



**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN  
EL CONTRATO DE SERVICIOS TITULADO  
“MANTENIMIENTO, SOPORTE TÉCNICO Y ADQUISICIÓN  
DE SOLUCIONES DE SEGURIDAD ANTIVIRUS PANDA,  
INSTALADAS EN LOS DIFERENTES PUESTOS Y  
SERVIDORES WINDOWS EXISTENTES EN LOS CENTROS  
DEPENDIENTES DE LA COMUNIDAD DE MADRID”, A  
CELEBRAR MEDIANTE PROCEDIMIENTO NEGOCIADO.**





## INDICE

<b>CLÁUSULA 1.-</b>	<b>INTRODUCCIÓN .....</b>	<b>3</b>
<b>CLÁUSULA 2.-</b>	<b>OBJETO .....</b>	<b>3</b>
<b>CLÁUSULA 3.-</b>	<b>ALCANCE .....</b>	<b>3</b>
<b>CLÁUSULA 4.-</b>	<b>DESCRIPCIÓN DEL ENTORNO TÉCNICO EXISTENTE .....</b>	<b>4</b>
<b>CLÁUSULA 5.-</b>	<b>DESCRIPCIÓN DE LOS SERVICIOS Y SUMINISTRO DE LICENCIAS .....</b>	<b>5</b>
5.1	SERVICIO DE MANTENIMIENTO CORRECTIVO .....	5
A.-	NOTIFICACIÓN DE INCIDENCIAS. ....	5
B.-	TIPIFICACIÓN DE INCIDENCIAS Y NIVELES DE SERVICIO .....	6
C.-	SOPORTE PRESENCIAL. ....	7
D.-	SEGUIMIENTO Y RESOLUCIÓN DE INCIDENCIAS. ....	8
5.2	SERVICIO DE SOPORTE PREMIUM.....	8
5.3	SERVICIO DE TÉCNICOS ESPECIALISTAS ON SITE .....	9
5.4	ADQUISICIÓN DE LICENCIAS.....	12
<b>CLÁUSULA 6.-</b>	<b>EQUIPO PRESTADOR DEL SERVICIO ON SITE .....</b>	<b>12</b>
6.1	TÉCNICOS ESPECIALISTAS EN SEGURIDAD DE PRODUCTOS PANDA. ....	13
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. ....	14
<b>CLÁUSULA 7.-</b>	<b>REQUISITOS DERIVADOS DE LA PRESTACIÓN DE LOS SERVICIOS .....</b>	<b>15</b>
7.1	ÁMBITO DE EJECUCIÓN.....	15
7.2	SERVICIO DE SOPORTE ON SITE: HORAS DE SERVICIO Y HORARIO DE PRESTACIÓN.....	16
7.3	DOCUMENTACIÓN. ....	16
<b>CLÁUSULA 8.-</b>	<b>CONDICIONES ADICIONALES A CUMPLIR .....</b>	<b>16</b>
<b>CLÁUSULA 9.-</b>	<b>SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO .....</b>	<b>17</b>
<b>CLÁUSULA 10.-</b>	<b>PLAZO DE GARANTÍA .....</b>	<b>18</b>
<b>CLÁUSULA 11.-</b>	<b>GESTIÓN DE LA SEGURIDAD.....</b>	<b>18</b>
<b>CLÁUSULA 12.-</b>	<b>PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL .....</b>	<b>24</b>
<b>CLÁUSULA 13.-</b>	<b>PROPIEDAD DE LOS TRABAJOS .....</b>	<b>29</b>
<b>CLÁUSULA 14.-</b>	<b>DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS .....</b>	<b>29</b>
<b>CLÁUSULA 15.-</b>	<b>CALIDAD DEL SERVICIO .....</b>	<b>29</b>
<b>CLÁUSULA 16.-</b>	<b>PLAZO DE EJECUCIÓN .....</b>	<b>29</b>
<b>CLÁUSULA 17.-</b>	<b>PENALIZACIONES.....</b>	<b>30</b>
<b>CLÁUSULA 18.-</b>	<b>CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS .....</b>	<b>30</b>





## 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 antivirus 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 soporte técnico de las soluciones de seguridad (Antivirus 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 antivirus 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.
- **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.
- **Adquisición con garantía de nuevas licencias de producto**, 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 1.972 Servidores Windows (en versiones 2000, 2003, 2008), 22 servidores de correo Exchange y 76.757 puestos de usuarios, distribuidos en más de 4.000 sedes.

