

# Pliego de Prescripciones Técnicas

---

---

***“ADQUISICIÓN DE LICENCIAS Y MANTENIMIENTO DE LAS  
SOLUCIONES DE SEGURIDAD DE ANTIVIRUS PARA  
SISTEMAS DE ALMACENAMIENTO NAS, EXISTENTES EN LA  
COMUNIDAD DE MADRID”***

---

---



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: **1276948164586199148871**



**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DENOMINADO “ADQUISICIÓN DE LICENCIAS Y MANTENIMIENTO DE LAS SOLUCIONES DE SEGURIDAD DE ANTIVIRUS PARA SISTEMAS DE ALMACENAMIENTO NAS, EXISTENTES EN LA COMUNIDAD DE MADRID”, A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO MEDIANTE CRITERIO ÚNICO**

**INDICE:**

<b>CLÁUSULA 1.-</b>	<b>INTRODUCCIÓN.....</b>	<b>3</b>
<b>CLÁUSULA 2.-</b>	<b>OBJETO .....</b>	<b>3</b>
<b>CLÁUSULA 3.-</b>	<b>ALCANCE.....</b>	<b>4</b>
	<b>DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE.....</b>	<b>4</b>
<b>CLÁUSULA 4.-</b>	<b>SERVICIO DE MANTENIMIENTO .....</b>	<b>4</b>
<b>CLÁUSULA 5.-</b>	<b>SERVICIO DE SOPORTE .....</b>	<b>5</b>
<b>CLÁUSULA 6.-</b>	<b>CONDICIONES ADICIONALES A CUMPLIR.....</b>	<b>8</b>
<b>CLÁUSULA 7.-</b>	<b>MEDIDAS DE SEGURIDAD Y COMPROMISOS DEL ADJUDICATARIO EN EL CASO DE ACCESO REMOTO A INFRAESTRUCTURAS DE LA AGENCIA .....</b>	<b>10</b>
<b>CLÁUSULA 8.-</b>	<b>SEGUIMIENTO Y CONTROL DE LOS SERVICIOS .....</b>	<b>11</b>
<b>CLÁUSULA 9.-</b>	<b>PROPIEDAD DE LOS TRABAJOS .....</b>	<b>11</b>
<b>CLÁUSULA 10.-</b>	<b>DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA. ....</b>	<b>11</b>
<b>CLÁUSULA 11.-</b>	<b>CALIDAD DEL SERVICIO .....</b>	<b>12</b>
<b>CLÁUSULA 12.-</b>	<b>PLAZO DE GARANTÍA .....</b>	<b>12</b>
<b>CLÁUSULA 13.-</b>	<b>PLAZO DE EJECUCIÓN .....</b>	<b>12</b>
<b>CLÁUSULA 14.-</b>	<b>CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS.....</b>	<b>12</b>
<b>ANEXO 1.-</b>	<b>GESTIÓN DE LA SEGURIDAD .....</b>	<b>14</b>
	<b>Protección de datos personales y Privacidad .....</b>	<b>14</b>
	<b>Seguridad en la utilización de medios electrónicos .....</b>	<b>19</b>
	<b>Medidas de Seguridad.....</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: **1276948164586199148871**

## CLÁUSULA 1.- 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, (B.O.C.M. Nº 311, de 30 de diciembre de 2005)*, 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)*, se configura como un ente público de los previstos en el *Artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid*, perteneciendo a la Administración Institucional de ésta, cuenta con personalidad jurídica propia, plena capacidad jurídica y de obrar, y autonomía de gestión.

La Agencia 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.

La prestación de los precitados servicios conlleva la elaboración de los planes de sistemas de información y de las comunicaciones de la Comunidad de Madrid, así como la dotación, administración y mantenimiento de las infraestructuras que los soportan, lo que se realiza a través de la *Subdirección General de Infraestructuras y Operaciones*.

Dentro de las soluciones de protección antimalware que la Agencia tiene implantadas en los distintos componentes soporte de los servicios TIC (puestos de usuario, servidores, entorno de correo, etc.) se dispone desde el año 2011 de la solución de antivirus para NAS (Network Attached Storage) de Trend Micro, como medida de protección instalada en los sistemas de almacenamiento que soportan el servicio de ficheros centralizados de los sistemas de la Comunidad de Madrid.

Para garantizar la operatividad y disponibilidad de este servicio y mantener unos niveles óptimos de seguridad, se considera necesario continuar con el mantenimiento de esta solución, objetivo de este Pliego de Cláusulas Técnicas.

## CLÁUSULA 2.- OBJETO

Es objeto del contrato la adquisición, mantenimiento y soporte de las soluciones de seguridad de antivirus para sistemas de almacenamiento NAS de los servicios de ficheros centralizados de la Comunidad de Madrid.



