

# Pliego de Cláusulas Técnicas

---

QUE HA REGIR EN EL CONTRATO DE SUMINISTRO DENOMINADO  
**“ADQUISICION Y MANTENIMIENTO DE LICENCIA CORPORATIVA  
DE UN SISTEMA DE GESTIÓN DE FIRMA BIOMÉTRICA”** A  
ADJUDICAR MEDIANTE PROCEDIMIENTO SIMPLIFICADO  
ORDINARIO CON CRITERIO PRECIO.



## ÍNDICE

<b>CLÁUSULA 1ª - INTRODUCCIÓN.....</b>	<b>3</b>
<b>CLÁUSULA 2ª - OBJETO .....</b>	<b>5</b>
<b>CLÁUSULA 3ª DESCRIPCIÓN DEL PRODUCTO .....</b>	<b>5</b>
<b>REQUISITOS DE FUNCIONALES.....</b>	<b>5</b>
<b>REQUISITOS TÉCNICOS.....</b>	<b>6</b>
<b>REQUISITOS DE INTEGRACIÓN.....</b>	<b>9</b>
<b>CLÁUSULA 4ª DESCRIPCIÓN DE LOS TRABAJOS.....</b>	<b>10</b>
4.1. ADQUISICIÓN DE LICENCIA CORPORATIVA DE UNA SOLUCIÓN SOFTWARE DE FIRMA BIOMÉTRICA (BASADA EN FIRMA MANUSCRITA).....	10
4.2. SOPORTE Y MANTENIMIENTO CORRECTIVO:.....	10
4.3. ACTUALIZACIÓN DE VERSIONES .....	12
<b>CLÁUSULA 5ª – CONDICIONES ADICIONALES A CUMPLIR .....</b>	<b>13</b>
5.1. DISPONIBILIDAD DE LOS MEDIOS.....	13
5.2. RESPONSABILIDAD DEL SUMINISTRO .....	13
<b>CLÁUSULA 6ª SEGUIMIENTO Y CONTROL DEL CONTRATO.....</b>	<b>13</b>
<b>CLÁUSULA 7ª – PROTECCION DE DATOS DE CARÁCTER PERSONAL .....</b>	<b>14</b>
<b>CLAUSULA 8ª DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA.....</b>	<b>19</b>
<b>CLÁUSULA 9ª PLAZO DE EJECUCIÓN .....</b>	<b>19</b>
<b>CLÁUSULA 10ª – PLAZO DE GARANTÍA .....</b>	<b>19</b>
<b>CLAUSULA 12ª CONSULTAS TÉCNICAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS.....</b>	<b>20</b>



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: 1240774707021165088207

**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SUMINISTRO DENOMINADO “ADQUISICION Y MANTENIMIENTO DE LICENCIA CORPORATIVA DE UN SISTEMA DE GESTIÓN DE FIRMA BIOMÉTRICA”, A ADJUDICAR MEDIANTE PROCEDIMIENTO SIMPLIFICADO ORDINARIO CON CRITERIO PRECIO.**

**CLÁUSULA 1ª - INTRODUCCIÓN**

La **Agencia para la Administración Digital de la Comunidad de Madrid**, en adelante la **Agencia**, según *Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas*, modificada parcialmente por la *Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015)*, tiene asignada, entre otras funciones, la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, (*Artículo 10 Tres - c*).

En concreto, es competencia de esta Agencia la prestación de los siguientes servicios:

- La administración, mantenimiento y soporte de los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones de cualquier especie que se encuentren instalados en la misma.
- El desarrollo y adquisición de aplicaciones informáticas y sistemas de información para la Comunidad de Madrid, y su mantenimiento y soporte posteriores, de acuerdo con las especificaciones funcionales y necesidades de los distintos centros directivos.
- La adquisición y dotación de infraestructuras físicas y lógicas de soporte de los sistemas de información y comunicaciones de la Comunidad de Madrid, y de sus servicios.

