III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

13523 *Resolución de 6 de noviembre de 2017, de la Secretaría de Estado de Función Pública, por la que se publica la Adenda de prórroga al Convenio de colaboración con la Comunidad de Madrid, para la prestación mutua de soluciones básicas de administración electrónica.*

La Secretaria de Estado de Función Pública y la Viceconsejera de Presidencia y Justicia han suscrito, con fecha 31 de octubre de 2017, un Convenio para la prestación mutua de soluciones básicas de administración electrónica.

Para general conocimiento y en cumplimiento de lo establecido en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se dispone la publicación del referido Convenio, como anejo a la presente Resolución.

Madrid, 6 de noviembre de 2017.–La Secretaria de Estado de Función Pública, Elena Collado Martínez.

ADENDA DE PRÓRROGA AL CONVENIO DE COLABORACIÓN ENTRE LA ADMINISTRACIÓN GENERAL DEL ESTADO (MINHAP) Y LA COMUNIDAD DE MADRID PARA LA PRESTACIÓN MUTUA DE SOLUCIONES BÁSICAS DE ADMINISTRACIÓN ELECTRÓNICA

En Madrid, a 31 de octubre de 2017.

REUNIDOS

De una parte, doña Elena Collado Martínez, Secretaria de Estado de Función Pública, nombrada para este cargo por el Real Decreto 437/2016, de 11 de noviembre, actuando en nombre y en representación de la Secretaría de Estado de Función Pública del Ministerio de Hacienda y Función Pública, en ejercicio de las funciones atribuidas por Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

De otra parte, doña Isabel Díaz Ayuso, en calidad de Viceconsejera de Presidencia y Justicia, de la Consejería de Presidencia, Justicia y Portavocía del Gobierno de la Comunidad de Madrid, nombrada por Decreto 85/2017, de 26 de septiembre, del Consejo de Gobierno («BOCM» número 230 del 27), y en virtud de la delegación de firma del Consejero de Presidencia, Justicia y Portavoz del Gobierno, atribuida en el artículo noveno de la Orden 3141/2017, de 16 de octubre («BOCM» número 250, de 16 de octubre). Y en virtud del artículo 42 b) de la Ley 1/1983, de 13 de diciembre, de Gobierno y Administración de la Comunidad.

Las partes intervienen en virtud de sus respectivos cargos, y en el ejercicio de las facultades y atribuciones que por ellos tienen concedidas, reconociéndose mutuamente capacidad y legitimación para suscribir la presente prórroga, y a tal efecto

EXPONEN

Primero.

Que con fecha 3 de noviembre de 2014, se firmó el Convenio de colaboración entre la Administración General del Estado (MINHAP) y la Comunidad de Madrid para la prestación mutua de soluciones básicas de Administración electrónica.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

Segundo.

Que, de conformidad con lo dispuesto en la disposición final segunda del Real Decreto 415/2016, de 3 de noviembre, por el que se reestructuran los departamentos ministeriales, el Ministerio de Hacienda y Función Pública asume las competencias del suprimido Ministerio de Hacienda y Administraciones Públicas.

La Secretaría de Estado de Función Pública, de acuerdo con lo dispuesto en el citado Real Decreto, asume las funciones de la suprimida Secretaría de Estado de Administración Pública.

Tercero.

Conforme lo establecido en la cláusula décima del convenio, éste tiene una duración de tres años pudiéndose prorrogarse por igual periodo de tiempo, mediante acuerdo expreso de las partes firmantes, que deberá ser formalizado antes de que finalice su plazo de vigencia.

Cuarto.

Que las obligaciones asumidas entre las partes firmantes de dicho Convenio de colaboración, se entienden vigentes desde la fecha de su firma hasta la fecha la extinción del mismo.

En consecuencia, con el fin de dar continuidad a la prestación del objeto de dicho Convenio, las partes firmantes de esta primera Adenda, estiman necesario continuar con dicha colaboración por un nuevo período de tres años, de conformidad a las siguientes

CLÁUSULAS

Primera. *Objeto de la prórroga.*

Las partes firmantes acuerdan la prórroga, por tres años, del Convenio de colaboración entre la Administración General del Estado (MINHAP) y la Comunidad de Madrid para la prestación mutua de soluciones básicas de Administración electrónica.

Por lo tanto, los efectos de la presente Adenda a este Convenio de colaboración, se extenderán desde el día 4 de noviembre de 2017 hasta el 3 de noviembre de 2020.

Asimismo, en el mismo acto se procede a la actualización del anexo técnico del convenio que contiene el detalle de las aplicaciones y sistemas que dan soporte al objeto del convenio que se anexa al presente acuerdo.

Segunda. *Obligaciones de las partes.*

Las partes intervinientes, se comprometen a continuar desarrollando las actuaciones precisas, dirigidas a dar continuidad al objeto de la colaboración.

Las obligaciones asumidas entre las partes firmantes, se entenderán vigentes hasta la extinción del Convenio de prórroga por el transcurso de los plazos.

Tercera. *Financiación de la adenda.*

De acuerdo con la cláusula novena del convenio, esta adenda no comporta obligaciones económicas entre las partes firmantes.

