por medio de un certificado de una firma electrónica calificada o de un sello electrónico calificado expedido de conformidad con la letra a) ob), od) utilizando otros métodos de identificación reconocidos a nivel nacional que aportan una seguridad equivalente en términos de fiabilidad a la presencia física.*
>
> *La seguridad equivalente será confirmada por un organismo de evaluación de la conformidad."*

De conformidad con el precepto transcrito, debe tenerse en cuenta que la identidad del empleado público titular del certificado calificado, ya se verifica cuando se expide éste.

En el mismo sentido, y en cuanto al uso de seudónimos, el artículo 17.3 de la LSE establece que los *"prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deben constatar la su verdadera identidad y conservar la documentación que le acredite."*

2.4. Sobre la normativa europea respecto al contenido de los certificados electrónicos.

Llegados a este punto, procede acudir a las previsiones contenidas en el ReIDAS.

Tal y como se señalaba en el dictamen CNS 17/2017, el artículo 50 del ReIDAS derogó *"la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, que España transpuso con la mencionada LSE, por lo que es necesario tener presente que la entrada en vigor de este ReIDAS,*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

de aplicación directa a cada Estado miembro desde el 1 de julio de 2016 (artículo 52), dejaría sin efecto aquellos preceptos de la LSE que se oponen."

Hecho este apunte, el artículo 51.2 del ReIDAS prevé como medidas transitorias que *"Los certificados reconocidos expedidos para las personas físicas conforme a la Directiva 1999/93/ CE se considerarán certificados calificados de firma electrónica conforme al presente Reglamento hasta que caduquen. "*

Así las cosas, una vez caducen los certificados emitidos con anterioridad al ReIDAS, los nuevos certificados que se emitan tendrán que ajustarse a lo que prevé esta norma europea.

En este sentido, los apartados 1 a 3 del artículo 28 del ReIDAS disponen que:

> *"1. Los certificados calificados de firma electrónica cumplirán los requisitos establecidos en el anexo I.*
> *2. Los certificados calificados de firma electrónica no estarán sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el anexo I.*
>
> *3. Los certificados calificados de firmas electrónicas podrán incluir atributos específicos adicionales no obligatorios. Estos atributos no afectarán a la interoperabilidad y el reconocimiento de las firmas electrónicas calificadas."*

Y el anexo I, al que se remiten los apartados 1 y 2 del precepto transcrito, establece los requisitos de los certificados calificados de firma electrónica, entre los que se incluye lo previsto en la letra "c":

> *c) al menos el número del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;"*

Así pues, el ReIDAS sólo requiere que el certificado calificado contenga el nombre de su titular o bien un seudónimo. Por el contrario, tal y como se ha expuesto, la LSE (artículo 11.2.e) exige incluir también el número de DNI, salvo que se utilice un seudónimo.

En relación a lo anterior, la Autoridad se pronunció en el dictamen CNS 17/2017 en los siguientes términos:

> *"Teniendo en cuenta que los Reglamentos son obligatorios en todos sus elementos y directamente aplicables a los Estados miembros (artículo 288 TFUE), habría que plantearse si la norma interna (LSE) puede establecer o prever más requisitos a la hora de identificar la persona firmante que los establecidos, en este caso, en el ReIDAS.*
>
> *Al respecto, conviene recordar que es jurisprudencia consolidada del Tribunal de Justicia de la Unión Europea (entre otros, sentencia de 14 de octubre de 2004, asunto c113/02, sentencia de 21 de diciembre de 2011, asunto c-316/10,*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

o sentencia de 25 de octubre de 2012, asunto c-592/11) que los Estados miembros pueden adoptar medidas de aplicación de un Reglamento siempre que éstas no obstaculicen su aplicabilidad directa, no oculten su naturaleza comunitaria y regulen el ejercicio del margen de apreciación que el Reglamento en cuestión les confiere, manteniéndose en cualquier caso dentro de los límites de sus disposiciones.

