

PLIEGO DE CLÁUSULAS TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE SERVICIOS DENOMINADO “AUDITORIA, ASESORÍA Y CONTROL DEL CUMPLIMIENTO EN MATERIA DE SEGURIDAD DE LA COMUNIDAD DE MADRID”, A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS

CLÁUSULA 1.- INTRODUCCIÓN

Tras la entrada en vigor del **Artículo 4** de la **Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas** (BOCM Núm. 311, de 31 de diciembre de 2015), que modifica parcialmente el **Artículo 10** de la **Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas**, la Agencia de Informática y Comunicaciones de la Comunidad de Madrid pasa a denominarse **Agencia para la Administración Digital de la Comunidad de Madrid**, manteniendo su naturaleza, así como sus funciones recogidas en el precitado **Artículo 10, Tres, c)**, entre las cuales se encuentra la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, y en concreto:

1. 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.
2. El desarrollo y adquisición de aplicaciones informáticas y sistemas de información para la Comunidad de Madrid, y su mantenimiento y soporte posteriores, de acuerdo con las especificaciones funcionales y necesidades de los distintos centros directivos.
3. La adquisición y dotación de infraestructuras físicas y lógicas de soporte de los sistemas de información de la Comunidad de Madrid, y de sus servicios.

La Agencia para la Administración Digital de la Comunidad de Madrid (en adelante **Madrid Digital**), en su ámbito competencial, tiene asignadas entre otras funciones (además de las enumeradas más arriba), las siguientes:

- El control del cumplimiento de la normativa a que deberán atenerse los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones desarrollados o adquiridos por la Comunidad de Madrid, a fin de asegurar su utilidad y compatibilidad.
- El aseguramiento de la integración efectiva en la infraestructura física y lógica gestionada por la Agencia, y la adecuación a los estándares y normativa aplicable, de todos aquellos sistemas materiales o lógicos relativos a la informática y las comunicaciones que hubieran sido o fueran en el futuro transferidos a la Comunidad de Madrid desde otras entidades estatales o locales, en cualquier ámbito.
- La elaboración de la normativa e instrucciones para la utilización de los diferentes equipamientos por los usuarios.
- La seguridad, confidencialidad, integridad y disponibilidad de la información tratada, en su ámbito de responsabilidad.

Dentro del precitado ámbito competencial, es necesario verificar el grado de adecuación a los estándares y normativa aplicable en materia de seguridad mediante la realización de las oportunas auditorías y ejercer el control del cumplimiento normativo de tal forma que se evidencien las posibles deficiencias en materia de seguridad mediante la instauración del servicio apropiado.



CLÁUSULA 2.- OBJETO

La prestación de los servicios de **auditoría, asesoría, control e implantación del marco normativo en la Comunidad de Madrid para dar cumplimiento a la legislación, procedimientos y códigos de buenas prácticas en materia de seguridad de la información y protección de datos**, de conformidad con lo establecido en el presente Pliego de Cláusulas Técnicas y en los *Anexos* al mismo.

CLÁUSULA 3.- ALCANCE

En el **Anexo I** al presente Pliego se recoge la **volumetría** de ficheros y sistemas de información objeto de los trabajos, existentes en la fecha de inicio de la licitación.

El ámbito de aplicación se extenderá a los ficheros y sistemas de información actualizados a la fecha de inicio de la licitación, siendo tarea del adjudicatario proceder a la revisión del alcance y la actualización pertinente como paso previo a la ejecución de cualquiera de los trabajos.

A tal efecto, **el contratista asumirá, sin coste adicional para Madrid Digital, un incremento en el alcance hasta un 10%**, derivado de la inscripción o incorporación de nuevos ficheros **y calculada para cada uno de los conceptos de auditoría**, respecto del número que se indica en el *Anexo I* al presente Pliego.

El alcance de los trabajos a desarrollar se detalla a continuación en distintos epígrafes que corresponden al objeto del contrato:

A) Servicios de auditoría en materia de seguridad.

