



**PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS  
TITULADO “ASISTENCIA TÉCNICA A LOS PROGRAMAS MICROSOFT INSTALADOS EN  
LOS SERVIDORES Y ORDENADORES PERSONALES DE LA COMUNIDAD DE MADRID” A  
CELEBRAR MEDIANTE PROCEDIMIENTO NEGOCIADO.**



**Agencia para la Administración Digital de la Comunidad de Madrid**

Dirección de Ingeniería, Soporte a Gestión de Aplicaciones y Centros de  
Competencia





## INDICE

1.	CLÁUSULA 1 – INTRODUCCIÓN .....	3
2.	CLÁUSULA 2 - OBJETO DEL CONTRATO .....	4
3.	CLÁUSULA 3 – DESCRIPCIÓN DE LOS REQUISITOS DEL SERVICIO DE SOPORTE TÉCNICO .....	4
4	CLÁUSULA 4 - CONDICIONES ADICIONALES A CUMPLIR.....	12
5	CLÁUSULA 5 – OBLIGACIONES DEL ADJUDICATARIO .....	14
6	CLÁUSULA 6 - DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA.....	14
7	CLÁUSULA 7 - SEGUIMIENTO Y CONTROL DEL SERVICIO .....	14
8	CLÁUSULA 8 – GESTIÓN DE LA SEGURIDAD.....	16
9	CLÁUSULA 9 - PLAZO DE GARANTÍA .....	31
10	CLÁUSULA 10ª – CALIDAD.....	31
11	CLÁUSULA 11ª – PLAZO DE EJECUCIÓN.....	31
12	CLÁUSULA 12ª – LUGAR DE PRESTACIÓN .....	31
13	CLÁUSULA 13ª – DOCUMENTACIÓN GENERADA DURANTE LA EJECUCIÓN DE LOS TRABAJO.....	31
14	CLÁUSULA 14ª – CONSULTAS TÉCNICAS SOBRE EL PLIEGO .....	32





## 1. CLÁUSULA 1 – INTRODUCCIÓN

La **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante la **Agencia**), según *Ley 7/2005, de 23 de diciembre*, de 23 de diciembre, de Medidas Fiscales y Administrativas (BOCM Núm. 311, de 30 de diciembre de 2005) modificada parcialmente por la *Ley 9/2015, de 28 de diciembre*, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015), tiene asignada entre otras funciones la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, a cuyo fin le corresponde la adquisición y dotación de infraestructuras físicas, lógicas, de soporte y servicios de los sistemas de información y comunicaciones de la Comunidad de Madrid (*Artículo 10-Tres-c*).

Para el ejercicio de las citadas funciones, la Agencia dispone de productos de la empresa Microsoft como software homologado para el puesto de trabajo de los usuarios de la Comunidad de Madrid, así como para el resto de servicios ofimáticos y de colaboración.

Desde el año 2002 se prestan en la Comunidad de Madrid los siguientes servicios ofimáticos con productos Microsoft:

### Servicio

Servicios de Directorio

Servicios de Ficheros e Impresión

Servicios de Correo Corporativo

Servicios de Colaboración

Servicios de Productividad Personal y Ofimática

Servicios de Gestión remota del puesto de trabajo

Servicios de Gestión de Servidores

Servicios de Proxy

Desde ese año la Agencia ha optado por los productos de la firma Microsoft como software de base para los ordenadores personales y servidores de propósito general, por lo que el tratamiento de la información y almacenamiento que realizan las aplicaciones utilizarán el sistema lógico basado en estos productos.

Para llevar a cabo la implantación y el mantenimiento adecuado y a nivel corporativo de los productos software que se encuentran instalados, es necesario contratar un soporte técnico para solucionar los problemas de configuración de los servidores, sistemas de correo, Directorio Activo, herramientas de colaboración, gestión remota, apoyo a los desarrolladores de aplicaciones sobre los nuevos sistemas operativos, así como al personal de la Agencia encargado de las tareas de soporte técnico.

Además se considera un factor crítico disponer de este tipo de soporte en el proyecto de actualización del sistema operativo de los puestos de trabajo desde Windows XP a Windows 8.1.





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

El objeto del contrato es la prestación de servicios de soporte técnico Microsoft Premier que permitan asegurar el correcto funcionamiento de todos los programas Microsoft actualmente instalados en todos los servidores y ordenadores personales de la Comunidad de Madrid de conformidad con los requerimientos establecidos en el presente Pliego de Cláusulas Técnicas y sus correspondientes Anexos.

En el Anexo I del presente Pliego de Cláusulas Técnicas se encuentra una relación de los servicios que se incluyen en el contrato y que son el objeto del mismo.

Los productos sobre los que se debe prestar el servicio de soporte son:

- **Software ofimático para clientes (Office):** Word, Excel, Outlook, PowerPoint, Access.
- **Sistemas operativos para servidores:** CIS Datacenter / Enterprise / Standard Windows Server License.
- **Software de servidor:** Windows CAL, SCCM CAL, SharePointCAL, Biztalk Server Enterprise, Exchange Server Enterprise, Exchange Server Standard, ForeFront TMG Enterprise, SharePoint Internet Sites Enterprise, SharePoint Server, SQL Server Standard, System Center Configuration Manager Server, System Center Operation Manager Server, System Center Operation Manager Server ML Enterprise Lync Server Enterprise, Lync Standard CAL y Lync Enterprise CAL.

## **3. CLÁUSULA 3 – DESCRIPCIÓN DE LOS REQUISITOS DEL SERVICIO DE SOPORTE TÉCNICO**

Los requisitos técnicos y de servicio mínimos se resumen en el Anexo I al presente pliego y recogen el alcance del servicio en cuanto a mantenimiento preventivo, mantenimiento correctivo, servicios de información, gestión técnica, servicios técnicos especializados y transferencia de conocimientos necesarios.

### **3.1 Mantenimiento preventivo**

#### **3.1.1 Mantenimiento preventivo en general**

El mantenimiento preventivo en los productos Microsoft no asociados a entornos o servicios críticos se realizará, de conformidad con la Agencia, y de acuerdo a las especificaciones siguientes:

- Se efectuará un estudio y revisión de la instalación y la configuración hardware y software de la base instalada de productos Microsoft, con el objetivo de mejorar el nivel de servicio y la disponibilidad de la información.
- Además del estudio que lleve a cabo de la base instalada, la empresa adjudicataria deberá proponer los planes de mejora y las actividades técnicas detalladas que optimicen la disponibilidad de los sistemas de información Microsoft.
- El adjudicatario deberá disponer de los medios técnicos y humanos necesarios para resolver cualquier consulta de soporte relacionada con el funcionamiento de los productos Microsoft, o con su integración con otros programas de otros fabricantes, que le sea planteada por parte de los técnicos de la Agencia.
- El adjudicatario se compromete a realizar una valoración previa del coste de las actuaciones propuestas por el mismo o por el personal técnico designado por la Agencia, derivadas de las tareas realizadas como mantenimiento preventivo.