Es decir, que la normativa de la UE figure en un Reglamento (como en este caso) no significa necesariamente que esté prohibida cualquier medida nacional de aplicación de esta normativa. Es más, el TJUE admite que, si bien, en atención a la naturaleza del Reglamento, sus disposiciones tienen efecto inmediato en los ordenamientos jurídicos nacionales, algunas disposiciones de los Reglamentos pueden requerir, para su ejecución, la adopción de medidas de aplicación por los Estados miembros. Es necesario, en palabras del Tribunal, remitirse a las disposiciones concretas de cada Reglamento para comprobar si éstas, interpretadas de conformidad con los objetivos de dicho Reglamento, prohíben, exigen o permiten que los Estados miembros adopten determinadas medidas de aplicación y, en particular en este último supuesto, si la medida se enmarca en el margen de apreciación reconocido en todos los Estados miembros."

Tal y como se ha avanzado, el anexo I del ReIDAS sólo exige, como contenido mínimo de los certificados calificados, la inclusión del nombre de la persona firmante (o de un pseudónimo), a efectos de permitir su identidad. Tal y como se señalaba en el dictamen CNS 17/2017, *"esta previsión, que facilitaría la interoperabilidad de las firmas electrónicas entre los Estados miembros, parece razonable, dado que en muchos países de la UE los ciudadanos no están obligados a disponer de un documento de identificación personal, como lo es el DNI en el caso de los ciudadanos españoles mayores de 14 años (Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI y sus certificados de firma electrónica)."*

Y se añadía que *"La exigencia de incluir el DNI en los certificados, a los que se refiere la LSE, sólo podría entenderse válida, en atención al ReIDAS, en la medida en que este dato se incorporara como atributo específico adicional no obligatorio y siempre que hacerlo no comprometiera la interoperabilidad y el reconocimiento de la firma electrónica calificada. En caso contrario, las previsiones de la LSE se verían desplazadas por lo establecido en el ReIDAS."*

2.5. Sobre la interoperabilidad.

En su escrito de respuesta al requerimiento que formuló esta Autoridad, la AOC invocaba que la normativa que determina de forma estandarizada la estructura (campos y contenidos) de un certificado electrónico, tiene por objetivo asegurar el reconocimiento e interoperabilidad de los certificados. Y añadía que la falta de inclusión del DNI en la estructura del certificado tendría consecuencias directas sobre la funcionalidad principal del certificado digital, hasta tal punto que

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

dejaría de ser reconocido como empleado público tanto por parte de la AGE, como de diferentes aplicaciones corporativas.

Al respecto, procede incidir de nuevo que de acuerdo con el ReIDAS, al que está sujeto el certificado electrónico de los empleados públicos, no sería obligatoria la inclusión del DNI (anexo I), sino que en todo caso la asignación de cualquier otra información (como podría ser el caso del DNI) estaría limitada a que esta asignación no fuera obligatoria (artículo 28.2 del ReIDAS) y al hecho de que no se comprometiera la interoperabilidad de la firma calificada (artículo 28.3 del ReIDAS).

Es decir, que la carencia del DNI no puede afectar a la interoperabilidad. En cambio, su inclusión en el certificado digital, sí puede llegar a perjudicarla.

En este punto, tal y como indica el considerante 54 del ReIDAS, *"La interoperabilidad y el reconocimiento transfronterizos de los certificados calificados es un requisito previo para el reconocimiento transfronterizo de las firmas electrónicas calificadas. Por consiguiente, los certificados calificados no deben estar sometidos a ningún requisito obligatorio que exceda de los requisitos establecidos en el presente Reglamento. No obstante, en el plano nacional debe permitirse la inclusión de atributos específicos, por ejemplo identificadores únicos, en los certificados calificados, a condición de que tales atributos específicos no comprometan la interoperabilidad y el reconocimiento transfronterizos de los certificados y las firmas electrónicas cualificados."*

Así las cosas, en el presente caso la interoperabilidad no sólo debe garantizarse a nivel estatal, sino en todos los Estados miembros de la Unión Europea. A su vez, el considerante 54 del ReIDAS incide en que la inclusión de otros atributos específicos en los certificados calificados no pueden comprometer la interoperabilidad, el reconocimiento transfronterizo de los certificados y las firmas electrónicas calificadas. Y, en este sentido, es cierto que dicho considerante se refiere a la posibilidad de que a nivel nacional se puedan incluir identificadores únicos, pero éstos no necesariamente deben ser el DNI. En efecto, estos identificadores únicos pueden ser cualquier dato pseudonimizado vinculado a la persona titular del certificado.