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: **1276948164586199148871**

### CLÁUSULA 3.- ALCANCE

Los servicios de mantenimiento y soporte demandados se ofrecerán sobre los productos **Trend Micro™ ServerProtect™**, instalados como protección antivirus del entorno NAS, y dimensionados para soportar el acceso concurrente de 15.001 usuarios a los sistemas de almacenamiento, así como el soporte Premium Support.

Además, se realiza la adquisición de 4.999 licencias adicionales que conlleva el mantenimiento y soporte de dichas licencias durante el plazo de garantía de 12 meses.

En caso de prórroga del contrato, y a la finalización del plazo de garantía, se incluirá el mantenimiento de las 4.999 licencias adquiridas al inicio del contrato, a través de una modificación del mismo.

La descarga de dichas licencias se hará a través de un código que se incluye en la consola de Trendmicro., el primer día de ejecución del contrato.

Por tanto, el alcance total de licencias es de 20.000 para los servicios que se detallan en el presente Pliego de Cláusulas Técnicas.

El detalle de los productos instalados es el siguiente:

SOLUCIONES DE SEGURIDAD ANTIVIRUS PARA NAS SOBRE LOS PRODUCTOS
Trend Micro™ ServerProtect™ for Storage:
<ul style="list-style-type: none"><li>• Adquisición y mantenimiento de 4.999 licencias adicionales</li><li>• Mantenimiento 15.001 licencias / usuarios concurrentes</li></ul>
Trend Micro Premium Support
100 horas de soporte in-situ

### DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE

El entorno del servicio de ficheros centralizados consta de varias cabinas de discos NetApp distribuidas en los distintos CPDs de la Comunidad de Madrid.

El servicio de ficheros está dimensionado para atender a 20.000 usuarios de forma concurrente.

La infraestructura de seguridad del servicio de antivirus para NAS está compuesta por un servidor Microsoft Windows 2012R2 con el Rol de Information Server y varios servidores Microsoft Windows 2012R2 con los roles de “**Scanner**” para proteger a las cabinas de almacenamiento.

La configuración actual de los servicios de protección antivirus para NAS está diseñada con una arquitectura de alta disponibilidad.

### CLÁUSULA 4.- SERVICIO DE MANTENIMIENTO

A continuación, se detallan los servicios que deberá prestar el adjudicatario para el mantenimiento de los productos.

- **Mantenimiento de las licencias de los productos software** indicados, durante toda la vigencia del contrato.
- **Actualización del fichero de firmas.** Acceso a las actualizaciones del fichero de firmas de malware a través de internet y compromiso por parte del adjudicatario de poner a disposición de la Agencia con periodicidad mínima diaria, el fichero con los nuevos patrones de detección de malware, así como las rutinas de desinfección asociadas.
- **Acceso a las mejoras de producto.** El adjudicatario se compromete a tener actualizados y a disposición de la Agencia una lista completa de los productos bajo soporte. Las actualizaciones se comunicarán a la Agencia mediante correo electrónico y el acceso a las mejoras del software antivirus estará disponible a través de internet.
- **Nuevas versiones.** Por una nueva versión se entenderá cualquier actualización de un producto, ya implique corrección de errores o defectos, introducción de mejoras, incorporación de funcionalidades o cambios introducidos por problemas de interoperabilidad con otros fabricantes con independencia de la denominación comercial que reciba.

Durante el periodo de vigencia del contrato el adjudicatario deberá facilitar, sin coste adicional, las nuevas versiones o actualizaciones de los componentes software a medida que sean liberadas por el fabricante, así como la documentación necesaria para llevar a cabo su implantación y configuración. El adjudicatario deberá analizar y comunicar el impacto de estas actualizaciones a la Agencia.

#### **CLÁUSULA 5.- SERVICIO DE SOPORTE**

El servicio de Soporte tiene por objeto establecer la asistencia técnica para el correcto funcionamiento de todos los productos Trend Micro, actualmente instalados en los servidores que conforman la infraestructura de seguridad de antivirus para NAS del servicio de ficheros centralizado de la Comunidad de Madrid, asegurando así que dichos servidores dispongan de las necesarias actualizaciones tanto del motor, como de los ficheros de firmas.

Las condiciones del servicio de soporte requerido serán las siguientes:

- **Servicio de soporte:** disponible de lunes a viernes, excluidos los días festivos de la Comunidad de Madrid, en el horario de 8:00 a 16:00 horas, extendido a 24x7 por el Soporte Avanzado denominado “Premium Support”, detallado más adelante.

