

El derecho de acceso a la información pública

Primer procedimiento de aplicación del sistema Cl@ve

La Ley 19/2013, de 9 de diciembre de transparencia, acceso a la información pública y buen gobierno configura el derecho de acceso a la información pública como un procedimiento administrativo que como tal, tiene las mismas exigencias y obligaciones que los procedimientos establecidos en otros ámbitos de la administración pública.

**GLORIA MARTÍNEZ
HERRAN
Y JOSÉ CARRERO
VIVAS**

Oficina de la
Transparencia
y Acceso a la
Información.
Ministerio de
la Presidencia

Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de la norma y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

El artículo 17 de la citada norma, establece que el procedimiento para el ejercicio del derecho de acceso se iniciará con la presentación de la correspondiente solicitud, que deberá dirigirse al titular del órgano administrativo o entidad que posea la información.

La solicitud podrá presentarse por cualquier medio que permita tener constancia de: la identidad del solicitante, la información que se solicita, una dirección de contacto preferentemente electrónica, a efectos de comunicaciones y en su caso, la modalidad que se prefiera para acceder a la información solicitada.

Por lo tanto, la ley exige no solo contar con la identidad del solicitante, sino tener constancia de esta, constancia que debe predicarse de todos los medios por los que pueda presentarse la solicitud, tanto los electrónicos como los presenciales.

Sin embargo, desde la puesta en marcha del Portal de la Transparencia del Gobierno de España y el inicio, por parte de los ciudadanos, del ejercicio de este derecho mediante la presentación de solicitudes de información pública, uno de los temas más cuestionados y que más críticas ha suscitado ha sido la elección del sistema Cl@ve, por primera vez en el ámbito de las Administraciones Públicas, para acreditar la identidad de los solicitantes en los procedimientos iniciados por vía elec-

Sobre el Portal

[Ley de Transparencia](#)

[Conozca el Portal](#)

[El Portal en cifras](#)

[Redes sociales y sugerencias](#)

[Iniciativas](#)

[Inicio](#) > [Sobre el Portal](#) > [Conozca el Portal de la Transparencia](#)

Conozca el Portal de la Transparencia

[Facebook](#) [Twitter](#) [LinkedIn](#) [YouTube](#) [RSS](#) [0](#) [+](#)

[Imprimir](#)

En esta página le explicamos qué es el Portal de la Transparencia y qué contiene.

Puede descargar este documento en formato PDF [📄](#)

[Sobre la Ley de Transparencia](#) ▾

[Sobre la Publicidad activa](#) ▾

[Sobre el Derecho de acceso a la información pública](#) ▴

¿Qué es el derecho de acceso a la información pública?

Es el derecho de acceso a acceder a información pública en los términos previstos en la Constitución artículo 105.b), entendiéndose como información pública los contenidos o documentos, cualquiera que sea su soporte o formato, que obren en poder de la administración y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Para más información sobre el derecho de acceso accede a la [Guía del Ciudadano: Derecho de Acceso](#)

¿Se puede pedir cualquier información?

El derecho de acceso a la información está sujeto a ciertos límites que tienen como objetivo proteger otros bienes jurídicos que pueden quedar desprotegidos si se da la información. Es decir, los límites existen para proteger información que no debe ser pública porque, si lo fuera, podría dañar a una persona o al interés público.

trónica. Se ha criticado, por parte de ciertas asociaciones y por muchos ciudadanos, la complejidad que supone la utilización de este sistema, la exigencia de formalidades innecesarias, a su juicio (como la necesidad de obtener una carta de invitación de la Agencia Estatal de Administración Tributaria por la que hay que aportar una cuenta bancaria y un número de teléfono móvil.....) y en definitiva, que esta complejidad puede suponer, para mucha gente, un elemento disuasorio para ejercitar el derecho de acceso a la información.

