I. DISPOSICIONES GENERALES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

14215 *Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve.*

El Consejo de Ministros, en su reunión de 19 de septiembre de 2014 y, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia y de los Ministros de Hacienda y Administraciones Públicas, del Interior, de Empleo y Seguridad Social y, de Industria, Energía y Turismo adoptó un Acuerdo por el que se aprueba Cl@ve, un sistema de identificación, autenticación y firma electrónica común para todo el Sector Público Administrativo Estatal que permitirá al ciudadano relacionarse electrónicamente con los servicios públicos a través de una plataforma común, mediante la utilización de claves concertadas previo registro como usuario de la misma, conforme a lo previsto en el artículo 13.2c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El citado Acuerdo publicado por Orden PRE/1838/2014, de 8 de octubre, determina en su apartado quinto, «Prescripciones Técnicas», que corresponde a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, establecer mediante resolución, las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, y determina los aspectos que dichas prescripciones deben incluir.

En virtud de lo anterior, esta Dirección de Tecnologías de la Información y de las Comunicaciones resuelve:

Primero.

1. Aprobar las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, en los términos recogidos en el Acuerdo de Consejo de Ministros de fecha de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, que se incluyen como anexo.
2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

Madrid, 14 de diciembre de 2015.–El Director de Tecnologías de la Información y las Comunicaciones, Domingo Javier Molina Moscoso.

PRESCRIPCIONES TÉCNICAS NECESARIAS PARA EL DESARROLLO Y APLICACIÓN DEL SISTEMA CL@VE

Índice

I. Objeto.
II. Ámbito de aplicación.
III. Propósito del sistema Cl@ve.
IV. Niveles de garantía, sistemas de identificación, y firma de documentos electrónicos.
V. Entidades encargadas del sistema, funciones y garantías aportadas por cada una.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

VI. Adhesión al sistema Cl@ve.
VII. Sistema de identificación e imputación de costes.
Anexo I. Procedimientos de registro, acceso al sistema y firma electrónica de documentos.

I. *Objeto*

Las presentes Prescripciones Técnicas tienen por objeto establecer los aspectos necesarios para el desarrollo y aplicación del sistema Cl@ve, así como para asegurar su funcionamiento e interoperabilidad.

II. *Ámbito de aplicación*

Las presentes Prescripciones Técnicas serán de aplicación a:

a) Los órganos y organismos públicos participantes en la construcción e implantación del sistema Cl@ve y garantes de su funcionamiento.
b) Los órganos y organismos públicos del Sector Público Administrativo Estatal obligados a habilitar el sistema Cl@ve en todos los servicios y trámites electrónicos dirigidos a los ciudadanos.
c) Otras Administraciones Públicas que se adhieran al sistema.
d) Las entidades del sector privado que participen en el futuro como proveedores de sistemas de identificación y firma electrónica integrados con Cl@ve.

III. *Propósito del sistema Cl@ve*

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica común para todo el Sector Público Administrativo Estatal, basado en el uso de claves concertadas, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El sistema Cl@ve está dirigido a ciudadanos españoles y extranjeros que cumplan los requisitos indicados en estas Prescripciones Técnicas y proporciona dos modalidades diferenciadas de identificación y autenticación basadas en el uso de claves concertadas para el acceso de los ciudadanos a los servicios electrónicos que hagan uso de este sistema, complementando los actuales sistemas de acceso mediante DNI-e y certificado electrónico reconocido.

Con este propósito, el sistema Cl@ve ofrecerá una interfaz amigable que permita al usuario seleccionar alguno de los sistemas de identificación y firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio.

Asimismo, el sistema Cl@ve permitirá al ciudadano el acceso al servicio de firma de documentos por medio de certificados electrónicos albergados tanto en modo local (por ejemplo en su PC) o en dispositivos conectados al mismo (por ejemplo, en el DNI-e) como en modo centralizado.

IV. *Niveles de garantía, sistemas de identificación, y firma de documentos electrónicos*

IV.1 Registro de usuarios.

Con objeto de garantizar un nivel adecuado de calidad en la identificación y autenticación que se llevan a cabo mediante el sistema Cl@ve, la utilización de dicho sistema requiere de un registro previo de los usuarios. Mediante dicho registro, se verifica la existencia de una persona física real asociada a la identidad electrónica que utilizará el sistema, se obtienen un conjunto de datos personales asociados a esa identidad, y se obtiene el consentimiento del usuario para que dichos datos personales sean incorporados al fichero de datos personales del sistema y sean tratados para la finalidad con la que se ha desarrollado el mismo.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

Se podrán registrar en Cl@ve ciudadanos españoles con Documento Nacional de Identidad (DNI) y ciudadanos extranjeros con Tarjeta de Identidad de Extranjeros (TIE) o Certificado de Ciudadano de la Unión Europea; en ambos casos los documentos habrán de estar en vigor. La posibilidad de registro podrá ser extendida a ciudadanos españoles residentes en el extranjero sin DNI en vigor, mediante la habilitación de procedimientos de verificación de la identidad equivalentes a los establecidos para los ciudadanos con DNI.