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

DESCRIPCIÓN	UDS.
<b>Licencias:</b> Panda Endpoint Protection Plus	78.751
<b>Licencias:</b> Panda Adaptative Defense	1.000

Los equipos se protegen mediante el software de antivirus Panda, existiendo una infraestructura de servidores, 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 XP y Windows 8 como sistema operativo.

La gestión centralizada de estos equipos se realiza mediante Microsoft System Center y políticas de Directorio Activo 2008, 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.

#### **A.-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.

Un **“incidente”** se define como una única cuestión de soporte y el esfuerzo necesario para resolverlo. Una única cuestión de soporte es un problema que no puede ser descompuesto en problemas subordinados.

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.

## **B.-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.

- **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.

### C.-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

#### **D.-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.

- **Generación de herramientas de desinfección especiales** específicas para redes, para todo el malware, que permitan eliminar la amenaza, y restaurar los equipos para dejarlos operativos, minimizando el coste de despliegue y de reparación ante una infección.

#### **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 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 antivirus a través de internet. Uso de las herramientas del contratista para permitir el despliegue de nuevas versiones del motor de antivirus en la red corporativa con un mínimo uso de los recursos de comunicaciones.
- **Generación de herramientas de desinfección especiales** específicas para redes, para todo el malware, 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 antivirus 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:
  - **Adecuación de los servidores:** Instalación y configuración del software Panda en los servidores de antivirus, conforme a los procedimientos establecidos.
  - **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 antivirus, 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 antivirus, con la solución

corporativa que mejor se adapte a sus necesidades. Para ello, será el adjudicatario el que deberá realizar las siguientes tareas:

- **Instalación de los servidores:** Instalación y configuración de los servicios de Antivirus 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 antivirus 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 antivirus 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 antivirus 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 antivirus 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.
- **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 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.
<b>Licencias:</b> Panda Endpoint Protection Plus	20.000
<b>Licencias:</b> Panda Adaptative Defense	2.000

Esta adquisición de licencias incluirán la garantía correspondiente.

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)
Panda Endpoint Protection Plus con 23 meses de garantía	9,09 €
Panda Endpoint Protection Plus con 18 meses de garantía	7,11 €
Panda Endpoint Protection Plus con 12 meses de garantía	4,74 €
Panda Endpoint Protection Plus con 6 meses de garantía	2,37 €
Panda Adaptative Defense con 12 meses de garantía	7,00 €
Panda Adaptative Defense con 6 meses de garantía	3,50 €

#### 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 - TÉCNICOS ESPECIALISTAS
<b>CATEGORÍA PROFESIONAL</b>
Técnico Senior
<b>TITULACIÓN</b>
Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.
<b>FORMACIÓN TÉCNICA</b>
<ul style="list-style-type: none"><li>- Diseño, Administración e implantación de Microsoft Windows XP (mínimo <b>20 horas</b>)</li><li>- Diseño, Administración e implantación de Microsoft Directorio Activo 2003. (mínimo <b>25 horas</b>)</li></ul>
<b>ACTIVIDAD PROFESIONAL</b>
<ul style="list-style-type: none"><li>- Al menos <b>18 meses</b> realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows XP, Windows Server 2000/2003</li><li>- Al menos <b>18 meses</b> de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.</li></ul>

REQUISITOS MÍNIMOS – JEFE DE PROYECTO
<b>CATEGORÍA PROFESIONAL</b>
Técnico Senior
<b>TITULACIÓN</b>
Ingeniería Técnica en Informática, Formación Profesional Grado Superior en informática o equivalente.
<b>FORMACIÓN TÉCNICA</b>

- Diseño, Administración e implantación de Microsoft Windows XP (mínimo **20 horas**)
- Diseño, Administración e implantación de Microsoft Directorio Activo 2003. (mínimo **25 horas**)

#### **ACTIVIDAD PROFESIONAL**

- Al menos **18 meses** realizando labores de administración, implantación, mantenimiento y soporte de los sistemas de seguridad basados en los sistemas Windows siguientes: Windows XP, Windows Server 2000/2003
- Al menos **18 meses** de experiencia en redes de más de 1.000 PC's distribuidos en varias sedes.
- Al menos **18 meses** de experiencia en la organización y gestión de equipos técnicos especialistas en la detección y remediación de incidencias de seguridad.
- Al menos **18 meses** de experiencia en proyectos de despliegue de soluciones de seguridad de PANDA.