- Las actuaciones de mantenimiento propuestas deberán contar con la aprobación del *Responsable del Contrato* designado por la Agencia para poder contabilizarse como actividades correspondientes a las descritas en el presente pliego. Será requisito previo a cada revisión de mantenimiento establecer y determinar el ámbito y número de jornadas u horas de trabajo que se requieran. Posteriormente se asignarán los recursos necesarios y se entregará al final de la misma un informe por escrito que documente las conclusiones y recomendaciones.
- Al inicio del contrato, se celebrará una reunión entre el *Responsable del Contrato designado por* la Agencia y la empresa adjudicataria, con objeto de planificar detalladamente las actividades necesarias para la consecución de los objetivos del servicio definidos en el presente Pliego.
- A requerimiento del *Responsable del Contrato* designado por la Agencia, y al menos con periodicidad mensual, el adjudicatario realizará un informe de seguimiento que resumirá los servicios proporcionados.
- La realización de las siguientes revisiones cuando el *Responsable del Contrato* designado por la Agencia lo determine:
  - Revisión de soporte: Soporte de planes específicos de despliegue de tecnología, migración o actualización, proporcionando recomendaciones para conseguir un entorno más estable y soportable.
  - Revisión de arquitectura tecnológica: Evaluación de un plan de despliegue de una tecnología específica. Esta evaluación debe dirigirse a identificar los riesgos existentes para alcanzar los objetivos de negocio establecidos en el plan de despliegue, enfocándose en que la Agencia obtenga el máximo provecho de lo que ofrece la tecnología de Microsoft para la arquitectura tecnológica global de la Agencia.
  - Revisión de diseño de aplicaciones: Evaluación de la arquitectura de una aplicación o revisión del diseño de componentes de un producto. Esta revisión, entre otros aspectos, está dirigida específicamente a evaluar la conformidad con las directrices de diseño de software de Microsoft, efectividad de comunicación de componentes distribuidos, diseño de código seguro y uso eficiente de servicios en tiempo de ejecución.
  - Revisiones de código: Examen crítico de aplicaciones para identificar problemas existentes o potenciales.
  - Revisiones personalizadas: Se realizarán para cubrir las necesidades específicas de la Agencia al uso de las tecnologías Microsoft.
  - Revisiones de configuración y operaciones: Donde se utilizarán las herramientas de diagnóstico desarrolladas por Microsoft para llevar a cabo dichos análisis de salud de los sistemas o chequeos (RAPs – Risk Assessment Program).
- **Servicio de Soporte “On-site”**. Será realizado por Ingenieros de soporte que se encargarán de las tareas de seguimiento semanal de los niveles de servicio definidos en el presente pliego y de la transferencia de conocimientos al personal de la Agencia.

El personal designado para estas tareas de soporte “on-site” deberá contar con los conocimientos técnicos y experiencia en los sistemas utilizados por la Agencia.







Los días de prestación de este servicio en las instalaciones de la CM se pactarán al inicio del contrato y solo podrá modificarse tras mutuo acuerdo entre las partes. El servicio de soporte "on-site" constará de las siguientes tareas:

- Proporcionar asistencia on-site los días pactados al comienzo del contrato.
- Apoyar al escalado y gestión de los incidentes y problemas técnicos que pudieran suceder.
- Evitar riesgos de producción comunes (actualizaciones de seguridad, documentación de procesos, procedimientos de recuperación de desastres, etc.).
- Colaborar con el TAM (Technical Account Manager) en el desarrollo de los servicios preventivos, agilizando la recogida de información, aportando su conocimiento y experiencia técnica y ayudando al personal técnico de la Agencia a poner en práctica, cuando sea posible y se acuerde con la Agencia, las recomendaciones del adjudicatario que puedan surgir de dichos servicios preventivos.

### **3.1.2 Mantenimiento preventivo en servicios críticos**

El mantenimiento preventivo en servicios críticos **se circunscribe a los entornos de Correo (Exchange y TMG) y Directorio (Directorio Activo)**. El Soporte preventivo de estos entornos incluye el mantenimiento preventivo anterior y se ampliará con los siguientes servicios:

- A requerimiento de la Agencia se efectuará un **estudio y revisión de la instalación y la configuración hardware y software** de la base instalada de los productos definidos como críticos, con el objetivo de mejorar el nivel de servicio y la disponibilidad de la información.
- **Operaciones de mantenimiento crítico.** A requerimiento de la Agencia, se solicitarán desplazamientos "on-site" de técnicos a instalaciones de la Comunidad de Madrid, para asistir en operaciones de mantenimiento con especial incidencia sobre los sistemas en producción que dan soporte a los entornos/servicios fijados como críticos.

Estas operaciones de mantenimiento se realizarán en horario 24 horas x 7 días a la semana.

La notificación de la necesidad por parte de la Agencia se realizará al *Responsable del Servicio* designado por el adjudicatario, y será de al menos cuatro días laborables de antelación, y constará de la información necesaria (hora, lugar, sistemas involucrados, etc.) para una correcta evaluación por parte del adjudicatario de los recursos necesarios para la intervención.

**Revisiones sobre los entornos críticos.** Con el objetivo de minimizar los riesgos sobre estos entornos, se realizarán revisiones anuales específicas y de análisis de riesgos para cada uno de ellos, y cuyo informe de resultados requerirá la conformidad de los responsables técnicos de la Agencia. El adjudicatario se obligará a participar en la posterior implementación conjunta de las recomendaciones/planes de mitigación propuestos como resultado de las revisiones.

Durante la ejecución de la propia revisión de salud se transferirá a los técnicos de la Agencia conocimiento sobre las herramientas utilizadas. Esa transferencia de conocimiento se completará con un informe detallado en el que se recopilará:

- Problemas presentes y/o potenciales, encontrados en el entorno y que podrían tener impactos negativos sobre el desarrollo del servicio.
- Puntos de mejora que ayuden a mantener el servicio en los mejores niveles de calidad.





- Planes de acción propuestos para solucionar los problemas y/o abordar los puntos de mejora identificados.
- **Revisiones del servicio de mensajería (Microsoft Exchange)**, con el objetivo de obtener una visión de la salud del entorno de producción del servicio de mensajería permitiendo:
  - Mantener los sistemas en un punto óptimo de rendimiento y soporte.
  - Identificar síntomas y/o problemas potenciales antes de que el entorno de producción resulte afectado.
  - Revisar los procesos críticos para reducir el tiempo de parada en caso de efectuar una recuperación de desastres.
  - Identificar y corregir cuellos de botella de rendimiento, incrementando la productividad y eficiencia del sistema de correo Exchange.
  - Identificar advertencias o alarmas que puedan afectar a los usuarios de forma negativa

El proceso de revisión hará uso de las necesarias herramientas para datos y estadísticas de los aspectos más críticos e importantes de un entorno Exchange como son: operaciones, rendimiento, infraestructura, seguridad y enrutamiento.