Por su parte, la **Viceconsejería de Hacienda y Empleo**, dependiente de la **Consejería de Economía, Empleo y Hacienda**, tiene encomendadas entre otras competencias, la de coordinar las actuaciones de la Consejería en materia de políticas de fomento de empleo, trabajo, prevención de riesgos laborales, formación profesional para el empleo, autónomos, economía social y responsabilidad social de las empresas, coordinando en el ámbito de empleo a las siguientes unidades:

- La **Dirección General de Trabajo**, a la que le corresponden las funciones inherentes a su condición de autoridad laboral y las de materia de mediación, arbitraje y conciliación
- La **Dirección General de Formación**, a la que le corresponden las competencias en materia de formación para el Empleo, y en particular:



- ✓ La planificación de la política de formación profesional para el empleo en el ámbito laboral, de conformidad con los estudios y análisis realizados por la Consejería en este ámbito.
  - ✓ El diseño, planificación y evaluación de estrategias, proyectos y políticas de formación para el empleo, así como de la formación dual no reglada.
  - ✓ El desarrollo y fomento de las relaciones institucionales con el tejido empresarial de la Comunidad de Madrid en lo relativo a la Formación Profesional dual.
  - ✓ La elaboración y ejecución de programas de formación para desempleados y ocupados en cualquiera de sus modalidades
  - ✓ La gestión y ejecución de la convocatoria de becas y cursos de formación para el empleo en España y en el extranjero, y de prácticas no laborales.
  - ✓ La convocatoria y gestión de las subvenciones y ayudas públicas en materia de formación para el empleo en el ámbito laboral.
  - ✓ La elaboración de los criterios para la evaluación y seguimiento de las políticas de formación para el empleo aprobadas y sus resultados.
  - ✓ La evaluación, seguimiento y control de la formación para el empleo en el ámbito laboral impartida al amparo de convocatorias de ayudas y subvenciones públicas.
  - ✓ La acreditación y registro de las entidades colaboradoras de formación profesional para el empleo y de formadores.
- La **Dirección General del Servicio Público de Empleo**, a la que le corresponden las competencias en materia de estudios y planificación en su área de competencia, y las relativas a la promoción del empleo, a la acreditación de cualificaciones profesionales, y a la evaluación y verificación de las políticas y los programas de empleo, cuando así proceda; y, en particular y entre otras:
- ✓ En materia de orientación e intermediación laboral:
    - El análisis de los perfiles de los demandantes de empleo, el diseño y seguimiento de los itinerarios y de las acciones y medidas que se ajusten a las necesidades de los demandantes de empleo y de las empresas.
    - La ejecución de la oferta de servicios de orientación e intermediación de los usuarios de las oficinas de empleo.
    - La prospección e identificación de ofertas de empleo potenciales por parte de los empleadores.

En concreto, como apoyo a las funciones que tiene asignadas la Dirección General de Formación, se requiere un Sistema de Control de Alumnos, que se desarrollará dentro del Sistema Integral de Empleo (SIE), para el seguimiento de la asistencia a cursos presenciales, especialmente en el ámbito de la formación a desempleados. Este sistema deberá permitir verificar con garantías



suficientes la asistencia de los alumnos que acudan a los cursos presenciales para recibir la formación, sin que sea necesaria la presencia en el lugar de un funcionario para dar fe de dicha asistencia ni tampoco para el alta del alumno en el sistema.

Una vez analizadas las diversas alternativas conocidas para dar solución a esta necesidad, la Comunidad de Madrid ha optado por una solución basada en Firma Biométrica (sobre firma manuscrita) capturada en un dispositivo digitalizador de tipo tableta. Se ha optado por una solución basada en parámetros biométricos por ser la que mejor garantiza la autenticidad sin requerir dispositivos o procedimientos que pueden ser complejos para muchos usuarios. Y por otro lado, la firma manuscrita de un acta de asistencia es algo aceptado entre los usuarios, frente a otras soluciones de captura de datos biométricos que no se han considerado tan eficaces o resultan demasiado intrusivos para el usuario.

### **CLÁUSULA 2ª - OBJETO**

La adquisición de una solución software centralizada con licencia corporativa para la Comunidad de Madrid, basada en Firma Biométrica (sobre firma manuscrita) capturada en un dispositivo digitalizador de tipo tableta, así como el soporte y mantenimiento correctivo y la actualización de versiones de la solución software, todo ello de conformidad con los requerimientos establecidos en el presente Pliego de Cláusulas Técnicas.

### **CLÁUSULA 3ª DESCRIPCIÓN DEL PRODUCTO**

#### **Requisitos funcionales**

El desarrollo de las funciones indicadas en la Cláusula 1.- INTRODUCCION, de un modo eficiente, requiere el manejo en las Oficinas de Empleo de un importante volumen de información relativa a cada una de las personas que perciben prestaciones de desempleo y formación para el empleo, con el fin de orientar y encauzar de modo personalizado las políticas activas de empleo.

Con el fin de dar soporte a estas funciones, desarrolladas principalmente en las Oficinas de Empleo, la Comunidad de Madrid, dentro del rediseño de los procedimientos relativos a la gestión de las políticas de Empleo que son de su competencia, ha decidido acometer el desarrollo de un Sistema Integral de Empleo (SIE) sobre la herramienta de Microsoft Dynamics CRM.

