

Pliego de Cláusulas Técnicas

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
mediante el siguiente código seguro de verificación: **1056380162805469598525**



PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIO DENOMINADO **“MANTENIMIENTO DE LAS SOLUCIONES DE SEGURIDAD DE ANTIVIRUS PARA SISTEMAS DE ALMACENAMIENTO NAS, EXISTENTES EN LA COMUNIDAD DE MADRID”**, A CELEBRAR MEDIANTE PROCEDIMIENTO SIMPLIFICADO ORDINARIO CON CRITERIO PRECIO

INDICE

CLÁUSULA 1.- INTRODUCCIÓN	3
CLÁUSULA 2.- OBJETO	4
CLÁUSULA 3.- ALCANCE	4
CLÁUSULA 4.- DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE	4
CLÁUSULA 5.- SERVICIO DE MANTENIMIENTO	4
CLÁUSULA 6.- SERVICIO DE SOPORTE.....	5
CLÁUSULA 7.- CONDICIONES ADICIONALES A CUMPLIR.....	9
CLÁUSULA 8.- MEDIDAS DE SEGURIDAD Y COMPROMISOS DEL ADJUDICATARIO EN EL CASO DE ACCESO REMOTO A INFRAESTRUCTURAS DE LA AGENCIA	10
CLÁUSULA 9.- SEGUIMIENTO Y CONTROL DE LOS SERVICIOS	11
CLÁUSULA 10.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	12
CLÁUSULA 11.- PROPIEDAD DE LOS TRABAJOS.....	16
CLÁUSULA 12.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA.	17
CLÁUSULA 13.- CALIDAD DEL SERVICIO	17
CLÁUSULA 14.- PLAZO DE GARANTÍA.....	17
CLÁUSULA 15.- PLAZO DE EJECUCIÓN	17
CLÁUSULA 16.- CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS	18



CLÁUSULA 1.- INTRODUCCIÓN

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

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

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

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*.

Asimismo, además de las precitadas funciones, la Agencia tiene encomendada la planificación técnica y la formación del personal de la Comunidad de Madrid en la utilización de los productos y del equipo lógico integrado en materia de informática y comunicaciones; y la de su propio personal, para el adecuado cumplimiento de los fines de la Agencia (*Artículo 10 - Tres - h*).

Entre 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 contar con el servicio de mantenimiento de esta solución, objeto de este Pliego de Cláusulas Técnicas.



CLÁUSULA 2.- OBJETO

La prestación del servicio de **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.

CLÁUSULA 3.- ALCANCE

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

El detalle de los productos instalados es el siguiente:

SOLUCIONES DE SEGURIDAD ANTIVIRUS PARA NAS SOBRE LOS PRODUCTOS
Trend Micro™ ServerProtect™ for NetApp
Trend Micro Control Manager Advanced
15.001 usuarios concurrentes

CLÁUSULA 4.- 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 15.001 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 5.- 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 6.- 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:** 24x7 asociado al Soporte Avanzado denominado “Gold Premium Support”, detallado más adelante.
El adjudicatario pondrá a disposición de la Agencia un **número de teléfono** para realizar cualquier consulta, que será atendido en lenguaje **castellano** por expertos del producto, 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 define “*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 se realizará 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.

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.

- **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, 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 (cuota variable) constará de un **máximo de 250** horas 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.

- **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 “*Gold 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 quedará cerrado hasta que la Agencia de 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.
 - **Visitas in situ e intervenciones remotas** si la Agencia lo permite.
 - **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.

CLÁUSULA 7.- CONDICIONES ADICIONALES A CUMPLIR
--

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.

Asimismo, en el plazo fijado en la Cláusula 14 del Pliego de Cláusulas Jurídicas, 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 “Gold 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.

Con carácter previo a la adjudicación del contrato, la empresa propuesta como adjudicataria aportará **Curriculum Vitae** del **Responsable del Servicio**, especificando la cualificación profesional del mismo (con detalle de perfil técnico, titulación, formación y experiencia), así como toda aquella documentación que la Agencia estime necesaria para la acreditación de los datos contenidos en dicho Currículum.

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 la **Cláusula 19 “Dirección de los trabajos”** del Pliego de Cláusulas Jurídicas.



El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que en cada fase del mismo 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 Administración de la Comunidad de Madrid.

