

Pliego de Cláusulas Técnicas que han de regir el contrato de suministros denominado “**Suministro e implantación de una Plataforma de Autenticación y Autorización de usuarios para servicios WiFi al ciudadano**”, a adjudicar mediante procedimiento simplificado ordinario con pluralidad de criterios.



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: **1239908592025115841080**



## **INDICE**

<b>CLÁUSULA 1º. INTRODUCCIÓN.....</b>	<b>3</b>
<b>CLÁUSULA 2º. OBJETO DEL CONTRATO .....</b>	<b>4</b>
<b>CLÁUSULA 3º. ÁMBITO Y ALCANCE .....</b>	<b>4</b>
<b>CLÁUSULA 4º. DESCRIPCIÓN DE LA PUESTA EN FUNCIONAMIENTO .....</b>	<b>5</b>
<b>CLÁUSULA 5º. REQUISITOS TÉCNICOS .....</b>	<b>7</b>
5.1 REQUISITOS TÉCNICOS DE LA PLATAFORMA .....	7
5.2 REQUISITOS TÉCNICOS DE LA APLICACIÓN DE GESTIÓN DE USUARIOS WIFI .....	8
<b>CLÁUSULA 6º. DOCUMENTACIÓN .....</b>	<b>10</b>
<b>CLÁUSULA 7º. MODELO DE PROPUESTA .....</b>	<b>11</b>
7.1 Propuesta técnica .....	11
7.1.1 Descripción de la plataforma propuesta .....	11
7.1.2 Plan de proyecto .....	13
7.1.3 Descripción de los actividades a realizar por el licitador .....	13
<b>CLÁUSULA 8º. SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO .....</b>	<b>13</b>
<b>CLÁUSULA 9º. GESTIÓN DE LA SEGURIDAD.....</b>	<b>14</b>
<b>CLÁUSULA 10º. PLAZO DE EJECUCIÓN .....</b>	<b>22</b>
<b>CLÁUSULA 11º. PROPIEDAD DE LOS TRABAJOS .....</b>	<b>23</b>
<b>CLÁUSULA 12º. DERECHOS SOBRE EL SOFTWARE, HARDWARE E INFRAESTRUCTURAS DE MADRID DIGITAL .....</b>	<b>23</b>
<b>CLÁUSULA 13º. PLAZO DE GARANTÍA .....</b>	<b>23</b>
<b>CLÁUSULA 14º. CONSULTAS SOBRE EL PLIEGO.....</b>	<b>23</b>
<b>ANEXO I. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES .....</b>	<b>24</b>



## **CLÁUSULA 1ª. INTRODUCCIÓN**

La Agencia para la Administración Digital de la Comunidad de Madrid, en adelante la Agencia, tras la entrada en vigor de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas (BOCM Núm. 311, de 30 de diciembre de 2005), modificada por la Ley 9/2015, de 28 de diciembre, 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.

En los últimos años la Comunidad de Madrid, en colaboración con la Agencia para la Administración Digital de la Comunidad de Madrid (en adelante, *Madrid Digital*), ha acercado sus servicios al ciudadano y ha dado respuesta a sus expectativas de acceso a los procedimientos administrativos por medios telemáticos.

Actualmente, la Administración autonómica se encuentra en un nuevo contexto de transformación digital que apuesta por la utilización de las Tecnologías de la Información y Comunicaciones (TIC) para mejorar la eficiencia, agilizar los procedimientos y mejorar la transparencia y el ahorro. Para ello, y en colaboración con las restantes Administraciones Públicas (AAPP) autonómicas y la Administración General del Estado (AGE), existe una fecha objetivo común con Europa en el año 2020.

Entre 2016 y 2020 *Madrid Digital* y sus proveedores deben estar preparados para prestar los servicios en un entorno exigente y cambiante en el que el uso masivo y eficiente de las TIC, la continua innovación en servicios y en procesos, y la transformación de la sociedad y los ciudadanos en digitales, motivados por el creciente y cambiante mundo de servicios digitales ofrecidos por empresas y Administración, actúen como dinamizadores de una demanda continua de clientes y usuarios.

El Plan de Transformación digital de la Administración General del Estado (AGE) y sus Organismos Públicos (OOPP) muestra qué cambios se deben afrontar, e introduce los *objetivos estratégicos* sobre los que se vertebra la Estrategia TIC para impulsar una verdadera transformación digital y que sin duda son de aplicación en otras AAPP.

Los objetivos estratégicos de *Madrid Digital* para este Pliego se concretan en:

- Prestar el servicio con un nivel de calidad conforme al estado del arte en infraestructuras TIC.
- Alinearse con la transformación digital de la Comunidad de Madrid.
- Mejorar la imagen del servicio por parte de los usuarios.

Estos objetivos estratégicos permiten identificar cambios que girarán en torno a la innovación en servicios, procesos y herramientas y en la gestión del cambio, todo ello sin incrementar los costes de los servicios gracias a las sinergias y eficiencias que se producirán con el uso de las TIC.

Dicha transformación digital, obligará a *Madrid Digital* y a sus proveedores a anticiparse y ser protagonistas y líderes en esta transformación digital, en la continua innovación en los servicios y procesos, y en la gestión del cambio. Siempre enfocados a **mejora, eficiencia, agilidad, transparencia y ahorro**.

Los servicios de acceso WiFi de los diferentes usuarios en centros de la Comunidad de Madrid, que presta actualmente *Madrid Digital*, deberán evolucionar para apoyar esa transformación digital de la CM.

En la actualidad, la Agencia dispone del software *Aruba Clearpass*, como principal solución de control de acceso a la red y definición de políticas de acceso a la misma en escenarios de movilidad, para redes y tecnologías de múltiples fabricantes de equipamiento de red. En particular, dicho producto se está utilizando para realizar el control de acceso a la red, auto-registro y gestión de identidades, ya sea directamente, o bien mediante integraciones con otros repositorios de identidades, para diferentes servicios de acceso WiFi en bibliotecas y otros centros de la Comunidad de Madrid a través de su módulo *Clearpass Guest*.