- Al finalizar el análisis se entregará un **informe de salud** con la información obtenida así como las recomendaciones para asegurar la salud del entorno de correo Exchange. En el informe se identificarán y clasificarán los riesgos en función del potencial impacto que pueden tener sobre el servicio. Las recomendaciones se ajustarán al entorno específico de la Agencia, tanto en lo que respecta a su infraestructura tecnológica como a los procesos que tiene implantados.
- El adjudicatario proporcionará un plan de acción concreto para la mitigación de cada uno de los riesgos identificados o la corrección de los problemas existentes, de forma que se pueda prevenir su ocurrencia o reducir el posible impacto. Al final del chequeo, el adjudicatario proporcionará el resultado del análisis, certificado por Microsoft, así como una guía con recomendaciones específicas para corregir los riesgos identificados. Las acciones derivadas de las recomendaciones realizadas alimentarán el plan de seguimiento semanal del servicio.
- **Revisiones del servicio de directorio corporativo (Microsoft Directorio Activo)**, con el objetivo de obtener una visión de la salud del entorno de producción del servicio de directorio permitiendo:
  - Reconocer los síntomas de posibles problemas antes de que estos ocurran, haciendo uso de una adecuada monitorización.
  - Comprensión de la replicación del directorio activo y capacidad de análisis problemas ante fallos.
  - Conocer las mejores prácticas de soporte del directorio.
  - Conocer problemas y errores comunes en la administración de los servicios de directorio.
  - Capacidad para afinar el directorio e incrementar la eficiencia en la administración del mismo.





- El proceso de revisión de salud del directorio activo hará uso de herramientas para recoger datos y estadísticas de los aspectos más importantes del directorio en Windows, como son: replicación de directorio, resolución de nombres, consistencia del "SYSVOL" y las políticas de grupo, backup y recuperación de desastres, y el comportamiento de los controladores de dominio.
- El adjudicatario garantizará que todas las herramientas utilizadas para la realización de la revisión de salud del directorio no introduzcan ninguna modificación en el entorno de producción, además de cumplir que el impacto sobre el uso de los recursos sea reducido y controlado.
- Al finalizar esta fase, se entregará un **informe de salud** con la información obtenida así como las recomendaciones para asegurar la salud del entorno de Directorio Activo. En el informe se identificarán y clasificarán los riesgos en función del potencial impacto que pueden tener sobre el servicio. Las recomendaciones se ajustarán al entorno específico de la Agencia, tanto en lo que respecta a su entorno tecnológico como a los procesos que tiene implantados.
- El adjudicatario proporcionará un "Plan de Acción" concreto para la mitigación de cada uno de los riesgos identificados o la corrección de los problemas existentes, de forma que se pueda prevenir su ocurrencia o reducir el posible impacto. Al final del chequeo, proporcionará el resultado del análisis, certificado por Microsoft, así como una guía con recomendaciones específicas para atajar los riesgos identificados. Las acciones derivadas de las recomendaciones realizadas alimentarán el plan de seguimiento semanal del servicio.

### 3.2 Mantenimiento correctivo

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 actualizados y a disposición de la Agencia, una lista completa de los productos bajo soporte y el nivel de servicio.

A continuación se detalla el compromiso que deberá cumplir el adjudicatario dependiendo de la severidad de dichos incidentes.

- **Notificación de incidencias.** Se requiere un soporte técnico telefónico y vía Internet en horario **24x7, 365 días** al año para la resolución de incidencias y problemas cuyos síntomas se manifiestan mientras se utilizan productos de Microsoft y donde hay una expectativa razonable de que el problema ha sido motivado por dichos productos de Microsoft.

La Agencia siempre definirá la severidad inicial del incidente y tendrá la posibilidad de abrir todos los incidentes de soporte directamente con los ingenieros de soporte del fabricante en España y a nivel mundial, mediante credenciales individuales de acceso telefónico para clientes Premier de Microsoft, dado que en su caso pueden tener acceso al código fuente de los productos. En el caso de que dicha severidad se defina con los grados más altos de criticidad, se incluirán las visitas "*on-site*" necesarias por parte de personal experto del adjudicatario.

Un "**incidente**" se define como una única cuestión de soporte y el esfuerzo razonablemente 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 aceptable. Un incidente puede requerir 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 la Agencia remotamente para analizar problemas. Esto será hecho exclusivamente con el consentimiento de la Agencia, y el personal del adjudicatario accederá exclusivamente a los sistemas autorizados por la Agencia. El adjudicatario deberá proporcionar a la Agencia software para asistirle en el diagnóstico y/o resolución del problema.
- **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 de Microsoft implican interacciones con productos de terceros, y la Agencia tenga acuerdos de soporte con dichos terceros, el adjudicatario compartirá información de diagnóstico y colaborará con ellos para proporcionar una solución.
- 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 acceso para el personal designado por el contratista para la ejecución de los trabajos al lugar donde se encuentren instalados los productos objeto del presente contrato.

### 3.2.1 Tipificación de incidencias y niveles de servicio:

Con el objetivo de dividir las incidencias según el impacto que tenga en el servicio al usuario y/o número de usuarios afectados, se establece por orden de severidad (de mayor a menor) la siguiente clasificación de incidencias y sus respectivos niveles de servicio:

- **Catastrófica**, incidencia que afecta de forma crítica al entorno de producción, dejando sin servicio a todos los usuarios de la Comunidad de Madrid. La incidencia necesita atención inmediata y ser escalada rápidamente a los equipos de producto. Se exige un **tiempo máximo de respuesta de 1 hora**.
- **Crítica**, incidencia que afecta de forma grave al entorno de producción, dejándolo inoperativo y afectando a un alto número de usuarios, o bien, aunque el entorno de producción de los sistemas de información esté operativo, se esté degradando o exista posibilidad de pérdida de información. El **tiempo máximo de respuesta para este nivel de servicio, es de 1 hora**.
- **Urgente**, incidencia que afecta al entorno de producción, de forma que aunque no exista posibilidad de parada del sistema, se observe un funcionamiento ralentizado o inadecuado del sistema. En este caso se exige un **tiempo máximo de respuesta de 2 horas**.
- **Importante**, incidencia que afecta a la productividad de un número pequeño de usuarios y que requiere una respuesta en un **tiempo máximo de 4 horas**.

Se entiende por **tiempo de respuesta** el tiempo transcurrido entre el momento en que se notifica la incidencia y el momento en que un recurso de la empresa adjudicataria, previa comunicación telefónica con el técnico que abre el incidente, informa a la Agencia de la posible causa de la incidencia y las acciones correctivas a realizar, con los plazos en los que se llevarán a cabo.





La severidad del incidente determinará los tiempos de respuesta estimados. Será responsabilidad de la Agencia calificar la incidencia que se produzca de acuerdo con la tipología anterior, notificándolo al adjudicatario para que proceda al efecto.

### **3.2.2 Soporte presencial en situaciones de incidencias catastróficas o críticas:**

- **Nivel de servicio general (Todos los productos excepto MS Exchange y D.A.)**

La determinación del tipo de soporte necesario en cada incidencia se determinará en función de la criticidad, teniendo la Agencia la posibilidad de exigir el soporte presencial al adjudicatario en las incidencias tipificadas como catastróficas o críticas.

El adjudicatario deberá garantizar el soporte presencial de un Ingeniero de Soporte en las instalaciones de la CM si se produce una **incidencia tipificada como crítica o catastrófica**. El horario de atención de este tipo de incidencias será de **24 horas, 7 días a la semana**.