A su vez, tal y como ya se ha expuesto, la norma *ETSI EN 319 412-2* tampoco requiere la inclusión del DNI para garantizar la interoperabilidad a nivel comunitario.

Por otra parte, en el dictamen CNS 17/2017 también se analizaba que la inclusión del dato DNI podría responder a la necesidad de garantizar la interoperabilidad entre las aplicaciones usuarias.

Ciertamente, el artículo 18.4 del ENI dispone que los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de forma que tanto la identificación como la firma electrónica generada a partir de los perfiles comunes de los campos de los certificados puedan ser reconocidos por las aplicaciones de las diferentes Administraciones públicas sin ningún tipo de restricción técnica, semántica u organizativa.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Ahora bien, tal y como se señalaba en el dictamen antes mencionado, si ésta es la finalidad perseguida, no parece que incluir el dato DNI en el campo *"CN"* del certificado sea la opción más adecuada, dada la casuística que suele producirse en la asignación de información a este tipo de certificados, fruto del amplio volumen de certificados a emitir (gran volumen de trabajadores públicos) ya la diversidad de prestamistas de servicios de certificación que pueden emitirlos. A estas circunstancias, de hecho, hace referencia el propio documento del MHAP.

2.6. Acerca del principio de minimización.

El artículo 5.1.c) del Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), contempla el principio de minimización como uno de los principios relativos al tratamiento de datos personales. De acuerdo con este principio los datos personales serán *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".*

Asimismo, el considerante 39 del RGPD establece que *"Las datos personales sólo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios."*

De conformidad con este principio de minimización, los datos de los trabajadores públicos incluidos en la configuración de los certificados de firma electrónica serán los mínimos necesarios para el cumplimiento de la finalidad pretendida.

De este modo, si la finalidad perseguida en un determinado contexto puede ser alcanzada sin necesidad de llevar a cabo el tratamiento de un determinado dato, sin verse por ello alterada o perjudicada tal finalidad, debería optarse necesariamente por esta posibilidad , dado que el tratamiento de datos de carácter personal supone, tal y como consagra el Tribunal Constitucional en la Sentencia núm. 292/2000, una limitación del derecho del afectado a disponer de la información referida a su persona.

Por su parte, el artículo 5 del ReIDAS en lo referente al tratamiento y protección de los datos, dispone lo siguiente:

> *"1. El tratamiento de las datos personales será conforme a lo dispuesto en la Directiva 95/46/ CE.*
>
> *2. Sin perjuicio de los efectos jurídicos que la legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas."*

La remisión del ReIDAS a la Directiva (UE) 95/46/CE, debe entenderse efectuada en el RGPD tal y como establece el artículo 94.2 del RGPD.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Pues bien, tal concretaba la Autoridad en el dictamen CNS 17/2017, *"Esta identificación del trabajador público, por aplicación del principio de minimización, debería producirse de la misma forma que si la actuación no se llevara a cabo por medios electrónicos. Es decir, debería facilitarse sólo su nombre y apellidos, información que podría completarse con la indicación de su cargo o puesto de trabajo y la Administración a la que pertenece."*

Por tanto, la persona empleada pública no tiene el deber de soportar que sea revelado el dato referente a su DNI, ya sea a través del aspecto o imagen que se genera al firmar electrónicamente, ni tampoco mediante la consulta de las propiedades de la firma del certificado calificado o reconocido.

Dicho esto, el artículo 53.1.b) de la LPAC reconoce el derecho de las personas interesadas a *"identificar a las autoridades y al personal al servicio de las administraciones públicas bajo cuya responsabilidad se tramiten los procedimientos."*

Tal y como indicaba la Autoridad en el dictamen CNS 17/2017, *"Tratándose de la identificación del trabajador público que firma un determinado documento administrativo, resulta suficiente, desde el punto de vista del principio de minimización, facilitar su nombre, apellidos y cargo, dado que se trata de la información personal mínima necesaria que requiere el ciudadano para conocer la identidad de la persona que le ha atendido en su actuación ante la Administración pública. Conocer el DNI del trabajador público, de hecho, no aportaría o mejoraría la identificación del trabajador, dado que el ciudadano no dispone de los medios adecuados para contrastar la veracidad de esta información personal."* Y se añadía que esta *"actuación por parte de los trabajadores públicos (firmar los documentos pertinentes) trasladada al ámbito de la administración electrónica no debe desmerecer su derecho fundamental a la protección de datos de carácter personal (artículo 18.4 CE) ."*