En el ejercicio de sus funciones, la Agencia presta servicios WiFi al ciudadano en Bibliotecas y otros edificios públicos. El crecimiento en el uso de los servicios WiFi prestados a ciudadanos para diferentes fines ha experimentado un gran crecimiento en el último año, motivo por el cual la actual plataforma *Clearpass* ha llegado al límite de su capacidad. Se espera que dicho uso siga creciendo en los próximos años, por lo que *Madrid Digital* necesita un aumento de capacidad inicial en la plataforma de autenticación, autorización y *accounting* (AAA) utilizada para el WiFi ciudadano, con capacidad de crecimiento para atender un mayor número de usuarios.

## **CLÁUSULA 2ª. OBJETO DEL CONTRATO**

**Suministro de una Plataforma de Autenticación, Autorización y Accounting (AAA) para los diferentes servicios WiFi que presta la Comunidad de Madrid, a través de *Madrid Digital*, a los ciudadanos**, incluyendo la implantación, migración de datos y traspaso de conocimientos al personal de la Agencia.

## **CLÁUSULA 3ª. ÁMBITO Y ALCANCE**

La plataforma de autenticación y autorización cuyo suministro es objeto de la presente licitación deberá cumplir con los siguientes requisitos mínimos:

- Alta disponibilidad, proporcionada por un mínimo de dos máquinas, en dos CPDs distintos, ubicando como mínimo una máquina en cada uno de los dos CPDs, sin conexión a nivel 2 entre los mismos.
- Máquinas virtuales o físicas para atender, sin ampliación de máquinas a un mínimo de 20.000 autenticaciones exitosas diarias y 100 intentos de autenticación por segundo.
- En caso de ofertarse licencias deberán contemplar las necesarias para autenticar a un mínimo de 7.500 usuarios diarios, 22.500 dispositivos, desde 7.500 puntos de acceso wifi y 100 *Network Access Servers* (NAS). Dichas licencias deberán ser otorgadas a Madrid Digital de forma **permanente**, no considerándose válidos esquemas basados en una suscripción anual de un cierto número de usuarios.
- La plataforma ofertada poseerá una arquitectura que permita triplicar el número de usuarios/dispositivos wifi diarios sin modificación de dicha arquitectura.

Para la prestación de los servicios actuales, la Agencia dispone de 2500 licencias de dispositivo, utilizadas para autenticar y autorizar el acceso a la red a través de portales cautivos con



autenticación basada en protocolo RADIUS y repositorios de credenciales variados ubicados en aplicaciones accesibles mediante web services, directorios LDAP o la propia base de datos local del producto.

Con objeto de alcanzar una mayor concurrencia de ofertas y la mejor solución técnico-económica, se admiten ofertas basadas tanto en software privativo como en software libre.

La plataforma debe dar cobertura a todas las versiones de los sistemas operativos de los clientes más populares (navegadores más utilizados en Windows, Android e IOS) asegurando la evolución y buen funcionamiento de la plataforma para versiones futuras.

Dentro del suministro se incluye la entrega de la documentación de proyecto descrita en la **cláusula 6ª**, necesaria para la operación de la plataforma por parte de *Madrid Digital*.

En la presente licitación *Madrid Digital* da la opción a los ofertantes de proponer una plataforma en formato virtual, sobre plataformas físicas y el hipervisor VmWare con el que cuenta actualmente la Agencia. No obstante, los ofertantes podrán ofertar en su propuesta el suministro de máquinas físicas dedicadas para la plataforma solicitada. En cualquier caso la plataforma se instalará en dos centros de proceso de datos de la Comunidad de Madrid.

Con objeto de poder contar con un entorno previo permanente de validación no productivo, o entorno de pre-producción, la propuesta deberá incluir dos equipos virtuales de capacidad mínima, con licencias permanentes, que se usarán tanto para la realización de las pruebas funcionales de validación como de prueba de nuevas funcionalidades o modificaciones de las existentes, incluidas actualizaciones de software.

## **CLÁUSULA 4ª. DESCRIPCIÓN DE LA PUESTA EN FUNCIONAMIENTO**

El adjudicatario será responsable de la puesta en funcionamiento del software descrito para ofrecer los servicios que actualmente presta la plataforma *Clearpass*, así como de la migración de la funcionalidad existente en el cluster actual relacionada con portales cautivos de login/registro, portales de gestión de usuarios, envío de SMS, validación bibliotecas, etc., en colaboración con el personal de *Madrid Digital*.

Para la consecución de los objetivos planteados, se requiere la realización de las siguientes actividades:

- Instalación y configuración de máquinas sobre infraestructura de la Agencia, en dos centros de procesos de datos de Madrid Digital, tanto para el entorno de producción como para el entorno previo.
- Instalación y migración de la configuración particularizada de los diferentes componentes sobre las máquinas virtuales desplegadas, así como la realización de las configuraciones necesarias para proveer de la funcionalidad requerida en este pliego.
- Traslado de la configuración actual de servicios Clearpass en el cluster actual, con todos sus componentes y personalizaciones necesarias, entre otros:
  - o servicios CPPM,
  - o roles de usuario,
  - o enforcement,
  - o portales cautivos,
  - o funcionalidad y diseño presentes en la personalización actual de la aplicación de alta de usuarios (*tipo operador o recepcionista*),
  - o auto provisión de usuarios con entrega de credenciales de usuario por SMS por medio de una integración desde Clearpass con un web service



- autenticación/autorización de usuarios sobre una lógica definida actualmente sobre servicio HTTP para usuarios de bibliotecas
  - perfiles de administración de usuarios
- Migración de las base de datos de usuarios presente en el cluster actual al nuevo cluster.
- En el caso de ofertarse *Aruba Clearpass*, traspaso de la información estadística relativa a servicios Guest al nuevo cluster existente el día anterior a la entrada en servicio del nuevo cluster.
- Migración de todos los datos relativos con los servicios de portal cautivo y su uso por parte de los usuarios actuales.
- Las pruebas y ajustes de rendimiento previas a la puesta en producción del nuevo cluster, así como la instalación y parcheado a la versión más actualizada del producto.
- Dos sesiones de transmisión de conocimiento para el personal relacionado con los servicios de Operación y Mantenimiento de *Madrid Digital*, de 4 horas cada una, a realizar en dos días diferentes, a acordar con *Madrid Digital* sobre la configuración realizada en el nuevo cluster.
- Durante el proceso de implantación, se prestará soporte a la entrada en producción del nuevo cluster y resolución de incidencias asociadas a la migración en un horario de atención 24x7 durante la primera semana y 12x5 durante las tres semanas siguientes.