El **tiempo máximo de respuesta**, en el que el Ingeniero **se presentará** en las instalaciones de la CM, dependiendo del horario en el que se notifique la incidencia crítica o catastrófica, será el siguiente:

- De lunes a viernes desde las 8:00 h hasta las 20:00 h.: **2 horas**.
- De lunes a viernes desde las 20:00 hasta las 8:00 del día siguiente, fines de semana y festivos: **4 horas**

En función del servicio descrito y tipificado por nivel de importancia, 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 reparaciones, tales como mano de obra, materiales o piezas de recambio, gastos de desplazamiento y transporte, impuestos, etc.

- **Nivel de servicio específico para MS Exchange y D.A.**

En el caso de que la situación catastrófica o crítica se produzca sobre el Directorio Activo o Exchange, el personal designado para realizar estas tareas de soporte presencial deberá contar con los conocimientos técnicos y experiencia en los sistemas utilizados por la Agencia.

Se establece en todo caso:

- Tiempo de respuesta máximo de **1 hora**.
- Tiempo máximo para que se persone un ingeniero cualificado en las instalaciones de la CM de **2 horas**.

### **3.2.3 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, se documentará e informará con el objeto de verificar la calidad de la solución.





Periódicamente, el responsable técnico nombrado 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.

#### **3.2.4 Resolución de problemas:**

La Agencia tendrá la posibilidad de poder solicitar directamente al fabricante el desarrollo de parches o 'hotfixes' asociados a posibles errores de producto, cambios de diseño de producto no críticos, o cambios de diseño de productos críticos.

Este tipo de solicitudes se realizará ante aquellos casos en que la complejidad de los posibles problemas detectados o el impacto en la actividad de la Agencia así lo requieran.

### **3.3 Servicios de Información**

Estos servicios proporcionarán información técnica acerca de los productos y herramientas de soporte que facilitarán la implementación y la operación de productos de Microsoft de una manera efectiva.

En concreto será obligatorio para el adjudicatario proporcionar la siguiente documentación e información:

- **Servicio Web** con boletines de noticias, con la última información de actualización de productos, alertas sobre nuevos virus, información de incidencias frecuentes y propuestas de resolución, etc., conteniendo al menos lo siguiente:
  - Boletines de noticias de producto actualizadas que documenten la información clave de operaciones y soporte sobre los productos de Microsoft.
  - Alertas a Problemas Críticos que notifiquen de manera anticipada sobre la existencia de problemas potenciales con un posible alto impacto.
  - Acceso a una herramienta que permita el envío de incidentes a los ingenieros de soporte y hacer un seguimiento de los mismos.
  - Acceso una base de datos de conocimientos y artículos técnicos, así como a herramientas y guías de soporte.
  - Participación en sesiones online a través de Internet sobre áreas clave de las Tecnologías de Microsoft (webcast de soporte).

En ese sentido el personal de la Agencia dispondrá de cuentas de acceso directo e ilimitado a la web "Microsoft Premier Online".

- **Sesiones Técnicas con Expertos de Soporte.** Estas sesiones presenciales se celebrarán en Madrid y serán impartidas en castellano por ingenieros de soporte especialistas en las áreas tecnológicas y productos específicos de interés por la Agencia.





- **Talleres (Workshops).** Se realizarán sesiones técnicas de trabajo específicas en determinados aspectos tecnológicos y estarán dirigidas a transferir el conocimiento sobre la utilización de herramientas de soporte, técnicas de resolución de problemas, aspectos técnicos de funcionamiento de productos y las mejores prácticas, que permita mejorar el conocimiento y mantenimiento de los productos Microsoft en la Agencia. Se podrán celebrar, bien en las instalaciones del adjudicatario, o bien en las instalaciones que la Agencia decida con el fin de maximizar el aprovechamiento de las mismas.

A solicitud de la Agencia, el adjudicatario estará obligado a realizar sesiones técnicas de trabajo dirigidas al personal designado por el *Responsable del Contrato* de la Agencia, con el objeto de transferir conocimiento sobre la utilización de herramientas de soporte, técnicas de resolución de problemas, aspectos técnicos de funcionamiento de productos y las mejores prácticas de explotación, y cualquier otra información que permita mejorar el conocimiento y mantenimiento de los productos Microsoft.

Asimismo el adjudicatario deberá documentar exhaustivamente las soluciones a las incidencias producidas, aportando cualquier información adicional que se le pueda requerir.

### **3.4 Soporte Técnico Especializado**

Será realizado por Ingenieros especialistas en los distintos productos de Microsoft. Estos trabajos se realizarán a petición de la Agencia y en un ámbito concreto, llevando a cabo actividades de asesoramiento en la adaptación de nuevos productos y/o versiones de productos ya instalados a la arquitectura de la Agencia. Analizarán las actuaciones que haya que realizar en los distintos componentes de la base instalada en la CM para incorporar nuevas versiones y/o productos Microsoft. Realizarán servicios de instalación conjunta con personal de la Agencia para nuevas versiones y Soporte a nuevas instalaciones/actualizaciones hasta la estabilidad en producción del producto.

#### **3.4.1 Migración de correo Exchange 2013**

En el ámbito del Soporte Técnico Especializado a la Migración de la plataforma de correo corporativo (institucional y sanidad) a Exchange 2013, se consideran los servicios de análisis y apoyo en las fases de migración y coexistencia, así como en la elaboración y adaptación de las guías de operación, mantenimiento y recuperación ante desastres. Apoyo en las pruebas de validación del entorno y durante el paso a producción, así como durante el piloto que se realice durante la migración de los buzones.

Es necesario tener en cuenta que el número de los buzones a migrar es aproximadamente 100.000, incluyendo todas las Consejería del entorno Institucional y Sanitario. También hay que destacar la criticidad de este servicio, teniendo en cuenta el elevado número de Altos Cargos que se encuentran afectados por esta migración.

## **4 CLÁUSULA 4 - CONDICIONES ADICIONALES A CUMPLIR**

### **4.1 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 el objeto del contrato.





#### **4.2 Responsable del Servicio**

El adjudicatario designará un *Responsable del Servicio* ante la Agencia.

*El licitador con carácter previo a la adjudicación del contrato, deberá aportar el Curriculum Vitae de dicho Responsable, y que deberá presentar debidamente firmado por la persona que ostente la representación, especificando su cualificación profesional (con detalle de categoría, titulación, formación y actividad profesional).*

Este Responsable se encontrará en permanente contacto con el personal de la Agencia designado por la Dirección de la Agencia.

Este responsable realizará, principal y específicamente las siguientes tareas:

- Tener actualizada y a disposición de la Agencia una lista completa de los productos bajo soporte y el nivel de servicio.
- Gestionar el contrato realizando las siguientes tareas:
  - Informes de las acciones de mantenimiento preventivo realizadas, y de propuestas de mejora de los servicios de información actuales.
  - Informes de las actividades de mantenimiento correctivo (gestión y resolución de incidencias) con descripción de las actividades realizadas y tiempo empleado en su resolución.

Estos informes serán como mínimo mensuales; quedando al designio de la Agencia disminuir la periodicidad de los reportes.