Cuarta. *Régimen jurídico.*

Salvo lo dispuesto en la disposición adicional octava de la Ley 40/2015, de 1 de octubre, que fuera de aplicación, esta adenda se rige por lo dispuesto en la normativa de aplicación en el momento de la firma del Convenio.

En prueba de conformidad, y para que conste a los efectos oportunos, las partes firman esta adenda de prórroga.–La Secretaria de Estado de Función Pública, Elena Collado Martínez.–La Viceconsejera de Presidencia y Justicia, Isabel Díaz Ayuso.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

ANEXO

Especificaciones técnicas de las soluciones básicas de Administración Electrónica

Apartados:

I) Red de comunicaciones de las Administraciones Públicas españolas: Servicio de conexión a la Red SARA.
II) utilización de sistemas de firma electrónica avanzada: sistemas de identificación, firma y representación.
III) Comunicaciones entre Administraciones Públicas por medios electrónicos:

III.a) Intermediación de datos entre Administraciones Públicas.
III.b) Sistema de Interconexión de Registros.

IV) Práctica de la notificación por medios electrónicos: Dirección electrónica habilitada y catálogo de procedimientos del Servicio de Notificaciones Electrónicas.

Apartado I) Red de comunicaciones de las Administraciones Públicas españolas: Servicio de conexión a la Red SARA

I.1 Descripción general.

I.1.1 Descripción de la Red SARA.

La Red SARA (Sistemas de Aplicaciones y Redes para las Administraciones) es un conjunto de infraestructuras de comunicaciones y servicios básicos que conecta las redes de las Administraciones Públicas Españolas e Instituciones Europeas facilitando el intercambio de información y el acceso a los servicios.

Su implantación responde a lo establecido en el artículo 155.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y a lo dispuesto en el artículo 13 del Real Decreto 4/2010 que regula el ENI y en la Resolución de 19 de julio de 2011 que aprueba la NTI de requisitos de conexión a la red de comunicaciones de las administraciones públicas españolas, estableciendo las condiciones en las que cualquier órgano de una administración o entidad de derecho público vinculada o dependiente de aquella, accederá a la Red SARA. El Acuerdo de Consejo de Ministros de 29 de abril de 2011 aprobó el «Plan de fomento para la incorporación del protocolo IPv6 en España». La Red SARA es esencial para este objetivo y ya ha incorporado este protocolo.

I.2 Requisitos técnicos.

La conexión a la Red SARA deberá garantizar el cumplimiento de los requisitos técnicos siguientes:

Los incluidos en la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones públicas españolas.

La Comunidad Autónoma de Madrid asume cualquier responsabilidad derivada de su uso de la Red SARA y de sus servicios, especialmente en materia de seguridad y en lo relativo a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

La Comunidad Autónoma de Madrid, informará periódicamente a la Secretaría General de Administración Digital, de cuantos datos sean requeridos en relación a la duración del acceso y la revisión de su estado y condiciones.

I.2.1 Servicios de soporte.

La Secretaría General de Administración Digital dispone de un servicio de soporte central al cual corresponde recibir la notificación de incidencias, la resolución de las

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

mismas cuando le corresponda, y la gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores, u otros organismos con acceso al Sistema), así como atender las consultas técnicas relacionadas con el servicio y las peticiones de nuevos accesos.

La Comunidad Autónoma de Madrid podrá disponer de un servicio de soporte adicional, a ser posible 24 × 7, con este mismo cometido, tanto para garantizar los servicios de la Red SARA como aquellos otros que no haya proporcionado la Secretaría General de Administración Digital.

A través de la Comisión de seguimiento se intercambiarán y actualizarán los contactos, tanto de los responsables de la conexión a la Red SARA en la Comunidad Autónoma de Madrid, como los de los servicios de soporte que correspondan.

I.2.2 Mantenimiento y resolución de incidencias.

La gestión, mantenimiento y resolución de incidencias de los elementos activos de la Red Corporativa de la Comunidad Autónoma de Madrid conectados a Red SARA se harán por la propia Comunidad Autónoma.

I.2.3 Niveles de servicio iniciales.

Se define el siguiente nivel de servicio inicial respecto al servicio de soporte central:

Tiempo de respuesta de soporte de Red SARA (24 × 7): 120 minutos.

La Comisión de Seguimiento podrá determinar nuevos valores cuando corresponda por motivos técnicos o legales.

Apartado II: Utilización de sistemas de firma electrónica avanzada: Sistemas de identificación, firma y representación

II.1 Plataforma de validación y firma electrónica @firma.

II.1.1 Descripción de @firma.

@firma es un conjunto de productos y servicios de certificación y firma electrónica desarrollada por la Secretaría General de Administración Digital, que se pone a disposición de las Administraciones Públicas y de sus entidades de derecho público vinculadas o dependientes, para fomentar la puesta en marcha y el despliegue de aplicaciones informáticas y servicios de Administración Electrónica que requieran validación de firma electrónica basada en certificados, autenticación, generación de firma electrónica o sellado de tiempo en su relación con los ciudadanos, empresas y organismos.