Así, se reclama un acceso electrónico fácil, rápido, efectivo y práctico a la información pública, exigiendo constancia de los datos identificativos de los ciudadanos, con los mismos requisitos, pero no más, que en el acceso no telemático, sin con-

troles ni comprobaciones añadidos, e incluso, la utilización del correo electrónico como medio de inicio del procedimiento.

Es curioso que en otros ámbitos en los que se regulan procedimientos administrativos de carácter económico o de seguridad social, nadie cuestiona que se soliciten salvaguardas en la acreditación de la identidad de los solicitantes por cuestiones de protección de datos, por cuestiones de carácter económico o por otras cuestiones de diversa índole. ¿Por qué entonces cuando hablamos del derecho de acceso a la información estas salvaguardas se consideran excesivas, a pesar que se exigen en la norma y se pide que se relaje su aplicación, en detrimento de la seguridad jurídica? ¿Es que el procedimiento de derecho de acceso previsto en la Ley de Trans-

parencia debe catalogarse como un procedimiento menor en el que los principios y bases que presiden las relaciones de los ciudadanos por medios electrónicos con las administraciones Públicas, no deben aplicarse en aras de una generalización de un acceso sin control, a la información de las administraciones públicas?

Más teniendo en cuenta, como se ha señalado, que el procedimiento regulado en la Ley de transparencia tiene las mismas características de cualquier procedimiento que se tramita ante las administraciones públicas: la respuesta al derecho de acceso toma forma de resolución dictada por el órgano que dispone de la información (en la mayoría de los casos con rango de Director General), frente a esta resolución, se puede interponer reclamación ante el Consejo de

Transparencia y Buen Gobierno (que sustituye al recurso administrativo que procediera) o directamente el recurso contencioso administrativo. Además, el ejercicio de este derecho puede afectar intereses legítimos de terceros, cuya opinión ha de tenerse en cuenta y ponderarse en el acto de resolución de las solicitudes planteadas.

Se trata, también de un procedimiento cuyo incumplimiento en alguno de sus plazos o trámites, puede suponer para el órgano obligado a resolver, la apertura de un expediente disciplinario.

En este contexto, no parece excesivo que la Ley 9/2013, de 9 de diciembre, exija al solicitante del derecho de acceso, una identificación para poder referir a esta persona física o jurídica toda la tramitación del procedimiento, máxime si se tiene en cuenta que la Ley no exige para la tramitación del procedimiento de derecho de acceso, la motivación de la solicitud.

Por ello es necesario que este procedimiento cuente con las mismas garantías y salvaguardas que las establecidas para cualquier otro procedimiento administrativo.

En el caso de las solicitudes de información por vía electrónica, conviene en primer lugar hacer algunas aclaraciones sobre dos procesos que parece que se entremezclan pero que son separados, aunque complementarios: *la obtención del medio* de identificación electrónica, que permite al ciudadano relacionarse con la Administración de forma telemática, y *el uso del medio* para utilizar los servicios electrónicos de la Administración y concretamente, en el caso que nos ocupa, el ejercicio del derecho de acceso a la información pública a través Portal de la Transparencia.

Ni que decir tiene que la obtención del medio se efectúa una sola vez y permite al titular su uso, anulación o revocación, y su renovación duran-

te el periodo de vigencia establecido para el mismo.

Hay que resaltar que la obtención del medio de identificación electrónica se puede realizar siempre de manera presencial, con la presentación del DNI (en vigor) como único medio de identificación, acompañado de la firma de un documento de solicitud que queda en poder de la Administración. La vinculación entre la identidad de la persona y el medio se lleva a cabo mediante esta comparecencia y es esta la que da validez a dicho medio en su utilización posterior, es lo que se denomina registro fuerte. Otra cosa es que para el uso práctico del medio se requieran elementos técnicos adicionales que hagan segura su utilización, como el teléfono móvil, tarjetas criptográficas etc..., que en ningún caso suponen comprobaciones adicionales de identificación.