El licitador propuesto como adjudicatario, con carácter previo a la adjudicación, deberá aportar los currículos de las personas asignadas a la ejecución del contrato, 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 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.

<b>CLÁUSULA 7.- REQUISITOS DERIVADOS DE LA PRESTACIÓN DE LOS SERVICIOS</b>
--

**7.1 ÁMBITO DE EJECUCIÓN.**

Los servicios de soporte on-site se prestarán inicialmente desde las oficinas centrales de la Agencia, estando previsto destacar un recurso en un centro del ámbito sanitario para mejora de la coordinación de actividades objeto del soporte en este entorno. 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. a 24:00 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.

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 semanales de actividad, con la descripción de las tareas realizadas, ajustándose al formato que el *Responsable del Contrato* designado por la Agencia determine.
- Informe consolidado mensual.
- 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.

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.

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

<b>CLÁUSULA 9.- SEGUIMIENTO Y CONTROL DE LA EJECUCIÓN DEL CONTRATO</b>
--

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 mensuales 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**

El adjudicatario deberá cumplir la normativa legal aplicable en materia de seguridad en el marco de los servicios prestados. Con carácter general deberá prestarse especial atención a la observancia de la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, el *Real Decreto 1720/2007, de 21 de diciembre*, por el que se aprueba el Reglamento de desarrollo de la anterior, la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos* y el *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica*.

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

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

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



naturaleza de la información y el servicio que soportan y los requerimientos de la distinta normativa que les aplique. Esta especificación de requisitos de seguridad se documentará conforme a lo establecido en los estándares de la Agencia al respecto de la materia.

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

#### **Documentación de seguridad**

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

- e) 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 que intervengan en la prestación del servicio y redactado de forma sencilla, precisa y comprensible.
- f) Un documento denominado **Documento de Seguridad**, coherente con los documentos de seguridad que exigen los *Reales Decretos 1720/2007*, y *3/2010* respectivamente, en lo que corresponda a cada uno, donde se encuentre la normativa de seguridad que recoja todas las medidas de seguridad propuestas, la forma de su cumplimiento y las responsabilidades asociadas, con indicación expresa de la identidad del Responsable de Seguridad del Servicio. Estas medidas de seguridad incluirán al menos las que se relacionan a continuación para cada uno de los ámbitos normativos.

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

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

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

Se registrará además en el *Documento de Seguridad*, si se diera la circunstancia, la relación de usuarios con privilegios de administración de los sistemas de información de la Agencia





(asociados a posibles tareas habituales o puntuales de mantenimiento, explotación de sistemas o cualquier otra que pudiera implicar el acceso a datos del entorno de producción de los sistemas de información de la Comunidad de Madrid).

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

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

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

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

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

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

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

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

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

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

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

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

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

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

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

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

- Guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el Equipo del Proyecto;
- Utilizar o transmitir la Información Confidencial exclusivamente para los fines del objeto del contrato;
- No realizar copia de la Información Confidencial sin el previo consentimiento escrito de la Agencia, excepto aquellas copias que sean necesitadas por el Equipo del Proyecto para su estudio interno;
- Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del objeto del contrato, y asegurarse de que dichas personas conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento;
- No facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito de la Agencia, y asegurarse de que, en caso de haber obtenido dicha autorización, dicho tercero firma un compromiso de confidencialidad en términos equivalentes a los del presente documento.
- Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del contrato o su contenido, deberá ser previamente aprobada por escrito por la Agencia.
- El Equipo del Proyecto procederá a destruir o a devolver a la Agencia toda la Información Confidencial a la finalización del objeto del contrato referido, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida.