- Coordinar y ser el interlocutor de las peticiones de servicio y de información de la Agencia con el resto de la organización del contratista.
- Coordinar el mantenimiento correctivo, garantizando que las incidencias que se produzcan son correctamente escaladas. En el caso de incidencias designadas como catastróficas o críticas por la Agencia esta coordinación deberá ser especialmente diligente y efectiva.
- Proponer mejoras en la infraestructura hardware y software que soporta a los productos Microsoft, como resultado del estudio que realice de la instalación existente.
- Informar y mantener al día a las personas designadas por la Agencia de las diversas fuentes de información técnica disponibles y del estado del arte de las tecnologías Microsoft.
- Mensualmente, al menos, mantener con los empleados designados por la Agencia, una reunión para revisar las actuaciones preventivas y reactivas realizadas, seguimiento y resolución de incidencias y revisión de informes. Adicionalmente se establecerá en esta reunión las líneas de trabajo del mes siguiente.
- Realizar una estimación previa de las actividades de soporte preventivo y correctivo, así como de todas las actividades de soporte que tengan un impacto en el desarrollo del contrato.

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







## **5 CLÁUSULA 5 – OBLIGACIONES DEL ADJUDICATARIO**

El adjudicatario asegurará la disponibilidad de los productos contratados durante el periodo de ejecución del presente contrato en el caso de que la evolución tecnológica de dichos productos suponga un cambio de denominación, y siempre que la funcionalidad de dichos productos sea la misma o aporte mejoras sobre las actuales.

## **6 CLÁUSULA 6 - DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS DE LA AGENCIA**

El contratista no adquiere ningún derecho sobre el hardware (material), software (aplicativos) 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 objeto 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 escrito de la Agencia.

## **7 CLÁUSULA 7 - SEGUIMIENTO Y CONTROL DEL SERVICIO**

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de la Agencia, con objeto de garantizar la correcta ejecución de los mismos.

De cara a alcanzar estos objetivos se define una estructura de seguimiento de dos niveles:

- Un nivel estratégico orientado a la evolución del contrato y la mejora de los servicios, que se encargará de velar porque la estrategia y objetivos de la contratación de certificados y servicios estén alineados con los de la Agencia, y de controlar y garantizar que todas las decisiones y operaciones se ajustan a dicha estrategia.
- Un nivel operativo ligado a la ejecución concreta de los certificados y servicios que se encargará de transformar las decisiones estratégicas en planes de acción y de dirigir y controlar los esfuerzos necesarios para su ejecución. En este nivel el adjudicatario se responsabiliza de la gestión, ejecución, supervisión técnica y control diario de los certificados y servicios.

Atendiendo a la estructura señalada se establecerán dos Comités diferenciados para el control y la toma de decisiones:

- **Comité de Seguimiento del Contrato (estratégico)**
- **Comité Operativo (operativo)**

### **7.1 Comité de seguimiento del contrato**

Estará compuesto por los siguientes miembros:

Por parte de la Agencia:

- El Subdirector General de Infraestructuras y Operaciones, a petición propia.
- El Director competente en materia de Ingeniería.
- El Director competente en materia de Producción.

Opcionalmente, y por indicación del responsable del contrato el/los Director/es competentes en materia de Servicios a Clientes o cualquier otro de la Agencia requerido.





Estos miembros podrán ser sustituidos por persona perteneciente a su Dirección, designada por ellos mismos con antelación suficiente.

Por parte de la empresa adjudicataria:

- El Responsable del Servicio ante la Agencia.

No obstante lo anterior, se podrá requerir la presencia de otros miembros distintos a los señalados que se estimen oportunos para la correcta realización de las sesiones de los mismos.

El Comité de Seguimiento del Contrato se desarrollará en reuniones con periodicidad trimestral, y tendrá entre otras, las siguientes funciones:

1. Monitorizar el avance global de los servicios.
2. Aprobar los cambios propuestos en el seno de los Comités Operativos que afectan de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o que, por su impacto o importancia estratégica, requieran la aprobación del Comité.
3. Revisar y aprobar el borrador de factura y resolver cualquier incidencia o problema relacionado con los certificados y servicios a facturar en el periodo objeto de revisión.
4. Cualquier otro asunto que el propio Comité considere de interés.

La Agencia podrá convocar reuniones extraordinarias por la existencia de circunstancias que lo hagan necesario.

Los acuerdos adoptados en el seno del Comité de Seguimiento deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas, y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

## **7.2 Comité operativo**

Estará formado como mínimo por los siguientes miembros:

Por parte de la Agencia:

- Los Jefes de las Áreas responsables del seguimiento de los servicios.
- Los Jefes de Unidad responsables de los servicios de Ingeniería del Puesto Ofimático Básico y de Correo Electrónico y Directorio Activo

Estos miembros podrán ser sustituidos por personal perteneciente a su Dirección, designada por ellos mismos con antelación suficiente.

Por parte de la empresa adjudicataria:

- Responsable del Servicio ante la Agencia.

No obstante lo anterior, se podrá requerir la presencia de otros miembros distintos a los señalados que se estimen oportunos para la correcta realización de las sesiones de los mismos.

El Comité Operativo se reunirá con periodicidad mensual y tendrá, entre otras, las siguientes funciones:

1. Seguimiento y evaluación del progreso de los trabajos objeto del contrato, tareas y actividades para la prestación del servicio y evaluación de riesgos.





2. Garantizar que el personal asignado por el contratista para la ejecución de los servicios está disponible, y cuenta con los medios, formación y soporte necesarios para la correcta ejecución de sus tareas.
3. Verificar el cumplimiento de los requisitos establecidos para la prestación del servicio y revisar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) de cada periodo.
4. Analizar y validar si procede las propuestas de mejora del servicio efectuadas por el adjudicatario. En caso de que las propuestas afecten de forma horizontal a diferentes ámbitos de servicio, procesos de gestión, o tengan impacto o importancia estratégica, serán elevadas al Comité de Seguimiento del Contrato.
5. Revisar el estado y evolución de los Planes de mejora acordados y cumplimiento de los compromisos aprobados.
6. Cualquier otro asunto que el propio Comité considere de interés.

Los acuerdos adoptados en el seno del Comité deberán serlo por mutuo acuerdo de las partes, elaborándose acta de cada una de las reuniones. El adjudicatario será responsable de la elaboración de las actas, y su traslado a revisión por los asistentes en las 48 horas siguientes a la finalización del Comité; la incorporación de las modificaciones o comentarios pertinentes fruto de su revisión y la presentación del acta definitiva para la firma de los asistentes.

### **7.3 Informes de Seguimiento del Servicio**

El adjudicatario proporcionará a la Agencia informes de gestión, en soporte electrónico compatible con Microsoft Office, con periodicidad trimestral, y con al menos 48 horas de antelación a las reuniones del Comité de Seguimiento, sin perjuicio de la potestad de la Agencia para exigir otros informes cuando así lo demande.

Asimismo, se emitirá un informe por el adjudicatario antes de la última semana de vigencia del contrato.

## **8 CLÁUSULA 8 – 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 así como 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:

- Definir, implementar y mantener una política de seguridad.
- Implantar las medidas de seguridad con el objeto de proteger los datos, infraestructuras, servicios y sistemas de información de la Comunidad de Madrid, en respuesta a los requisitos especificados en este clausulado.





- 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.

Los siguientes apartados establecen las condiciones y medidas en materia de seguridad que el adjudicatario deberá implantar y mantener para la prestación de los servicios. 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 sujeto a lo dispuesto en la legislación vigente y al cuerpo normativo de seguridad de la Agencia.