De esta forma se establece un ecosistema de seguridad e interoperabilidad al permitir verificar el estado y validez de los distintos certificados electrónicos empleados por el ciudadano en cualquier procedimiento telemático, entre ellos, los del DNI-e, y se da cumplimiento al 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, que establece en el artículo 25.1 que «El Ministerio de la Presidencia (ahora Ministerio de Hacienda y Administraciones Públicas) gestionará una plataforma de verificación del estado de revocación de los certificados admitidos en el ámbito de la Administración General del Estado y de los organismos públicos dependientes o vinculados a ella».

El artículo 47 de dicho Real Decreto, establece la necesidad de incorporar una referencia temporal de los documentos administrativos electrónicos, siendo una de las modalidades de referencia temporal, el «Sello de tiempo», entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento. El sello de tiempo es una parte

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

indispensable de la firma electrónica, sobre todo en el caso de las firmas longevas, que necesiten ser validadas mucho tiempo después de su generación.

La Secretaría General de Administración Digital, en el ejercicio de sus competencias de desarrollo, impulso, planificación y ejecución de proyectos dirigidos a facilitar el acceso de los ciudadanos a la Administración Electrónica, proporciona la Plataforma @firma, como plataforma de validación de certificados y firma electrónica, que facilita el cumplimiento del derecho de los ciudadanos a la utilización de medios de identificación y firma electrónica, según los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Dicha plataforma se complemente con la TS@, para la generación y verificación de los sellados de tiempo.

A efectos del presente apartado se utilizará la referencia a @firma para referirse al conjunto de servicios prestados por la plataforma.

II.1.2 Servicios incluidos.

Los servicios ofrecidos por @firma son:

Validación de firmas y certificados electrónicos a través de la Plataforma @firma.

Firma electrónica de ficheros y formularios en entorno cliente, tanto en equipos de sobremesa como plataformas móviles, a través del Cliente @firma.

Sellado de tiempo mediante la Autoridad de Sellado TS@.

Bróker de proveedores de servicios de identidad (cl@ve).

@firma habilita a cualquier aplicación informática de la Comunidad Autónoma de Madrid a validar certificados digitales y firmas electrónicas en procesos de autenticación y firma, entre los certificados digitales admitidos por la Plataforma.

Asimismo, la plataforma dispone de entornos de prueba para facilitar la integración de aplicaciones y poder garantizar la correcta operación con carácter previo a la puesta a disposición de los usuarios finales.

II.1.3 Especificaciones técnicas.

II.1.3.1 Características de @firma.

Para facilitar al máximo la integración con las arquitecturas, aplicaciones y soluciones ya existentes, @firma es «no intrusiva», es decir, no modifica ni impacta en los esfuerzos ya realizados en sistemas y aplicaciones existentes.

Sus principales características son:

Se basa en Servicios Web que son utilizados por las distintas AAPP.

Es una plataforma validación MultiAC (múltiples Autoridades de certificación), MultiPolítica, MultiCertificados, MultiFirma, MultiFormatos..., de tal manera que permite la utilización de múltiples tipos de Certificados y Autoridades de Validación a los ciudadanos, en su relación telemática con las distintas Administraciones Públicas.

Proporciona seguridad a las firmas electrónicas, a través de las funciones de Sellado de Tiempo y actualización de firmas a formatos longevos.

Permite la validación de firmas electrónicas realizadas con certificados electrónicos reconocidos expedidos por Prestadores de Servicios de Certificación europeos en cumplimiento de la legislación europea vigente en materia de firma electrónica.

Facilita la integración de la firma electrónica en los portales de Administración electrónica, a través del Cliente @firma, un componente MultiSistema Operativo y MultiNavegador.

Proporciona las máximas garantías de seguridad y robustez, garantizando en su funcionamiento:

Un rendimiento óptimo,
Alta disponibilidad,
Interoperabilidad, y
Portabilidad.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

II.1.3.2 Modo de acceso a la plataforma @firma.

El acceso a los servicios de la Plataforma se realiza exclusivamente a través de la Red SARA, descrita en su correspondiente apartado, excepto cuando se despliegue la solución sobre una infraestructura propia de la Comunidad de Madrid (plataforma federada).

Las solicitudes de acceso se realizarán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

II.1.3.3 Auditabilidad.

@firma registra todas las peticiones realizadas, identificando siempre al empleado público y/o aplicación (mediante certificado electrónico), el momento de dicha petición y el proceso que se han realizado. Estas peticiones podrán ser auditadas a través de los elementos de auditoría de los que dispone la Secretaría General de Administración Digital, por ejemplo para certificar que no se produce «no repudio» de transacciones.

@firma no almacena los documentos incluidos en las peticiones de validación o solicitud de firma, y actúa únicamente como responsable del tratamiento de los datos de carácter personal incluidos en los certificados, pero no como responsable de dichos datos. La aplicación usuaria deberá ser responsable de declarar los datos de carácter personal que traten sus aplicaciones ante la AEPD o equivalente.

II.1.3.4 Servicios de soporte a usuarios.

En el estado actual de definición, los servicios de soporte a usuarios cuentan con las siguientes características:

Alcance.

El servicio de soporte y atención a usuarios abarca a los siguientes interlocutores:

Para el primer nivel: los propios organismos usuarios de la Plataforma.

Para el segundo nivel: CAU para atender a agentes externos al servicio como organismos, otros CAUs de los organismos o de los Prestadores de Servicio de Certificación (PSCs).