Existirán dos modalidades o niveles de garantía de registro asociados a la forma y a las garantías que ofrezca la comunicación de la información de registro por parte del ciudadano:

a) Nivel Básico, en el que los datos del registro de usuario son facilitados por el ciudadano de forma telemática, pero sin una autenticación previa mediante certificado electrónico reconocido. La identificación se realizará utilizando datos conocidos por el ciudadano y la administración.

b) Nivel Avanzado, en el que los datos del registro de usuario son facilitados por el ciudadano, bien de forma presencial en una oficina ante un empleado público habilitado al efecto, o bien, son comunicados de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.

El nivel de garantía asociado al procedimiento de registro empleado quedará almacenado en el sistema Cl@ve, y podrá ser utilizado para seleccionar los modos de identificación válidos para cada procedimiento, en aplicación del principio de proporcionalidad previsto en el artículo 4 de la Ley 11/2007, de 22 de junio.

IV.2 Modalidades de identificación.

El sistema Cl@ve proporcionará a los usuarios dos modalidades de identificación electrónica basadas en el uso de claves concertadas, cada una de las cuales proporcionará dos niveles distintos de garantía en la autenticación:

c) Cl@ve ocasional o Cl@ve PIN: Modalidad de identificación para el acceso al sistema en el cual la contraseña, limitada a un solo uso, está formada por una clave aportada por el usuario más un código que recibe en su dispositivo móvil y que tiene una validez muy limitada en el tiempo. Está orientado a usuarios que acceden esporádicamente a los servicios.

El sistema de acceso basado en Cl@ve ocasional podrá ser denominado indistintamente Cl@ve PIN cuando sea mostrado a los usuarios del sistema para facilitar su identificación y acceso.

d) Cl@ve permanente: Modalidad de identificación para el acceso al sistema por medio de un identificador (Número de DNI o NIE del usuario) y una contraseña que debe ser custodiada por el ciudadano. La validez de la contraseña es duradera en el tiempo, pero no ilimitada. Adicionalmente, y cuando el tipo de trámite lo requiera, la modalidad de identificación Cl@ve permanente podrá proporcionar un nivel superior de garantía en la autenticación, para lo cual requerirá la utilización de una verificación de seguridad adicional mediante un código de un solo uso (OTP, «Once Time Password») y validez limitada en el tiempo enviado al dispositivo móvil del usuario. Está orientado principalmente para uso por parte de usuarios habituales.

Los requisitos de seguridad de las contraseñas para este sistema se publicarán en el portal Cl@ve (www.clave.gob.es)

El usuario podrá elegir en el momento de iniciar sesión en el Sistema Cl@ve qué modalidad de identificación prefiere utilizar, en función de las limitaciones establecidas por el proveedor de servicios electrónicos integrado con Cl@ve en cuanto a los niveles de garantía exigidos por el procedimiento o trámite al que se desea acceder.

IV.3 Firma de documentos electrónicos.

El sistema Cl@ve permitirá también el acceso a servicios de firma electrónica, en particular, a servicios de firma de documentos electrónicos mediante certificados

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

electrónicos centralizados, todo ello a efecto de su presentación ante las Administraciones Públicas en aquellos trámites en que la firma mediante certificados electrónicos sea requerida o admitida. Se tendrán en cuenta las siguientes consideraciones:

a) Para poder acceder al servicio, el usuario deberá solicitar previa y expresamente la emisión de los certificados electrónicos centralizados correspondientes que posibilitan la firma mediante la plataforma Cl@ve.

b) Los certificados electrónicos centralizados serán emitidos con las mismas garantías de identificación del DNI electrónico del ciudadano

c) Para realizar la solicitud, y para el acceso ulterior al servicio, será necesario en todo caso que el usuario se haya registrado en Nivel Avanzado y haya activado su Cl@ve permanente. Además se requerirá en el momento de la identificación la utilización de una verificación de seguridad adicional mediante un código de un solo uso y validez limitada en el tiempo que se enviará al teléfono móvil del usuario registrado.

A estos efectos, es de aplicación lo dispuesto en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

IV.4 Punto de acceso al sistema Cl@ve.

Para facilitar el acceso a los servicios de identificación y autenticación del sistema Cl@ve, se creará un punto de acceso electrónico desde el que el ciudadano podrá identificarse de acuerdo a los diferentes niveles de garantía previstos en estas Prescripciones Técnicas. Con este propósito, el punto de acceso presentará un menú que permitirá al usuario elegir la modalidad de identificación electrónica deseada de entre las opciones puestas a disposición por el proveedor del servicio electrónico que soporta el tipo de trámite o procedimiento que desee realizar, de acuerdo con los niveles de garantía en el registro y la autenticación exigidos por dicho trámite o procedimiento.

El punto de acceso permitirá acceder a los servicios de identificación y autenticación previstos en el sistema Cl@ve, así como, en el futuro, a otros sistemas de identificación, entre ellos los sistemas de identificación electrónica de ámbito europeo admitidos en virtud de la normativa de la Unión Europea aplicable. Asimismo, el proveedor del servicio a efectos del cumplimiento del artículo 13 de la Ley 11/2007, podrá optar por habilitar sistemas de identificación no basados en claves concertadas complementarios al sistema Cl@ve, o por habilitar el acceso mediante el sistema Cl@ve a los medios de identificación previstos en el artículo 13.2, apartados a) y b) de la Ley 11/2007, opción que deberá incluir en todo caso los sistemas de firma electrónica incorporados al Documento Nacional de Identidad.