La operación de la plataforma, o la atención y resolución de incidencias diarias de usuario no están incluidos en este contrato.

La garantía del suministro permitirá a *Madrid Digital* abrir casos de soporte por consultas o incidencias a la empresa propietaria del desarrollo software o diseño e integración de componentes software, acceder a documentación actualizada del producto, descargar versiones del producto que corrijan errores funcionales o parches de seguridad, así como parches correctivos, todos ellos incluyendo su procedimiento de instalación. Asimismo, la garantía incluirá la solución a problemas de integración de la plataforma con controladores WiFi, switches, sistemas operativos (Windows, Android e IOS) y navegadores ampliamente difundidos (Explorer, Edge, Firefox, Chrome y Safari, al menos).

En el caso de que la oferta incluya el suministro de hardware, deberá incluir obligatoriamente una garantía, incluyendo actualizaciones de firmware y reposición de piezas averiadas al siguiente día laborable durante el plazo de garantía.

El software será instalado en las dependencias de *Madrid Digital* y debe incluir:

- Indicación de los **prerrequisitos** necesarios por la herramienta para su provisión en la infraestructura de virtualización basada en VmWare de *Madrid Digital* o prerrequisitos de máquinas físicas (espacio en rack, núm. tomas de red/ alimentación, potencia y refrigeración)
- Suministro de las versiones software más modernas recomendadas para un servicio en producción para el despliegue de las máquinas virtuales por parte de personal de *Madrid Digital*.

Para la ejecución del contrato la empresa adjudicataria designará un interlocutor único, que centralizará la recogida de información para la ejecución de los trabajos y al que se comunicarán los problemas observados por *Madrid Digital* durante la ejecución. Dicho interlocutor dispondrá de





los conocimientos y las capacidades técnicas necesarios para permitir a la empresa adjudicataria cumplir con sus obligaciones.

Además, incluirá el procedimiento de escalado a la empresa desarrolladora del software/integradora de componentes software de incidencias de soporte que *Madrid Digital* desee abrir durante el periodo de garantía, con teléfono de atención u otros canales que permitan la apertura de casos en horario 24x7 y respuesta con análisis previo de la incidencia o petición de información adicional en menos de 24 horas. En el caso de que el suministrador forme parte del proceso de escalado definido por la empresa proveedora de un software privativo, el adjudicatario estará obligado a suministrar la asistencia técnica requerida para el análisis, y corrección en su caso, de los problemas reportados durante ese plazo de tiempo, así como a responder a las consultas planteadas por *Madrid Digital*.

*Madrid Digital* proporcionará acceso al personal autorizado de la empresa adjudicataria a cualquier Producto para cumplir con las obligaciones asumidas por la empresa adjudicataria.

## **CLÁUSULA 5ª. REQUISITOS TÉCNICOS**

### **5.1 REQUISITOS TÉCNICOS DE LA PLATAFORMA**

Aparte de los requisitos relacionados con las prestaciones y capacidad mínima de la plataforma solicitada en el presente pliego, la plataforma ofertada deberá cumplir obligatoriamente los siguientes requisitos:

- ADM-1. Contará con una herramienta o procedimiento documentado de configuración y personalización de los portales cautivos en servicio y de definición de nuevos portales cautivos, que podrán diferir en la modalidad en que gestionan a los usuarios que pueden acceder al servicio
- ADM-2: Existirán 4 opciones de gestión de usuarios para un portal cautivo:
  - ✓ Sin página de registro ni gestión de usuarios. El portal deberá integrarse a través de *web service* o LDAP externo.
  - ✓ Registro de usuarios por un operador.
  - ✓ Autorregistro por parte del usuario con indicación del nº de teléfono móvil con entrega de contraseña por SMS utilizando el *web service* desarrollado por *Madrid Digital* para integrarse con las plataformas de entrega masiva de las que dispone.
  - ✓ Autorregistro por parte del usuario con indicación del e-mail de un *sponsor*. La plataforma enviará un e-mail con un enlace a dicho *sponsor* que permitirá la aprobación del mismo y, consecuentemente, la activación del usuario para poder autenticarse.
- ADM-3. Existirá una herramienta de explotación de la información de uso del servicio y de medida de la capacidad utilizada, incluyendo tanto autenticaciones exitosas como fallidas. Será posible extraer gráficas de uso sobre periodos de datos históricos, así como el periodo de retención de datos recomendado.
- ADM-4. Herramienta de auditoría que permita extraer tanto la fecha, hora y servicio en que se autentica a un login concreto, como fecha, hora y login de Registrador WiFi que realiza una operación sobre un login de usuario WiFi concreto.



