

Pliego de Prescripciones Técnicas

**“DISEÑO, MANTENIMIENTO, SOPORTE TÉCNICO Y
ADQUISICIÓN DE SOLUCIONES DE SEGURIDAD
ANTIMALWARE PANDA, INSTALADAS EN LOS
DIFERENTES PUESTOS Y SERVIDORES WINDOWS
EXISTENTES EN LOS CENTROS DEPENDIENTES DE
LA COMUNIDAD DE MADRID”**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1259294353114119598927**



PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SERVICIOS DENOMINADO “DISEÑO, MANTENIMIENTO, SOPORTE TÉCNICO Y ADQUISICIÓN DE SOLUCIONES DE SEGURIDAD ANTIMALWARE PANDA, INSTALADAS EN LOS DIFERENTES PUESTOS Y SERVIDORES WINDOWS EXISTENTES EN LOS CENTROS DEPENDIENTES DE LA COMUNIDAD DE MADRID” A ADJUDICAR POR PROCEDIMIENTO NEGOCIADO SIN PUBLICIDAD.

CONTENIDO

CLÁUSULA 1.- INTRODUCCIÓN.....	4
CLÁUSULA 2.- OBJETO	4
CLÁUSULA 3.- ALCANCE	4
CLÁUSULA 4.- DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE	5
CLÁUSULA 5.- DESCRIPCIÓN DE LOS SERVICIOS Y SUMINISTRO DE LICENCIAS	6
5.1 Servicio de mantenimiento, soporte y actualización	6
5.1.1 Notificación de incidencias	6
5.1.2 Tipificación de incidencias y niveles de servicio.	6
5.1.3 Soporte presencial	8
5.1.4 Seguimiento y resolución de incidencias	9
5.2 Servicio de Soporte Premium	9
5.3 Servicio de técnicos especialistas On Site	10
5.4 CYTOMIC Threat Hunting Service 8x5 (Pool de Threat Hunters).....	12
5.5 Adquisición de licencias	13
CLÁUSULA 6.- EQUIPO PRESTADOR DEL SERVICIO ON-SITE	14
6.1 Técnicos especialistas en seguridad de productos panda	14
6.2 Verificación de la capacidad de los componentes del equipo adscrito a la ejecución del contrato, sustitución de los componentes de dicho equipo y seguimiento y control de los trabajos.	16
CLÁUSULA 7.- REQUISITOS DERIVADOS DE LA PRESTACIÓN DE LOS SERVICIOS	18
7.1 Ámbito de ejecución	18
7.2 Servicio de soporte on site: horas de servicio y horario de prestación	18
7.3 Documentación	18
CLÁUSULA 8.- CONDICIONES ADICIONALES A CUMPLIR	18
CLÁUSULA 9.- SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO	19
CLÁUSULA 10.- PLAZO DE GARANTÍA.....	19
CLÁUSULA 11.- GESTIÓN DE LA SEGURIDAD	20
11.1 Protección de datos personales y Privacidad	20
11.1.1 Normativa	20
11.1.2 Obligaciones del Adjudicatario en calidad de Encargado del Tratamiento.....	20



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

11.1.3	Obligaciones de la Agencia Madrid Digital para la prestación del servicio.....	24
11.1.4	Sub-encargos de tratamiento asociados a Subcontrataciones	24
11.1.5	Tratamiento de datos personales.....	24
11.2	Deber de Información.....	25
11.3	Seguridad en la utilización de medios electrónicos	25
11.3.1	Normativa	25
11.3.2	Conformidad con el Esquema Nacional de Seguridad	25
11.4	Medidas de Seguridad	26
11.4.1	Documentación de seguridad	26
11.4.2	Confidencialidad y deber de secreto.....	26
CLÁUSULA 12.-	PROPIEDAD DE LOS TRABAJOS	26
CLÁUSULA 13.-	DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS.....	27
CLÁUSULA 14.-	CALIDAD DEL SERVICIO	27
CLÁUSULA 15.-	PLAZO DE EJECUCIÓN.....	27
CLÁUSULA 16.-	PENALIDADES	27
CLÁUSULA 17.-	CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS	28
ANEXO I: PENALIDADES		29

CLÁUSULA 1.- INTRODUCCIÓN

La **Agencia para la Administración Digital de la Comunidad de Madrid**, según se establece 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, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente la seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad (*Artículo 10, Tres*)

Dentro de las soluciones de protección antimalware que esta Agencia para la Administración Digital de la Comunidad de Madrid, en adelante **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 1997 de la solución de antimalware PANDA, como solución de seguridad corporativa para puestos y servidores Windows.

Para garantizar la operatividad y disponibilidad de este servicio se requiere la actualización periódica de la información de firmas de malware empleada en la detección local de ataques, así como servicios de análisis on-line prestados por proveedores especializados y soporte técnico experto para contención de ataques, por lo que se considera necesario continuar con los servicios de mantenimiento y soporte de esta solución, para lo que es necesario realizar esta contratación.

CLÁUSULA 2.- OBJETO

La prestación de los servicios de mantenimiento y actualización de licencias, soporte técnico avanzado y especializado, servicio de "Threat Hunting", "caza de amenazas" de las soluciones de seguridad (Antimalware Panda), instaladas en puestos y servidores Windows en centros dependientes de la Comunidad de Madrid, y la adquisición de nuevas licencias del producto durante la vigencia del contrato.

CLÁUSULA 3.- ALCANCE

Los servicios demandados serán los siguientes:

- **El mantenimiento, soporte y actualización** de las distintas versiones de software de antimalware Panda disponibles en la Comunidad de Madrid de los productos:
 - **Panda Endpoint Protection Plus**, que incluye licencias para puestos de usuario (PC's de sobremesa y portátiles), servidores Windows y servidores de correo Exchange,
 - **Panda Adaptive Defense**, que incluye licencias para puestos de usuario con seguridad especial.