Para el tercer nivel: CAU que atiende las peticiones de actuación en sistemas y desarrollos del CAU de 2.º nivel.

Niveles adicionales:

Prestadores de Servicio de Certificación (PSCs).

Gestores del proyecto de la Secretaría General de Administración Digital.

Otros proveedores de servicios e infraestructura base para solicitar su asistencia ante incidencias o actuaciones preventivas en los sistemas.

Funciones.

Las funciones del servicio de soporte y atención al usuario son:

Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una web).

Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).

Evaluación, investigación y diagnóstico de las incidencias y peticiones.

Escalado funcional a los diferentes niveles de soporte.

Escalado jerárquico, de manera que los diferentes niveles de responsabilidad de las organizaciones implicadas posean visibilidad de los casos más relevantes y puedan tomar las acciones necesarias para minimizar el impacto de dichas incidencias.

Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

II.1.3.5 Aseguramiento de la calidad de servicio.

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.

Se contemplarán tanto los parámetros propios del servicio (disponibilidad de los servicios de validación y firma o de sellado de tiempo contemplados en @firma, estado de las comunicaciones, monitorización de sistemas), como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

II.2 Plataforma Cl@ve.

II.2.1 Descripción del sistema Cl@ve.

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 contraseña), 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 electrónica 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 implementar 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.

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, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, regula el funcionamiento de este sistema.

Aunque el alcance inicial del sistema es el Sector Público Administrativo Estatal, podrán adherirse al mismo mediante convenio otras Administraciones Públicas en las condiciones técnicas, económicas y organizativas que se determinen.

II.2.1.1 Funcionamiento de la plataforma (identificación y autenticación).

En lo que respecta a la identificación y autenticación, Cl@ve adopta la filosofía de un sistema de federación de identidades electrónicas, integrando a diferentes actores:

Proveedores de servicios de administración electrónica (SP): Entidades que proporcionan servicios de administración electrónica y utilizan la plataforma para la identificación y autenticación de ciudadanos.

Proveedores de servicios de identificación y autenticación (IdP): Entidades que proporcionan mecanismos de identificación y autenticación de los ciudadanos para ser utilizados como medios comunes por otras entidades.

Pasarela / Gestor de Identificación: Sistema intermediador que posibilita el acceso de los proveedores de servicios a los distintos mecanismos de identificación.

De acuerdo con esta aproximación, los SP únicamente tienen que integrarse con el Gestor de Identificación, encargándose este de establecer las relaciones pertinentes con los distintos sistemas de identificación. Para ello se establecen círculos de confianza entre los distintos actores que se integran entre sí, soportadas por el intercambio de certificados electrónicos y el envío de mensajes firmados entre ellos.

Para implementar esta federación de identidades, la solución desarrollada para Cl@ve se basa esencialmente en los resultados obtenidos por los proyectos STORK y STORK 2.0, adaptándolos convenientemente a las necesidades del proyecto. Esto supone que la interoperabilidad en Cl@ve se consigue con la utilización del estándar SAML 2.0, un framework basado en XML para reunir y organizar información de seguridad e identidad e

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

intercambiarla entre diferentes dominios, y que la integración entre sistemas se realiza no de manera directa, sino siempre a través redirecciones desde el navegador el usuario.

En relación a los mecanismos de identificación, Cl@ve contempla inicialmente la utilización de dos tipos de claves concertadas:

Cl@ve PIN: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios, provisto por la Agencia Estatal de Administración Tributaria (AEAT).

Cl@ve permanente: sistema de contraseña de validez duradera en el tiempo pero no ilimitada, orientado a usuarios habituales, provisto por la Gerencia de Informática de la Seguridad Social (GISS).

Ambos mecanismos de identificación contemplan la posibilidad de que el usuario reciba en su teléfono móvil, mediante un mensaje corto de texto (SMS), un código que deberá utilizar durante el proceso de autenticación. La provisión del servicio de envío de dicho SMS no es objeto del presente Convenio, y deberá ser gestionada directamente por las entidades que se integran con la plataforma, en este caso la Comunidad Autónoma de Madrid.

Además de los dos mecanismos de identificación anteriores, Cl@ve se integra con otros dos sistemas de identificación adicionales:

@firma, para la gestión de la identificación mediante certificados electrónicos y DNI electrónico.

Nodo EIDAS, la plataforma europea de interoperabilidad que permite el reconocimiento transfronterizo de identidades electrónicas, previsto en el Reglamento (UE) número 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 (reglamento eIDAS).

II.2.1.2 Funcionamiento de la plataforma (firma mediante certificados centralizados).

El sistema Cl@ve permitirá también el acceso a servicios de firma electrónica, en particular, a servicios de firma de documentos electrónicos mediante certificados electrónicos personales centralizados, si el usuario no usase otros certificados admitidos, todo ello a efectos de su presentación ante las Administraciones Públicas en aquellos trámites en que sea requerido o admitido el uso de certificados electrónicos. Se tendrán en cuenta las siguientes consideraciones:

Para poder acceder al servicio, el usuario deberá solicitar previa y expresamente la emisión de sus certificados electrónicos personales centralizados. La emisión al ciudadano de su certificado electrónico centralizado para firma se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma con la plataforma Cl@ve. El sistema informará al ciudadano de que se le va a emitir su certificado centralizado y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice su uso bajo el control exclusivo de su titular.