- ADM-5. Herramienta de evaluación y diagnóstico de problemas de funcionamiento de la plataforma AAA.
- ADM-6. Herramienta de gestión de usuarios que realicen administración y operación de la plataforma.
- APP-1. Aplicación de gestión de usuarios WiFi por Registradores WiFi de acuerdo a los requisitos solicitados.
- SRV-1. Contará con un/os servidor/es RADIUS de autenticación de usuarios, que proporcionen una integración completa al menos con controladores HPE-Aruba, incluyendo los componentes, incluidos en la plataforma, que permitan la integración con:
  - ✓ Web service actual de autenticación de la aplicación Absyssnet
  - ✓ Web service actual de envío de mensajes SMS a la plataforma *on-premise* con la que cuenta Madrid Digital, y que es compartida por otras aplicaciones
  - ✓ Paso de información de login e IP a cortafuegos Palo Alto a través de uno sus APIs de integración
  - ✓ Al menos dos Directorios Activos Microsoft distintos, sin relación de confianza entre los mismos, para:
    - la administración y operación de la plataforma
    - la autenticación de empleados públicos que actúen como Registradores WiFi
- SRV-2. Contará con un servidor/es web que presenten el portal cautivo al usuario. El certificado de servidor seguro de dicho portal cautivo será suministrado por *Madrid Digital*.
- SRV-3. Contará con una base de datos en configuración de alta disponibilidad conteniendo, entre otros, las credenciales de los ciudadanos y los perfiles de Registradores WiFi que sean necesarios. La configuración del cluster de base de datos podrá ser *activo-standby*, pero ante problema en la instancia principal de base de datos, la instancia secundaria deberá asumir el rol de la principal transparentemente, sin intervención manual de ningún operador.
- SRV-4. Desde el portal cautivo de login del usuario del servicio existirá un enlace al portal de autorregistro, en los portales que cuenten con esta opción.
- SRV-5. El autorregistro de usuarios estará protegido por mecanismos que eviten que robots puedan generar registros automatizados, ya sean de tipo *captcha* o equivalentes.
- SRV-6. Será posible preconfigurar los atributos RADIUS que se devolverán en la respuesta a la petición de autenticación de un usuario, de forma que, en función del tipo de usuario autenticado las cualidades del servicio wifi recibido puedan ser distintas (como limitaciones de ancho de banda aplicables al usuario, por ejemplo)
- SRV-7. La plataforma permitirá configurar funcionalidades de *MAC-caching*, manejando una base de datos de dispositivos que almacene datos como el usuario que se autenticó, rol/tipo de usuario y duración del cacheo de la dirección MAC.

## 5.2 REQUISITOS TÉCNICOS DE LA APLICACIÓN DE GESTIÓN DE USUARIOS WIFI

- **RQ01.** Los usuarios principales de la aplicación serán empleados habilitados por la Comunidad de Madrid para registrar usuarios del servicio WiFi, que se llamarán Registradores WiFi. Dichos empleados tendrán login en uno de los Directorios Activos Microsoft de la Comunidad de Madrid.
- **RQ02.** Con objeto de facilitar las solicitudes para que los empleados puedan acceder a la aplicación como Registradores WiFi, existirán diferentes grupos, que serán accesibles por la





plataforma de autenticación en la fase de autorización inmediatamente posterior a la de autenticación de usuario por la aplicación. Inicialmente existirán los siguientes grupos de Registradores WiFi, en función de su ámbito de actuación en la Comunidad de Madrid:

- Hospitales
  - Albergues Juveniles
  - Asuntos Sociales
  - Secretarios/as de dirección
- **RQ03.** Los usuarios registrados por la aplicación serán ciudadanos cuyas credenciales de acceso al servicio WiFi estarán almacenadas en el módulo de base de datos de la plataforma de autenticación.
- **RQ04.** Los usuarios a registrar pueden estar vinculados directamente o no al servicio prestado en el centro de la Comunidad de Madrid donde se presta el servicio WiFi. En el momento del registro se indicará su tipología, que quedará almacenada en un rol de usuario. Inicialmente existirán los siguientes:
- Ciudadano
  - Socio
  - Formador
  - Alumno
  - Visitante
- **RQ05.** Una vez autenticado y autorizado, un registrador WiFi podrá realizar las siguientes operaciones:
- Búsqueda de usuarios
  - Alta de usuario
  - Baja de usuario
  - Cambio de contraseña
  - Cambio de caducidad de la cuenta de usuario
- **RQ06.** Al dar de alta a un usuario del servicio WiFi el Registrador deberá indicar los siguientes datos:
- Nombre y apellidos
  - Dirección
  - N° de documento identificativo (NIF, NIE, N° de pasaporte, carné), que será el login de acceso al servicio WiFi
  - Caducidad, indicada como un periodo de tiempo a partir del momento actual
  - Confirmación de que el registrador ha verificado la identidad del usuario solicitante.
  - Tipo de usuario
- **RQ07.** Tras indicar el Registrador los datos anteriores, se generará un recibo imprimible indicando:
- El nombre de red WiFi a utilizar.
  - Usuario
  - Contraseña
  - Fecha de caducidad del usuario actual
- **RQ08.** La aplicación contará internamente con una relación configurable que asocie tipo de usuario a nombre de red WiFi a utilizar, que aparecerá en el documento con las credenciales que se entregará al usuario. Inicialmente dicha asociación será la siguiente:



- Ciudadano – SSID-1
  - Socio – SSID-2
  - Formador – SSID-3
  - Alumno – SSID-4
  - Visitante – SSID-5
- 
- **RQ09.** (Opcional) Con el fin de que la contraseña del usuario del servicio WiFi no quede comprometida, será configurable que un usuario pueda acceder a la aplicación o no, a través de internet para modificar su contraseña, siempre que su cuenta no esté dada de baja o haya caducado.
  - **RQ010.** La baja de un usuario efectuada por un Registrador WiFi no implicará el borrado de los datos del mismo, sino que será una baja lógica “disable”
  - **RQ011.** Debido a la movilidad de usuarios por diferentes centros de la Comunidad de Madrid, cada uno de los cuales podrá tener desplegado un servicio WiFi diferente, y a que la base de datos de la plataforma de autenticación es única, un Registrador WiFi podrá modificar los siguientes datos conociendo el documento que sirva para la identificación del usuario, independientemente de que la cuenta esté dada de baja o esté caducada:
    - Caducidad de la cuenta
    - Contraseña
  - **RQ012.** Cuando un registrador solicite un cambio de contraseña para un usuario dado, la aplicación generará una secuencia aleatoria de 6 dígitos y un recibo imprimible idéntico al originado en el proceso de alta.
  - **RQ013.** Cuando un registrador cambie la caducidad de la cuenta de un usuario dado, la aplicación presentará la misma lista de caducidades existente en el momento del alta, que será configurable en la aplicación. Inicialmente los plazos de caducidad disponibles serán 15 días, 1 mes y 3 meses.