Las diversas Sedes Electrónicas de la Administración que requieran utilizar un sistema de identificación y autenticación de los previstos en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberán ofrecer, como mínimo, alguno de los sistemas de identificación mediante claves concertadas que se integren en la nueva plataforma Cl@ve.

Con este propósito, dichas Sedes Electrónicas deberán integrarse con el sistema Cl@ve actuando como proveedoras de servicios, redirigiendo automáticamente al ciudadano desde la sede electrónica al Punto de Acceso del sistema Cl@ve cuando el ciudadano desee realizar un trámite o procedimiento que precise algún sistema de identificación y autenticación de los previstos en el sistema Cl@ve. En esa redirección, las entidades deberán especificar el nivel de garantía en la autenticación que requiere el procedimiento o trámite al que desea acceder el ciudadano, pudiendo opcionalmente especificar también el nivel exigido de calidad en el registro. Una vez realizada la verificación de la identidad por parte de la entidad responsable de la modalidad de identificación seleccionada, el usuario será redirigido automáticamente al punto de origen, junto con el resultado de la autenticación, los datos que permiten identificar de manera no ambigua al ciudadano, y los niveles de garantías asociados a esa identidad.

Cuando el ciudadano se haya identificado y autenticado previamente en un servicio electrónico integrado con Cl@ve a través del Punto de Acceso, desde este Punto de

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

Acceso se le dará la posibilidad de acceder a otro servicio electrónico sin necesidad de identificarse de nuevo, siempre que el proveedor de este segundo servicio lo permita. Esto supondrá que el ciudadano no tendrá que introducir los datos de identificación asociados a su Cl@ve PIN o Cl@ve Permanente.

Para asegurar esta integración con el Punto de Acceso del sistema Cl@ve, las entidades usuarias del sistema deberán seguir las especificaciones técnicas de integración definidas por las entidades responsables del mismo. Con el objeto de facilitar dicha integración, se habilitará un conjunto de componentes comunes, orientados a simplificar el manejo de los mensajes de petición y respuesta intercambiados durante el proceso de identificación y autenticación, que las entidades usuarias podrán incorporar a sus servicios electrónicos. Dichas especificaciones y componentes comunes se publicarán en el Centro de Transferencia de Tecnología.

La transmisión de información entre el Punto de Acceso del sistema Cl@ve y las sedes electrónicas integradas se protegerá de acuerdo con las mejores prácticas técnicas con objeto de asegurar la privacidad, confidencialidad e integridad de dicha información. En este sentido, el Punto de Acceso del sistema Cl@ve no almacenará ningún dato de carácter personal, sino únicamente información técnica no vinculada a personas físicas o jurídicas, con el objeto de garantizar, en el caso de que se produzca un incidente, la reconstrucción, con la participación del proveedor del servicio electrónico al que accede el usuario y del proveedor del servicio de identificación de la modalidad de identificación escogida por este, de la secuencia de mensajes intercambiados entre los distintos actores del sistema para determinar el momento en que se produjo ese incidente y su naturaleza.

En el caso particular de los servicios electrónicos ofrecidos por los propios proveedores de servicios de verificación de la identidad de Cl@ve (AEAT y Seguridad Social, inicialmente), esta redirección al Punto de Acceso del sistema Cl@ve podrá ser sustituida por un acceso directo y equivalente a los servicios de verificación de la identidad de Cl@ ve ofrecidos por dicho proveedor, siempre que el servicio electrónico no exija otro tipo de identificación diferente.

Adicionalmente, para facilitar el acceso a los servicios de firma electrónica con certificados electrónicos centralizados y presentar a los ciudadanos un mecanismo de firma uniforme en todo el sistema, se habilitará un conjunto de componentes de firma comunes que deberán ser integrados en las sedes electrónicas que requieran la realización de firma electrónica en sus trámites o procedimientos.

El Anexo I detalla los procedimientos de registro en el sistema Cl@ve, acceso al sistema Cl@ve y firma electrónica de documentos con certificados electrónicos centralizados asociados a los niveles de garantía del sistema Cl@ve previstos en estas Prescripciones Técnicas.

IV.5 Seguridad.

El sistema Cl@ve y todos los servicios asociados se implementarán garantizando su funcionamiento conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007, de 22 de junio, en el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero y conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

V. *Entidades encargadas del sistema, funciones y garantías aportadas por cada una*

V.1 Registro de usuarios.

La Agencia Estatal de Administración Tributaria (AEAT) actuará como organismo principal responsable del sistema de Registro de usuarios de Cl@ve.

A tales efectos, este organismo será responsable del funcionamiento de los sistemas de registro de usuarios descritos en estas Prescripciones Técnicas, así como de los

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del registro de usuarios.

Inicialmente, con el fin de ofrecer un mejor servicio a los ciudadanos, estarán habilitadas y dispondrán de los medios necesarios para realizar funciones de registro de usuarios del sistema Cl@ve, además de la red de oficinas de la AEAT, las entidades gestoras de la Seguridad Social.

La Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) podrá acordar la adhesión al sistema de otros órganos y organismos del Sector Público Administrativo Estatal para actuar como oficina de registro de usuarios Cl@ve a fin de ofrecer a los ciudadanos nuevos puntos presenciales de registro, así como de órganos y organismos públicos pertenecientes a otras Administraciones.