Los certificados electrónicos personales serán emitidos con las mismas garantías de identificación del DNI electrónico del ciudadano.

En cualquier proceso de firma electrónica con el certificado centralizado, deberá garantizarse que el acceso a dicha clave sólo podrá ser efectuado por el titular de la misma, por lo que para su uso se deberá haber autenticado previamente al ciudadano mediante un mínimo de 2 factores de autenticación, como por ejemplo los mecanismos de identificación Cl@ve PIN y Cl@ve permanente.

II.2.2 Uso del sistema Cl@ve.

Las condiciones técnicas, económicas y organizativas para la incorporación al sistema Cl@ve de la Comunidad Autónoma de Madrid, están determinadas por la Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve. Eventualmente, la Comunidad Autónoma podrá constituir Oficinas de Registro Presencial del sistema Cl@ve, para lo cual deberá estar a lo dispuesto 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.

Las solicitudes de acceso se realizarán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

II.2.2.1 Auditabilidad.

El sistema Cl@ve registrará todas las peticiones realizadas, identificando siempre a la entidad que realiza la petición y el momento de dicha petición, así como la operación efectuada y la respuesta proporcionada por el sistema. Estas peticiones podrán ser auditadas a través de los elementos de auditoría de los que disponen las entidades que intervienen en la operación del sistema, de acuerdo con las responsabilidades asignadas a cada una establecidas en la 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 sistema Cl@ve no almacena los datos de carácter personal incluidos en las respuestas a las peticiones de identificación y autenticación, y actúa únicamente como responsable del tratamiento de los datos de carácter personal incluidos en los certificados, pero no como responsable de dichos datos. La aplicación usuaria deberá ser responsable de declarar los datos de carácter personal que traten sus aplicaciones ante la AEPD o equivalente.

II.2.2.2 Servicios de soporte a las entidades usuarias.

El servicio de soporte y atención a entidades usuarias del sistema Cl@ve será prestado en sus diferentes niveles por los siguientes actores:

Centro de Atención a Integradores y Desarrolladores (CAID) de la Secretaría General de Administración Digital, como punto de contacto con las entidades usuarias.

Servicios de soporte de los Proveedores de Servicios de Identificación (AEAT o GISS), en el caso de que sea necesaria su participación.

Las funciones de este servicio de soporte y atención a las entidades usuarias son:

Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una web).

Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).

Evaluación, investigación y diagnóstico de las incidencias y peticiones.

Escalado funcional a los diferentes niveles de soporte.

Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

II.2.2.3 Aseguramiento de la calidad de servicio.

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.

Se contemplarán tanto los parámetros propios del servicio como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

II.3 Registro Electrónico de Apoderamientos.

II.3.1 Descripción general.

El registro electrónico de representación y apoderamientos (REA), permite hacer constar y gestionar las representaciones que los interesados otorguen a terceros, con el fin de actuar en su nombre de forma electrónica ante las Administraciones Públicas y/o sus organismos públicos vinculados o dependientes.

Los actores que intervienen en un apoderamiento son:

El ciudadano que actúa como poderdante puede apoderar a cualquier otro ciudadano o empresa para que actúe en su nombre.

El ciudadano que actúa como apoderado puede representar a cualquier otro ciudadano o empresa.

El apoderamiento se inscribe en el Registro para un determinado trámite o conjunto de ellos. La descripción, la gestión de los trámites y las categorías es competencia de cada organismo que se adhiere al REA.

El registro REA permite, previa identificación con certificado digital o DNI electrónico realizar ciertas operaciones necesarias para inscribir o gestionar el apoderamiento:

Como poderdante:

Crear un apoderamiento sobre un trámite o una categoría de trámites.
Consultar sus apoderamientos.
Revocar sus apoderamientos.
Modificar la vigencia de sus apoderamientos.

Como apoderado:

Consultar sus apoderamientos.
Renunciar a apoderamientos.
Confirmar apoderamientos, para trámites o categorías que así lo requieran.

Un organismo puede realizar la gestión y consulta de los apoderamientos de su competencia en REA, bien a través del subsistema Intranet del REA, o bien integrando sus propias aplicaciones con el Registro a partir de los servicios Web puestos a disposición por el sistema. El sistema permite a los organismos la descarga de sus trámites y categorías en diversos formatos normalizados.

II.3.2 Especificaciones técnicas.

II.3.2.1 Modos de acceso al REA.

II.3.2.1.1 Acceso a través de una aplicación Web.

El acceso a la aplicación se realiza exclusivamente a través de la Red SARA.

Las solicitudes de acceso se harán a través del centro de soporte, atendiendo al procedimiento establecido al efecto.

El manual de usuario de la aplicación puede consultarse en:

http://administracionelectronica.gob.es/ctt/rea/

II.3.2.1.2 Acceso a través de una interfaz de servicios Web.

El acceso a los servicios Web del REA se realiza exclusivamente a través de la Red SARA.