## **8.1 Protocolos y Procedimientos de Seguridad**

### **8.1.1 Criterios de clasificación de los servicios**

El adjudicatario tipificará cada servicio prestado según los siguientes criterios de clasificación:

- Lugar de ejecución del servicio: En función del lugar principal en el que se desarrollen los servicios se distinguen dos casos:
  1. Comunidad de Madrid: El proveedor presta el servicio principalmente en dependencias de la Comunidad de Madrid.
  2. Remoto: El proveedor presta el servicio principalmente desde sus propias dependencias.
- Propiedad de las infraestructuras TIC utilizadas: En función de quién sea el propietario de las principales infraestructuras TIC (comunicaciones, equipos de usuario, software) utilizadas para prestar el servicio se distinguen dos casos:
  1. Comunidad de Madrid: La mayor parte de las infraestructuras TIC utilizadas para prestar el servicio son propiedad de la Comunidad de Madrid, siendo las proporcionadas por el adjudicatario una minoría o complementarias.
  2. Adjudicatario: La mayor parte de las infraestructuras TIC utilizadas para prestar el servicio son propiedad del proveedor del servicio, siendo poco significativas dentro del servicio las proporcionadas por la Comunidad de Madrid.
- Nivel de acceso a información y sistemas de la Comunidad de Madrid: En función del nivel de acceso a la información y a los sistemas de información de la Comunidad de Madrid se distinguen cuatro casos:
  1. Sin acceso: El servicio provisto no requiere de conocimiento de información ni la utilización de los sistemas de información de la Comunidad de Madrid, de modo que el personal que presta el servicio no dispone de cuentas de usuario en dichos sistemas.
  2. Con acceso de nivel de usuario: El servicio provisto requiere de acceso a la información o la utilización de los sistemas de información de la Comunidad de Madrid, de modo que el personal que presta el servicio dispone de cuentas de usuario que les permiten acceder a alguno de dichos sistemas con privilegios habituales.
  3. Con acceso privilegiado: El servicio provisto requiere de la capacidad de acceso privilegiado a información o sistemas de información de la Comunidad de Madrid, con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.





4. Con acceso físico: El servicio provisto requiere el acceso físico a los sistemas de información de la Comunidad de Madrid, con capacidad para intervenir, retirar, cambiar, guardar, trasladar o destruir sistemas o soportes con información.

#### **8.1.2 Definición e implantación de los protocolos y procedimientos**

El adjudicatario deberá definir los protocolos y procedimientos de actuación específicos en materia de seguridad, en función de las características de cada uno de los servicios prestados a la Agencia y de la clasificación realizada de los mismos.

En función de cada una de las tres categorías en las que se encuadre cada servicio, el proveedor deberá desarrollar y cumplir los requisitos expresados en este clausulado, con protocolos y procedimientos específicos. A continuación se relacionan los dominios de seguridad que se deberán contemplar:

- Documentación de Seguridad.
- Organización de la seguridad.
- Obligaciones del personal.
- Formación del personal.
- Gestión de incidencias de seguridad.
- Gestión de soportes de información.
- Acceso lógico.
- Acceso físico.
- Segregación de funciones.

Los requisitos de seguridad específicos de cada dominio, asociado a la clasificación de los servicios quedan explicados en los apartados siguientes.

#### **8.1.3 Documentación de seguridad**

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

1. 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 para todos los miembros de la organización que intervengan en la prestación del servicio y redactado de forma sencilla, precisa y comprensible.
2. 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 Coordinador de Seguridad (denominado SEG). El Documento de Seguridad incluirá asimismo la clasificación de cada uno de los servicios según la tipificación del apartado anterior, y la asignación de cada usuario a







cada tipo de servicio, los procedimientos y protocolos desarrollados y el nivel de cumplimiento de cada usuario y del tipo del servicio.

#### **8.1.4 Organización de seguridad**

Todas las responsabilidades en el ámbito descrito de seguridad deben estar claramente definidas.

Se debe proponer un Coordinador de Seguridad que asuma la tarea general del desarrollo y la implementación de la seguridad y fundamente la identificación de medidas de seguridad. Esta figura tendrá las funciones y perfil descritos en la Cláusula ORGANIZACIÓN DEL EQUIPO PRESTADOR DEL SERVICIO.

#### **8.1.5 Obligaciones del personal**

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".

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.
- Comunicar por el canal establecido cualquier incidencia que se detecte y que tenga relación con la Información Confidencial, los recursos de la Comunidad de Madrid o el servicio que se le presta.
- 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, según el criterio o indicación de la Agencia.

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.

Se deberá acreditar el conocimiento y compromiso de la cláusula de seguridad de este pliego por parte de todos los usuarios, y especialmente las referidas a las obligaciones contraídas por cada una de las personas que presta el servicio, 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.

#### **8.1.6 Formación y concienciación del personal**

El contratista se compromete a formar a su personal sobre las obligaciones que deben contraer respecto de la cláusula de seguridad de este pliego y de los protocolos y procedimientos de seguridad definidos y desarrollados para dar respuesta a la misma, para lo cual programará las acciones formativas necesarias.

El adjudicatario deberá 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. La formación será presencial, al inicio de la prestación del servicio y cada seis meses, y virtual o a través de los medios de comunicación que estime oportuno cada dos meses.

El personal asignado a servicios con acceso privilegiado y físico requerirá una formación específica adicional, con una periodicidad mínima trimestral. Asimismo el adjudicatario deberá acreditar que este personal ha superado en cada convocatoria una prueba objetiva de aprovechamiento de la formación y concienciación.

#### **8.1.7 Gestión de incidentes de seguridad**

El adjudicatario deberá contar con un proceso de gestión de incidentes de seguridad que deberá seguir todo el personal al que le aplique cualquier tipo de acceso (tanto privilegiado como no privilegiado) a los datos o a los sistemas de información de la Comunidad de Madrid independientemente del lugar en el que se presten.

El proceso deberá cumplir las siguientes medidas:

- a) Deberá existir un medio de comunicación de incidencias, un equipo gestor de las mismas y un Coordinador de Seguridad.
- b) Todo el personal asignado al servicio deberá comunicar por el canal establecido cualquier incidencia que se detecte y que tenga relación con la información, los recursos de la Comunidad de Madrid o el servicio que se le presta. La falta de comunicación será considerada como una falta grave en la prestación del servicio y motivará la adopción de todas las medidas necesarias para evitar que ello se vuelva a producir.
- c) Cualquier usuario podrá trasladar al Coordinador de Seguridad sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que pueda tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.





- d) Se deberá notificar al gestor de incidencias cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
- e) Todas las actividades relacionadas con la gestión de incidencias, desde su notificación hasta su solución o archivo deberá quedar registrado en un Registro de Incidencias, que estará disponible permanentemente y a disposición de la Agencia.

El proceso incluirá los siguientes procedimientos:

- Análisis de la causa del incidente.
- Contención.
- Implementación de la acción correctiva.
- Comunicaciones a los afectados.
- Reporte de la acción a los interlocutores apropiados.