En virtud de lo anterior, se ha habilitado para actuar como oficinas de registro presencial del sistema Cl@ve a la Red de oficinas de Información y Atención al Ciudadano de las Delegaciones y Subdelegaciones de Gobierno.

Los órganos y organismos distintos de la AEAT que actúen como oficinas de registro tendrán que cumplir los requisitos establecidos en la Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

La DTIC mantendrá la relación de oficinas de registro de Cl@ve en el Punto de Acceso General http://administracion.gob.es.

V.2 Modalidad de identificación Cl@ve ocasional (Cl@ve PIN).

La AEAT actuará como organismo principal responsable del sistema de acceso basado en Cl@ve ocasional.

A tales efectos, la AEAT será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello.

En consecuencia, la AEAT será responsable del funcionamiento del sistema de acceso basado en Cl@ve ocasional descrito en estas Prescripciones Técnicas así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve ocasional.

V.3 Modalidad de identificación Cl@ve permanente

La Gerencia de Informática de la Seguridad Social (GISS) actuará como organismo responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente.

A tales efectos, la GISS será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello, entre los que se cuenta una copia replicada del fichero de usuarios del sistema Cl@ve, necesario para verificar la identidad y las garantías de acceso.

En consecuencia, la GISS será responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve permanente.

V.4 Emisión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de emisión y custodia de certificados electrónicos centralizados de usuarios para firma mediante la plataforma Cl@ve será, en el ejercicio de sus competencias, la Dirección General de la Policía (DGP), de acuerdo a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y al Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

Para realizar estas funciones, la DGP utilizará la Infraestructura de Clave Pública correspondiente al DNI electrónico actualmente existente.

La DGP, en el ejercicio de sus competencias, es responsable del funcionamiento del servicio de emisión y custodia de certificados electrónicos centralizados de usuarios, actuando como prestador de servicios de confianza de acuerdo con el Reglamento (UE) No 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 y por la que se deroga la Directiva 1999/93/CE, y conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 59/2003 de 19 de diciembre de Firma electrónica, y en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

V.5 Gestión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de almacenamiento y gestión de certificados electrónicos centralizados de usuarios para el sistema Cl@ve será la DGP.

Este organismo estará habilitado y dispondrá de los medios necesarios para realizar las funciones de almacenamiento y gestión de certificados descrita. Igualmente dispondrá de una copia replicada del fichero de certificados electrónicos indicado.

La GISS actuará como prestador de servicios de firma con certificado electrónico centralizado, para lo cual dispondrá de un respaldo de aquella información almacenada y gestionada por la DGP necesaria para la firma. Dicha información estará sujeta a los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

La DGP es responsable del funcionamiento del servicio de almacenamiento y gestión de certificados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.6 Firma de documentos electrónicos mediante certificados electrónicos centralizados.

La entidad encargada de gestionar el entorno de creación de firma electrónica, en nombre del firmante, de documentos electrónicos mediante certificados electrónicos centralizados será la GISS que actuará como organismo responsable de este servicio, en unión con la DGP. A tales efectos, ambas entidades serán las habilitadas y dispondrán de los medios necesarios para realizar dichas funciones de firma de documentos electrónicos.

En consecuencia, ambos organismos serán los responsables del funcionamiento del servicio de firma de documentos electrónicos mediante certificados electrónicos centralizados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.7 Punto de acceso al sistema Cl@ve.

La entidad encargada de realizar las funciones correspondientes a la provisión del punto de acceso al sistema Cl@ve, de desarrollar los componentes comunes para facilitar la integración con este punto de acceso, y de desarrollar los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados será la DTIC.

La DTIC será responsable del funcionamiento del punto de acceso al sistema Cl@ve, de los componentes comunes para facilitar la integración con este punto de acceso y de los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados descritos en estas Prescripciones Técnicas, así

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del punto de acceso y los componentes comunes de integración.

V.8 Garantía de alta disponibilidad.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve establecerán un sistema de alta disponibilidad del servicio ofrecido.

V.9 Garantía de fiabilidad del entorno de creación de firma electrónica.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve aplicarán procedimientos de seguridad específicos en materia de gestión y administración, y utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante.

VI. *Adhesión al sistema Cl@ve*

El ámbito de aplicación del sistema Cl@ve podrá extenderse a otras Administraciones Públicas, mediante la formalización de un convenio al efecto con el Ministerio de Hacienda y Administraciones Públicas. En dicho convenio se establecerán las condiciones técnicas, económicas y organizativas de aplicación a otras Administraciones Públicas que complementarán, en su caso, a las establecidas en las presentes Prescripciones Técnicas.

VII. *Sistema de identificación e imputación de costes*

Con objeto de garantizar la sostenibilidad del sistema Cl@ve, se implementarán mecanismos para identificar y eventualmente imputar los costes de mantenimiento y explotación del sistema a las diferentes entidades usuarias, basados en el uso efectivo del mismo por parte de dichas entidades.