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

CLÁUSULA 8.- MEDIDAS DE SEGURIDAD Y COMPROMISOS DEL ADJUDICATARIO EN EL CASO DE ACCESO REMOTO A INFRAESTRUCTURAS DE LA AGENCIA

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.
- 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 9.- 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 bimestrales 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 10.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Normativa aplicable.

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

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

Medidas de seguridad de carácter mínimo.

1. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el RD 1720/2007 respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (Artículo 9.2. LOPD):
 - 1.1. En la fase de diseño funcional del sistema de referencia se realizará un estudio previo de datos de carácter personal a tratar, su naturaleza y las medidas de seguridad que requieran de conformidad con la naturaleza de los datos y los requerimientos del RD 1720/2007. Si procede igualmente se propondrá la correspondiente creación e inscripción en la Agencia Española de Protección de Datos (en adelante 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 la Agencia, y en concreto:
 - 1.2.1. Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
 - 1.2.2. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. El adjudicatario se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
 - 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. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por la Agencia.

- 1.2.4. 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.
 - 1.2.5. 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.
 - 1.2.6. Solo con el consentimiento expreso y escrito de la Agencia, el equipo prestador del servicio objeto del contrato tendrá acceso y tratará datos de carácter personal contenidos o soportados en los equipos o recursos mantenidos.
 - 1.2.7. Deberán realizarse, como mínimo semanalmente, copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
 - 1.2.8. 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.
 - 1.2.9. 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.
 - 1.2.10. 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 la Agencia podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.
- 1.3.3. Será necesaria la autorización de la Agencia para la ejecución de los procedimientos de recuperación de los datos.
- 1.4. Además de las medidas enumeradas en los anteriores apartados 2.1, 2.2 y 2.3, 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 fines policiales; o aquéllos que contengan datos derivados de actos de violencia de género, deberán observar las siguientes medidas:
 - 1.4.1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control de la Agencia.
 - 1.4.2. Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en la normativa de protección de datos personales, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.
 - 1.4.3. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
 - 1.4.4. El período mínimo de conservación de los datos registrados será de dos años. El adjudicatario 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.

Personal prestador del servicio.

2. Quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal firmarán un documento por el que quedarán obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar la relación contractual. Así como a la renuncia expresa de los derechos de propiedad intelectual que les pudiera corresponder y compromiso del cumplimiento de las obligaciones de protección de datos de carácter personal.

El adjudicatario nombrará de entre los miembros del equipo prestador del servicio a un Responsable de Seguridad, que se encargará de la puesta en práctica y de la inspección de las medidas de seguridad, informando de su nombre y puesto a la Agencia.

El adjudicatario se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanen, para lo cual programará las acciones formativas necesarias.

El personal prestador del objeto del contrato tendrá acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

Cesión o comunicación de datos a terceros.

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

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

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

En el caso de que el adjudicatario 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.

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

La contratación de las funciones propias del Encargado del Tratamiento de datos de carácter personal, será realizada de conformidad con lo dispuesto en el Artículo 21 RD 1720/2007, y 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 adjudicatario como encargado del tratamiento de datos personales. Sin perjuicio de las instrucciones que, adicionalmente, pudieran establecerse por el Encargado del Tratamiento, el adjudicatario queda sujeto en el tratamiento de datos personales a las instrucciones procedentes del Responsable del Fichero.

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

Derecho de información en la recogida de datos.

6. Los datos personales recogidos podrán ser incorporados y tratados en el fichero PROVEEDORES, cuya finalidad es la solicitud de ofertas, selección y compra de bienes y servicios requeridos tanto por la Agencia como por la C.M., inscrito en el Registro General de Protección de Datos de la AEPD (www.agpd.es), y no podrán ser cedidos salvo en los supuestos previstos en la Ley. El responsable del fichero es la Agencia, 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.

CLÁUSULA 11.- 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 12.- 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.

CLÁUSULA 13.- 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 14.- 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 15.- PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **DOCE MESES**, desde el 1 de marzo de 2018 hasta el 28 de febrero de 2019.

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 16.- 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.

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

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:

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

ELABORADO Y PROPUESTO POR:
La Directora de Producción y Gestión de Infraestructuras

Fdo.: Julia Molina Franquelo

APROBADO POR:
El Consejero Delegado de la Agencia para la Administración Digital de la C.M.

Fdo.: Blas Labrador Román



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1056380162805469598525**