El adjudicatario pondrá a disposición de la Agencia un **número de teléfono** para realizar cualquier consulta que será atendido por expertos del producto en lenguaje **castellano** y atenderá de forma personal cualquier consulta o incidencia relacionada con la detección de virus o con la configuración del producto.

- **Notificación de incidencias:** como sistema preferente de notificación de incidencias, el adjudicatario pondrá a disposición de la Agencia un número de teléfono de soporte técnico. Las incidencias también se podrán notificar electrónicamente a través de un sitio Web exclusivo.

Se definirá “*incidente*” como cualquier suceso inesperado o no deseado con consecuencias en detrimento de la operatividad, disponibilidad o seguridad de los sistemas de información.

la Agencia y los ingenieros de soporte asignados por el adjudicatario acordarán cual es el problema a resolver, así como los parámetros para una resolución adecuada, pudiendo requerir

múltiples llamadas telefónicas, así como trabajo de investigación fuera de línea para alcanzar la solución final.

La Agencia tendrá acceso a los ingenieros de soporte del fabricante para la notificación y tratamiento de incidencias relacionadas con el servicio.

El horario de notificación de incidencias será de 24 horas, 7 días a la semana.

- **Diagnóstico Remoto:** a petición de la Agencia, el adjudicatario podrá acceder a los sistemas de la Agencia remotamente para analizar problemas. Esto será hecho exclusivamente con el consentimiento de la Agencia, y el personal del adjudicatario accederá exclusivamente a los sistemas autorizados por la Agencia. El adjudicatario deberá proporcionar a la Agencia software para asistirle en el diagnóstico y/o resolución del problema.

- **Niveles de servicio:**

Se definen los siguientes niveles de criticidad ante los posibles incidentes en los productos objeto de soporte.

- **Niveles de prioridad:**

Se tendrán en cuenta tres niveles de prioridad para calificar la criticidad de la incidencia:

- Nivel 1. Criticidad Alta. Imposibilidad de trabajar con el recurso. Pérdida del 100% de su funcionalidad. Repetición de una incidencia de severidad media.
- Nivel 2. Criticidad Media. Dificultad para trabajar normalmente con el recurso. Pérdida parcial de su funcionalidad. Repetición de una incidencia de severidad baja.
- Nivel 3. Criticidad Baja. Degradación esporádica de la funcionalidad.

- **Tiempos máximos de respuesta:**

El **tiempo de respuesta** se define como el tiempo transcurrido desde que se notifica una incidencia hasta que un técnico de la empresa adjudicataria realiza la primera comunicación, según los canales establecidos, informando sobre el análisis de las causas de la incidencia y las acciones correctivas a realizar, con los plazos en los que se llevarán a cabo.

Para el cómputo de los tiempos máximos de respuesta se tendrá en cuenta el horario de servicio establecido anteriormente (24x7). Quedando definidos de la siguiente manera:

Prioridad	Tiempo máximo de respuesta
1	1 hora
2	4 horas
3	8 horas

La Agencia pondrá a disposición del adjudicatario los medios y recursos necesarios para facilitar su labor, facilitándole la información que precise para ello, así como el acceso al lugar donde se encuentren instalados los productos objeto del presente contrato, al personal destinado por el adjudicatario a la ejecución de los trabajos.

- **Seguimiento y resolución de incidencias:** Los técnicos de la Agencia estarán permanentemente informados del estado de las incidencias. Una vez resuelta la incidencia, se documentará e informará con el objeto de verificar la calidad de la solución.

El adjudicatario pondrá a disposición de la Agencia de forma mensual un informe del histórico de incidencias producidas con:

- Descripción detallada de la solución aplicada.
- Tiempo de respuesta desde el registro del incidente.
- Tiempo de resolución empleado hasta el cierre del incidente.
- Identificación del personal técnico involucrado por ambas partes.
- Número de horas empleadas en la resolución de incidentes.

➤ **Coordinación entre diversos fabricantes.** El adjudicatario trabajará con otros proveedores clave en la resolución de problemas en entornos heterogéneos. Cuando los problemas notificados sobre productos Trend Micro implican interacciones con productos de terceros, y la Agencia tenga acuerdos de soporte con dichos terceros, el adjudicatario compartirá información de diagnóstico y colaborará con ellos para proporcionar una solución.

➤ **Asistencia in situ:** el adjudicatario pondrá a disposición de la Agencia un servicio de asistencia in-situ como apoyo a la resolución de incidencias del servicio fuera del horario de soporte establecido para realizar trabajos orientados a la modificación de configuraciones de los productos, actualización de versiones o implantación de nuevas funcionalidades.

Estos servicios de asistencia in-situ se facilitarán por ingenieros técnicos especialistas en seguridad del adjudicatario, con experiencia demostrable en instalación y configuración del software que compone la plataforma.