Las versiones de los productos de antimalware Panda Endpoint Protección plus y Panda Adaptive Defense, se unifican y pasan a denominarse **Cytomic EPDR (Endpoint Protection Detection Response)**.

- **Soporte técnico Premium**, que permita realizar consultas sobre los productos Panda objeto de mantenimiento y contar con tiempos de respuesta máximos para resolver las infecciones de malware de la forma más rápida y eficiente posible.



- **Soporte Técnico especializado On-Site**, con localización 24x7 los 365 días del año, que incluirá el conjunto de tareas necesarias para la implantación, mantenimiento y puesta en producción de los servicios de seguridad Panda, así como la monitorización, la gestión de incidentes de seguridad en la base instalada y su resolución mediante la mecanización y automatización de tareas. Este soporte técnico dispondrá de las herramientas de detección y desinfección de malware necesarias para el servicio.
- **Cytoxic Threat Hunting (“caza de amenazas”) Service**, servicios de búsqueda proactiva de nuevas amenazas avanzadas y las TTPs (tácticas, técnicas y procedimientos) que usan los atacantes en sus reconocimientos y ataques, a través del análisis de la información generada por los puestos, pcs y servidores.
- **Adquisición con garantía de nuevas licencias de productos**, a demanda de la Agencia durante el periodo de vigencia del contrato, que permita incorporar la solución de seguridad de forma homogénea en situaciones de crecimiento de la planta instalada en la Comunidad de Madrid.

El servicio se prestará bajo la dirección y supervisión directa del Responsable del Contrato que la Agencia designe.

El conjunto de las actividades a realizar, para garantizar un nivel de calidad adecuado, deberá ser ejecutado, finalizado y verificado en tiempo y forma según la normativa procedimental establecida por la Agencia, utilizando para ello las herramientas que determine el Responsable del Contrato.

CLÁUSULA 4.- DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE

El entorno ofimático de la Comunidad de Madrid consta de aproximadamente 2.300 Servidores Windows (en versiones 2012, 2016, 2019), 32 servidores de correo Exchange, 82.719 pcs, puestos de usuarios Windows y 2.700 portátiles, distribuidos en más de 4.000 sedes.

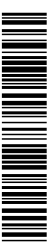
Una vez iniciada la ejecución del contrato, el adjudicatario deberá mantener y actualizar las licencias actuales, que a continuación se describen:

DESCRIPCIÓN	UDS.
Licencias: Cytomic EPDR	87.751

Los equipos se protegen mediante el software de antimalware Panda, existiendo una infraestructura de servidores en la nube, para realizar las actualizaciones de los ficheros de firmas, y la gestión de seguridad de los puestos y servidores Windows.

Todos los puestos de usuario están homologados y estandarizados mediante imágenes denominadas **POBs**, puesto ofimático básico, que contiene los programas de software y la configuración definida como estándar para los usuarios de la Comunidad de Madrid. La mayoría de los equipos disponen de Microsoft Windows 8.1 y Windows 10 como sistema operativo.

La gestión centralizada de estos equipos se realiza mediante Microsoft System Center y políticas de Directorio Activo, así como las consolas de administración propias de Panda.



CLÁUSULA 5.- DESCRIPCIÓN DE LOS SERVICIOS Y SUMINISTRO DE LICENCIAS

5.1 Servicio de mantenimiento, soporte y actualización

El adjudicatario deberá realizar los trabajos necesarios para la resolución de los problemas técnicos que puedan surgir durante el plazo de ejecución del contrato, comprometiéndose a tener actualizada y a disposición de la Agencia una lista completa de los productos bajo soporte y el nivel de servicio.

A continuación, se detalla el nivel de servicio que deberá cumplir el adjudicatario dependiendo de la criticidad de dichos incidentes.

5.1.1 Notificación de incidencias

Al notificar una incidencia, la Agencia tendrá **acceso preferente a los ingenieros de soporte** del adjudicatario. Como sistema preferente de notificación de incidencias, el adjudicatario pondrá a disposición un **número de teléfono** de soporte técnico durante **24 horas al día / 7 días a la semana**. Las incidencias también se podrán notificar electrónicamente, en el mismo horario, a través de un **sitio Web exclusivo**.

Para supuestos de **incidencias críticas, altas o medias**, los técnicos designados por la Agencia, dispondrán de un número de teléfono móvil en el que podrán contactar directamente con el Responsable designado por el adjudicatario.

Antes de que el adjudicatario proporcione soporte en un incidente, 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. Un incidente puede requerir la realización de múltiples llamadas telefónicas, así como trabajo de investigación fuera de línea para alcanzar la solución final.

- **Diagnóstico Remoto.** A petición de la Agencia, el adjudicatario podrá acceder a los sistemas de ésta remotamente para analizar problemas. Este acceso se efectuará exclusivamente con el consentimiento de la Agencia, y el personal del adjudicatario accederá exclusivamente a los sistemas autorizados por ésta. El adjudicatario deberá proporcionar a la Agencia software para asistirle en el diagnóstico y/o resolución del problema.
- **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 Panda impliquen 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.

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 contratista a la ejecución de los trabajos.

5.1.2 Tipificación de incidencias y niveles de servicio.

Las incidencias se tipifican según su **impacto** en el servicio en:

- **Impacto Alto:** Indisponibilidad de los puestos de trabajo y los servidores Windows. Es el caso de mayor criticidad que puede tener una incidencia.

Síntomas: Servicio afectado para más del 15% de usuarios.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

- **Impacto Medio:** Problema con alguna funcionalidad de los puestos de trabajo y los servidores Windows que no suponga la inoperatividad de los mismos.

Síntomas: Servicio afectado entre un 2% y el 15% de usuarios.

- **Impacto Bajo:** Problemas con alguna funcionalidad de los puestos de trabajo y los servidores Windows sin impacto en los mismos.

Para cualquier incidencia que no se encuentre dentro de las especificadas anteriormente se describe este síntoma: Servicio afectado para menos del 2% de usuarios.