Para ello, desde la DTIC se llevará un censo de las entidades integradas con el Punto de Acceso del sistema Cl@ve, de modo que únicamente las entidades incluidas en el censo puedan hacer uso del mismo. Cada petición de identificación y autenticación recibida por el Punto de Acceso se asociará a una entidad usuaria a través del identificador de entidad emisora que deberá incluirse en dichas peticiones, dejando una traza en el registro de actividad del sistema. Dichas trazas, que contendrán para cada petición la entidad emisora, el resultado y la modalidad de identificación utilizada, serán objeto de tratamiento para determinar el uso efectivo del sistema realizado por cada entidad y por consiguiente para realizar la imputación de costes.

Asimismo, para las funciones de firma de documentos electrónicos mediante certificados electrónicos centralizados, las entidades participantes en la provisión del servicio, GISS y DGP, implementarán un sistema de identificación e imputación de costes equivalente al anterior, basado en un censo de entidades integradas con el sistema de firma y un registro de actividad en el que se almacenarán las trazas de las peticiones de firma mediante certificados electrónicos centralizados recibidas.

ANEXO I

Procedimientos de registro, acceso al sistema y firma electrónica de documentos

Se describen a continuación los procedimientos inicialmente previstos en relación al registro de usuarios, así como de acceso al sistema y firma de documentos electrónicos. Estos procedimientos podrán ser adaptados de acuerdo a las necesidades y a la evolución del sistema Cl@ve para una mejor prestación del servicio a los ciudadanos.

La información actualizada de los procedimientos podrá encontrarse en www.clave.gob.es.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

1. Procedimientos de alta en el registro.

Existirán tres procedimientos de registro diferenciados en el sistema Cl@ve: registro telemático sin certificado electrónico reconocido, registro telemático con DNI electrónico o certificado electrónico reconocido, y registro presencial.

1.1 Registro telemático sin certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Básico.

Este procedimiento de registro se inicia mediante la solicitud por parte del ciudadano ante la entidad responsable del Registro, o a instancias de esta última sin solicitud previa, utilizando para esta identificación inicial del ciudadano un dato conocido por el ciudadano y la entidad. Una vez verificada la identidad, se remitirá a la dirección postal del ciudadano que conste en la entidad responsable del registro una carta de invitación al sistema Cl@ ve, en la que se incluirá un código seguro de verificación (CSV).

Una vez recibida la carta, el ciudadano puede acceder a la aplicación de registro en Cl@ve, donde se le solicitan los datos personales necesarios para completar el registro, así como el código CSV de la comunicación emitida. Como medida de seguridad adicional en el momento del registro, también se solicitará un dato de verificación conocido por el ciudadano y la entidad.

Como respuesta, se emite un acuse de recibo firmado electrónicamente por el sistema con un CSV que incluye los datos proporcionados, y que incluirá el código de activación asociado al registro realizado.

1.2 Registro telemático con DNI electrónico o certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

Los ciudadanos con certificado electrónico reconocido o DNIe, podrán formalizar el registro en el sistema Cl@ve mediante una aplicación web sin necesidad de acudir a ninguna oficina.

El ciudadano accederá al punto de registro telemático de Cl@ve y se identificará con su certificado reconocido o DNIe. La aplicación de registro tomará del certificado los datos identificativos del ciudadano, y los verificará contra los que figuren en su DNI. Puesto que se tomarán como ciertos para su incorporación al registro los datos correspondientes al DNI, si los datos del DNI y del certificado no coinciden exactamente, se informará de esta discrepancia al ciudadano para que efectúe las correcciones pertinentes en la información proporcionada.

A continuación se le pedirán los otros datos necesarios para el registro, incluidos su número de teléfono móvil y su dirección de correo electrónico y firmará con su certificado esta solicitud, incluyendo la selección de la casilla donde declara haber leído y estar de acuerdo con los términos y condiciones de uso.

Se le dará un acuse de recibo firmado por el sistema con los datos proporcionados, documento que incluirá el código de activación asociado al registro realizado. El sistema informará al usuario de la utilidad del código de activación y se recalcará la importancia de su conservación para poderlo usar como factor de autenticación en caso de olvido de contraseña.

1.3 Registro presencial.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

El ciudadano podrá registrarse en persona en cualquiera de las oficinas de registro autorizadas del sistema Cl@ve. Estas oficinas contarán con una aplicación de registro que les permitirá, una vez identificado el ciudadano ante un empleado público, formalizar el registro. Para asegurar el estricto control por parte del usuario de los medios de

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

identificación utilizados en el sistema, no se permitirá que el registro presencial sea realizado por una persona en representación de otra.

El proceso de registro presencial se realizará de acuerdo con lo establecido en la Resolución de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

1.4 Bienvenida al sistema Cl@ve.

Una vez completado el registro en Cl@ve en cualquiera de las modalidades descritas anteriormente, el ciudadano recibirá, en el número de teléfono que acaba de registrar, un SMS de bienvenida al sistema.

A partir de la recepción de dicho SMS, el ciudadano registrado puede ya utilizar el sistema Cl@ve PIN y acceder a los sistemas de activación de contraseña del sistema Cl@ ve permanente.

1.5 Obtención de nivel avanzado de garantía de registro.

Determinados servicios de Administración Electrónica requieren que el registro en Cl@ ve se haya realizado con un nivel de garantía de registro avanzado, esto es, de forma presencial o telemáticamente con DNI electrónico o certificado electrónico reconocido.