El servicio de asistencia in situ constará de un **máximo de 100 horas anuales** a ejecutar durante el plazo de ejecución del contrato, previa solicitud por el Responsable del Contrato designado por la Agencia.

En el caso de no consumirse la totalidad de las horas anteriormente indicadas, no se originará ningún tipo de derecho de indemnización para el adjudicatario.

Dentro de esta asistencia in situ se realizarán **al menos 2 sesiones de transferencia de conocimiento** acordadas entre el adjudicatario y el personal responsable de la Agencia, tanto en relación a los contenidos concretos como a las horas necesarias para acometerlo.

En caso de no ejecutarse las horas correspondientes a una anualidad, las sobrantes podrán ser utilizadas en la anualidad siguiente.

➤ **Servicio de soporte especializado:** el adjudicatario estará obligado a realizar los acuerdos necesarios con el fabricante para facilitar acceso directo de la Agencia a los siguientes servicios de Trend Micro, asociados a su servicio “Premium Support”:

- **Asignación de un Gestor de cuentas técnico (TAM)**, para asesoramiento técnico especializado, localizable vía consola, teléfono móvil, correo electrónico y teléfono fijo.
- **Soporte 24x7**
- **Designación de 6 contactos** para la comunicación y apertura de incidencias.
- **Backup de otro TAM** para vacaciones y visitas a clientes del TAM asignado
- **Asignación por parte de la Agencia de la prioridad de los casos.** Un caso no queda cerrado hasta que la Agencia da su conformidad.



- **Soporte en la planificación de migración de versiones**, instalación de productos y parches y consultas de configuración
- Dentro del soporte técnico se contemplan los siguientes **servicios**:
  - ✓ Realización de consultas sobre el uso de productos objeto del contrato.
  - ✓ Solicitud de ayuda en las instalaciones
  - ✓ Realización de cualquier consulta técnica referente a los productos en mantenimiento.
  - ✓ Realización del ajuste de parámetros de funcionamiento del software y/o hardware.
  - ✓ Información sobre cualquier incidencia técnica acerca del mal funcionamiento de los productos objeto del Pliego.
  - ✓ Solicitud de actualización de productos y manuales.
- **Envío periódico de todas las nuevas versiones de software**, firmware, así como de los parches publicados
- **Prioridad** en la resolución de casos y desarrollo de parches cuando estos son escalados a desarrollo.
- **Acceso directo por parte del personal de la Agencia a recursos en línea mejorados del fabricante**, que faciliten información sobre los desarrollos de los productos, las cuestiones de asistencia técnica, el estado de los casos de servicio, y las amenazas potenciales que puedan afectar al servicio, incluyendo:
  - **Herramienta de gestión de casos**, que permita realizar un seguimiento del estado del servicio.
  - **Acceso a la Base de conocimiento**, que facilite información de seguridad detallada y completa, así como información de malware y procedimientos para su tratamiento.
- **Avisos de malware y ataques** sucedidos en otros clientes para evitar que ocurran en la Agencia.
- Una vez remitida una incidencia por parte de la Agencia, será su CSM asignado el encargado de velar por su resolución.



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: **1276948164586199148871**

<b>CLÁUSULA 6.-           CONDICIONES ADICIONALES A CUMPLIR</b>
---

- El adjudicatario deberá contar con los medios propios, de toda índole, necesarios para proporcionar el soporte técnico requerido para llevar a cabo con éxito los servicios objeto del contrato, incluida la formación del personal asignado a la ejecución del mismo.
- Asimismo, el adjudicatario responderá siempre de la adecuación del personal asignado a la prestación del servicio objeto del contrato. A tal efecto, durante la ejecución de los trabajos, la Agencia podrá comprobar la adecuación del personal asignado al servicio contratado y verificar dicha capacidad en cualquier momento.
- El adjudicatario facilitará a la Agencia las especificaciones técnicas y sobre las infraestructuras que fueran necesarias para la buena adaptabilidad de los productos software en mantenimiento y actualización.