Asimismo, las incidencias se clasifican según la **urgencia** en:

- **Urgencia Alta:**
 - Departamentos, centros y servicios considerados como críticos dentro de la Comunidad de Madrid (Por ejemplo, los servicios de Emergencias, Urgencias, 112, etc.).
 - Todos los Hospitales de la Comunidad de Madrid, bajo el ámbito de gestión de la Agencia.
 - Algunos proyectos requieren de la disponibilidad del servicio durante alguna de sus fases, y la incidencia en el mismo determina que las incidencias sean calificadas como críticas.
 - Cuando las incidencias afecten al grupo de altos cargos y personal relacionado con los mismos.
- **Urgencia Media:**
 - Todos los servidores Windows, a excepción de los descritos en los sistemas del apartado anterior.
- **Urgencia Baja:**
 - Los puestos de trabajo de los usuarios de la Comunidad de Madrid, a excepción de los mencionados en los apartados anteriores.

Tabla de Prioridades: Será responsabilidad de la Agencia calificar la incidencia que se produzca de acuerdo con la siguiente tipología, notificándolo al adjudicatario para que proceda al efecto.

La prioridad de una incidencia se establecerá combinando el Impacto y la Urgencia y se aplicarán los criterios establecidos en la siguiente tabla:

PRIORIDAD		IMPACTO		
		Alto	Medio	Bajo
URGENCIA	Alta	CRÍTICA	ALTA	MEDIA
	Media	ALTA	MEDIA	BAJA
	Baja	MEDIA	BAJA	BAJA

Tiempos de respuesta de incidencias: El tiempo de respuesta se define como el tiempo transcurrido entre el momento en que se notifica la incidencia y el momento en 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.

Los tiempos de respuesta se detallan en la tabla siguiente:

PRIORIDAD	Tiempo Máximo de Respuesta
CRÍTICA	4 horas
ALTA	4 horas
MEDIA	5 horas
BAJA	6 horas

Nota: Para el cómputo de los tiempos máximos de respuesta se tendrá en cuenta todos los días naturales.

5.1.3 Soporte presencial

La determinación del tipo de soporte necesario en cada incidencia se llevará a cabo en función de la prioridad, teniendo la Agencia la posibilidad de exigir soporte presencial al adjudicatario en las incidencias tipificadas como críticas, altas o medias.

El adjudicatario deberá garantizar el soporte presencial de un Ingeniero de Soporte en las instalaciones de la Comunidad de Madrid, si se produce una incidencia tipificada como crítica, alta o media. El horario de atención de este tipo de incidencias será de 24 horas, 7 días a la semana los 365 días del año.

El **tiempo máximo de soporte presencial**, en el que el Ingeniero se presentará en las instalaciones de la Comunidad de Madrid, dependiendo del horario en el que se notifique la incidencia, será el siguiente:

- **De lunes a viernes desde las 8:00 h. hasta las 22:00 h.:** 1 hora para las incidencias críticas y altas, y 2 horas para las incidencias de prioridad media.
- **De lunes a viernes desde las 22:00 h. hasta las 8:00 h. del día siguiente, fines de semana y festivos:** 2 horas para incidencias críticas y 3 horas para el resto, según se describe en la tabla adjunta.

En función del servicio descrito y tipificado por nivel de prioridad, el adjudicatario deberá disponer de los medios técnicos y humanos necesarios para garantizar el soporte, tanto presencial como telefónico, a fin de cumplir con los niveles de servicio exigidos.

En el precio del contrato quedan incluidos, en todo caso, los gastos ocasionados para solucionar las incidencias, tales como mano de obra, gastos de desplazamiento y transporte, impuestos, etc.

PRIORIDAD	Tiempo de Soporte Presencial	
	Lunes a viernes de 8:00 h. a 22:00 h.	Lunes a viernes de 22:00 h. a 8:00 h., fin de semana y festivos
CRÍTICA	1 hora	2 horas
ALTA	1 hora	3 horas
MEDIA	2 horas	3 horas
BAJA	N/A	N/A



5.1.4 Seguimiento y resolución de incidencias

El adjudicatario informará del orden de las actuaciones a seguir para asegurar la resolución de las incidencias, según los niveles de servicio establecidos en el presente Pliego de Cláusulas Técnicas.

Los técnicos de la Agencia estarán permanentemente informados del estado de la incidencia. Una vez resuelta la incidencia, se documentará e informará con el objeto de verificar la calidad de la solución.

Periódicamente, el responsable técnico designado por el adjudicatario, generará un informe 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.

Se emplearán los sistemas y procesos establecidos en la Agencia para el registro, seguimiento, gestión y resolución de las incidencias.

5.2 Servicio de Soporte Premium

El servicio de soporte de productos Panda, tiene por objeto establecer el mantenimiento y la asistencia técnica que permita asegurar el correcto funcionamiento de todos los programas Panda objeto del contrato, actualmente instalados en todos los puestos y servidores de la Comunidad de Madrid.

El objetivo que se persigue con este servicio es garantizar la disponibilidad y acceso de los distintos equipos de la Comunidad de Madrid a los servidores que disponen de las actualizaciones tanto del motor, como de los ficheros de firmas, de manera que se optimicen los recursos de la red y se mantengan actualizados todos los puestos diariamente de manera rápida y fiable.