El catálogo de incidentes de seguridad es el que se relaciona a continuación:

- **ACCESOS NO AUTORIZADOS:** Esta categoría comprende las siguientes actividades:
  1. Uso compartido, o sospecha, de credenciales de acceso.
  2. Uso, o sospecha, de credenciales de un tercero.
  3. Accesos no autorizados, o sospecha, con o sin daños visibles a los componentes tecnológicos.
  4. Robo de información.
  5. Borrado de información.
  6. Alteración de la información.
  7. Intentos de acceso no autorizado.
  8. Abuso o mal uso de los servicios informáticos internos o externo que requieren autenticación.
- **CÓDIGO MALICIOSO:** Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica. Son parte de esta categoría:
  1. Virus informáticos.
  2. Troyanos
  3. Gusanos informáticos
- **DENEGACIÓN DEL SERVICIO:** Esta categoría incluye los eventos que ocasionan la pérdida de un servicio en particular. Los síntomas para determinar un incidente de esta categoría son:
  1. Tiempos de respuesta muy bajos sin razones aparentes.
  2. Servicios internos inaccesibles, sin razón aparente.
  3. Servicios externos inaccesibles, sin razón aparente.
- **INTENTO DE OBTENCIÓN DE INFORMACIÓN:** Esta categoría agrupa los eventos que buscan obtener información sobre la infraestructura tecnológica. Son parte de esta categoría:





1. Sniffers
2. Detección de Vulnerabilidades
- **MAL USO DE LOS RECURSOS TECNOLÓGICOS:** Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por su mal uso. Son parte de esta categoría:
  1. Mal uso o abuso de servicios informáticos internos o externos.
  2. Uso de la Red de Comunicaciones de la Comunidad de Madrid para acceso o descarga de datos, ficheros, archivos, etc. no relacionados con el objeto del presente contrato
  3. Violación de las normas de acceso a internet de la Comunidad de Madrid. Acceso a información englobada o relacionada con cualquiera de estas categorías: pornografía infantil, violencia, incitación al odio, discriminación y violencia racial o de otro tipo, materiales que pueden afectar al desarrollo físico y mental de los menores, así como otras categorías tales, sexo, intolerancia, drogas, desnudos, incitación a la comisión de delitos y cualesquiera otros que pudieran no ser necesarios para la prestación de los servicios que son objeto del presente contrato.
  4. Mal uso del correo electrónico de la empresa que pudiera tener un impacto en los usuarios y sistemas de información de la Comunidad de Madrid.
  5. Violación de las normas, políticas y procedimientos de seguridad

El adjudicatario deberá poner a disposición de la Agencia con periodicidad mensual de un informe de incidentes de seguridad relacionados con el servicio prestado, detallando la información asociada a cada uno de los incidentes que se recoja en el registro de incidentes habilitado en el ámbito de la prestación del servicio.

#### **8.1.8 Gestión de soportes de información**

Se deberá evitar la revelación, modificación o destrucción no autorizada de los activos propiedad de la Comunidad de Madrid, tanto soportes electrónicos como no electrónicos –soporte papel– durante su custodia y transporte, e implantar una política de borrado y destrucción segura de los mismos.

Los soportes que contienen información confidencial, una vez finalizada su función, deberán ser destruidos físicamente, borrados o sobre-escritos utilizando técnicas que hagan imposible recuperar la información original.

#### **8.1.9 Acceso lógico**

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 las normas y procedimientos disponibles para la gestión de identidades de la Agencia y de la Comunidad de Madrid.

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

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 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.

#### **8.1.10 Acceso físico**

Se definirán los requisitos específicos para garantizar la seguridad dentro de las oficinas administrativas, zonas abiertas al público, las salas de servidores y centros de explotación, zonas de archivo, salas de equipamiento eléctrico o comunicaciones, y cualquier otra zona que en virtud del activo albergado deba ser considerada como segura.

Por tanto, el control de acceso deberá ser acorde con la clasificación de los activos y la función de tratamiento que en ellas se desarrolle. Asimismo se generará un protocolo de acceso a las instalaciones de la Comunidad de Madrid, de acuerdo con los procedimientos vigentes de acceso de esta Administración.

El personal asignado a los servicios cuya ubicación sea la Comunidad de Madrid o su tipo de acceso sea físico estará obligado a llevar una acreditación en lugar visible y a seguir un protocolo de normas de actuación específico.

Todos los costes de los medios técnicos y materiales que sean precisos para poder cumplir con lo establecido en el protocolo de acceso y para facilitar y proporcionar la acreditación del personal, serán soportados por cuenta de la empresa prestadora del servicio.

#### **8.1.11 Segregación de funciones**

Se deberá introducir en todos los ámbitos de la seguridad donde sea posible la segregación de funciones con el fin de que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Se debiera separar la iniciación de un evento de su autorización y se debiera considerar la posibilidad de colisión en el diseño de los controles.

Como mínimo deberá implantarse la segregación de funciones en los servicios con acceso de tipo privilegiado y físico. La tabla resumen de aplicación de las tipologías de servicios definidas se muestra a continuación:





	UBICACIÓN		INFRAESTRUCTURA		ACCESO			
	CM	Remoto	CM	Adjudicatario	Sin acceso	Usuario	Privilegiado	Físico
Documentación de Seguridad	X	X	X	X	X	X	X	X
Organización de la seguridad	X	X	X	X	X	X	X	X
Funciones y obligaciones del personal	X	X	X	X	X	X	X	X
Formación del personal	X	X	X	X	X	X	X	X
Gestión de Incidencias de seguridad	X	X	X	X	X	X	X	X
Gestión de soportes de información	X		X	X				X
Acceso lógico	X	X	X	X		X	X	X
Acceso físico	X	X	X	X	X	X	X	X
Segregación de funciones							X	X

## 8.2 Protección de Datos de Carácter Personal

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

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona, en adelante LOPD.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en los términos previstos en su Disposición Transitoria Segunda).

Disposiciones de desarrollo de las normas anteriores en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

## 8.3 Medidas de seguridad de carácter mínimo

- No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por el R.D. 1720/2007 respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. (Artículo 9.2. LOPD):
  - En la fase de diseño funcional, y si del estudio previo de cada sistema de referencia procediera se propondrá la correspondiente creación e inscripción en la Agencia Estatal de Protección de Datos, en adelante AEPD.
  - 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:





- i. 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.
  - ii. 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 Agencia. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por la Agencia. 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.
  - iii. 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.
  - iv. 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.
  - v. 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.
  - vi. 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.
  - vii. 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.
  - viii. 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
- c. 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 aquellos 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:

- i. 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.
  - ii. 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.
  - iii. Será necesaria la autorización de la Agencia para la ejecución de los procedimientos de recuperación de los datos.
- d. Además de las medidas enumeradas en los anteriores apartados, 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); 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:
- i. 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.
  - ii. 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.
  - iii. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. El registro de los accesos deberá integrarse con el sistema de información de la Comunidad de Madrid para la gestión y explotación de la información resultante de los accesos (SGUR).
  - iv. 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.







- v. 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.

#### **8.4 Cesión o comunicación de datos a terceros**

1. 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 la Agencia, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
2. 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 exonerará al equipo prestador del servicio de su obligación de tratar dicha Información Confidencial como estrictamente confidencial aún finalizada la relación convencional existente entre las mismas.

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

3. De acuerdo con lo dispuesto en la letra c) del apartado Tres del artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas, 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 del Real Decreto 1720/2007, de 21 de diciembre, se limitará a los servicios que constituyen el objeto del presente contrato.