- Todos los gastos ocasionados por los desplazamientos del personal prestador del servicio durante el cumplimiento de las obligaciones derivadas del contrato serán por cuenta del adjudicatario.
- Para el caso de que los servicios contratados puedan implicar para el adjudicatario, por razones de cumplimiento de plazos u otros motivos, la decisión de prestación de los mismos en régimen de turnos o en sábados o festivos, o en horario nocturno, la Agencia no aceptará costes adicionales por estas circunstancias, que deberán ser asumidos siempre por el adjudicatario.
- En el caso de que se presten servicios en las instalaciones de la Agencia, el personal de la empresa adjudicataria que ejecute por cuenta de ésta trabajos directamente relacionados con el objeto del presente contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por la propia empresa adjudicataria, salvo que por razones operativas asociadas a la naturaleza del servicio a prestar, la Agencia proporcione medios, en todo caso con carácter transitorio, a la empresa adjudicatario, ya que se utilizarán únicamente durante la ejecución del contrato y además su uso estará limitado exclusivamente al desarrollo de los trabajos que constituyen el objeto del mismo.
- De conformidad con lo establecido en el *Pliego de Cláusulas Administrativas Particulares*, el licitador que presente la mejor oferta, con carácter previo a la adjudicación del contrato deberá aportar acreditación vigente como **partner de Trend Micro**, para la prestación de los servicios de mantenimiento y soporte técnico de soluciones de seguridad de antivirus Trend Micro para NAS, asociados a su servicio **“Premium Support”**, así como el compromiso de mantener dicha acreditación durante el período de ejecución del presente contrato.
- El adjudicatario designará a un **Responsable del Servicio** ante la Agencia.

El licitador que presente la mejor oferta, con carácter previo a la adjudicación del contrato, deberá aportar “Curriculum Vitae” del Responsable del Servicio, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando su cualificación profesional (con detalle de categoría, titulación, formación y actividad profesional).

Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la Dirección de la Agencia designe, a los efectos que se señalan en el *Pliego de Cláusulas Administrativas Particulares*.

El adjudicatario, a través del **Responsable del Servicio**, y con la periodicidad que en la Agencia determine, informará sobre la planificación de trabajos, el estado de ejecución del contrato y, en su caso, sobre las incidencias producidas. En particular, este responsable realizará, entre otras, las siguientes *tareas*:

- **Coordinar el apoyo técnico y la formación necesaria** que el adjudicatario suministrará al equipo humano que realice los trabajos objeto del contrato, en todas aquellas materias que sean necesarias para el perfecto desempeño de los mismos.
- **Impartir con exclusividad** instrucciones específicas sobre el trabajo a realizar al personal del adjudicatario, siempre teniendo en cuenta la base de las instrucciones genéricas que se desprendan de lo establecido en el presente Pliego y encaminadas al buen término del servicio.
- **Supervisar el servicio de mantenimiento y soporte a prestar**, e informar a la Agencia de las posibles incidencias, seguimiento o desviaciones de plazos.



- **Ejercer el mando sobre el equipo de trabajo**, que estará siempre bajo la disciplina laboral y el poder de dirección del adjudicatario, con independencia de que, para el mejor cumplimiento del servicio, en determinados momentos pueda el adjudicatario destacar personal del equipo prestador del servicio en cualquier centro de trabajo, oficinas o ubicaciones de la Comunidad de Madrid.

<b>CLÁUSULA 7.- MEDIDAS DE SEGURIDAD Y COMPROMISOS DEL ADJUDICATARIO EN EL CASO DE ACCESO REMOTO A INFRAESTRUCTURAS DE LA AGENCIA</b>
---

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 la Agencia que alberguen datos o información de la Comunidad de Madrid durante el periodo de ejecución de los servicios y del periodo de garantía de los mismos deberá estar a disposición de la Agencia, y contemplará las acciones de realizadas por cada usuario, el motivo, la solicitud y autorización de la Agencia, 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 la Agencia. 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.

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: **1276948164586199148871**

- 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.

#### **CLÁUSULA 8.- SEGUIMIENTO Y CONTROL DE LOS SERVICIOS**

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

- Seguimiento continuo de la evolución del servicio entre el Responsable del Servicio 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 servicio.
- Elaboración de informes bimensuales de seguimiento, asociados a las visitas in-situ que realice el TAM, con detalle de estado general del servicio y recomendaciones para prevención de problemas.

#### **CLÁUSULA 9.- PROPIEDAD DE LOS TRABAJOS**

Todos los estudios y documentos, así como los productos y subproductos elaborados por el adjudicatario como consecuencia de la ejecución del contrato serán propiedad de la Agencia, 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 la Agencia.

#### **CLÁUSULA 10.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA.**

El adjudicatario no adquiere ningún derecho sobre el hardware (material), software 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 adjudicatario no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato, no pudiendo transmitir dicho conocimiento, sin el consentimiento expreso y escrito de la Agencia.



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: **1276948164586199148871**

#### **CLÁUSULA 11.- CALIDAD DEL SERVICIO**

Durante el periodo de ejecución del contrato, el adjudicatario propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada. No obstante, la Administración podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, la Agencia podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

#### **CLÁUSULA 12.- PLAZO DE GARANTÍA**

Se establece un plazo de garantía de **DOS 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, y debido a las particularidades propias de la elaboración de aplicativos y de la técnica de sistemas informáticos, el adjudicatario responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiera, 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 trabajo.