La obtención no presencial, o registro débil, de un medio electrónico de identidad, válido para la Administración, solamente es posible para los sistemas de identificación con nivel básico de seguridad, basados en una clave PIN de varios usos o una clave permanente. Resaltamos que para el procedimiento del derecho de acceso se admite este nivel básico de seguridad, no siendo así para otros procedimientos administrativos.

El registro no presencial del medio pretende suplir la no comparecencia del interesado mediante la aportación telemática de datos personales (por ejemplo algunos dígitos del nº de cuenta corriente) y el envío al domicilio de un código seguro de verificación (carta de invitación) que permite completar el proceso de registro. Este proceso puede resultar complejo, pero su finalidad no es otra que evitar, con el nivel de seguridad adecuado, la suplantación de identidad del solicitante del medio electrónico.

A continuación se detallan las di-

ferentes opciones de identificación que admite el sistema Cl@ve en función de su nivel de seguridad en la identificación del usuario:

- Nivel básico con registro débil: Permiten el acceso a servicios mediante el uso de una clave PIN de varios usos o una clave permanente sin envío de mensaje de SMS. Se apoyan en un *registro no presencial del titular* en el sistema, a partir de una carta de invitación solicitada por el usuario.

- Nivel básico con registro fuerte: Permiten el acceso a servicios mediante el uso de una clave PIN de varios usos o una clave permanente sin envío de mensaje de SMS. Se apoyan en un *registro del titular presencial o electrónico con certificado electrónico reconocido*.

- Nivel sustancial: Permiten el acceso a servicios mediante el uso de una clave PIN de un solo uso, una clave permanente, complementado con envío de SMS, o un certificado electrónico reconocido software. Se apoyan en un *registro del titular presencial o electrónico con certificado electrónico reconocido*.

- Nivel alto: Permiten el acceso a servicios mediante el uso de un certificado electrónico reconocido hardware o el DNI-electrónico. Se basan en un *registro presencial o en electrónico mediante otro certificado electrónico del mismo nivel*.

Los certificados electrónicos reconocidos de uso habitual son el DNIe, que requiere de un lector de tarjeta criptográfica, y el de la Fábrica Nacional de Moneda y Timbre (FNMT), que puede instalarse en tarjeta o directamente en el ordenador del usuario titular y cuya obtención no conlleva gastos.

Una vez obtenido el medio de identificación electrónica, su utilización es bastante simple y *se reduce a introducir la clave o PIN que el medio requiere* en el momento que el sistema informático lo demanda, que suele ser el momento previo al acceso al

formulario o información solicitada.

Cabe señalar también que una comprobación que siempre se realiza en la utilización de un medio electrónico de identificación, es la comprobación de vigencia del medio. Dado que el periodo de validez es limitado y que el propio titular puede cancelarlo o revocarlo, es una comprobación imprescindible para evitar usos fraudulentos, constituye una garantía para su titular y no requiere de actuación adicional alguna por su parte. En este sentido hay un paralelismo claro con la fecha de caducidad del DNI, su comprobación habitual en numerosos trámites y la obligación de renovarlo por parte de su titular.

Podemos concluir que el ejercicio del derecho de acceso a la información pública, por medios electrónicos, requiere el nivel mínimo de seguridad posible para un procedimiento administrativo; el proceso de identificación es sencillo porque se reduce a introducir una clave o PIN cuando el sistema lo solicita, y, finalmente, no se necesitan elementos adicionales de identificación.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, (derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que entrará en vigor el 2 de octubre de 2016) reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas, con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.