Dentro del SIE, se dará respuesta a diversos procesos operativos de la Consejería de Economía, Empleo y Hacienda, los cuales fueron incluidos dentro del contrato de Servicios de Desarrollo y Mantenimiento del Sistema Integral de Empleo.



En concreto, uno de los subsistemas a desarrollar es el de Gestión de Formación que requiere de un módulo de Control de Alumnos para el seguimiento de la asistencia a los cursos presenciales.

El procedimiento de verificación de asistencia, básicamente seguirá los siguientes pasos:

1. El alumno recibirá una convocatoria al curso en el que vendrá incluido algún código único de validación por alumno y convocatoria, y que solo deberá recibir el alumno al que corresponda cada código. Este código único podrá estar soportado por un código de barras, código QR, código alfanumérico u otra solución.
2. El alumno asistirá al centro de formación, según la convocatoria del curso, donde se capturará el código único de su convocatoria y firmará en un dispositivo digitalizador de tipo tableta el acta de asistencia al curso.
3. En los días sucesivos de asistencia, el alumno firmará su asistencia en el acta correspondiente a cada día utilizando el indicado dispositivo digitalizador de tipo tableta. Opcionalmente se podrá requerir que esos días también se lleve el código de la convocatoria.

El sistema de Control de Alumnos deberá cotejar los códigos de asistencia, junto con las firmas realizadas, permitiendo generar alertas cuando éstas no cumplan los requisitos de autenticación establecidos. Igualmente, el sistema ofrecerá un cuadro de mandos para el seguimiento de los cursos que ha autenticado, permitiendo realizar consultas por curso o por alumno, así como generar de forma automática informes a la finalización de los distintos cursos, u otro tipo de informes de seguimiento definidos por el gestor de la solución.

Para la realización de esta solución, se plantea implantación de una solución software de firma biométrica centralizada con licencia corporativa para la Comunidad de Madrid, a la que se accederá desde los distintos centros de formación autorizados mediante un dispositivo digitalizador que podrá ser autónomo (tipo tableta) o basarse en un PC con Windows versión 7 o superior y pantalla táctil. La solución centralizada deberá permitir utilizar las firmas recogidas de los alumnos en un curso para el cotejo de las firmas que realicen en los cursos sucesivos.

### Requisitos técnicos

La empresa adjudicataria, deberá ser capaz de proporcionar la licencia corporativa y los servicios relacionados en el objeto del contrato que nos ocupa, teniendo que cumplir con los siguientes técnicos:

- A la solución software se accederá desde los distintos centros de formación autorizados mediante un dispositivo digitalizador tipo tableta, que podrá ser autónomo o basarse en un PC con Sistema Operativo Windows versión 7 o superior y pantalla táctil. Su instalación se



realizará en todos los centros de formación en los que se vaya a impartir formación para el empleo en modalidad presencial y determinada por la Consejería de Economía, Empleo y Hacienda, todo ello de conformidad con los requerimientos establecidos en el presente Pliego de Cláusulas Técnicas.

- Se proporcionará una solución de gestión con roles diferenciados para los gestores de formación de la Consejería (funcionarios), y centros de formación. En ambos casos, el acceso de gestión podrá ser multidispositivo y podrá realizarse desde Internet o desde la red corporativa de la Comunidad de Madrid.
- Se planteará una solución tecnológica que estará disponible para los centros de formación que preferentemente estará basada en un PC con Sistema Operativo Windows 7 o superior y pantalla táctil, proporcionado por el centro. Esta solución capturará y almacenará de forma securizada (cifrada) las características biométricas de la firma manuscrita:
  - Coordenadas x,y en función del tiempo.
  - Presión ejercida.
  - Velocidad y aceleración en cada trazo.
  - Las inflexiones y cambios de dirección.
  - Trazos en vuelo.
  - Así como cualquier característica biométrica que pueda ser específica de una firma manuscrita, y que el adjudicatario considere como necesaria.
- La solución se integrará con el Módulo de Control de Alumnos del Sistema Integral de Empleo de la Comunidad de Madrid, desde la que se le proporcionará la relación de alumnos de los distintos cursos, y centro en el que se impartirá.
- La solución debe mostrar en el dispositivo digitalizador el documento electrónico a firmar, junto con el nombre y apellidos del interesado y un espacio para insertar el grafo (firma manuscrita) del firmante. Se debe poder personalizar la apariencia del documento mostrado para la firma, permitiendo la incorporación de imágenes corporativas (de la Comunidad de Madrid, de la Consejería de Economía, Empleo y Hacienda, etc.) y textos variables (con el nombre, apellidos, DNI, nombre del curso, etc.).
- La solución permitirá la creación de un modelado de la firma sin necesidad de su registro previo, a partir de un número de capturas de la firma del alumno.
- La solución debe realizar la verificación de la firma en tiempo real, evitando intentos de fraude o de suplantación de identidad. Ante cualquier incidencia en la validación de la firma se le podrá comunicar al alumno para que la repita, la solución deberá registrar dicho incidente.
- La solución debe realizar una vinculación biunívoca de los elementos biométricos con el documento firmado.
- Imposibilidad de incrustar la firma biométrica recogida en otros documentos.