Las reglas de validación que se aplican son las que define el lenguaje WSDL y los documentos esquema XSD.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

Los Servicios Web disponibles son los siguientes:

1. Consulta de Apoderamientos WS.
2. Dar de Alta Apoderamientos WS.
3. Revocar Apoderamientos WS.
4. Modificar Apoderamientos WS.
5. Renunciar Apoderamientos WS.
6. Confirmar Apoderamientos WS.
7. Descarga de Apoderamientos WS.
8. Descarga de Categorías y Trámites WS.

La descripción detallada de los servicios Web puede consultarse en:

http://administracionelectronica.gob.es/ctt/rea/

II.3.3 Servicios de soporte a las entidades usuarias.

El servicio de soporte a usuarios tiene las siguientes características:

Alcance. El servicio de soporte y atención a usuarios abarca a los siguientes interlocutores:

Para el primer nivel: los propios organismos usuarios del REA.
Para el segundo nivel: CAU para atender a agentes externos al servicio como organismos, otros CAUs de los organismos.
Para el tercer nivel: CAU que atiende las peticiones de actuación en sistemas y desarrollos del CAU de 2.º nivel.
Niveles adicionales:

Gestores del proyecto de la Secretaría General de Administración Digital.
Los proveedores de servicios e infraestructura base para solicitar su asistencia ante incidencias o actuaciones preventivas en los sistemas.

Funciones. Las funciones del servicio de soporte y atención al usuario son:

Recepción de solicitudes a través de los canales de entrada que se establezcan (formularios a través de una página web).
Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades (a partir del cruce entre la urgencia y el impacto en el servicio).
Evaluación, investigación y diagnóstico de las incidencias y peticiones.
Escalado funcional a los diferentes niveles de soporte.
Escalado jerárquico, de manera que los diferentes niveles de responsabilidad de las organizaciones implicadas posean visibilidad de los casos más relevantes y puedan tomar las acciones necesarias para minimizar el impacto de dichas incidencias.
Seguimiento de incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

II.3.4 Aseguramiento de la calidad de servicio.

La calidad del servicio se medirá mediante la continua revisión de los valores de aquellos parámetros que midan los niveles de servicio.
Se contemplarán tanto los parámetros propios del servicio como los de soporte a los usuarios para la gestión y resolución de consultas e incidencias.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

Apartado III) Comunicaciones entre Administraciones Públicas por medios electrónicos

Subapartado III.a) Intermediación de datos entre Administraciones Públicas.

III.a.1 Descripción general.

III.a.1.1 Descripción.

La plataforma de intermediación de datos permite a las Administraciones Públicas interesadas la consulta por medios electrónicos de datos de ciudadanos de los que ya disponen otras Administraciones Públicas por su competencia.

De esta forma, el ciudadano no tiene que aportar los documentos acreditativos de los mismos. Asimismo, la Administración Pública puede realizar comprobaciones de dichos datos. Para ello debe existir el adecuado soporte legal o que el ciudadano haya dado su consentimiento.

III.a.1.2 Servicios incluidos.

Los servicios ofrecidos por la plataforma de intermediación de datos entre administraciones son:

Conexión a la plataforma de intercambio de datos.

Servicio de comunicación de cambio de domicilio a organismos de la Administración General del Estado.

Carta de servicios.

La carta de servicios recogerá en este servicio los efectos que se derivan del intercambio de datos entre Administraciones Públicas para la prestación de un servicio determinado, así como los requisitos para su tramitación, el plazo para su efectividad y cualquier otra información que deba conocer el interesado, y será actualizada con los nuevos servicios intermediados que se incorporen.

III.a.2 Especificaciones técnicas.

III.a.2.1 Características de la plataforma de intermediación de datos entre administraciones.

La plataforma de intermediación de datos es un servicio horizontal que permite integrar múltiples Administraciones Públicas, tanto para proveer datos a otras Administraciones Públicas como para consultar datos de otras, de forma segura.

III.a.2.2 Modo de acceso a la plataforma de intermediación de datos.

El acceso a los servicios de la plataforma se realiza exclusivamente a través de la Red SARA, descrita en su correspondiente apartado.

III.a.2.3 Especificaciones de seguridad.

Debido a la criticidad de la información intercambiada, para asegurar plenas garantías de seguridad, confidencialidad y protección de datos se cumplirán las siguientes especificaciones:

Autenticación: identificación de los usuarios que acceden al servicio mediante certificado electrónico reconocido en vigor que cumpla la recomendación UIT X.509 versión 3 o superiores, o mediante otros sistemas de identificación recogidos en la Ley 11/2007 para la identificación de las Administraciones Públicas.

Gestión de autorizaciones: Sólo se dará acceso a los empleados públicos y las aplicaciones, y sólo para realizar aquellas consultas para las que han sido habilitados.

Firma electrónica: Todas las peticiones irán firmadas (XMLDSig) con certificado electrónico (X509 v3).

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

Trazabilidad: El sistema registrará todas las consultas realizadas, identificando siempre al empleado público y/o aplicación (mediante certificado electrónico), el momento de dicha consulta (sellado en tiempo) y la finalidad con la que se han realizado. El sistema garantiza la integridad de los datos registrados mediante el uso de firma electrónica.

Confidencialidad: El sistema garantizará la confidencialidad de los datos intercambiados. Todas las comunicaciones que se realicen entre distintos organismos van sobre protocolo https (SSL) y además la red SARA proporciona, en el tramo troncal, medidas adicionales de cifrado de datos.