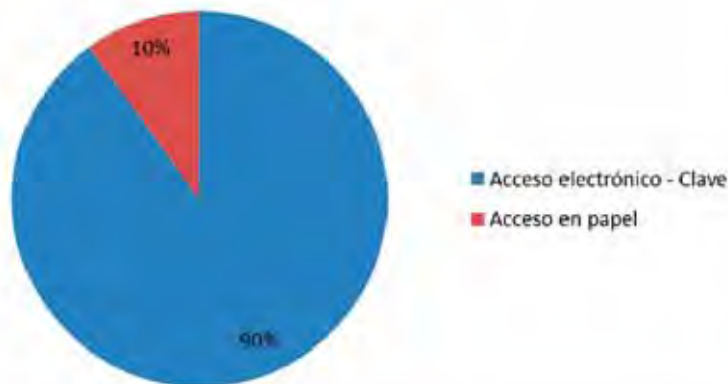
En el Título II de la citada Ley, que se refiere al régimen jurídico de la administración electrónica, en concreto, en su artículo 13, que regula las formas de identificación y autenticación, tras citar los sistemas de firma electrónica incorporados al DNI y los sistemas de firma electrónica avanzada, se refiere a otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro

previo como usuario, en los términos y condiciones que, en cada caso, se determinen.

Por su parte, el artículo 11 del Real Decreto 1671/2009, de 6 de noviembre por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos señala que, cuando el sistema de firma electrónica se refiera a la totalidad de la

Monográfico

Tipo de acceso al Derecho de Acceso	Número de solicitudes	Porcentaje sobre el total
Acceso electrónico - Clave	2961	89,9%
Acceso en papel	331	10,1%
Total	3292	



Administración General del Estado, se requerirá Acuerdo de Consejo de Ministros para la aprobación del mismo.

En este contexto, la Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros de 19 de septiembre de 2014, por el que se aprueba Cl@ve, lo regula como la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Para la elección de este sistema en el ejercicio del Derecho de acceso reconocido en la Ley 19/2013 de transparencia, acceso a la información pública y buen gobierno se consideraron sus principales ventajas:

- Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contra-

seña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

- Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos.

- Se trata de una plataforma común para la identificación, autenticación y firma electrónica, un sistema interoperable y horizontal que evita a las Administraciones Públicas tener que implantar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración.

- Cl@ve permite que las aplicaciones de administración electrónica puedan definir el nivel de aseguramiento en la calidad de la autenticación que desean, en base a los datos que tratan y a la clasificación de seguridad siguiendo las recomendaciones

del Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica). El ciudadano usuario de los servicios de administración electrónica, puede entonces escoger el identificador que desea usar, entre los disponibles para el nivel de aseguramiento requerido por la aplicación.

- Cl@ve contempla la utilización de sistemas de identificación basados en claves concertadas (sistemas de usuario y contraseña) y certificados electrónicos (incluyendo el DNI-e).

Adicionalmente, Cl@ve está preparada para incorporar en el futuro, conforme se vayan integrando en el sistema de reconocimiento transfronterizo de identidades electrónicas previsto en la legislación europea, mecanismos de identificación de otros países de la Unión Europea.

En definitiva Cl@ve se configura como un sistema colaborativo de identificación, autenticación y firma electrónica, llamado a resolver las limitaciones de los actuales, integrando los sistemas de claves concertadas de la Administración ya existentes en uno único y abriendo su utilización a la totalidad del Sector Público Administrativo estatal y permitiendo también integrarse al resto de Administraciones Públicas cuando esté disponible, habilitando de este modo la extensión práctica de los servicios de Administración Electrónica a la gran mayoría de ciudadanos españoles.

Si se hace un análisis de los datos disponibles hasta el momento, de todas las solicitudes de derecho de acceso que se han recibido hasta el día 6 de noviembre de 2015 (3329), 2974 lo han hecho a través de la aplicación GESAT, a la que se accede a través del Portal de la Transparencia del Gobierno de España, y por tanto utilizando el sistema Cl@ve, y 331 se han recibido en papel a través de

registro o de correos. Ello permite señalar que la mayoría de solicitudes se han recibido por vía telemática, a pesar de las dificultades señaladas para su utilización, y solo un porcentaje residual lo han hecho a través de papel, vía a la que también han acudido a los ciudadanos entendiendo su uso como válido.