## **CLÁUSULA 6ª. DOCUMENTACIÓN**

Durante el periodo de ejecución del contrato, el adjudicatario deberá elaborar y facilitar a *Madrid Digital* la siguiente documentación:

- **Proyecto técnico**, con la descripción completa de:
  - todos los equipos y software instalables al amparo del contrato, incluidas, en su caso, las características técnicas de las máquinas virtuales a desplegar por Madrid Digital.
  - descripción de las funcionalidades soportadas por cada equipo o componente software,
  - configuración de red, de sistema y de producto, y usuarios privilegiados de administración
- **Guía de operación de la plataforma**, incluyendo:
  - Procedimiento de login en las distintas herramientas
  - Procedimiento de alta y baja de usuarios administrativos
  - Procedimiento de alta y baja de usuarios WiFi
  - Procedimiento de modificación de portales cautivos existentes
  - Procedimiento de modificación de la web de Registradores WiFi
  - Procedimiento de creación de nuevos portales cautivos
  - Procedimiento de arranque y parada de componentes
  - Descripción de informes y estadísticas
  - Guía de resolución de problemas típicos

En caso de que la oferta no consista en una solución basada en Aruba Clearpass:

- **Guía del Registrador WiFi**, para usuario final, describiendo:
  - Alta, baja y modificación de los usuarios WiFi

Adicionalmente, la empresa adjudicataria se compromete a facilitar a *Madrid Digital* las **instrucciones necesarias**, así como las operaciones y manuales de utilización, a los que están sometidos los productos para su correcta utilización y operatividad

El proyecto técnico se entregará en castellano, en formatos pdf y Word.

## **CLÁUSULA 7ª. MODELO DE PROPUESTA**

La presente cláusula describe cómo debe ser la estructura y formato con que se deberá realizar la documentación técnica de las ofertas que presenten cada uno de los licitadores, que se entregará en el Sobre nº 2 "DOCUMENTACIÓN TÉCNICA" y dentro del Sobre 2-A.

Con carácter obligatorio, deberá presentarse en **papel** y en **soporte digital**, compatible con las herramientas instaladas en *Madrid Digital* (aplicaciones de ofimática de Microsoft).

La documentación técnica estará compuesta por:

- Propuesta técnica, acompañada de un índice, que deberá entregarse obligatoriamente, y cuya estructura y formato se especifica en la presente cláusula. Consistirá en un único documento que no podrá exceder en ningún caso de las 25 páginas, a una sola cara con espaciado 1,5 y tamaño de letra equivalente a Arial 11.

### **7.1 Propuesta técnica**

Los licitadores del proyecto contemplado por el presente pliego, deberán contestar con una propuesta técnica concisa, clara y detallada, que conteste punto por punto cada uno de los apartados relacionados a continuación, describiendo la solución ofertada.

La propuesta técnica se ceñirá exclusivamente a los apartados que se definen a continuación:

#### **7.1.1 Descripción de la plataforma propuesta**

La solución propuesta deberá contener las especificaciones técnicas básicas de todos los elementos que lo componen, de modo que cumplan los requerimientos descritos en el presente pliego cubriendo, al menos, los siguientes aspectos:

- **Breve resumen de las características de la plataforma ofertada:**
  - ✓ Si incluye suministro de plataforma hardware o se suministran imágenes de máquinas virtuales
  - ✓ Si se trata de una plataforma que limita por licencia el número de usuarios autenticados de dispositivos que solicitan autenticación, o por otro concepto.
  - ✓ Descripción de los componentes necesarios para poder crecer en capacidad, ya sean licencias, máquinas virtuales, y forma de reparto de peticiones entre los componentes de un mismo nivel para poder atender volúmenes crecientes de peticiones
  - ✓ Si además de integrarse con los controladores WiFi de marca HPE-Aruba soporta la integración con controladores WiFi o switches de otros fabricantes.



- ✓ El tipo de adquisición que debería realizar *Madrid Digital* y forma de ampliar la plataforma para dos escenarios: duplicar y cuadruplicar el número de usuarios actuales.
- ✓ Si se trata de una plataforma con licencia de software libre o privativo, ya sea en su totalidad o en alguno de sus componentes.
- **Descripción de la plataforma de AAA.** Los licitadores deberán describir explícitamente los componentes de la plataforma donde residirán las siguientes funciones:
  - ✓ Herramienta de configuración de los portales cautivos en servicio y de definición de nuevos portales cautivos, que podrán diferir en la modalidad en que gestionan a sus usuarios: sin gestión de usuarios (integración a través de *web service* o LDAP externo) registro por un operador, autorregistro con entrega de SMS o autorregistro con aprobación en segunda fase por un *sponsor*.
  - ✓ Herramienta de explotación de la información de uso del servicio y de medida de la capacidad utilizada, incluyendo tanto autenticaciones exitosas como fallidas. Se indicarán las funcionalidades relacionadas con análisis de tendencias y posibilidad de extraer información gráfica de periodos de datos históricos, así como el periodo de retención de datos recomendado.
  - ✓ Herramienta de auditoría que permita extraer tanto la fecha, hora y servicio en que se autentica a un login concreto, como fecha, hora y login de Registrador WiFi que realiza una operación sobre un login de usuario WiFi concreto.
  - ✓ Herramienta de evaluación y diagnóstico de problemas de funcionamiento de la plataforma AAA
  - ✓ Herramienta de gestión de usuarios que realicen administración y operación de la plataforma
  - ✓ Aplicación de gestión de usuarios WiFi por Registradores WiFi de acuerdo a los requisitos solicitados
  - ✓ Base de datos en configuración de alta disponibilidad conteniendo, entre otros, las credenciales de los ciudadanos y los perfiles de Registradores WiFi que sean necesarios
  - ✓ Servidor/es RADIUS de autenticación de usuarios, que proporcionen una integración completa al menos con controladores HPE-Aruba, incluyendo los componentes, incluidos en la plataforma, que permitan la integración con:
    - Web service de autenticación de la aplicación Absyssnet
    - Web service de envío de mensajes SMS a la plataforma *on-premise* con la que cuenta Madrid Digital, y que es compartida por otras aplicaciones
    - Paso de información de login e IP a cortafuegos Palo Alto a través de uno sus APIs de integración
    - Al menos dos Directorios Activos Microsoft distintos, sin relación de confianza entre los mismos, para:
      - la administración y operación de la plataforma
      - la autenticación de empleados públicos que actúen como Registradores WiFi
  - ✓ Servidor/es web que presentan el portal cautivo al usuario



- **Descripción de la arquitectura de red del servicio**

Dado que se solicita una plataforma de alta disponibilidad, se incluirá una descripción detallada de la topología de la red, así como si requerirá de servicios de balanceo DNS proporcionados por *Madrid Digital* o resolverá esta problemática con mecanismos internos. Deberán contemplarse al menos dos escenarios: la incomunicación de las sedes con la plataforma de AAA y la caída de alguno de los componentes internos de la plataforma, en particular la base de datos de usuarios.