A continuación, se describe las condiciones que definen el servicio de soporte Premium:

- **Servicio de soporte técnico personal 24 horas al día 365 días al año.** Servicio de atención al cliente, atendido por expertos del producto a través de teléfono, para la resolución de cualquier consulta o incidencia relacionada con la detección de virus o con la configuración del producto, 24 horas al día los 365 días al año.
- **Soporte técnico preferente.** Vía de comunicación exclusiva para contactar con el departamento de soporte Premium. Para atender estas consultas de forma preferente, se registrarán las personas de la Agencia para la Administración Digital de la Comunidad de Madrid, que serán las autorizadas para utilizar estas vías de comunicación exclusivas.
- **Servicio de soporte telefónico VIP,** consultor técnico en soporte, identificado como responsable de la resolución de las incidencias, y con preferencia en el soporte frente a otros clientes. La resolución de las incidencias será responsabilidad del técnico asignado durante todo el “ciclo de vida de la incidencia”.
- **Actualización del fichero de firmas (Intelligent Updates).** Acceso a las actualizaciones del fichero de firmas de virus a través de internet. El contratista se compromete a actualizar TODOS



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

LOS DÍAS el fichero con las nuevas detecciones de virus, así como las rutinas de desinfección que se incorporan al fichero de firmas de forma incremental.

- **Acceso a las mejoras de producto (Intelligent Upgrades).** Acceso a las mejoras del software antimalware a través de internet. Uso de las herramientas del contratista para permitir el despliegue de nuevas versiones del motor de antimalware en la red corporativa con un mínimo uso de los recursos de comunicaciones.
- **Generación de herramientas de desinfección especiales** específicas, para todo el malware detectado, que permitan eliminar la amenaza, y restaurar los equipos para dejarlos operativos, minimizando el coste de despliegue y de reparación ante una infección.

5.3 Servicio de técnicos especialistas On Site

La figura de los **Técnicos Especialistas en Seguridad** destacados en la Agencia facilitará las labores de coordinación y resolución eficiente de problemas, así como el seguimiento, planificación de las actuaciones y el mantenimiento de las infraestructuras.

El trabajo de estos especialistas en seguridad consistirá en la realización de todas las actividades asociadas al mantenimiento preventivo, correctivo (descrito en el apartado anterior) y evolutivo:

- **Mantenimiento preventivo:** Consistirá en la realización de una serie de revisiones a nuestros sistemas para determinar la salud y el estado de nuestra infraestructura. Se plantearán planes de acción y acciones correctoras, así como guías de buenas prácticas para operar y mantener la infraestructura y el servicio de forma eficiente.
- **Mantenimiento correctivo:** Tratamiento especializado de incidentes y problemas, así como de puesta en práctica de soluciones en el menor tiempo posible.
- **Mantenimiento evolutivo:** Adecuación de las infraestructuras de seguridad para atender las nuevas sedes, traslados, etc. Así como la actualización de nuevas versiones de producto y su implantación en los equipos de la Comunidad de Madrid.

A continuación, se describen algunas de las actividades más significativas:

- **Mantenimiento de la infraestructura del servicio de antimalware Panda:** El objetivo que se persigue con el mantenimiento de este servicio es garantizar la disponibilidad y acceso de los distintos equipos de la Comunidad de Madrid a los servidores que disponen de las actualizaciones tanto del motor, como de los ficheros de firmas, de manera que se optimicen los recursos de la red y se mantengan actualizados todos los puestos diariamente de manera rápida y fiable. Para ello, será necesario realizar las siguientes tareas:
 - **Certificación de nuevas versiones:** Certificación de las nuevas versiones de producto conforme a los procedimientos establecidos, realizando las pruebas en entornos restringidos de laboratorio, validando el plan de pruebas en las distintas plataformas hardware y software de puestos homologados.
 - **Elaboración de paquetes de nuevas versiones:** Elaboración de los paquetes de software para distribuirlos a través de Microsoft System Center, plan de pruebas para validar su distribución en las distintas plataformas de hardware y de las versiones de software de los puestos de la Comunidad de Madrid, y colaboración en la distribución en las fases de despliegue del piloto y su puesta en producción.
 - **Definición de procedimientos manuales:** Elaboración de los procedimientos manuales de instalación y configuración para aquellos equipos que no se pueda automatizar su instalación.



- **Elaboración de los Informes y documentación:** Elaboración de informes y la documentación relativa a los procedimientos operativos para la gestión del software de antimalware, así como del seguimiento de las incidencias en el servicio, etc.
- **Extensión del servicio de mantenimiento y soporte técnico a los nuevos centros de la Comunidad de Madrid:** El objetivo que se persigue es dotar a los nuevos centros de la Comunidad de Madrid de los servicios de seguridad de antimalware, con la solución corporativa que mejor se adapte a sus necesidades. Para ello, será el adjudicatario el que deberá realizar las siguientes tareas:
 - **Instalación del antimalware en los servidores:** Instalación y configuración de los servicios de Panda en los servidores Windows de los nuevos centros, conforme a los procedimientos establecidos.
 - **Adecuación de los puestos e instalación del cliente:** Instalación y configuración del cliente de antimalware en los puestos de los nuevos centros, conforme a los procedimientos establecidos.
 - **Implantación de procedimientos operativos:** Colaboración en la elaboración de la documentación de implantación, revisión y mantenimiento de los procedimientos para prestar los servicios de seguridad de antimalware de puestos y las actividades formativas necesarias para la difusión de los procedimientos operativos.
- **Mantenimiento de la base instalada:** El objetivo que se persigue es la realización de las labores de administración del entorno de seguridad ofimático descrito con anterioridad, dichas tareas serán asignadas y planificadas por el jefe de proyecto, entre ellas podemos destacar:
 - Tareas asociadas al mantenimiento correctivo y evolutivo de los sistemas de antimalware ofimáticos.
 - Seguimiento y atención a las incidencias de seguridad.
 - Colaboración en la solución de incidencias, su documentación, y publicación conforme a los procedimientos establecidos.
 - Colaboración en el despliegue y seguimiento en la distribución del software de antimalware en los puestos de la Comunidad de Madrid.
 - Generación de procedimientos, documentación, pruebas, e implantación en el entorno de producción.
 - Elaboración de paquetes y distribución de parches críticos de seguridad, cambios de configuración, y utilidades de desinfección en los equipos de la Comunidad de Madrid.
 - Seguimiento y control de la base instalada.
 - Elaboración y generación de informes de la base instalada.
- **Mecanización y automatización de tareas:** Elaboración, prueba, e implantación de la automatización de tareas y la mecanización de procedimientos que permitan su implementación a través de directivas de Directorio Activo de Microsoft, así como de paquetes de Microsoft SMS que permitan la configuración y adaptación de los puestos conforme a los procedimientos establecidos.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