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: 1240774707021165088207



- Los datos o parámetros biométricos nunca deberán quedar en posesión de ninguno de los actores que puedan hacer uso de dichos datos o parámetros (gestor del sistema de control y seguimiento de la asistencia a cursos presencial, desarrollador del Módulo de Control de Alumnos del S.I.E., suministrador de la solución de firma biométrica), ya que son datos sensibles que permitirían la falsificación posterior de las firmas. Por ello, se deberá realizar una encriptación de estos datos y parámetros biométricos mediante un sistema de encriptación propio del dispositivo hardware digitalizador donde se recoge la firma manuscrita (que no es conocido ni accesible por el fabricante del software) o bien utilizando un certificado de un tercero de confianza.
- Posibilidad de comprobar la firma del titular mediante la identificación del firmante (autenticación).
- Posibilidad de demostrar la validez de la firma en un proceso litigioso. Un perito calígrafo podría analizar si los datos almacenados son coherentes con la firma manuscrita del usuario.
- Confidencialidad de los datos biométricos y Protección de la información conforme a la LOPD. Definir un procedimiento de detección y notificación a la autoridad competente de incidentes de seguridad que afecten a datos de carácter personal.
- Garantizar la simetría probatoria, de forma que tanto la entidad que utiliza la aplicación como el propio firmante están en igualdad de condiciones para ejercer el derecho a la prueba respecto a si un documento firmado es válido o si una firma pertenece o no a una persona.
- Autenticidad del documento. Capacidad de detección de cualquier cambio posterior a la firma (integridad del documento firmado).
- El documento electrónico firmado junto con los datos biométricos del firmante deben ser cifrados utilizando un certificado válido y reconocido por una Autoridad de Certificación, que garantice el cumplimiento de los principios básicos de una firma electrónica avanzada: Autenticación, integridad del documento firmado y no repudio. En ese momento se añadirá un sellado de tiempo que indique la fecha de la firma.
- Se generará un documento en formato PDF protegido contra escritura, que contendrá la firma escaneada (grafo del firmante), relacionada con un fichero validable y descifrable que contiene toda la información.
- Esa información se almacenará en un servidor central, que garantice un soporte duradero, seguridad y acceso a los datos en base a permisos.
- Se debe garantizar una comunicación segura entre servidor y dispositivo.
- La solución comparará las firmas realizadas por los alumnos en cada curso, o en varios cursos en el caso de alumnos que realicen varios, y proporcionará un cuadro de mandos (por alumnos, cursos, academias y por periodos temporales) en el que puedan consultarse



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: **1240774707021165088207**



la información relacionada con esas comparaciones, dando un grado de similitud de dichas firmas.

### **Requisitos de integración**

Este software biométrico debe ser capaz de integrarse con el Sistema de Control de Alumnos y dar cumplimiento a los requerimientos que se indican a continuación.

El adjudicatario, en el momento de la entrega del software, deberá entregar un documento explicativo y detallado que contenga las acciones a realizar para integrar este software con el SIE y en concreto con el sistema de Control de Alumnos, según las funcionalidades descritas.

El sistema de Control de Alumnos estará desarrollado en el entorno tecnológico de Microsoft Dynamics CRM en su versión 2016 o superiores.

#### Entorno Tecnológico Microsoft Dynamics CRM:

La solución CRM instalada en la Agencia en la actualidad se compone de los siguientes componentes:

- Componentes Core:
  - a. .NET como plataforma de desarrollo y ejecución de aplicaciones.
  - b. Servidores de CRM. Servidor de aplicación y negocio basado en MS Dynamics CRM 2016 o superiores y que alberga la capa de presentación y la lógica de negocio de la aplicación.
  - c. Servidores de BBDD. Servidores de BBDD, basados en MS SQL Server 2014 o superior y cuya función es la de albergar la capa de datos de la aplicación.
  - d. Servidor de integración. Servidor encargado albergar los procesos de integración con CAE Oracle y la capa de datos de la aplicación
- Componentes auxiliares:
  - a. Gestión documental con SharePoint.
  - b. Esquema de BBDD CAE Oracle: Esquema de BBDD Oracle réplica de los datos que CAE Oracle pone a disposición para la integración diaria con CRM.