Integridad: Todas las consultas que se realicen, así como las respuestas que se devuelvan serán firmadas electrónicamente para garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

Sellado de tiempo: Para certificar la fecha y el tiempo de las actividades y sucesos registrados en la plataforma de intermediación de datos se hará uso de una marca de tiempo o, en su caso, del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica de la Secretaría General de Administración Digital, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del padrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

Auditabilidad: Cada petición y su correspondiente respuesta se registra en el sistema con la consiguiente firma electrónica y sellado de tiempo. Todas las peticiones van identificadas con un identificador único, que permite su posterior recuperación ante posibles reclamaciones o auditorías del servicio.

Auditoría: La plataforma de intermediación de datos dispondrá de un módulo de auditoría, en el que quedarán registrados todas las consultas de datos realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría de la plataforma.

Calidad de la información: La calidad de los datos será responsabilidad del organismo que los custodia.

Administración delegada: para facilitar la gestión de usuarios (altas/bajas/modificaciones) el sistema permite que cada organismo pueda tener un administrador encargado de esta gestión. Para ello, se da la posibilidad de limitar la administración del sistema por organismos.

Política de seguridad común: las medidas de seguridad necesarias para proteger debidamente la información y los servicios de intermediación ofrecidos se definirán sobre:

a) Cumplimiento de los criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores, y aquellas que sean de aplicación del 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.

b) Realización de análisis y gestión de riesgos, preferiblemente con la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

c) Cumplimiento de la normativa de Protección de Datos de Carácter Personal, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

III.a.2.4 Especificaciones de disponibilidad.

Se promoverá que la plataforma de intermediación de datos esté disponible los 7 días de la semana las 24 horas del día. Los organismos cedentes deberán contar con la misma disponibilidad en sus sistemas o plataformas.

III.a.2.5 Incorporación de nuevos servicios.

Las administraciones adheridas a este Convenio podrán incorporar nuevos conjuntos de datos intermediados, promoviendo la correspondiente actualización de la Carta de Servicios e informando de los nuevos servicios intermediados a la Secretaría General de Administración Digital para actualizar la Carta de Servicios.

III.a.2.6 Incorporación de nuevos intermediadores de datos.

Las Administraciones Públicas usuarias de este servicio podrán desarrollar sus propios intermediadores de datos, en cuyo caso se conectarán a la plataforma de intermediación de datos como un usuario más, atendiendo los mismos requisitos y obligaciones que la plataforma en cuanto a seguridad y niveles de servicio.

Subapartado III.b) Sistema de Interconexión de Registros.

III.b.1 Descripción general.

III.b.1.1 Descripción del Sistema de Interconexión de Registros.

El Sistema de Interconexión de Registros (SIR) es la infraestructura de las Administraciones Públicas que:

Interconecta las oficinas de registro (presenciales y electrónicas), utilizando la Norma Técnica de Interoperabilidad (N.T.I.) prevista en la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, en su punto k) Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (denominado también SICRES 3.0).

Permite el intercambio de asientos registrales en forma de comunicaciones electrónicas seguras entre las Oficinas de Registro y los Organismos Competentes, aportando evidentes beneficios tanto al ciudadano como a las Administraciones Públicas.

Da cumplimiento a la obligación legal del Artículo 24.4 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

La remisión electrónica de los documentos presentados por el ciudadano o por las propias Administraciones Públicas que estuvieran originalmente en papel, aporta grandes ahorros en coste y tiempo, y garantiza la disponibilidad de dichos documentos. Asimismo, y aplicando la normativa correspondiente, es posible digitalizar con plena cobertura legal para crear copias auténticas, y devolver el papel al ciudadano en ventanilla, minimizando los costes de manipulación y tránsito del papel.

La plataforma está construida con componentes de fuentes abiertas lo que facilita su soporte, transferencia y reutilización por cualquier Administración u Organismo.

III.b.1.2 Servicios incluidos.

Los servicios ofrecidos para la integración con el SIR son:

La conexión a la propia plataforma tecnológica.

La oficina para la certificación de la NTI SICRES 3.0 y la integración en SIR, gestionada por la Secretaría General de Administración Digital, que está disponible a aquellas Administraciones que deseen adaptarse integrar sus aplicativos de registro en SIR,

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

ofreciendo soporte y certificación mediante la ejecución y validación de la correspondiente batería de pruebas normalizada.

Directorio Común de Unidades Orgánicas y Oficinas (DIR 3), de consumo obligado por la plataforma SIR para el adecuado direccionamiento de los asientos de registro.

Asimismo, es necesario adoptar una operativa que incluye obligatoriamente:

Procedimiento de digitalización, para la adecuada remisión de los anexos a los asientos registrales.

Gestión de excepciones en la documentación física.

Procedimientos para la gestión de originales, compulsas y fotocopias.

Procedimientos de recepción y reenvío de asientos, con o sin documentación física.

Gestión de excepciones en caso de error humano.

Métricas de calidad.

Es opcional:

Indicadores de evolución y cumplimiento procedimental.

III.b.2 Especificaciones técnicas.

III.b.2.1 Características del Sistema de Interconexión de Registros.