- **Incidentes de Ciberseguridad:** El equipo del adjudicatario colaborará de forma activa en la respuesta a cyber-amenazas e Incidentes de seguridad dentro del proceso de Respuesta a Incidentes de la Agencia, entre ellas podemos destacar:
 - Monitorización del cumplimiento de las políticas de seguridad establecidas por la Agencia e informar de las deficiencias identificadas.
 - Notificación y elaboración de informes de comportamientos anómalos detectados.
 - Gestión de los Indicadores de Ataques (IoA) notificados por el servicio de Threat hunting y canalizarlos a los equipos internos de la Agencia para su investigación y resolución de los mismos.
 - Definición de informes donde se vea el alineamiento con las métricas de seguridad establecidas por la Agencia.
 - Establecimiento de métricas para poder medir la mejora de la seguridad dentro de los informes a presentar a la Agencia en las reuniones de seguimiento trimestrales.
 - Mantenimiento del historial de incidentes de seguridad y de las incidencias de los distintos productos contratados.
 - Reducir el tiempo de respuesta cuando se identifique un incidente de seguridad, desde su fase inicial, reportando la forma de contenerlo/remediarlo.
 - Mejora del tiempo de recuperación objetivo (RTO) cuando se identifique un incidente cibernético confirmado.
 - Búsqueda proactiva de amenazas dentro del ámbito de puestos y servidores de la Agencia, mejorando los tiempos de detección actuales y buscando la anticipación proactiva de caza de amenazas.
 - Mejora de los protocolos de escalado de incidentes de seguridad dentro de Agencia y su evaluación en términos de eficacia, con objetivo final de la mejora de dicho proceso.
 - Análisis de los Indicadores de Compromiso, en adelante IOCs, y búsqueda de esos IOCs dentro de los equipos bajo el ámbito de responsabilidad de la Agencia y la monitorización de los mismos. Verificación de la detección por parte de las herramientas de Panda de dichos IOCs.

- **Consideraciones adicionales:**

La responsabilidad organizativa sobre el equipo humano del adjudicatario destinado a atender los servicios objeto del contrato, estará siempre bajo la disciplina laboral y el poder de dirección del contratista. En ningún caso podrá impartir directrices de índole técnica ni priorizar los trabajos técnicos, limitándose a impartir directrices organizativas y funcionales con el fin de asegurar el correcto desarrollo de las directrices técnicas marcadas por la dirección de la Agencia.

El contratista asegurará la mejor calidad del servicio, realizando los procesos de acuerdo a los plazos y procedimientos acordados, de forma que no impacte negativamente en los sistemas productivos.

5.4 CYTOMIC Threat Hunting Service 8x5 (Pool de Threat Hunters)

CYTOMIC Threat Hunting Service es un servicio exclusivo que el adjudicatario presta a grandes cuentas (Clientes Enterprise), y que se centra en la búsqueda proactiva de nuevas amenazas



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

avanzadas y en la búsqueda proactiva de las tácticas, técnicas y procedimientos, en adelante TTPs, que usan los atacantes en sus reconocimientos y ataques.

Durante el plazo de ejecución del contrato, los **servicios de CYTOMIC Hunting Service 8x5**, descritos en este pliego, deberán prestarse por el adjudicatario en la franja horaria de 08:00 h. a 17:00 h., de lunes a viernes. No están incluidos fines de semana, ni días festivos.

El servicio de Cytomic Threat Hunting 8x5 incluye:

- Detección de amenazas avanzadas, ataques en fase temprana, etc., de forma proactiva.
- Notificación por email ante ciber-ataques o potenciales amenazas.
- Seguimiento Post-incidente para asegurarnos la resolución de incidentes críticos.
- Reporte mensual de la actividad realizada.
- Almacenamiento de la telemetría durante un año. La telemetría almacenada debe permitir a los equipos de ciberseguridad detectar ataques que se iniciaron hace 365 días.

El Hunting proactivo permite:

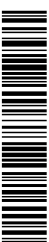
- **Detectar “ataques” en fase temprana.** Son ataques que aún están en sus fases iniciales que en caso de no controlarse pueden acabar comprometiendo a parte o a toda la organización.
- **Detectar equipos comprometidos.** Se trata de equipos comprometidos por ataques que se han saltado las diferentes protecciones establecidas por la organización. En algunos casos se trata de equipos comprometidos hace días, semanas o incluso meses que no son detectados por utilizar técnicas “fileless”, ataques de malware sin fichero. Estos equipos comprometidos no actúan de forma inmediata y permanecen a la espera para conseguir la información que necesitan para alcanzar el objetivo de su ataque.
- **Detectar malas prácticas.** Las malas prácticas detectadas se comunican a la Agencia para confirmar que es una mala práctica y no un principio de ataque. La Agencia debe establecer los medios para eliminar estas malas prácticas y reducir la superficie de ataque para hackers o personal interno, denominado “insiders”.
- **Detectar comportamientos anómalos de usuarios y equipos.** Estos comportamientos anómalos son comunicados a la Agencia para confirmar si se trata o no de un principio de ataque, o de un ataque en curso.

5.5 Adquisición de licencias

Durante la ejecución del contrato la Agencia podrá adquirir nuevas licencias del producto para su instalación en equipos de la Comunidad de Madrid, a fin de hacer frente a crecimientos de la planta instalada, en las siguientes cantidades máximas:

DESCRIPCIÓN	UDS.
Licencias: Cytomic EPDR	14.000
Licencias: Módulo Cytomic Insight + Patch + SiemConnect (IPS)	101.751
Licencias: Endpoint Protection Plus Android	6.000

Esta adquisición de licencias incluirá la garantía correspondiente.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

Las solicitudes de adquisición de licencias se realizarán a demanda del Responsable del Contrato designado por la Agencia, y se facturarán con el siguiente desglose de precios unitarios, al que se le aplicará la baja obtenida, en su caso, como resultado de la adjudicación.