En definitiva, de acuerdo con todo lo expuesto en esta resolución, cabe concluir que no es necesaria la inclusión del DNI en los certificados calificados de los empleados públicos, ni para su identificación (en particular, ante la ciudadanía) , ni tampoco para garantizar la interoperabilidad.

En efecto, tal y como ya se indicaba en el dictamen CNS 17/2017, el ReIDAS no impide la emisión de certificados calificados de firma electrónica con seudónimo, es decir, certificados en los que no constan datos personales identificativos (nombre, apellidos o DNI) de la persona firmante. Y se añadía que *"El prestador de servicios de certificación será quien disponga de la información que vincula un certificado calificado con una persona concreta. La utilización de seudónimos, por tanto, es una opción igualmente válida a efectos de establecer la identidad de la persona firmante, sin que ello merme el uso, la capacidad o la funcionalidad de los certificados cualificados."*

Por su parte, el artículo 5.2 del ReIDAS ya prevé que los Estados miembros no pueden prohibir el uso de seudónimos en las transacciones electrónicas.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Así pues, nada impide que en los campos que integran el certificado digital en los que consta el DNI de los empleados públicos (CN, Surname y SerialNumber), este dato se sustituya por un seudónimo único asignado por la AOC o por la Administración o entidad donde presta servicios el empleado.

Al mismo tiempo, el uso de seudónimos en los campos indicados, también garantiza la interoperabilidad del certificado calificado, teniendo en cuenta que el dato sustituido (el DNI) no es necesario de acuerdo con los requisitos de los certificados calificados de firma electrónica exigidos por ReIDAS (anexo I) y que la propia la LSE admite su uso (art. 11.2.e) sin restringirlo a ningún supuesto específico.

En definitiva, desde la perspectiva del principio de la minimización de los datos, la inclusión del DNI en los certificados calificados o reconocidos, es un dato inadecuado, no pertinente y no limitado al necesario para su utilización.

2.7. Acerca de la protección de datos en el diseño.

Llegados a este punto, cabe poner de manifiesto que una de las obligaciones que impone el RGPD (artículo 25.1) a los responsables de los tratamientos es la protección de datos en el diseño:

> *"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, al objeto de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."*

Así, el responsable del tratamiento debe implementar las medidas adecuadas, técnicas y organizativas, para poner en práctica los principios de protección de datos. Tal y como indica el considerante 78 del RGPD *"Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible las datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que traten datos personales para cumplir su función, debe enlentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos."

La protección de datos en el diseño debe implementarse tanto en el momento de determinar los medios del tratamiento, como también una vez iniciado el tratamiento. En este último supuesto, el responsable sigue teniendo la obligación de hacer efectivos los principios relativos al tratamiento y, por lo que aquí interesa, de analizar periódicamente si los datos personales que son objeto de tratamiento todavía son adecuados, pertinentes y limitados.

2.8. Sobre los seudónimos.

En el dictamen CNS 17/2017, esta Autoridad ya analizaba la posibilidad de utilizar pseudónimos de forma generalizada en los certificados calificados de los empleados públicos. En concreto, allí se indicaba lo siguiente:

> *"Esta posibilidad, si bien podría resultar conflictiva en atención a las previsiones de la Ley 40/2015 (el artículo 43.2 permite limitar los datos de identificación del trabajador en el certificado, empleando en su lugar el número de identificación profesional, pero sólo por motivos de seguridad pública), resulta plenamente aplicable de acuerdo con el Anexo I del ReIDAS.*
>
> *Cabe recordar que cada entidad de prestación de servicios de certificación puede establecer su propia declaración de prácticas de certificación y definir, por tanto, los perfiles de los certificados que emite (artículo 19 LSE).*
>
> *Así pues, el Consorci AOC podría establecer, en el perfil de certificado calificado de trabajador público, que la identificación de la persona firmante se llevará a cabo, con carácter general, a través de un seudónimo. Este pseudónimo podría ser el nombre y apellidos del trabajador público y, en su caso, cargo o categoría, siempre que, por motivos de seguridad pública, no se requiera preservar su anonimato.*
> *De esta forma se evitaría la difusión del dato DNI que pudiera constar en alguno de los campos de información que constituyen la estructura del certificado.*
>
> *En caso de que, ciertamente, por razones de seguridad pública, debiera garantizarse el anonimato del trabajador público, el seudónimo podría ser su código de identificación profesional, en la medida en que éste no esté relacionado con datos personales del trabajador público (como el número de DNI), o cualquier otro indicador proporcionado por la Administración pública en la que presta sus servicios.*
>
> *En ambos casos debería indicarse claramente que se trata de un seudónimo (anexo I ReIDAS)."*

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

Así las cosas, teniendo en cuenta el principio de minimización de los datos (art. 5.1.c RGPD) y la obligación de garantizar la protección de datos en el diseño (art. 25.1 RGPD), la AOC debe adoptar las medidas adecuadas para que en los certificados calificados emitidos a empleados públicos, no conste su DNI, como las que se acaban de transcribir.

En este sentido, cabe advertir que estas medidas no pueden restringirse sólo a los supuestos previstos por el MHAP (información clasificada, seguridad pública, defensa nacional u otras actuaciones en las que esté legalmente justificado el anonimato), que se rigen por su normativa específica tal y como dispone el artículo 4.4 de la LSE.

Por tanto, deben aplicarse a todos los empleados públicos.

2.9. Sobre la responsabilidad de la AOC.

En el presente caso, debe tenerse en cuenta que, para la emisión de certificados calificados a empleados públicos, la AOC seguía los parámetros establecidos por el MHAP, los cuales prevén la inclusión del DNI en los certificados.

Lo anterior podía dar pie a interpretar que, de acuerdo con dichas indicaciones del MHAP, la regla general era que en los certificados emitidos a empleados públicos debía incluirse el DNI y que el uso de seudónimo sólo estaba reservado a unos casos concretos.

Por estos motivos se ha considerado que la AOC habría actuado con el convencimiento de que no cometía ninguna infracción de la normativa sobre protección de datos al incluir el DNI de los empleados públicos en el certificado calificado, a efectos de garantizar su reconocimiento y su interoperabilidad.

Así pues, por aplicación del principio de responsabilidad o culpabilidad (art. 28 LRJSP), no procede iniciar un procedimiento sancionador, en tanto que en este caso concreto, puede resultar excesivo invocar la falta de diligencia de la entidad.

Todo ello, sin perjuicio de la advertencia y medidas correctoras que se requerirán más adelante, para evitar la revelación del DNI de sus empleados como causa del uso de certificados cualificados.

2.10. Sobre la responsabilidad del ARC y de una entidad local.

Por su parte, el ARC y la entidad local donde presta servicios la segunda persona denunciante (de la que no se tiene constancia y no era objeto de denuncia), serían responsables de implementar las medidas adecuadas para modificar el aspecto o la imagen de la firma de sus empleados públicos basada en un certificado calificado, a fin de garantizar que no se puede visualizar el DNI. Está en

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

decir, de crear un nuevo aspecto de la firma que incorporara únicamente los datos relativos al nombre y apellidos y cargo, a través del software empleado para la firma electrónica.

No obstante, no se puede atribuir a estas entidades que en el certificado calificado de los empleados públicos que emite una entidad prestadora de servicios de certificación cualificados (AOC), se incorpore el DNI de su titular.

A su vez, si no se hubiera incorporado este dato al certificado, la imagen o apariencia que se genera al firmar electrónicamente, en ningún caso incluiría el DNI. En este punto, procede la remisión a lo expuesto en el apartado anterior respecto a las previsiones de la normativa española y las indicaciones del MHAP respecto a la inclusión del DNI en los certificados digitales.

Pues bien, el conjunto de las circunstancias señaladas también llevan a concluir que no procede la incoación de un procedimiento sancionador contra estas entidades, en aplicación del principio de responsabilidad o culpabilidad.