Para facilitar al máximo la integración con las arquitecturas, aplicaciones y soluciones ya existentes, la plataforma SIR es «no intrusiva», es decir, no modifica ni impacta en los esfuerzos ya realizados en sistemas y aplicaciones existentes.

III.b.2.2 Modo de acceso al Sistema de Interconexión de Registros.

El acceso a los servicios del SIR se realiza exclusivamente a través de la Red SARA, descrita en su correspondiente apartado.

III.b.2.3 Elementos de acceso al Sistema de Interconexión de Registros.

El acceso a los servicios del SIR se realiza mediante el Componente de Intercambio Registral (CIR), un componente que cede a la Secretaría General de Administración Digital cuya función es la de determinar con qué parte se debe producir el intercambio de cada asiento registral (es decir, entre la administración origen y la correspondiente administración destino), y realizar dicho intercambio y reintentar en caso de fallo. Garantiza, asimismo, que los nodos que participan en el proceso de intercambio están autorizados, y que la comunicación cumple con el estándar de interoperabilidad establecidos (SICRES 3.0).

III.b.2.4 Auditabilidad.

SIR registra todas las transacciones realizadas, identificando siempre el intercambio realizado, el momento en que se ha hecho, y el resultado del mismo. Estas consultas podrán ser auditadas a través de los elementos de auditoría y traza de los que dispone la Secretaría General de Administración Digital, por ejemplo, para certificar que no se produce rechazo de intercambios.

III.b.2.5 Niveles de servicio de partida.

Inicialmente los niveles de servicio serán los siguientes:

Servicios de soporte:

Los que correspondan a @firma.

Servicios de intercambio:

El carácter de intercambio entre pares (es decir, entre administración origen y administración destino) impide establecer niveles de servicio con carácter exhaustivo en toda la red.

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

La Comisión de seguimiento podrá determinar nuevos valores cuando corresponda por motivos técnicos o legales.

Apartado IV) Práctica de la notificación por medios electrónicos: Plataforma notific@ y dirección electrónica habilitada

IV.1 Descripción general.

IV.1.1 Descripción.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas establece en su artículo 43.1 que «Las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica de la Administración u Organismo actuante, a través de la dirección electrónica habilitada única o mediante ambos sistemas, según disponga cada Administración u Organismo».

La Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre, fija las condiciones que ha de reunir la entidad habilitada para la prestación del servicio de dirección electrónica, así como las condiciones para su prestación, establece en su artículo 2.1 que «la titularidad de la dirección electrónica a partir de la que se construyan las direcciones electrónicas habilitadas de los interesados corresponde al Ministerio de la Presidencia».

En aplicación de lo dispuesto en la normativa anteriormente citada, el Ministerio de Hacienda y Administraciones Públicas ha desarrollado un servicio de notificaciones electrónicas y de dirección electrónica habilitada para la Administración General del Estado, que es prestado en colaboración con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM), gracias al Acuerdo de Encomienda Marco de Gestión de la Administración General del Estado (Ministerio de Hacienda y Administraciones Públicas) a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda para la prestación de los servicios de notificaciones electrónicas y de dirección electrónica habilitada, suscrito el 26 de junio de 2015.

Por otro lado, la Plataforma Notific@ es la solución tecnológica del servicio de gestión de notificaciones declarado como servicio compartido por la Comisión de Estrategia TIC en su reunión de 15 de septiembre de 2015. La entrega de las notificaciones/comunicaciones que se gestionan a través de esta Plataforma se realiza por:

Comparecencia en sede, lo que se proveerá a través de la Carpeta Ciudadana alojada en el Punto de Acceso General electrónico de la Administración, o en las sedes electrónicas de los emisores de dichas notificaciones/comunicaciones.

Y en función de diversas condiciones como, por ejemplo las establecidas por el destinatario para su relación con la Administración, se pueden servir también por alguna de estas vías:

En soporte papel, lo que se obtendrá mediante la colaboración de los CIE's y de los servicios postales correspondientes.

Dirección Electrónica Habilitada, para aquellos destinatarios que se adhieran a este sistema de forma voluntaria y aquellos otros que estuvieran obligados a usarla. En esta vía se coopera con la Fabrica Nacional de Moneda y Timbre como proveedor de los servicios de DEH.

En todos los casos la Plataforma Notific@, proporciona mediante diversos métodos, información al organismo emisor sobre el estado de la notificación/comunicación emitida.

IV.1.2 Coste asociado al servicio.

Los servicios estándar prestados por la Plataforma Notific@ se realizarán sin coste. En el caso de la Dirección Electrónica Habilitada, los costes asociados a la gestión de la

cve: BOE-A-2017-13523
Verificable en http://www.boe.es

entrega de la notificación (buzón, puesta a disposición, entrega, acuses de recibo, etc.), se inscribirán dentro de las relaciones entre la FNMT-RCM y el usuario del servicio.

Igualmente si se hace uso de la vía de puesta a disposición a través de distribución postal y soporte papel, los costes se inscribirán dentro de las relaciones con los Centros de Impresión y Ensobrado y el Operador postal.

IV.2 Descripción técnica del sistema.

Puede consultarse en:

https://administracionelectronica.gob.es/ctt/notifica/

cve: BOE-A-2017-13523
Verificable en http://www.boe.es