Adquisición de licencias bajo demanda	
Descripción de licencia	Precio Adquisición (IVA no incluido)
Cytomic EPDR con 35 meses de garantía	17,50 €
Cytomic EPDR con 30 meses de garantía	15,00 €
Cytomic EPDR con 24 meses de garantía	12,00 €
Cytomic EPDR con 18 meses de garantía	9,00 €
Cytomic EPDR con 12 meses de garantía	6,00 €
Cytomic EPDR con 6 meses de garantía	3,00 €
Cytomic (Insight + Patch + SiemConnect) con 35 meses de garantía	2,57 €
Cytomic (Insight + Patch + SiemConnect) con 30 meses de garantía	2,20 €
Cytomic (Insight + Patch + SiemConnect) con 24 meses de garantía	1,76 €
Cytomic (Insight + Patch + SiemConnect) con 18 meses de garantía	1,32 €
Cytomic (Insight + Patch + SiemConnect) con 12 meses de garantía	0,88 €
Cytomic (Insight + Patch + SiemConnect) con 6 meses de garantía	0,44 €
Endpoint Protection Plus Android con 35 meses de garantía	5,40 €
Endpoint Protection Plus Android con 30 meses de garantía	4,63 €
Endpoint Protection Plus Android con 24 meses de garantía	3,70 €
Endpoint Protection Plus Android con 18 meses de garantía	2,78 €
Endpoint Protection Plus Android con 12 meses de garantía	1,85 €
Endpoint Protection Plus Android con 6 meses de garantía	0,93 €



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

CLÁUSULA 6.- EQUIPO PRESTADOR DEL SERVICIO ON-SITE

Para la prestación de los servicios de soporte on-site, objeto del contrato, el adjudicatario pondrá a disposición de la Agencia un equipo formado por, al menos, **DOS técnicos especialistas en seguridad de productos PANDA y UN jefe de proyecto**, con la cualificación y el perfil técnico mínimo, que a continuación se detalla.

6.1 Técnicos especialistas en seguridad de productos panda

Todo el equipo, jefe de proyecto y técnicos especialistas, deberán disponer de formación especializada en seguridad de productos Panda, y amplios conocimientos del entorno Microsoft.

REQUISITOS MÍNIMOS – JEFE DE PROYECTO	
CATEGORÍA PROFESIONAL	
Jefe de Proyecto	
TITULACIÓN	
Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.	
FORMACIÓN TÉCNICA	
<ul style="list-style-type: none"> - Conocimientos en diseño, Administración e implantación de Microsoft Windows 10. - Conocimientos en diseño, Administración e implantación de Microsoft Directorio Activo 2019. - Conocimientos en productos Panda 	
ACTIVIDAD PROFESIONAL	
<ul style="list-style-type: none"> - Al menos 48 meses realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 10 y 8.1, Windows Server 2019, 2016, y 2012. - Al menos 48 meses de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes. - Al menos 48 meses de experiencia en la organización y gestión de equipos técnicos especialistas en la detección y remediación de incidencias de seguridad. - Al menos 48 meses de experiencia en proyectos de despliegue de soluciones de seguridad de PANDA. 	

REQUISITOS MÍNIMOS – TÉCNICO ESPECIALISTA SENIOR	
CATEGORÍA PROFESIONAL	
Técnico Senior	
TITULACIÓN	
Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.	
FORMACIÓN TÉCNICA	
<ul style="list-style-type: none"> - Conocimientos en diseño, Administración e implantación de Microsoft Windows 10. - Conocimientos en diseño, Administración e implantación de Microsoft Directorio Activo 2019. - Conocimientos en productos Panda 	



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

ACTIVIDAD PROFESIONAL

- Al menos **36 meses** realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 10 y 8.1, Windows Server 2019, 2016, y 2012,
- Al menos **36 meses** de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.

REQUISITOS MÍNIMOS - TÉCNICO ESPECIALISTA

CATEGORÍA PROFESIONAL

Técnico

TITULACIÓN

Bachillerato, Formación Profesional Grado Superior en informática o equivalente.

FORMACIÓN TÉCNICA

- Conocimientos en diseño, Administración e implantación de Microsoft Windows 10.
- Conocimientos en diseño, Administración e implantación de Microsoft Directorio Activo 2019.
- Conocimientos en productos Panda

ACTIVIDAD PROFESIONAL

- Al menos **24 meses** realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows 10 y 8.1, Windows Server 2019, 2016, y 2012,
- Al menos **24 meses** de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.

El licitador propuesto como adjudicatario, con carácter previo a la adjudicación, deberá aportar los currículos de las **personas asignadas a la prestación del servicio on-site**, que deberán presentarse debidamente cumplimentados y firmados por la persona que ostente la representación, especificando la cualificación profesional de cada uno de ellos, con detalle de categoría, titulación y actividad profesional.

6.2 Verificación de la capacidad de los componentes del equipo adscrito a la ejecución del contrato, sustitución de los componentes de dicho equipo y seguimiento y control de los trabajos.

El equipo humano que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por los componentes ofertados por el adjudicatario y responderá siempre a los requisitos mínimos que en el presente Pliego de Cláusulas Técnicas se señalan para los mismos.

▪ Condicionantes del equipo de trabajo ofertado:

El contratista responderá siempre de la adecuación del personal asignado a la ejecución de los trabajos, de manera que durante la ejecución de los trabajos y con anterioridad o posterioridad a



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

los pagos, la Agencia podrá comprobar la adecuación del personal asignado al servicio contratado y verificar dicha capacidad en cualquier momento.