#### **CLÁUSULA 13.- PLAZO DE EJECUCIÓN**

El plazo de ejecución del contrato será de **DOCE MESES**, comprendidos entre el día **1 de marzo de 2020 y el 28 de febrero de 2021**.

Si en la fecha de inicio de la ejecución, los trabajos objeto del contrato no hubieran comenzado y no se pudiera contar en tal fecha con la disponibilidad del equipo necesario para la atención de los mismos, la Agencia quedará facultada para instar la **resolución** del contrato.

#### **CLÁUSULA 14.- CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS**

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones técnicas referidas a las especificaciones recogidas en el presente Pliego de Cláusulas Técnicas, los licitadores deberán remitir por correo electrónico las preguntas e información que consideren necesarias para elaborar la Propuesta Técnica.

La dirección de correo donde los licitadores deberán dirigir sus consultas o aclaraciones es la siguiente:

[madriddigital.sistemas@madrid.org](mailto:madriddigital.sistemas@madrid.org)

Así mismo los licitadores para formular sus consultas o aclaraciones, las cuales deberán realizarse en castellano, deberán cumplimentar la siguiente plantilla:



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: **1276948164586199148871**

Nº Cuestión	Cláusula / Apartado	Página	Párrafo	Descripción de la consulta
1				
2				

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con Madrid Digital, 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.

Por su parte la Agencia se compromete a responder en los términos indicados en la Cláusula 10 del Pliego de Cláusulas Administrativas Particulares.



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: **1276948164586199148871**

## ANEXO 1.- GESTIÓN DE LA SEGURIDAD

### Protección de datos personales y Privacidad

#### Normativa

Los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD), *Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)* y la normativa complementaria.

El contratista se somete expresamente a la normativa nacional y de la Unión Europea en materia de protección de datos.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

La Agencia Madrid Digital, en virtud de lo previsto en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de medidas fiscales y administrativas de la Comunidad de Madrid (BOE núm. 52, jueves 2 marzo 2006) y lo establecido en la citada Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, actuará en calidad de Encargado del Tratamiento de la Comunidad de Madrid en el ámbito de su competencia. Y como Responsable del Tratamiento para aquellos tratamientos así previsto en el registro de actividades de tratamiento ([www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos](http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos)).

#### Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento

Para el cumplimiento del objeto de este pliego, el adjudicatario deberá tratar los datos personales de los cuales Madrid Digital es Responsable o Encargado del Tratamiento de la manera que se especifica más adelante, en el apartado denominado “Tratamiento de datos personales”.

Ello conlleva que el adjudicatario actúe en calidad de Encargado del Tratamiento y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Si el adjudicatario destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerada también como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación de lo estipulado en el apartado referido al “Tratamiento de Datos Personales”, el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que Madrid Digital estuviese de acuerdo con lo solicitado emitiría un apartado referido al “Tratamiento de Datos Personales” actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario garantiza el cumplimiento de las siguientes obligaciones, complementadas con lo detallado en el apartado referido al “Tratamiento de Datos Personales:



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: **1276948164586199148871**



- a) Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Pliego o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de Madrid Digital Madrid Digital por escrito en cada momento. El adjudicatario informará inmediatamente a Madrid Digital Madrid Digital cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.
- b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato.
- c) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad, necesarias o convenientes, para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso. En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detallados en el apartado referido al "Tratamiento de Datos Personales".
- d) Mantener absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato, así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.
- e) Llevar un listado de personas del equipo prestador del servicio que están autorizadas para tratar los Datos Personales objeto de este pliego, así como los roles asignados a cada una de ellas y la relación de permisos y perfiles autorizados que son estrictamente necesarias para el desempeño de las funciones encomendadas. Garantizar que cada una de las personas del equipo prestador del servicio se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición de Madrid Digital Madrid Digital dicha documentación acreditativa.
- f) Garantizar la formación e información necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.
- g) Salvo que cuente en cada caso con la autorización expresa de Madrid Digital Madrid Digital, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.
- h) Nombrar Delegado de Protección de Datos en caso de que sea necesario según el RGPD, o alternativamente, nombrar Responsable de Seguridad del Servicio del adjudicatario a efectos de protección de los Datos Personales en calidad de responsable del cumplimiento de la regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad. Así como comunicar la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por el adjudicatario.
- i) Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, a devolver (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario por causa del tratamiento; y destruir (iii) los soportes y documentos en que cualquiera de estos datos consten cuando no tengan la consideración de entregable del servicio contratado, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. El Encargado del