### 7.1.2 Plan de proyecto

Incluirá un cronograma con las fases previstas y duración de las mismas para cumplir con los objetivos del contrato. La migración del servicio actual deberá realizarse con un impacto mínimo en el servicio.

### 7.1.3 Descripción de las actividades a realizar

Incluirá las actividades de suministro, instalación, configuración, migración de datos, migración del servicio, transmisión de conocimiento y condiciones de la garantía.

En relación a la documentación técnica se tendrá en cuenta que en el **Sobre 2-B** se incluirá la declaración del Anexo IX del Pliego de Cláusulas Jurídicas, relativa a los **Criterios de adjudicación números 1.2 y 1.3.** La información relativa a estos criterios irá exclusivamente en este sobre 2-B

## **CLÁUSULA 8ª. SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO**

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

- Seguimiento continuo de la evolución del proyecto entre el *Responsable de Proyecto* por parte del adjudicatario y el *Responsable del Contrato* que *Madrid Digital* designe.
- *Madrid Digital* determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control del proyecto

## **CLÁUSULA 9ª. GESTIÓN DE LA SEGURIDAD**

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención a la observancia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la anterior y el 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.

Respecto a la gestión, administración y operación de los sistemas de información y de los datos a que se tenga acceso, todo ello dentro de la realización de los trabajos objeto del presente contrato, se deberán cumplir los requisitos de seguridad recogidos en este clausulado en todas las infraestructuras, servicios y sistemas del adjudicatario que den servicio a *Madrid Digital* en el desarrollo del contrato.

El adjudicatario estará obligado a la realización así como al mantenimiento de los registros de evidencias del cumplimiento durante al menos todo el período de ejecución del contrato de las actividades relacionadas a continuación:

- a) Definir, implementar y mantener una política de seguridad de la información.
- b) Implementar los análisis, ingeniería y contramedidas de seguridad con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información, mediante la ejecución de los controles que den respuesta a los requisitos especificados en este clausulado; todo ello integrado en una gestión de análisis y gestión del riesgo.
- c) Extender lo especificado en el punto anterior a los posibles contratos o relaciones con terceros vinculados a sistemas de información, productos y servicios que estén relacionados con la prestación del servicio objeto del contrato.
- d) En la fase de diseño funcional de los desarrollos objeto del contrato se realizará un estudio previo de su naturaleza y las medidas de seguridad que requieran de conformidad con la naturaleza de la información y el servicio que soportan y los requerimientos de la distinta normativa que les aplique. Esta especificación de requisitos de seguridad se documentará conforme a lo establecido en los estándares de *Madrid Digital* al respecto de la materia.

Los siguientes apartados establecen las condiciones y medidas en materia de seguridad que el adjudicatario deberá implantar y mantener para la prestación del servicio. Estas condiciones y medidas se considerarán como de obligado cumplimiento y con carácter de mínimos, teniendo en cuenta que el adjudicatario podrá implantar adicionalmente otros que considere adecuados o necesarios a lo largo de la ejecución del contrato. En todo caso, se estará a lo dispuesto en los estándares de seguridad de *Madrid Digital*. Asimismo, *Madrid Digital* podrá modificar esta relación de requisitos mínimos en cualquier momento, comunicando dicha variación al adjudicatario, quién estará obligado a adecuar sus sistemas a la modificación.

### **Documentación de seguridad**

El adjudicatario deberá entregar los siguientes documentos, que deberán estar permanentemente actualizados y a disposición de Madrid Digital en cualquier momento de la ejecución del contrato:

- a) Un documento denominado **Política de Seguridad**, que estará basada en la Política de Seguridad Corporativa de *Madrid Digital*, que consistirá en un documento de alto nivel que defina lo que significa la 'Seguridad de la Información' en la organización y aplicable al servicio prestado. El documento deberá estar accesible por todos los miembros de la organización que intervengan en la prestación del servicio y redactado de forma sencilla, precisa y comprensible.
- b) Un documento denominado **Documento de Seguridad**, coherente con los documentos de seguridad que exigen los Reales Decretos 1720/2007, y 3/2010 respectivamente, en lo que



corresponda a cada uno, donde se encuentre la normativa de seguridad, que recoja todas las medidas de seguridad propuestas, la forma de su cumplimiento y las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio. Estas medidas de seguridad incluirán al menos las que se relacionan a continuación para cada uno de los ámbitos normativos.

### **Usuarios de sistemas de información**

Los usuarios de los sistemas de información relacionados con el objeto del servicio deberán estar identificados y autorizados por el adjudicatario y quedar así reflejado en el Documento de Seguridad, previamente a efectuar cualquier uso de los sistemas mediante el correspondiente procedimiento que incluya los procesos de identificación, autenticación y autorización.

En el Documento de Seguridad se incluirá además la correspondencia y relación de los perfiles y las funciones asociadas al servicio prestado para *Madrid Digital*, así como las personas asociadas a dichos perfiles que pudieran tener acceso a información de la Comunidad de Madrid, y el tipo de información a la que pudieran tener acceso, ya sea datos de carácter personal, de administración electrónica u otro tipo.

Se registrará además en el Documento de Seguridad, si se diera la circunstancia, la relación de usuarios con privilegios de administración de los sistemas de información de *Madrid Digital* (asociados a posibles tareas habituales o puntuales de mantenimiento, explotación de sistemas o cualquier otra que pudiera implicar el acceso a datos del entorno de producción de los sistemas de información de la Comunidad de Madrid).

En el caso de utilizar sistemas de información de la Comunidad de Madrid, deberán acreditarse previamente de acuerdo con la política de gestión de identidades corporativa de *Madrid Digital*.