Todo ello, sin perjuicio de la advertencia y medidas correctoras que se requerirán más adelante, para evitar la revelación del DNI de sus empleados como causa del uso de certificados cualificados.

3. De conformidad con todo lo expuesto en los apartados 2.9 y 2.10 del fundamento de derecho 2º, procede acordar su archivo.

4. El artículo 58.2.a) del RGPD faculta a las autoridades de control, en ejercicio de sus poderes correctivos, a fin de formular una advertencia al responsable, si las operaciones de tratamiento previstas pueden infringir lo dispuesto en el RGPD . A su vez, el artículo 8.2.c) de la Ley 32/2010 faculta a la directora de la Autoridad para requerir a los responsables ya los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación en la legislación vigente.

Es en virtud de esta facultad que, a pesar de la decisión de archivo basada en los argumentos expresados en el apartado 2.9 y 2.10 de los fundamentos de derecho 2º, por un lado, procede advertir tanto a la AOC, como a la ARC, que el tratamiento del DNI de los empleados públicos en el marco de la configuración o utilización de los certificados calificados o reconocidos, infringe la normativa sobre protección de datos.

Y por otra, también se considera procedente efectuar los siguientes requerimientos.

4.1. Por un lado, es necesario requerir a la AOC para emprender las acciones pertinentes para evitar que en los certificados cualificados emitidos a empleados públicos no conste su DNI, como las que se han expuesto en esta resolución.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

4.2. Por otra parte, es necesario recomendar a la ARC que, mientras la AOC no implemente la anterior medida correctora, lleve a cabo las siguientes actuaciones:

4.2.1. Modificar el aspecto o la imagen de la firma de sus empleados efectuada a través de un certificado calificado, de forma que no aparezca su DNI. A modo de ejemplo, la ARC puede definir en el programa empleado para firmar electrónicamente, los datos que son visibles una vez firmado electrónicamente un documento.

4.2.2. En relación con todos los documentos electrónicos dirigidos a otros órganos o particulares firmados por sus empleados mediante un certificado calificado, remitir únicamente a los sus destinatarios una copia auténtica del original (esta acción evita que se pueda visualizar el DNI de la persona firmante).

Cabe decir que de conformidad con el artículo 27.2 de la LPAC, las copias auténticas tienen la misma validez y eficacia que los documentos originales.

Esto, sin perjuicio de otras medidas como utilizar un sello de órgano.

Y, en cuanto a la publicación de documentos electrónicos, al margen de las actuaciones ya indicadas, tal y como se señalaba en el dictamen CNS 1/2019, también se podrían publicar los documentos electrónicos sin incorporar las firmas; o bien, convertir el documento a publicar en formato “imagen”, lo que no permitiría acceder a las propiedades de la firma.

Dado que se desconoce el ente local donde presta servicios la segunda persona denunciante, quien dirigía su escrito de denuncia contra la entidad que consideraba que era la prestamista de servicios de certificación cualificados, no se puede efectuar ningún requerimiento al respecto.

Resolución

Por tanto, resuelvo:

1. Archivar las actuaciones de información previa números IP 84/2019 e IP 110/2019, relativas al Consorcio de Administración Abierta de Cataluña (IP 84/2019 e IP 110/2019) ya la Agencia de Residuos de Cataluña (IP 84/2019).

2. Advertir a la AOC y al ARC que, en caso de que no implementen las medidas indicadas en el fundamento de derecho 4º, las operaciones de tratamiento que se han abordado en la presente resolución podrían infringir lo dispuesto en la normativa de protección de datos.

3. Notificar esta resolución a la AOC, a la ARC ya las dos personas denunciantes.

Calle Rosselló, 214, esc. A,1r 1a
08008 Barcelona

4. Ordenar la publicación de la resolución en la web de la Autoridad (www.apd.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con el artículo 14.3 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, las personas interesadas pueden interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevé el artículo 123 y siguientes de la Ley 39/2015. También se puede interponer directamente un recurso contencioso administrativo ante los juzgados de lo contencioso-administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998 , de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Asimismo, las personas interesadas pueden interponer cualquier otro recurso que considere conveniente para defender sus intereses.

La directora,