El contenido del servicio contratado estará determinado por el conjunto de derechos y obligaciones que, en virtud del presente contrato, asume el contratista como encargado del tratamiento de datos personales. Sin perjuicio de las instrucciones que, adicionalmente, pudieran establecerse por el Encargado del Tratamiento, el contratista queda sujeto en el tratamiento de datos personales a las instrucciones procedentes del Responsable del Fichero.

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







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

Los datos personales recogidos podrán ser incorporados y tratados en el fichero PROVEEDORES, cuya finalidad es la solicitud de ofertas, selección y compra de bienes y servicios requeridos tanto por la Agencia como por la C.M., inscrito en el Registro General de Protección de Datos de la AEPD ([www.agpd.es](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.

### **8.6 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.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el ENS, se aplicarán de forma obligatoria las medidas de seguridad indicadas en su anexo II pertenecientes al marco organizativo. Respecto a los marcos operacional o de protección se atenderá, en su caso, a lo establecido en la declaración de aplicabilidad del servicio de Atención de Usuarios objeto de este contrato.

El Documento de Seguridad reflejará, además de lo estipulado con carácter general en el apartado Documentación de Seguridad, 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.

### **8.7 Propiedad de los trabajos**

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

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

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





### **8.8 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, smartphones, 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.

### **8.9 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:

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





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

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.

#### **9 CLÁUSULA 9 - PLAZO DE GARANTÍA**

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

Hasta que no tenga lugar la finalización del periodo de garantía, el adjudicatario responderá de la correcta ejecución de los trabajos contratados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de la Agencia los hayan examinado o reconocido durante su elaboración o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del trabajo.

#### **10 CLÁUSULA 10ª – CALIDAD**

Durante la ejecución del contrato, la Agencia podrá establecer acciones de aseguramiento de la calidad sobre la actividad desarrollada y los productos obtenidos. A tal fin, la Agencia podrá incorporar al proyecto los recursos que considere oportunos para garantizar su correcta ejecución.

#### **11 CLÁUSULA 11ª – PLAZO DE EJECUCIÓN**

El plazo de ejecución del presente contrato será de **TREINTA Y SEIS MESES (de 1 de septiembre de 2016 a 31 de agosto de 2019)**.

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

#### **12 CLÁUSULA 12ª – LUGAR DE PRESTACIÓN**

El lugar de prestación de estos servicios se realizará en la sede de la Agencia, situada en la calle Embajadores, número 181, de Madrid, de conformidad con la Agencia.

#### **13 CLÁUSULA 13ª – DOCUMENTACIÓN GENERADA DURANTE LA EJECUCIÓN DE LOS TRABAJOS**

La documentación generada durante la ejecución del contrato será propiedad exclusiva de la Agencia, y el adjudicatario no podrá trasladar su contenido o copia de la misma a terceros, sin la expresa autorización de la Agencia.

Toda la documentación se entregará en castellano, correctamente encuadernada y con una copia de cada documento. Asimismo, se entregará una copia de dicha documentación en soporte magnético compatible con las herramientas instaladas en la Agencia.





**14 CLÁUSULA 14ª – CONSULTAS TÉCNICAS SOBRE EL PLIEGO**

Durante el periodo de presentación de ofertas y ante cualquier duda o necesidad de aclaración referida a las especificaciones del Pliego de Cláusulas Técnicas, el licitador puede dirigirse a:

*La Agencia para la Administración Digital de la Comunidad de Madrid*

*Dirección de Ingeniería, Soporte a Gestión de Aplicaciones y Centros de Competencia*

*Área de Arquitecturas*

*Personas de contacto: Javier Gil López – José Antonio Campos*

*Tfno.: 91.580 50 00*

*Horario de consulta: 10:00 a 14:00h (De lunes a viernes)*

ELABORADO Y PROPUESTO POR: 19/07/2016

*La Directora de Producción y Gestión de Infraestructuras*

Fdo.: Julia Molina Franquelo

APROBADO POR: 21 JUL. 2016

*El Consejero Delegado de la Agencia para la Administración Digital de la C.M.*

Fdo.: Blas Labrador Román





**- ANEXO I -**

**REQUISITOS MÍNIMOS DEL SERVICIO SOPORTE PREMIER POR AÑO**

Componente	Descripción del Servicio	Detalle del Servicio	Cantidad Anual
Servicios Proactivos	Asesoramiento en problemas no incluidos en el Servicio de Resolución de Problemas y asistencia consultiva en cuestiones de diseño e implantación de tecnología Microsoft	Asistencia de Soporte de desarrollo e infraestructura	Incluido
		Servicios de Soporte para Operaciones de IT	
		Evaluaciones de Riesgos y Revisiones de Salud	
		Revisiones de Soporte y Remediación	
		Talleres (Workshops y Workshops Plus)	
		Sesiones de Transferencia de Conocimiento	
		Servicios de Soporte al Desarrollo	
Soporte para la resolución de problemas	Asistencia en la resolución de problemas en productos con tecnología Microsoft, así como soporte en entornos críticos con reacción inmediata (Directorio Activo y correo Exchange). Soporte con ingeniero Onsite	Soporte para la resolución de problemas	Incluido
		Cobertura 24x7	
		Gestión de Situaciones Catastróficas y Críticas 24x7	
		Soporte rápido in-situ	
		Desarrollo de hotfixes a medida	
		Servicios de Misión Crítica (Directorio Activo y Exchange)	
		Ingeniero de Soporte Generalista On-Site	2.520 horas
Servicios de Información	Información técnica sobre productos y herramientas de soporte de Microsoft	Acceso a la Web exclusiva Microsoft Premier Online	Incluido
		Acceso a los boletines de noticias de producto	
		Acceso a Web Response para la gestión de incidentes	
		Acceso a Knowledge Base confidencial para Partners	
		Participación en webcast de soporte	
		Descarga de actualizaciones de software y service packs	
Soporte Técnico Especializado	Acciones dirigidas al asesoramiento estratégico empresarial	Análisis de adaptabilidad de productos de Microsoft a la Agencia	Incluido
		Soporte en nuevas versiones y en su posible inclusión en la base instalada de la Agencia.	
		Servicios de instalación conjunta con personal de la Agencia para nuevas versiones.	
		Soporte a nuevas instalaciones/actualizaciones hasta la estabilidad en producción del producto	
Soporte Técnico Especializado para la Migración de la plataforma de Correo Exchange	Análisis y apoyo en las fases de diseño de la migración y coexistencia de ambas infraestructuras. Elaboración y adaptación de guías de operación y apoyo en el paso a producción, pruebas de validación y apoyo en el piloto de migración de buzones	Análisis y apoyo en la fase de diseño de migración y coexistencia. Apoyo en la elaboración y adaptación de las guías de operación. Apoyo durante el paso a producción y pruebas de validación del entorno y durante el piloto de migración de buzones por un máximo de 1.220 horas de servicio presencial	Incluido
Gestión Técnica de la Cuenta	Gestión, informes, plan de servicios y seguimiento técnico de la cuenta	Gestión Técnica de un gestor TAM (Technical Account Manager)	Incluido
		Plan de Servicios de Soporte	Incluido