### **También deberá cumplir con los siguientes requisitos legales:**

Se debe garantizar que la Firma Biométrica cumple los principios básicos de una firma electrónica avanzada, por lo que se atenderá al cumplimiento de:



- Ley 59/2003 de firma electrónica.

Artículo 3.2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Artículo 3.9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica.

También se garantizará el cumplimiento de estas otras leyes:

- Ley 15/1999 de protección de datos personales.

El sistema considera la firma manuscrita vinculada al firmante como un dato de carácter personal que requiere protección de nivel alto.

- Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo de 23 de julio del 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior por el que se deroga la Directiva 1999/93/CE.

#### **CLÁUSULA 4ª DESCRIPCIÓN DE LOS TRABAJOS**

El alcance específico de los trabajos para cada uno de los servicios citados será:

##### **4.1. Adquisición de Licencia corporativa de una solución software de Firma Biométrica (basada en firma manuscrita).**

Esta licencia deberá cumplir con las características descritas en la CLÁUSULA 3ª - DESCRIPCIÓN DEL PRODUCTO. El adjudicatario, durante el periodo fijado para la ejecución del suministro, impartirá una sesión específica informativa, para el personal seleccionado por la Agencia, con una duración máxima de 6 horas.

##### **4.2. Soporte y Mantenimiento Correctivo:**

El adjudicatario prestará apoyo de segundo nivel ante las incidencias reportadas por los usuarios al Centro de Atención a Usuarios de la Agencia. El soporte de primer nivel ante los usuarios será prestado por el Centro de Atención a Usuarios de la Agencia, que reencaminará las incidencias



no solucionadas al equipo aportado por el adjudicatario. Por tanto, no se producirá un contacto directo entre los usuarios y el adjudicatario.

El adjudicatario procederá a la gestión y resolución de las incidencias reportadas por la Agencia.

El adjudicatario garantizará la corrección de los defectos encontrados en el producto, corrigiendo la versión y poniéndola a disposición de la Agencia en los plazos establecidos en los acuerdos de nivel de servicio.

**El horario de atención y soporte** será de lunes a viernes de 8:00 a 20:00 horas, excepto festivos.

**El Acuerdo de Nivel de Servicio (ANS)** que la Agencia solicita al adjudicatario para el Soporte y Mantenimiento Correctivo contempla, que el tiempo de respuesta y resolución, ante cualquier incidencia recibida, se resuelva dependiendo del grado de criticidad.

Por **tiempo de respuesta** se entiende el tiempo transcurrido desde que se notifica la incidencia hasta que un técnico de la empresa adjudicataria se pone en contacto con personal de la Agencia con el objeto de recabar datos y solucionar la incidencia, dentro del horario de atención.

Por **tiempo de resolución** es el tiempo máximo transcurrido desde que se notifica la incidencia hasta que el sistema quede operativo, dentro del horario de atención. El tiempo de resolución se computa dentro del horario de atención:

- **Criticidad 1**: Produce una situación de emergencia en la que el software afectado no se puede ejecutar, está inoperante, produce resultados incorrectos o falla.

**Respuesta:** El adjudicatario proporcionará una respuesta en remoto y, cuando así se requiera, el desplazamiento *in situ* por parte de una persona cualificada de su organización para empezar a diagnosticar y corregir un error de Criticidad 1, en menos de 4 horas.

**Resolución:** El adjudicatario deberá resolver los problemas de Criticidad 1 en menos de veinticuatro (24) horas.

Si la solución aportada no fuera una solución definitiva, será planteada como una solución temporal de emergencia. Si esta solución temporal de emergencia es aceptable, la clasificación de Criticidad para este problema cambiará a Criticidad 2.

- **Criticidad 2**: Produce una situación de degradación en la que el rendimiento (respuesta) del software afectado cae bajo cargas de trabajo razonables. O bien, hay un fuerte impacto en la utilización del software, pero es utilizable aunque de forma incompleta por la inoperatividad de uno o más funciones o comandos.

**Respuesta:** El proveedor proporcionará una respuesta en remoto y, cuando así se requiera, el desplazamiento on site por parte de una persona cualificada de su



organización para empezar a diagnosticar y corregir un error de Criticidad 2, en menos de 8 horas.