Se deberá acreditar el conocimiento y compromiso de la cláusula de seguridad de este Pliego por parte de todos los usuarios, quedando registrado en el Documento de Seguridad, así como la renuncia expresa de los derechos de propiedad intelectual que les pudiera corresponder. Las obligaciones subsistirán aun después de finalizar la relación contractual.

El contratista se compromete a formar e informar a su personal en las obligaciones que de estas cláusulas y la normativa que se menciona dimanar, para lo cual programará las acciones formativas necesarias.

Las relaciones de usuarios mencionadas deberán estar permanentemente actualizadas durante la prestación del servicio.

### **Protección 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 Persona, 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 R.D. 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 el Registro General de Protección de Datos de la AEPD.
  - 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 *Madrid Digital*, 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.
    - 1.2.3 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 *Madrid Digital*. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por *Madrid Digital*. 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.
    - 1.2.4 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.
    - 1.2.5 Solo con el consentimiento expreso y escrito de *Madrid Digital*, 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.
    - 1.2.6 Deberán realizarse, como mínimo semanalmente, copias de respaldo, salvo que en dicho 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.
    - 1.2.7 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.
    - 1.2.8 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.



- 1.2.9 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 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 *Madrid Digital* 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 *Madrid Digital* 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 2.2); 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 *Madrid Digital*.
- 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 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 *Madrid Digital*, 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 *Madrid Digital*, el equipo prestador del servicio procederá a destruir o a devolver a *Madrid Digital* 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 exonerará 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, Madrid Digital*, 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 *R. D. 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 *Madrid Digital* como por la C.M., 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 *Madrid Digital*, 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*.

### **Medidas de seguridad y compromisos del adjudicatario en materia de seguridad de los servicios de administración electrónica**

El adjudicatario asumirá el cumplimiento de lo establecido en el Esquema Nacional de Seguridad (Real Decreto 3/2010, de 8 enero - ENS) en lo referido a la adopción de medidas de seguridad de los servicios prestados. Se tendrá en cuenta la aplicación de las medidas de seguridad establecidas en el Anexo II del ENS, a una o varias dimensiones de seguridad y según el nivel determinado en cada caso.

El adjudicatario deberá realizar las acciones necesarias para concienciar regularmente al personal interviniente en la prestación del servicio acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos.

Se formará regularmente al personal interviniente en la prestación del servicio en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán las medidas de seguridad indicadas en su anexo II, ya sean pertenecientes al marco organizativo, operacional o de protección.

El Documento de Seguridad reflejará, además de lo estipulado con carácter general, la relación de las medidas de seguridad y de la forma en la que se procederá al cumplimiento en materia de seguridad en los sistemas de información de administración electrónica en el transcurso del desarrollo de los trabajos.

### **Medidas de seguridad y compromisos del adjudicatario en el caso de acceso remoto a infraestructuras de *Madrid Digital***

En el caso de que el adjudicatario acceda de forma remota desde sus instalaciones a infraestructuras de la Comunidad de Madrid, será de aplicación lo especificado a continuación.

La información asociada a los accesos a infraestructuras de producción de *Madrid Digital* que alberguen datos o información de la Comunidad de Madrid durante el período de ejecución de los servicios y del período de garantía de los mismos deberá estar a disposición de *Madrid Digital*, y contemplará las acciones de realizadas por cada usuario, el motivo, la solicitud y autorización de *Madrid Digital*, el mecanismo utilizado, así como todos los datos referidos a los dispositivos y mecanismos utilizados.

Además, se deberán cumplir las siguientes medidas de seguridad:

- No se habilitarán ni utilizarán las funciones de las aplicaciones o sistemas operativos que permitan guardar o recordar las credenciales de acceso de forma automática.
- Las infraestructuras del adjudicatario que se utilicen para dar cumplimiento al objeto del contrato y que deban acceder a la red corporativa de la Comunidad de Madrid deberán estar aisladas lógicamente y físicamente, de forma que dichas infraestructuras se utilicen de forma exclusiva para la prestación de los servicios, debiéndose asegurar que no existen conexiones



directas entre cualquier otra red distinta de la habilitada para la prestación del servicio y cualquier red de la Comunidad de Madrid a la que se acceda en virtud del contrato ya sea una red pública (ej. Internet) o privada, exceptuándose las conexiones autorizadas requeridas para la prestación del servicio.

- Entre cada red, subred o servicio de comunicaciones se implantarán cortafuegos (firewalls), que deberán estar configurados con la política del menor privilegio, bloqueando o denegando cualquier tipo de tráfico no autorizado o innecesario para la prestación del servicio. De la misma forma se permitirán únicamente los puertos, protocolos o servicios autorizados por *Madrid Digital*. Cualquier puerto, protocolo o servicio no especificado como autorizado se denegará por defecto.
- Los accesos a Internet se efectuarán obligatoriamente a través de proxies con sistema de identificación de su uso.
- El uso del correo electrónico deberá contar con filtro antivirus debidamente actualizado periódicamente.
- No se compartirán las cuentas de correo asignadas de forma personal, ni se podrá desviar de forma automática el correo electrónico profesional a cuentas particulares.
- El adjudicatario deberá implantar un Plan de Contingencia que ofrezca respuesta a emergencias, operaciones de respaldo y restauración y contingencias, que, al menos, garantice la correcta operación y entrega de los servicios según los niveles de servicio especificados en el apartado correspondiente.
- Se implementarán salvaguardas para detectar o minimizar la modificación o destrucción no autorizada de datos.
- Se mantendrá y ejecutará una política de respaldo automático de datos, verificación y restauración (en su caso).
- La información que deba suprimirse deberá destruirse de tal forma que sea imposible su recuperación.
- Se incluirá un sistema de protección antivirus, actualizado periódicamente y de forma automática, y que deberá utilizarse sobre cualquier fichero, soporte y software antes de que cualquiera de éstos resida o se instale en los sistemas de información. La frecuencia de actualización será como mínimo semanal.

### **Propiedad de los trabajos**

Todos los derechos de propiedad intelectual o industrial sobre los trabajos, informes, estudios y documentos elaborados por la empresa adjudicataria y el personal encargado de la ejecución del objeto de la relación contractual serán propiedad de *Madrid Digital*, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello la empresa contratista.