Los ciudadanos que se hayan registrado en Cl@ve de forma telemática con una carta de invitación con un código seguro de verificación (CSV), y que por tanto dispongan únicamente de un nivel de garantía de registro básico, podrán solicitar la obtención del nivel avanzado personándose en las oficinas de registro o accediendo mediante DNIe o certificado electrónico reconocido a los sistemas de registro de Cl@ve.

1.6 Tratamiento del procedimiento de alta de un número de teléfono ya registrado.

El tratamiento descrito a continuación es común a los tres procedimientos de alta descritos anteriormente.

Por motivos de seguridad, el sistema requiere que un número de teléfono esté asignado a un único ciudadano usuario del sistema Cl@ve. En el caso de que un ciudadano intente registrarse con un teléfono que ya está dado de alta en el sistema asignado a otro usuario registrado, se seguirá este procedimiento para completar el registro:

1. Se explicará al ciudadano la situación detectada y se enviará un SMS con un código de un solo uso al número de teléfono móvil que se pretende registrar para que el usuario, o en su caso el empleado público que atiende el registro presencial, lo aporte en ese mismo momento para demostrar que el ciudadano es el poseedor del teléfono.
2. El sistema comprobará la validez del código de un solo uso aportado y en el caso de ser correcto se completará el registro y se procederá a revocar el número de teléfono al usuario que lo tenía anteriormente asignado. En caso contrario no se podrá completar el proceso de registro.
3. El usuario cuyo número de teléfono haya sido revocado en aplicación de este procedimiento no causará baja en el sistema Cl@ve, pero no podrá hacer un uso efectivo del mismo. Si el usuario intenta acceder al sistema se le informará que su usuario ha sido revocado por razones de seguridad con el fin de garantizar una asociación única con el número de teléfono móvil, y se le invitará a subsanar esta incidencia aportando un nuevo número de teléfono mediante el procedimiento establecido al efecto.
4. A los exclusivos efectos de informar al usuario que ha sido revocado su número de teléfono en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia y que pueda proceder a subsanarla, en su caso.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

2. Procedimientos de baja en el registro.

Se habilitarán tres procedimientos de baja en el sistema Cl@ve:

2.1 Procedimiento de baja por renuncia.

El ciudadano puede renunciar a la utilización del sistema Cl@ve en cualquier momento, incluso aunque no se haya dado de alta en el mismo.

La renuncia podrá llevarse a cabo en el portal www.clave.gob.es, identificándose ante él y eligiendo en las opciones de usuario la de renuncia al sistema. En este caso el sistema deberá mostrar primero una pantalla de aviso para informar al usuario de que ya no podrá acceder al sistema y que si posteriormente quiere darse da alta deberá proceder de nuevo al procedimiento de registro como usuario. Si el ciudadano confirma esta pantalla, el sistema marcará al usuario como dado de baja por renuncia. Indistintamente podrá realizar esta petición usando DNIe o certificado electrónico reconocido o de manera presencial en una oficina. Si el registro se ha realizado a nivel básico, mediante carta de invitación, la renuncia también se podrá tramitar mediante el código CSV incluido en la misma.

Si un ciudadano renuncia al sistema, se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica Cl@ve.

2.2 Procedimiento de revocación de oficio.

El sistema Cl@ve podrá gestionar la revocación de oficio de usuarios registrados en el sistema cuando concurran circunstancias que pongan en riesgo la seguridad del mismo, como un uso fraudulento o desleal del sistema o cuando se produzca una modificación sustancial de los datos de identificación utilizados en el registro, como son el cambio del nombre o los apellidos en su DNI o la nacionalización o expulsión de extranjeros.

A los exclusivos efectos de informar al usuario que ha sido revocado en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia.

La revocación solo podrá dar lugar a una nueva alta cuando se hayan modificado las circunstancias que motivaron la misma.

Los efectos de la revocación serán los mismos que los de la renuncia, de forma que se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

2.3 Procedimiento de baja por fallecimiento.

El sistema Cl@ve gestionará automáticamente y de oficio la baja de los usuarios fallecidos de los que se tenga constancia y se encuentren registrados. Los efectos de la baja por fallecimiento serán los mismos que los de la renuncia: se revocará el certificado electrónico centralizado del usuario, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

3. Procedimientos de modificación de datos en el registro.

Se habilitarán los siguientes procedimientos de modificación de datos del registro:

3.1 Procedimiento de modificación del número de móvil.

Si el ciudadano desea modificar el número de móvil que notificó durante el acto del registro, deberá acudir de nuevo a una oficina de registro donde le actualizarán, previa identificación con su DNI, TIE o Certificado de Ciudadano de la Unión Europea, el número de teléfono móvil en la base de datos y le proporcionarán un nuevo código de registro para futuras operaciones, teniendo que firmar de nuevo el correspondiente documento de

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

aceptación. También podrá hacer la operación de forma telemática, si el usuario dispone de un certificado electrónico reconocido o DNIe.

En el caso de que el nuevo número de teléfono móvil ya esté dado de alta en el sistema, se aplicará el procedimiento de alta de un número de móvil ya registrado descrito anteriormente.

El procedimiento de modificación del número de móvil no implica la revocación del certificado electrónico centralizado del ciudadano ni la desactivación de su usuario y contraseña de acceso.