**Resolución:** El adjudicatario deberá resolver los problemas de Criticidad 2 en menos de cuarenta y ocho horas (48). La solución será entregada de la misma forma que los errores de Criticidad 1.

- **Criticidad 3:** Produce una situación inconveniente, en la cual el software afectado es utilizable, pero no proporciona alguna función de la manera más conveniente o expeditiva, y el usuario sufre poco o ningún impacto.

**Respuesta:** El adjudicatario proporcionará una respuesta en remoto y, cuando así se requiera, el desplazamiento on site por parte de una persona cualificada de su organización para empezar a diagnosticar y corregir un error de Criticidad 3 en menos de dos (2) días.

**Resolución:** El adjudicatario deberá resolver los problemas de Criticidad 3 en menos de cinco (5) días. La solución será entregada de la misma forma que los errores de Criticidad 1.

#### 4.3. Actualización de Versiones

Durante el plazo de ejecución del contrato, el adjudicatario, además de la resolución de incidencias, incluirá el suministro e instalación de nuevas versiones del software adquirido, como consecuencia de la aparición de nuevas funcionalidades, así como de la inclusión de mejoras en cuanto a prestaciones y rendimientos, incluyendo la solución a problemas existentes en versiones anteriores.

A este respecto, el adjudicatario deberá:

- Informar a la Agencia, de las actualizaciones que incorpore a su producto.
- Permitir el acceso a las nuevas versiones, para ello deberá habilitar un “sitio web” desde el cual los instaladores podrán bajarse desde internet una versión auto-instalable del producto.

El proveedor proporcionará soporte on-line para que los instaladores puedan resolver las incidencias que surjan durante este proceso.

El adjudicatario suministrará lo necesario para que, si la Agencia lo decide, pueda crear un nuevo “sitio web” en sus instalaciones para servir como punto de descarga del producto.



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: 1240774707021165088207

## **CLÁUSULA 5ª – CONDICIONES ADICIONALES A CUMPLIR**

### **5.1. Disponibilidad de los medios**

El adjudicatario deberá contar con los medios propios necesarios de toda índole, necesarios de cara al soporte técnico que pudiera necesitar, para llevar a cabo con éxito los trabajos objeto del contrato.

### **5.2. Responsabilidad del Suministro**

El adjudicatario designará un *Responsable del Suministro* ante la Agencia.

El licitador propuesto como adjudicatario, con carácter previo a la adjudicación del contrato, deberá aportar el **Currículum Vitae** de dicho Responsable, y que deberá presentar debidamente firmado por la persona que ostente la representación, especificando su cualificación profesional (con detalle de categoría, titulación, formación y actividad profesional).

Este Responsable se encontrará en permanente contacto con el personal de la Agencia designado por la Dirección de la misma.

Este responsable realizará, principal y específicamente las siguientes tareas:

- Coordinar y ser el interlocutor de las peticiones de servicio y de información de la Agencia con el resto de la organización del contratista.
- Proponer mejoras en la infraestructura hardware y software que soporta al producto adquirido, sobre la instalación existente.
- Informar y mantener al día a las personas designadas por la Agencia de las diversas fuentes de información técnica disponibles.

El incumplimiento de las precitadas obligaciones, parcial o totalmente, facultará a la Agencia para instar la **resolución** del contrato.

## **CLÁUSULA 6ª SEGUIMIENTO Y CONTROL DEL CONTRATO**

El seguimiento y control del contrato se efectuará sobre las siguientes bases:

- Seguimiento continuo de la evolución del contrato entre el *Responsable del Suministro* por parte del adjudicatario y el *Responsable del Contrato* que la Agencia designe.
- La Agencia determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control del contrato.



## **CLÁUSULA 7ª – PROTECCION DE DATOS DE CARÁCTER PERSONAL**

En el caso de que el contratista, en el ejercicio de la prestación del servicio, tuviera que tratar ficheros con datos de carácter personal en el marco del objeto del presente contrato, cumplirá con la legislación vigente en materia de protección de datos de carácter personal conforme a lo dispuesto en las leyes y decretos que se relacionan a continuación:

- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, en adelante LOPD.
- *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (en los términos previstos en su Disposición Transitoria Segunda).
- Disposiciones de desarrollo de las normas anteriores en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

### Medidas de seguridad de carácter mínimo

- 1 No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el *RD 1720/2007* respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (*Artículo 9.2. LOPD*):
  - 1.1 En la fase de diseño funcional, y si del estudio previo de cada sistema de referencia procediera se propondrá la correspondiente creación e inscripción en la Agencia Española de Protección de Datos.
  - 1.2 Los diseños, desarrollos o mantenimientos de software deberán, con carácter general, observar los **estándares** que se deriven de la **normativa de seguridad** de la información y de protección de datos de la Agencia, y en concreto:
    - 1.2.1 Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
    - 1.2.2 Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado por la Agencia. La salida de



soportes y documentos fuera de los locales deberá ser también autorizada por la Agencia. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

1.2.3 Lo relativo a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Con una periodicidad no superior a un año se cambiarán las contraseñas asignadas a los usuarios, las cuales, mientras estén vigentes, se almacenarán de forma ininteligible.