- La empresa contratista formará e informará de estas obligaciones al personal que participe en el desarrollo del contrato, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.

### **Restricciones generales**

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

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación, distribución o cesión de datos, medios u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos o PDA's.
- La posesión, distribución, cesión, revelación o alteración de cualquier información sin el consentimiento expreso del propietario de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PINs) o permitir el uso de mecanismos de acceso, sean locales o remoto a usuarios no autorizados.
- Inutilizar o suprimir cualquier elemento de seguridad o protección o la información que generen.

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

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

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



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

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

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

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

#### **CLÁUSULA 12.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

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

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter 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 contratista 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 contratista se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
- 1.4.5. Cuando se transmitan datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

#### **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 contratista 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 contratista 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 contratista tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con un fin distinto al que figure en el objeto del contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

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

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

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

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 contratista como encargado del tratamiento de datos personales. Sin perjuicio de las instrucciones que, adicionalmente, pudieran establecerse por el Encargado del Tratamiento, el contratista queda sujeto en el tratamiento de datos personales a las instrucciones procedentes del Responsable del Fichero.

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

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

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 Comunidad de Madrid, inscrito en el Registro General de Protección de Datos de la AEPD ([www.agpd.es](http://www.agpd.es)), y no podrán ser cedidos salvo en los supuestos previstos en la Ley. El responsable del fichero es la Agencia, 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 13.- PROPIEDAD DE LOS TRABAJOS**

Todos los informes, estudios y documentos, elaborados por el contratista 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.

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

#### **CLÁUSULA 14.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS.**

El contratista 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 contratista 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 15.- 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 Agencia 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 16.- PLAZO DE EJECUCIÓN**

El plazo de ejecución del contrato será de **VENTICUATRO MESES**, desde el 1 de septiembre de 2016 hasta el 31 de agosto de 2018.

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 17.- PENALIZACIONES**

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 penalizaciones que se indican en el ANEXO I.

#### **CLÁUSULA 18.- CONSULTAS SOBRE EL PLIEGO DE CLÁUSULAS TÉCNICAS**

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

Agencia para la Administración Digital de la Comunidad de Madrid  
Dirección de Ingeniería, Soporte a Gestión de Aplicaciones y Centros de Competencia  
Área de Seguridad de Sistemas y Comunicaciones  
Unidad de Servicios de Seguridad de Sistemas  
eMail: [ICM\\_SEGURIDAD\\_SISTEMAS@madrid.org](mailto:ICM_SEGURIDAD_SISTEMAS@madrid.org)



## ANEXO I: PENALIZACIONES

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 penalizaciones que se indican a continuación:

SERVICIOS DE SOPORTE TÉCNICO			
TIPO DE SERVICIO	NIVEL DE SERVICIO EXIGIDO		PENALIZACIONES
<b>Incidencias Prioridad Crítica</b>	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.
<b>Incidencias Prioridad Alta</b>	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.
<b>Incidencias Prioridad Media</b>	Tiempo máximo de respuesta	5 horas	50 €, por cada hora que exceda el plazo máximo fijado.
	Tiempo máximo Soporte presencial (lunes a viernes de	2 horas	50 €, por cada hora que exceda el plazo máximo fijado.



	8:00 a 22:00 horas, excepto festivos)		
	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.
<b>Incidencias Prioridad Baja</b>	Tiempo máximo de respuesta	6 horas	50 €, por cada hora que exceda el plazo máximo fijado.
<b>Rotación equipo de trabajo</b>	El incumplimiento respecto al <b>número máximo de sustituciones</b> permitidas		3.000 € por cada cambio que supere el máximo permitido

<p><i>ELABORADO Y PROPUESTO POR:</i></p> <p><i>La Subdirectora General de Infraestructuras y Operaciones</i></p> <p><i>Fdo.: Zaida Sampredo Préstamo</i></p>	<p><i>APROBADO POR:</i></p> <p><i>El Consejero Delegado de la Agencia para la Administración Digital de la C.M.</i></p> <p><i>Fdo.: Blas Labrador Román</i></p>
--	---