3.2 Procedimiento de modificación de otros datos.

El usuario registrado en el sistema puede modificar otros datos asociados al registro, a excepción del número de DNI y del nombre y los apellidos.

Estas modificaciones se podrán realizar telemáticamente en el portal www.clave.gob.es o en una de las oficinas de registro.

El procedimiento de modificación de estos datos no generará un nuevo código de activación aunque sí el documento de aceptación de condiciones, donde se incluirán los nuevos datos declarados por el ciudadano.

4. Procedimiento de uso de Cl@ve PIN.

En la Modalidad de Identificación Cl@ve ocasional, el usuario aportará la primera parte de su clave y recibirá un código en su dispositivo móvil, de validez muy limitada en el tiempo, que conjuntamente conforman el código de acceso.

Para reforzar la seguridad del sistema de identificación y autenticación se divide el código de acceso (Cl@ve PIN) en dos partes:

- Clave de acceso: la define el usuario cada vez que solicita un Cl@ve PIN. No tiene que ser siempre la misma.
- PIN: la envía el sistema Cl@ve al móvil del usuario cuando lo solicita.

De manera que la unión de ambos datos conforma el Código de Acceso.

Código de Acceso (Cl@ve PIN) = Clave de Acceso + PIN.

Este sistema permite al ciudadano tener el control sobre una parte del código de acceso de forma que es el usuario quien lo define cada vez que solicita un PIN. Como medida de seguridad adicional, este código nunca se envía en claro al sistema Cl@ve. De esta manera, se logra que, aunque otra persona pudiera tener acceso a estos mensajes, no podría suplantar al usuario pues le faltaría conocer la parte del código que define el propio usuario.

Se definen los siguientes procedimientos relativos a la obtención y utilización del sistema Cl@ve PIN:

4.1 Procedimiento de obtención de Cl@ve PIN.

Para la obtención de un PIN en el sistema Cl@ve, el solicitante deberá acceder al portal de gestión de la Cl@ve ocasional, donde deberá introducir su usuario Cl@ve (número del DNI o NIE), información de contraste conocida por ambas partes, elegir una clave de acceso, que no es necesario que sea siempre la misma, y solicitar un nuevo PIN. Como resultado, el sistema Cl@ve enviará un código al teléfono móvil registrado con el que el usuario podrá completar la autenticación.

4.2 Procedimiento de utilización de Cl@ve PIN.

Para completar la autenticación en el sistema el usuario deberá introducir su usuario Cl@ve (DNI o NIE) y su código de acceso formado por la clave seleccionada en el momento de la obtención y el PIN recibido en su teléfono móvil.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

Si el solicitante introduce erróneamente el código de acceso más veces de las permitidas, por motivos de seguridad, se bloqueará el acceso de forma temporal.

La validez del PIN es la siguiente:

• Validez temporal: Se deberá utilizar el PIN que se ha recibido en el teléfono móvil para completar el acceso al sistema antes de 10 minutos. Pasado ese tiempo, si no se ha llegado a acceder a Cl@ve, se deberá solicitar un nuevo PIN.

• Número de usos: El PIN se configura como una clave de un solo uso (OTP), de forma que se garantice que siempre que se solicite una autenticación con Cl@ve PIN se fuerce al usuario a iniciar el proceso de solicitud de un nuevo PIN para poder autenticarse en esa sesión.

• Sesión: Una vez identificado mediante Cl@ve PIN se puede acceder a los servicios que permitan Cl@ve hasta que se produzca la desconexión de la Sede Electrónica o se cierre el navegador.

5. Procedimientos de activación y gestión de contraseñas.

Se definen los siguientes procedimientos relativos a la activación de cuentas de usuario en el sistema Cl@ve y gestión de las contraseñas:

5.1 Procedimiento de activación.

Para la activación de la cuenta de usuario en el sistema Cl@ve, necesaria para poder utilizar la modalidad de identificación de Cl@ve permanente, el solicitante deberá acceder al portal www.clave.gob.es, donde deberá introducir su identificador de usuario Cl@ve (DNI o NIE), su dirección de correo electrónico y el código de activación que se le ha suministrado en el acto del registro. Si son correctos, el sistema le enviará un mensaje al móvil con un código de un solo uso que el usuario deberá introducir en el sistema y, una vez comprobado, le permitirá introducir la contraseña que prefiera para acceder ulteriormente a Cl@ve, cumpliendo con las características mínimas de seguridad definidas.

Si el solicitante introduce erróneamente el código de activación más veces de las permitidas, el código de activación quedará bloqueado por motivos de seguridad y se precisará la generación de uno nuevo.

5.2 Procedimiento de cambio de contraseña.

Las contraseñas de los usuarios caducarán en el plazo determinado por la política de seguridad del sistema, plazo que se comunicará en el portal www.clave.gob.es. En cualquier caso, el usuario podrá cambiar la contraseña de acceso en cualquier momento. Para ello accederá al sistema con su usuario y contraseña y dentro de las opciones de usuario elegirá cambiar contraseña. Introducirá la nueva contraseña y el sistema le enviará un código de un solo uso al móvil para confirmar la operación.

Esta operación podrá realizarse también accediendo con DNIe o certificado reconocido, en cuyo caso no hará falta el código de un solo uso.