La falsedad en el nivel de conocimientos técnicos del personal ofertado, así como la sustitución de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y requisitos exigidos en los apartados siguientes, facultará a la Agencia para instar la **resolución** del contrato.

▪ **Constitución inicial del equipo de trabajo:**

El equipo de trabajo que se incorporará tras la formalización del contrato para la ejecución de los trabajos deberá estar formado por los componentes ofertados por el adjudicatario. La autorización de cambios puntuales en la composición del mismo requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de posibles candidatos con un perfil de cualificación técnica igual o superior al de la persona que se pretende sustituir.
- Aceptación por el *Responsable del Contrato* designado por la Agencia de los candidatos propuestos.

▪ **Modificaciones en la composición del equipo de trabajo:**

La valoración final de la calidad de los servicios prestados por las personas adscritas a la ejecución del contrato corresponde al Responsable del Contrato designado por la Agencia, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otro de igual perfil técnico-profesional, si existen razones justificadas que lo aconsejen.

Si es el adjudicatario el que propone el cambio de una de las personas del equipo de trabajo, deberá solicitarlo por escrito con quince días de antelación, y se autorizará por la Agencia en las mismas condiciones que se requieren para la autorización de cambios puntuales en la composición del equipo de trabajo inicial.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones en los componentes del equipo de trabajo, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario.

Cuando se trate de modificaciones en el equipo adscrito a la ejecución del servicio, imputables al contratista, se establece un número máximo de sustituciones de 1 recurso durante la ejecución del contrato. A los efectos de su cómputo, no se tendrán en cuenta las modificaciones en el equipo que sean consecuencia de incapacidad temporal o permanente del recurso sustituido.

Asimismo, durante todo el plazo de ejecución del contrato, el adjudicatario deberá mantener los niveles de calidad del servicio objeto del mismo, por lo que deberá instrumentar los servicios de suplencia que estime oportunos, que serán cubiertos siempre con el mismo personal suplente, a los efectos de ocasionar el mínimo impacto en la prestación del servicio.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

CLÁUSULA 7.- REQUISITOS DERIVADOS DE LA PRESTACIÓN DE LOS SERVICIOS

7.1 Ámbito de ejecución

Los servicios de soporte on-site se prestarán, preferentemente, desde las oficinas centrales de la Agencia, sin perjuicio que previa autorización de la Agencia pudiera prestarse de forma remota. Esta distribución inicial no implica que no puedan realizarse tareas en cualquier sede de la Comunidad de Madrid, a petición de la Agencia. A tal efecto, todos los gastos ocasionados por los desplazamientos y estancia del personal adscrito a la prestación del servicio durante el cumplimiento del contrato, serán por cuenta del adjudicatario.

Para los servicios que se presten en las instalaciones de la Agencia, el personal de la empresa contratista 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 contratista, 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 contratista, 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.

7.2 Servicio de soporte on site: horas de servicio y horario de prestación

Durante el plazo de ejecución del contrato, los **servicios de soporte on-site**, descritos en este pliego, deberán prestarse por el adjudicatario en la franja horaria de 08:00 h - 09:00 h. a 17:00 h - 18:00 h., de lunes a viernes.

La Agencia establecerá los turnos necesarios dentro de la franja horaria a la que se hace referencia para la prestación del servicio, sin que ello suponga coste adicional alguno.

Durante el plazo de ejecución del contrato y dentro de la prefijada franja horaria, el adjudicatario deberá prestar un servicio de, al menos, **5.760 horas anuales** (1.920 horas anuales por cada persona del equipo de trabajo).

No obstante, a petición del *Responsable del Contrato* designado por la Agencia, hasta el **4 %** de las horas de servicio referidas podrán exigirse fuera de la franja horaria anteriormente citada.

7.3 Documentación

A continuación, se detalla la documentación que se exigirá al adjudicatario, durante la prestación del servicio:

- Informes mensuales de actividad, con la descripción de las tareas realizadas, ajustándose al formato que el *Responsable del Contrato* designado por la Agencia determine.
- Informe consolidado trimestral.
- Actas de las reuniones de seguimiento.

CLÁUSULA 8.- CONDICIONES ADICIONALES A CUMPLIR

▪ Disponibilidad de medios:

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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

En el caso de que los servicios contratados puedan implicar, por razones de cumplimiento de plazos u otros motivos, para el contratista la decisión de ejecución de los servicios en régimen de turnos o en sábados o festivos, o en régimen de nocturnidad, la Agencia no aceptará costes adicionales por estas circunstancias, que deberán ser asumidos siempre por el contratista.

▪ **Responsable de Servicio:**

El adjudicatario designará como Responsable del Servicio al Jefe de Proyecto del equipo prestador del servicio, que será el responsable del mismo ante la Agencia. Este responsable será el interlocutor único y se encontrará en permanente contacto con el personal que la Dirección de la Agencia designe.

El contratista, 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 contratista suministrará al equipo humano que desarrolle los trabajos objeto del contrato, en todas aquellas materias que sean necesarias para el perfecto desempeño de los mismos.
- Diariamente, impartir con exclusividad al personal asignado por el contratista a la ejecución del contrato instrucciones específicas sobre el trabajo a realizar, 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 proyecto.
- Supervisar y controlar el trabajo y las actividades realizadas, e informar a la Agencia de las posibles incidencias y seguimiento o desviaciones de plazos.
- Ejercer el mando y el poder organizativo sobre el equipo encargado de la prestación de los servicios objeto del contrato, que estará siempre bajo la disciplina laboral y el poder de dirección del contratista, con independencia de que, para el mejor cumplimiento del servicio, en determinados momentos pueda el contratista destacar personal del equipo prestador del servicio en cualquier centro de trabajo, oficinas o ubicaciones de la Comunidad de Madrid.

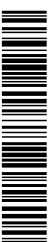
CLÁUSULA 9.- SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO

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 y el Responsable del Contrato que la Agencia designe. En concreto, el adjudicatario designará como único interlocutor ante la Agencia, al Responsable del Servicio que será quien represente al equipo de trabajo y asistirá a las reuniones trimestrales de seguimiento de proyecto, donde se entregará y analizará un informe consolidado de las actividades desarrolladas en el último periodo.
- La Agencia determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control del servicio.