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: 1276948164586199148871



Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con Madrid Digital Madrid Digital. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

- j) Según corresponda, llevar a cabo las instrucciones para el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que se especifiquen, equipamiento que podrá estar bajo el control de Madrid Digital Madrid Digital o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por Madrid Digital Madrid Digital, según se establezca en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.
- k) Salvo que se indique otra cosa en el apartado referido al “Tratamiento de Datos Personales” o se instruya así expresamente por Madrid Digital Madrid Digital, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Pliego o demás documentos contractuales, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito a Madrid Digital Madrid Digital de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a Madrid Digital Madrid Digital, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

- l) Con el objeto de dar cumplimiento al artículo 33 RGPD, comunicar a Madrid Digital para la Administración Digital de la Comunidad de Madrid, de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.
- m) Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable) ante el Encargado del Tratamiento, éste debe comunicarlo a Madrid Digital Madrid Digital con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derechos, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho. Asistirá a Madrid Digital Madrid Digital, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.
- n) Colaborar con Madrid Digital Madrid Digital en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de



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: **1276948164586199148871**

medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de riesgos e impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

Asimismo, pondrá a disposición de Madrid Digital Madrid Digital, a requerimiento de esta, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Pliego y demás documentos contractuales y colaborará en la realización de auditorías e inspecciones llevadas a cabo, en su caso, por Madrid Digital Madrid Digital.

- o) En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de Madrid Digital Madrid Digital, que contenga, al menos, las circunstancias a que se refiere dicho artículo.
- p) Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición de Madrid Digital Madrid Digital a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición de Agencia Madrid Digital toda información, certificaciones y auditorías realizadas en cada momento.
- q) Derecho de informar: El encargado del tratamiento, en el caso de realizar la recogida de los datos personales, debe facilitar a los interesados la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe aprobar por Madrid Digital Madrid Digital antes del inicio de la recogida de los datos.

La presente cláusula y las obligaciones en ella establecidas constituyen el contrato de encargo de tratamiento entre Madrid Digital Madrid Digital y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este pliego y su contrato, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este pliego no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de Madrid Digital Madrid Digital y que no esté referido en el presente pliego, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el apartado referido al "Tratamiento de Datos Personales". Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales responsabilidad de Madrid Digital Madrid Digital no contemplados en el apartado referido al "Tratamiento de Datos Personales" el adjudicatario deberá ponerlo en conocimiento de Agencia Madrid Digital, en concreto de su Delegado de Protección de Datos (Dirección de Seguridad Corporativa), con la mayor diligencia y a más tardar en el plazo de 72 horas.

#### **Obligaciones de Madrid Digital Madrid Digital para la prestación del servicio**

- a) Facilitar el acceso del encargado a los datos a los que se refiere el apartado primero del apartado referido al "Tratamiento de Datos Personales".
- b) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.



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: **1276948164586199148871**

### Sub-encargos de tratamiento asociados a Subcontrataciones

Cuando el pliego permita la subcontratación de actividades objeto del servicio contratado, y en caso de que el adjudicatario pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario lo pondrá en conocimiento previo de Madrid Digital Madrid Digital, identificando qué tratamiento de datos personales conlleva, para que Madrid Digital Madrid Digital decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a Madrid Digital Madrid Digital la decisión de si otorgar, o no, dicho consentimiento):

- a) Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones de Madrid Digital Madrid Digital.
- b) Que el adjudicatario y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente pliego, el cual será puesto a disposición de Madrid Digital Madrid Digital a su mera solicitud para verificar su existencia y contenido.

El adjudicatario informará a Madrid Digital Madrid Digital de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así a Madrid Digital Madrid Digital la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta de Madrid Digital Madrid Digital a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

### Tratamiento de datos personales

Madrid Digital solo autorizará al adjudicatario a acceder a datos de carácter personal en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, en cuyo caso el adjudicatario asumirá la condición de encargado de tratamiento conforme al artículo 28 del Reglamento General de Protección de Datos, con las obligaciones que lleva aparejadas.

Salvo autorización expresa y por escrito de Madrid Digital, el adjudicatario tendrá prohibido el acceso a los datos personales que se conserven en cada una de las dependencias o sistemas a cuyo interior o contenido deba de acceder. En consecuencia, el adjudicatario habrá de impartir las instrucciones oportunas a su personal para que éste se abstenga de examinar el contenido de los documentos que, en soporte informático, en soporte papel o en cualquier otro tipo de soporte, se encuentre en el interior de las dependencias o sistemas en los que desarrollen sus actividades.