5.3 Procedimiento de restablecimiento de contraseña.

Este procedimiento será necesario si el ciudadano olvida su contraseña o ésta queda bloqueada al producirse el número máximo de intentos fallidos en la introducción de la misma. En tal caso habrá de establecerse una contraseña nueva.

Para restablecer la contraseña, el ciudadano accederá al sistema con su usuario y seleccionará la opción de «restablecimiento de contraseña». El sistema le pedirá el código de activación que se le entregó en el proceso de registro y que deberá coincidir con el que consta en la base de datos. Si es correcto, el sistema enviará un código de seguridad al móvil del ciudadano, código que deberá introducir para restablecer la contraseña.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

5.4 Procedimiento de recuperación del código de activación.

Si el usuario desea restablecer la contraseña y no dispone del código de activación, podrá obtener un nuevo código de activación acudiendo a una oficina de registro o telemáticamente autenticándose mediante certificado electrónico reconocido o DNIe o mediante Cl@ve PIN. Esta operación no precisa la emisión del documento de aceptación puesto que el ciudadano no está declarando ningún dato nuevo.

6. Procedimientos de gestión de certificados y firma electrónica.

Los siguientes procedimientos son de aplicación en relación a los certificados electrónicos centralizados para firma.

6.1 Procedimiento de emisión de los certificados centralizados para firma con la plataforma Cl@ve.

Una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados electrónicos centralizados para firma mediante la plataforma Cl@ve, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma con el sistema Cl@ve.

El sistema informará al ciudadano de que se le va a emitir su certificado, así como de las garantías de seguridad ofrecidas por la Administración para la custodia y acceso al mismo, y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice, con un alto nivel de confianza, su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

6.2 Procedimiento de firma con certificado electrónico centralizado.

El procedimiento de firma electrónica con certificado electrónico centralizado garantizará que el acceso a los datos de creación de firma asociados al certificado sólo sea efectuado por el titular del mismo, por lo que para su uso se deberá haber autenticado previamente al ciudadano mediante dos factores de autenticación: la pareja identificador de Cl@ve con su contraseña de Cl@ve permanente, y un código de un solo uso (OTP) enviado por SMS a su móvil.

6.3 Procedimiento de renovación de los certificados electrónicos centralizados.

La renovación de los certificados centralizados para firma mediante la plataforma Cl@ve se podrá llevar a cabo de forma automática siempre y cuando se cumplan los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial. En caso contrario, para renovar su certificado el ciudadano tendrá que personarse en una oficina de registro para que se le provea de un nuevo código de activación y pueda volver a activarse su usuario y sus certificados.

La renovación automática se producirá cuando el ciudadano se disponga a firmar, se haya autenticado para poder acceder a su clave de firma y se detecte en ese momento que su certificado está caducado o próximo a caducar, hasta 2 meses antes de la fecha de expiración de su validez. En ese caso el sistema Cl@ve emitirá y almacenará automáticamente los nuevos certificados revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos reconocidos.

En todo caso el sistema informará al ciudadano de que se ha procedido a la renovación automática de sus certificados y le comunicará el nuevo periodo de validez de los mismos, informando también de que los anteriores certificados han sido revocados, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es

6.4 Procedimiento de revocación.

La revocación de los certificados electrónicos centralizados del ciudadano se llevará a efecto en caso de renuncia o baja voluntaria del ciudadano en el sistema, en el caso de baja por fallecimiento y en el caso de revocación de oficio del acceso al sistema llevada a cabo por la Administración en las circunstancias que se determinen.

Una vez revocado un certificado, el sistema garantizará que no se podrá utilizar a partir de ese momento durante un proceso de firma.

El sistema podrá permitir también, con las garantías que se consideren necesarias, que el propio ciudadano pueda solicitar tanto presencial como telemáticamente la revocación exclusiva de su certificado electrónico de firma centralizado, sin necesidad de darse de baja en el sistema Cl@ve. La revocación deberá constatarse documentalmente, por lo que en cualquiera de estos procedimientos el ciudadano deberá firmar la solicitud de renuncia o revocación, ya sea con un certificado electrónico reconocido o de forma manuscrita.

7. Procedimientos de incorporación de registros de otros censos.

Tal y como establece el Acuerdo del Consejo de Ministros de creación de Cl@ve, para incorporar al Censo Cl@ve usuarios registrados en otros sistemas de identificación, autenticación y firma que existan con anterioridad al propio acuerdo, se deberá solicitar el consentimiento expreso del ciudadano.

En cualquier caso, los procedimientos de incorporación asegurarán que en estos censos se han cumplido los requisitos necesarios para poder asignar el nivel de garantía de registro y el sistema de identificación y autenticación correspondientes en el sistema Cl@ve. Asimismo, el procedimiento deberá permitir comprobar la veracidad y exactitud de los datos aportados desde los otros censos y se solicitará al usuario la aportación de los datos complementarios necesarios para completar el registro, todo ello manteniendo las mismas garantías que aplican al procedimiento de alta de usuarios en el sistema Cl@ve.

Se integrarán en una primera fase los censos del sistema PIN24H de la AEAT y del sistema usuario-contraseña de la Seguridad Social. En cualquier caso, la incorporación de registros de otros censos requerirá la autorización de la DTIC.

cve: BOE-A-2015-14215
Verificable en http://www.boe.es