1.2.4 Solo con el consentimiento expreso y escrito de la Agencia, el equipo prestador del servicio objeto del contrato tendrá acceso y tratará datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.

1.2.5 Deberán realizarse, como mínimo semanalmente, copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

1.2.6 Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento.

1.2.7 Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

1.2.8 Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado

1.3 Además de las medidas hasta aquí enumeradas, los tratamientos de datos de carácter personal relativos a la comisión de **infracciones** administrativas o penales, procedimientos **tributarios**, o aquéllos que contengan datos que ofrezcan una definición



La autenticidad de este documento se puede comprobar en [www.madrid.org/csv](http://www.madrid.org/csv) mediante el siguiente código seguro de verificación: **1240774707021165088207**



de las características o de la **personalidad** de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, deberán observar las siguientes medidas:

1.3.1 Deberá establecerse un sistema de registro de entrada y de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada.

1.3.2 Exclusivamente el personal autorizado por la Agencia podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

1.3.3 Será necesaria la autorización de la Agencia para la ejecución de los procedimientos de recuperación de los datos.

**1.4** Además de las medidas enumeradas en los anteriores apartados 1.1, 1.2 y 1.3, los tratamientos de datos de carácter personal relativos a **ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual** (salvo los tratados para verificar meras transferencias dinerarias, o los referentes exclusivamente al grado o condición de discapacidad o invalidez con motivo del cumplimiento de deberes públicos, a los que se les aplican las medidas del anterior apartado 1.2); los que contengan o se refieran a datos recabados para **finés policiales**; o aquéllos que contengan datos derivados de actos de **violencia de género**, deberán observar las siguientes medidas:

1.4.1 La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de la Agencia.

1.4.2 Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en la normativa de protección de datos personales, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.



1.4.3 De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

El registro de los accesos deberá integrarse con el sistema de información de la Comunidad de Madrid para la gestión y explotación de la información resultante de los accesos (SGUR).

1.4.4 El período mínimo de conservación de los datos registrados será de dos años. El contratista se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

1.4.5 Cuando se transmitan datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

#### Cesión o comunicación de datos a terceros

- 2 Los datos de carácter personal o documentos objeto del tratamiento **no podrán ser comunicados a un tercero** bajo ningún concepto, sin el consentimiento del titular del dato y el conocimiento de la Agencia, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
- 3 El contratista tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con un fin distinto al que figure en el objeto del contrato, ni los **comunicará**, ni siquiera para su conservación, a otras personas.

A la finalización del contrato, según el criterio o indicación de la Agencia, el equipo prestador del servicio procederá a destruir o a devolver a la Agencia toda la información confidencial o cualquier dato de carácter personal que haya sido susceptible de ser tratado durante la prestación del servicio, independientemente de que haya sido de forma escrita, grabada o empleando cualquier otro soporte en que pudiera recogerse.

La destrucción o devolución de la información confidencial o cualquier dato de carácter personal no exonerarán al equipo prestador del servicio de su obligación de tratar dicha Información Confidencial como estrictamente confidencial aún finalizada la relación convencional existente entre las mismas.



En el caso de que el contratista destine los datos a **otra finalidad, los comunique o los utilice incumpliendo** las estipulaciones del contrato, será considerado como único responsable, respondiendo de las infracciones en que hubiera incurrido personalmente.

- 4 De acuerdo con lo dispuesto en la *letra c) del apartado Tres del artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas*, la Agencia, que **actúa en nombre y por cuenta del Responsable del Fichero o Tratamiento**, ejerce como función la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente la administración, mantenimiento y soporte de los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones de cualquier especie que se encuentren instalados en la misma.

La contratación de las funciones propias del *Encargado del Tratamiento* de datos de carácter personal, será realizada de conformidad con lo dispuesto en el artículo 21 del Real Decreto 1720/2007, de 21 de diciembre, se limitará a los servicios que constituyen el objeto del presente contrato.