Las actividades de tratamiento a las que pudiera tener acceso el adjudicatario, en aquellos supuestos en que resulte imprescindible para la ejecución del contrato, se encuentran enmarcadas por la norma de la Comunidad de Madrid relativa a las funciones y competencias del Responsable del Tratamiento, así como lo recogido en el Registro de Actividades de Tratamiento publicado en [www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos](http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos).

En concreto, el Encargado de Tratamiento realizará los siguientes tratamientos en el marco de dicha prestación de servicios: Recogida, Registro, Consulta, Modificación, Supresión, Conservación, Destrucción, Difusión intranet/internet, Transmisión por redes públicas/privadas.

### Deber de Información

Los datos de carácter personal del adjudicatario serán tratados por Madrid Digital Madrid Digital para ser incorporados al sistema de tratamiento "Gestión de los expedientes de adquisición y contratación",



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: **1276948164586199148871**

cuya finalidad es la gestión administrativa de los expedientes de contratación de Madrid Digital y la gestión administrativa de los pedidos a los proveedores de adquisición de bienes y servicios.

Finalidad necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Los datos de carácter personal podrán ser comunicados a Unidades Administrativas encargadas de su tramitación, Boletines oficiales, Intervención General o la Cámara de Cuentas.

Se conservarán durante el tiempo que es necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran de dicha finalidad y del tratamiento de los datos.

Los derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, se pueden ejercitar ante Madrid Digital Madrid Digital, C/Embajadores, 181, 28045 - Madrid o en la dirección de correo electrónico [protecciondatosmadriddigital@madrid.org](mailto:protecciondatosmadriddigital@madrid.org).

Asimismo, los datos del personal del adjudicatario, así como de sus empresas contratistas, si las hubiere, serán tratados por Madrid Digital cuando sea necesario para dar cobertura a la realización de los trabajos objeto del contrato. Su tratamiento quedará incorporado al registro de actividades de tratamiento de Madrid Digital. Estos datos personales podrán ser comunicados a usuarios y clientes de Madrid Digital cuando así lo requiera la prestación del servicio y se conservarán durante el tiempo que sea necesario para cumplir con la finalidad para la que se recabaron.

## **Seguridad en la utilización de medios electrónicos**

### **Normativa**

El adjudicatario está obligado al cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad, ENS, (Real Decreto 3/2010 de 8 enero) en lo referido a la adopción de medidas de seguridad de las soluciones tecnológicas o la prestación de servicios ofertados.

El adjudicatario deberá concienciar regularmente al personal 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 en aquellas materias que requieran para el desempeño de sus funciones, en cuanto al servicio prestado.

### **Conformidad con el Esquema Nacional de Seguridad**

La Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, determina que cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad según corresponda.

Por ello, Madrid Digital podrá solicitar en todo momento al adjudicatario los correspondientes informes de Autoevaluación o Auditoría, al objeto de verificar la adecuación e idoneidad de lo manifestado en las Declaraciones o Certificados de Conformidad, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de contrato.



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: **1276948164586199148871**

## Medidas de Seguridad

### Documentación de seguridad

El adjudicatario deberá poseer al inicio de la prestación de los servicios, los siguientes documentos, los cuales deberán estar permanentemente actualizados y a disposición de Madrid Digital a lo largo 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 y redactado de forma sencilla, precisa y comprensible.
- b) Un documento denominado “Documento de Seguridad” coherente con los hitos y medidas de seguridad que se exigen en la presente cláusula y que recoja la información estructurada y ordenada de forma que describa la relación de las medidas de seguridad propuestas por el adjudicatario para dar respuesta a lo contenido en el presente pliego y que acredite la forma en la que se procederá al cumplimiento de las mismas. Asimismo, deberá, identificar las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio y del Delegado de Protección de Datos del adjudicatario.

### Confidencialidad y deber de secreto

El adjudicatario se compromete de forma específica a tratar como confidencial toda aquella información responsabilidad de Madrid Digital a la que pueda tener acceso, con motivo de la prestación de sus servicios y se compromete a que dichos datos permanezcan secretos incluso después de finalizado el presente Acuerdo.

Debiendo el adjudicatario mantener dicha información en reserva y secreto y no revelarla de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.

A estos efectos, el adjudicatario se compromete a tomar, respecto de sus empleados o colaboradores, las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como encargado de tratamiento y que, en consecuencia, deben respetar, así como a garantizar que los datos personales que conozcan en virtud de la prestación del servicio permanecen secretos incluso después de finalizado el presente Acuerdo por cualquier causa.

Dicha obligación de información a los empleados y colaboradores del adjudicatario se llevará a cabo de modo tal que permita la documentación y puesta a disposición de Madrid Digital del cumplimiento de aquella obligación.

*La Directora de Producción y Gestión de Infraestructuras*

*Fdo. : Julia Molina Franquelo*