La empresa adjudicataria y su personal renuncia expresamente a cualquier derecho que sobre los trabajos realizados pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de *Madrid Digital*.

Específicamente, todos los derechos de explotación y titularidad de las aplicaciones informáticas instaladas en Madrid Digital y programas de ordenador desarrollados al amparo del contrato resultante de la adjudicación resultante de la presente licitación corresponden únicamente a *Madrid Digital*.

### **Sigilo y Confidencialidad de la información tratada**

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o



conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

Esta obligación no se limita al tiempo de ejecución del correspondiente contrato al que está asociado el proyecto indicado, sino que deberá ser respetada aun después de su cumplimiento o resolución.

Cualquier Información, fuese cual fuere su naturaleza (bien técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por *Madrid Digital* o la Comunidad de Madrid o cualquier tercero que tenga relaciones contractuales con la misma, en relación con el objeto del presente Pliego, será considerada como "Información Confidencial", incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

La empresa adjudicataria y el personal encargado de la realización de las tareas (en adelante el Equipo del Proyecto) se obligan a:

1. Guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el Equipo del Proyecto;
2. Utilizar o transmitir la Información Confidencial exclusivamente para los fines del objeto del contrato;
3. No realizar copia de la Información Confidencial sin el previo consentimiento escrito de *Madrid Digital*, excepto aquellas copias que sean necesitadas por el Equipo del Proyecto para su estudio interno;
4. Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento;
5. No facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito de *Madrid Digital*, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los del presente documento.
6. Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del contrato o su contenido, deberá ser previamente aprobada por escrito por *Madrid Digital*.
7. El Equipo del Proyecto procederá a destruir o a devolver a *Madrid Digital* toda la Información Confidencial a la finalización del objeto del contrato referido, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida.
8. La empresa contratista formará e informará de estas obligaciones al personal que participe en el desarrollo del contrato, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.

### **Restricciones generales**

En el marco de la ejecución del contrato, y respecto a los sistemas de información que le dan soporte, las siguientes actividades están específicamente prohibidas:

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.



- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remoto a usuarios no autorizados.
- Inutilizar o suprimir cualquier elemento de seguridad o protección o la información que generen.

### **Auditoría de la seguridad y trazabilidad de los servicios**

El adjudicatario adquirirá el compromiso de ser auditado por personal autorizado por *Madrid Digital* en cualquier momento en el desarrollo de los trabajos, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

Asimismo, y en el marco de la ejecución de los trabajos, y con el fin de garantizar la seguridad de la información manejada, *Madrid Digital* se reserva la capacidad de monitorizar la actividad de los sistemas, por lo que se informará a los usuarios de este aspecto.

La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- a) Documentación de los procedimientos.
- b) Registro de incidencias.
- c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

Se deberá implementar un proceso de revisión continua con el fin de detectar vulnerabilidades en los procesos y sistemas. Estas revisiones deberán ser periódicas y realizarse al menos trimestralmente, poniendo a disposición de *Madrid Digital* los resultados de dichas revisiones. Al menos se deberán revisar las configuraciones de seguridad con intervalos no superiores a un trimestre, poniendo a disposición de *Madrid Digital* los resultados de dichas revisiones.

Las evaluaciones no deberán tener impacto en los servicios, y deberá informarse a *Madrid Digital* del inicio y finalización de las mismas y solicitar la autorización previamente a su realización.

### **CLÁUSULA 10ª. PLAZO DE EJECUCIÓN**

El plazo de ejecución del contrato será de **tres meses** desde el día siguiente a la formalización del contrato.

Si a los **dos** meses de la ejecución del contrato, los trabajos objeto del mismo no hubieran comenzado y, por motivos imputables al adjudicatario, no se pudiera contar con la disponibilidad en tal fecha de los sistemas necesarios para la prestación de los servicios de autenticación, **la Agencia** quedará facultada para instar la **resolución** del contrato.

## **CLÁUSULA 11º. PROPIEDAD DE LOS TRABAJOS**

Todos los informes, sistemas, estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato **serán propiedad de Madrid Digital**, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este Pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de *Madrid Digital*.

## **CLÁUSULA 12º. DERECHOS SOBRE EL SOFTWARE, HARDWARE E INFRAESTRUCTURAS DE MADRID DIGITAL**

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

El contratista no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato y no podrá transmitirla sin el consentimiento expreso y por escrito de *Madrid Digital*.

## **CLÁUSULA 13º. PLAZO DE GARANTÍA**

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

Hasta que no tenga lugar la finalización del periodo de garantía, el adjudicatario responderá de la correcta realización de los trabajos contratados, de los equipamientos instalados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de *Madrid Digital* los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales, e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

## **CLÁUSULA 14º. CONSULTAS SOBRE EL PLIEGO**

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

**Agencia para la Administración Digital de la Comunidad de Madrid**  
**C/Embajadores, 181, 28045 - MADRID**

▪ **Consultas Técnicas**

Dirección de ingeniería, soporte a gestión de aplicaciones y centros de competencia

Área de Arquitecturas.

Email: [icm\\_sgtsoporte@madrid.org](mailto:icm_sgtsoporte@madrid.org)

Tfno.: 91 580 50 00. Horario de consultas: de 9:00 a 14:00 horas, de lunes a viernes



## **ANEXO I. ACUERDOS DE NIVEL DE SERVICIO Y PENALIZACIONES**

- **Tipo de servicio:** Puesta en servicio funcionalmente completa en los entornos de producción y propio de la plataforma de autenticación y autorización solicitada.
  - Nivel de servicio exigido: Plazo máximo de 2 meses desde el inicio del contrato
  - Penalización: 2,5% del importe del contrato, sin incluir IVA, por cada semana de retraso imputable al adjudicatario hasta un tope de 4 semanas.

<p><i>ELABORADO Y PROPUESTO POR:</i> <i>La Directora de Ingeniería, Soporte a Gestión de Aplicaciones y Centros de Competencia</i></p> <p><i>Fdo. : Ana García Ranera</i></p>	<p><i>APROBADO POR:</i> <i>El Consejero Delegado de la Agencia para la Administración Digital de la C.M.</i></p> <p><i>Fdo.: Blas Labrador Román</i></p>
---	--