El contenido del servicio contratado estará determinado por el conjunto de derechos y obligaciones que, en virtud del presente contrato, asume el contratista como encargado del tratamiento de datos personales. Sin perjuicio de las instrucciones que, adicionalmente, pudieran establecerse por el **Encargado del Tratamiento**, el contratista queda sujeto en el tratamiento de datos personales a las instrucciones procedentes del **Responsable del Fichero**.

El contratista se obliga a cumplir las medidas de seguridad establecidas en el *Artículo 9 de la LOPD*, las previstas en el *RD 1720/2007*, en los mismos términos que el **Responsable del Tratamiento**

#### Derecho de información en la recogida de datos

- 5 Los datos personales recogidos podrán ser incorporados y tratados en el fichero **PROVEEDORES**, cuya finalidad es la solicitud de ofertas, selección y compra de bienes y servicios requeridos tanto por la Agencia para la Administración Digital como por la Comunidad de Madrid, inscrito en el *Registro General de Protección de Datos de la AEPD* ([www.agpd.es](http://www.agpd.es)), y no podrán ser cedidos salvo en los supuestos previstos en la ley. El responsable del fichero es la Agencia para la Administración Digital de la C.M., y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es la *calle Embajadores Nº 181, de Madrid*, todo lo cual se informa en cumplimiento del *Artículo 5 de la LOPD*.



## **CLAUSULA 8ª DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA**

El contratista no adquiere ningún derecho sobre el hardware (material), software (aplicativos) e infraestructuras propiedad de **la Agencia**, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanadas del contrato.

El contratista no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato, no pudiendo transmitir dicho conocimiento, sin el consentimiento escrito de **la Agencia**.

## **CLÁUSULA 9ª PLAZO DE EJECUCIÓN**

El plazo de ejecución del contrato será desde el día siguiente a la fecha de formalización del mismo hasta el 31 de mayo de 2019, con los siguientes plazos parciales:

- Suministro: deberá concluir como máximo el 31 de marzo de 2018.
- Servicio: catorce meses a contar desde el 1 de abril de 2018.

Para el caso de **actualizaciones y versiones sucesivas** se entregarán en el plazo de **un mes**, una vez que estén disponibles en el mercado.

Si en el plazo fijado en el contrato para la entrega del suministro, por motivos imputables al adjudicatario, no se pudiera contar con la disponibilidad de la solución objeto del contrato, esta Agencia quedará facultada para instar la resolución del mismo.

## **CLÁUSULA 10ª – PLAZO DE GARANTÍA**

Se establece un plazo de garantía de **CATORCE MESES**, cuyo cómputo se iniciará desde la fecha de recepción o conformidad.

Hasta que no tenga lugar la finalización del periodo de garantía, el adjudicatario responderá de los bienes suministrados, de los defectos que en ellos hubiera y de los servicios prestados, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de la Agencia los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del contrato.



### **CLÁUSULA 11ª ENTREGA**

El contratista pondrá a disposición del Área designado por la Agencia, lo necesario para la activación de la licencia adquirida, en la Sede de la Agencia (c/Embajadores, 181 Madrid).

### **CLAUSULA 12ª CONSULTAS TÉCNICAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS**

Durante el periodo de licitación y ante cualquier duda o necesidad de aclaración referida al Pliego de Cláusulas Técnicas los licitadores podrán dirigirse a la siguiente dirección de correo electrónico:

[ICM\\_SGTSOPORTE@madrid.org](mailto:ICM_SGTSOPORTE@madrid.org)

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con la Agencia, para cualquier tipo de consulta o aclaración sobre los términos expuestos en el presente Pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Así mismo los licitadores para formular sus consultas o aclaraciones deberán cumplimentar una plantilla con la siguiente estructura:

Nº DE CONSULTA	CLAÚSULA	PÁGINA	PÁRRAFO	DESCRIPCIÓN DE LA CONSULTA
1.				
2.				

En el asunto del correo electrónico deberá tener el siguiente texto: **Consulta Pliego FIRMABIO.**

Por su parte, la Agencia, se compromete a responder con la suficiente antelación, distribuyendo, entre todos los licitadores, todas las respuestas a las consultas y aclaraciones efectuadas, sin identificar la procedencia de ellas.

<b>ELABORADO Y PROPUESTO POR:</b> <i>La Directora de Servicios a Clientes de Economía, Empleo y Hacienda de la Agencia para la Administración Digital de la C.M.</i>  <i>Fdo.: Marta Bilbao Egado</i>	<b>APROBADO POR:</b> <i>El Consejero Delegado de la Agencia para la Administración Digital de la C.M.</i>  <i>Fdo.: Blas Labrador Román</i>
--	--