De todo lo expuesto, pueden extraerse las siguientes conclusiones:

- El derecho de acceso a la información pública se configura en la Ley de Transparencia como un procedimiento administrativo que se inicia con la presentación de la solicitud por una persona por cualquier medio que permita tener constancia de la identidad del solicitante.
- La presentación electrónica de la solicitud, debe de realizarse respetando este principio y con las debidas garantías de seguridad jurídica que la normativa predica de las relaciones del ciudadano con la administración, utilizando medios electrónicos.
- La presentación en papel, por medio de registro, debe respetar de la misma forma que la anterior, las debidas garantías de seguridad jurídica que están presentes en cualquier procedimiento tramitado ante las administraciones públicas y la propia ley prevé los mecanismos para que esta se produzca.
- En el caso de presentación de solicitudes por vía electrónica, es fundamental la elección de un sistema de autenticación electrónica que permita conciliar un adecuado equilibrio entre seguridad jurídica y facilidad de acceso de los ciudadanos a la información pública.
- La petición que hacen ciertas organizaciones sociales de suprimir el requisito de la utilización de sistemas seguros para la relación con las administraciones públicas por vía electrónica, promoviendo el derecho de acceso a la información simplemente por correo electrónico, po-

drían conducir de facto a peticiones masivas sin reglas de procedimiento, sin plazos debidamente acreditados mediante registros públicos y sin la certeza de cumplir con las obligaciones previstas en la propia Ley de transparencia y otras leyes que regulan el procedimiento administrativo en nuestro ordenamiento jurídico

En este contexto y, en la medida que Cl@ve, como hemos visto, comprende un gama muy variada, a elección del ciudadano, de sistemas de autenticación para acreditar la identidad por medios electrónicos, es por lo que se entiende que este sistema es lo suficientemente amplio como para garantizar al ciudadano una mayor flexibilidad y variedad en sus relaciones electrónicas con la Administración Pública.

Es cierto que para utilizar las claves concertadas el ciudadano debe registrarse en el sistema, aportando algún dato que permita su acreditación, sobre todo si el proceso se hace en su totalidad de manera electrónica. Sin embargo se considera que es imprescindible este proceso si se quiere dotar al sistema de la seguridad jurídica necesaria a la que obliga la norma. Si no se desarrollan garantías suficientes en la aplicación del proceso, podría darse el caso de que alguien pudiera suplantar la firma y la personalidad del ciudadano, llevando a cabo actuaciones que pudieran perjudicar al sujeto en cuestión.

Además el sistema Cl@ve ofrece la ventaja de referirse al ámbito de la administración (sector público administrativo) que se corresponde con el ámbito del Portal de la Transparencia del Gobierno de España.

Por ello se estima que, si bien el sistema previsto para el acceso electrónico a este procedimiento introduce una serie de dificultades para su utilización, propias del uso de un medio tecnológico, estas dificultades son las mismas que las que se exigen

Adicionalmente, Cl@ve está preparada para incorporar en el futuro, conforme se vayan integrando en el sistema de reconocimiento transfronterizo de identidades electrónicas previsto en la legislación europea, mecanismos de identificación de otros países de la Unión Europea.

para el acceso a otros procedimientos administrativos que se tramitan de forma electrónica. Por ello, entendemos que si el sistema Cl@ve no se considera disuasorio o excluyente para la presentación de solicitudes por vía telemática en otros procedimientos administrativos, tampoco ha de considerarse como discriminatorio para el ejercicio del derecho de acceso a la información pública por parte del ciudadano.

El reto tecnológico es encontrar un medio de identificación electrónica al alcance de todos los ciudadanos, que a su vez garantice la seguridad jurídica que debe presidir las relaciones por vía electrónica de los ciudadanos con las Administraciones Públicas.