CLÁUSULA 10.- PLAZO DE GARANTÍA

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



Hasta que no finalice el periodo de garantía, 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 ejecución o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

CLÁUSULA 11.- GESTIÓN DE LA SEGURIDAD

11.1 Protección de datos personales y Privacidad

11.1.1 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), y la normativa complementaria.

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).

11.1.2 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 la Agencia 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 la Agencia 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.

La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

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:

- 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 la Agencia Madrid Digital por escrito en cada momento. El adjudicatario informará inmediatamente a la Agencia 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 la Agencia 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 la Agencia 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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

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 Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con la Agencia 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 la Agencia Madrid Digital o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

la Agencia Madrid Digital, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

- n) Colaborar con la Agencia 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 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 la Agencia 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 conllevará un acceso accidental o incidental a Datos Personales responsabilidad de la Agencia 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.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

11.1.3 Obligaciones de la Agencia 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.

11.1.4 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 la Agencia Madrid Digital, identificando qué tratamiento de datos personales conlleva, para que la Agencia 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 la Agencia 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 la Agencia 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 la Agencia Madrid Digital a su mera solicitud para verificar su existencia y contenido.

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

11.1.5 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.

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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

11.2 Deber de Información

Los datos de carácter personal del adjudicatario serán tratados por la Agencia Madrid Digital para ser incorporados al sistema de tratamiento “Gestión de los expedientes de adquisición y contratación”, cuya finalidad es la gestión administrativa de los expedientes de contratación de la Agencia 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 la Agencia Madrid Digital, C/Embajadores, 181, 28049 - Madrid o en la dirección de correo electrónico 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 la Agencia. 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.

11.3 Seguridad en la utilización de medios electrónicos

11.3.1 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.

11.3.2 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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de contrato.

11.4 Medidas de Seguridad

11.4.1 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 la Agencia 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 la Agencia, 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.

11.4.2 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 la Agencia Madrid Digital del cumplimiento de aquella obligación.

CLÁUSULA 12.- PROPIEDAD DE LOS TRABAJOS

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



Los adjudicatarios renuncian expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución de los contratos pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de Madrid Digital.

CLÁUSULA 13.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS

Los contratistas no adquieren ningún derecho sobre el hardware (material), software e infraestructuras propiedad de Madrid Digital, salvo el de acceso indispensable al mismo para el cumplimiento de las tareas que se desprenden de las obligaciones dimanadas del contrato.

Los contratistas no podrán utilizar la información obtenida en la actividad desarrollada como consecuencia de este contrato, y no podrán transmitirla sin el consentimiento expreso y escrito de Madrid Digital.

Finalizado el presente contrato, los desarrollos software, herramientas y licencias incluidas en el alcance de los servicios del presente pliego pasarán a ser propiedad de Madrid Digital.

CLÁUSULA 14.- 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, Madrid Digital podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, Madrid Digital podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

CLÁUSULA 15.- PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **TREINTA Y SEIS MESES**, desde el 1 de septiembre de 2020 hasta el 31 de agosto de 2023.

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.- PENALIDADES

Si el contratista, por causas imputables al mismo, incumpliera las obligaciones asumidas en virtud del contrato, y de conformidad con los niveles de servicio establecidos en el presente Pliego de Cláusulas Técnicas, la Agencia procederá a la imposición de las penalidades que se indican en el **ANEXO I**.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

CLÁUSULA 17.- CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS

Durante el periodo de licitación y ante cualquier necesidad de aclaración sobre cuestiones referidas a las especificaciones recogidas en el presente pliego de prescripciones técnicas, el licitador podrá dirigirse a:

Agencia para la Administración Digital de la Comunidad de Madrid

Dirección de Ciberseguridad, Protección de Datos y Privacidad

Área de Ciberseguridad de Sistemas

Unidad de Protección Antimalware Puestos y Servidores

email: md_seguridad_sistemas@madrid.org



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1259294353114119598927**

ANEXO I: PENALIDADES

Si el contratista, por causas imputables al mismo, incumpliera las obligaciones asumidas en virtud del contrato, y de conformidad con los niveles de servicio establecidos en el Pliego de Cláusulas Técnicas, la Agencia procederá a la imposición de las penalidades que se indican a continuación:

SERVICIOS DE SOPORTE TÉCNICO			
TIPO DE SERVICIO	NIVEL DE SERVICIO EXIGIDO		PENALIDADES
Incidentes Prioridad Crítica	Tiempo máximo de respuesta	4 horas	100 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	1 hora	100 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	2 horas	100 €, por cada hora que exceda el plazo máximo fijado.
Incidentes Prioridad Alta	Tiempo máximo de respuesta	4 horas	100 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	1 hora	100 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	3 horas	100 €, por cada hora que exceda el plazo máximo fijado.
Incidentes Prioridad Media	Tiempo máximo de respuesta	5 horas	50 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 8:00 a 22:00 horas, excepto festivos)	2 horas	50 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de 22:00 a 8:00 horas, sábados, domingos y festivos)	3 horas	50 €, por cada hora que exceda el plazo máximo fijado.



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**

SERVICIOS DE SOPORTE TÉCNICO			
TIPO DE SERVICIO	NIVEL DE SERVICIO EXIGIDO		PENALIDADES
Incidencias Prioridad Baja	Tiempo máximo de respuesta	6 horas	50 €, por cada hora que exceda el plazo máximo fijado.
Rotación equipo de trabajo	El incumplimiento respecto al número máximo de sustituciones permitidas		3.000 € por cada cambio que supere el máximo permitido

La Directora de Ciberseguridad, Protección de Datos y Privacidad

Fdo.: Esther Muñoz Fuentes



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **1259294353114119598927**