1. Auditoría de los procedimientos e instrucciones vigentes en materia de seguridad de datos personales:

Auditoría de los procedimientos e instrucciones vigentes en materia de seguridad de datos personales, de conformidad con lo establecido en los *Artículos 96 y 100 del Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD*, respecto a los ficheros de datos de carácter personal en los que Madrid Digital figura como Responsable del Fichero o Encargado del Tratamiento.

Esta auditoría habrá de verificar el grado de cumplimiento de las medidas de seguridad del nivel correspondiente establecidas en el citado Reglamento, respecto de los ficheros mixtos o automatizados con datos de carácter personal de nivel medio o alto, cuya titularidad recae en distintos Centros de la Comunidad de Madrid y en los que Madrid Digital figura como Responsable del Fichero o Encargado del Tratamiento.

El alcance de esta auditoría es la revisión y verificación del grado de cumplimiento de las medidas de seguridad en los centros de tratamiento, locales, otras instalaciones, equipos, sistemas, aplicaciones, programas, personas que intervengan en el tratamiento, comunicaciones e infraestructura tecnológica y organizativa de los sistemas de información, así como en las normas, procedimientos y estándares que afecten a los ficheros relacionados.

2. Auditoría de los controles establecidos en la norma ISO-IEC-27002:

Auditoría de los Sistemas de Información bajo la responsabilidad de Madrid Digital con los que se presta el servicio informático que precisa el Organismo Pagador de la Comunidad de Madrid de los gastos financiados por los fondos europeos agrícolas, en cuanto al cumplimiento de los controles establecidos en



la norma ISO-IEC-27002. Todo ello de conformidad con las acciones de control relacionadas con lo dispuesto en el artículo 18 de la Ley 9/1990, de 8 de noviembre, reguladora de la Hacienda de la Comunidad de Madrid, y el Reglamento (UE) no 885/2006 de la Comisión, de 21 de junio, por el que se establecen las disposiciones de aplicación del Reglamento (UE) no 1290/2005, del Consejo, en lo que se refiere a la autorización de los organismos pagadores y otros órganos y a la liquidación de cuentas del FEAGA y del FEADER.

Esta auditoría deberá determinar la conformidad de los Sistemas de Información con la norma *ISO-IEC-27002 en su última versión*, su grado de implantación real y su eficacia. Para ello se realizará un análisis de la documentación existente y una revisión de las exclusiones según la Declaración de Aplicabilidad, se revisarán las políticas, la implantación de los controles de seguridad según la norma *ISO-IEC-27002* y la eficacia del sistema en su conjunto.

3. Auditoría de los sistemas de información al servicio de la Administración de Justicia:

Auditoría de los Sistemas de Información al servicio de la Administración de Justicia que son responsabilidad de Madrid Digital, en cuanto a los criterios generales de seguridad que han de contemplar según acuerdo del *Pleno, de 13 de septiembre de 2007, del Consejo General del Poder Judicial*, y en concreto el criterio Auditoría que regula la necesidad de que los Sistemas de Información al servicio de la Administración de Justicia se sometan a una auditoría que verifique su cumplimiento y el de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años.

Dicha auditoría deberá identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

4. Auditoría de la seguridad de los Sistemas de Información relativos al Esquema Nacional de Seguridad:

Auditoría de la seguridad de los Sistemas de Información a los que se refiere 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*, verificando el cumplimiento de los requisitos establecidos por el mismo en los *Capítulos II y III* y en los *Anexos I y II* del citado Esquema.

Se realizará un análisis de riesgos de los Sistemas de Información que identifique y valore los activos más valiosos, las amenazas, las vulnerabilidades, las salvaguardas y el riesgo residual.

Se realizará una auditoría que emita una opinión independiente y objetiva sobre el cumplimiento de los requisitos y la correcta mitigación de los riesgos observados de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera, y para satisfacerse internamente, o bien frente a terceros que pudieran estar relacionados, sobre el nivel de seguridad implantado. Todo ello según lo dispuesto en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y específicamente dentro de los requisitos del artículo 34 (Auditoría de la seguridad), y del Anexo III (Auditoría de la Seguridad) del 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 y sus posteriores modificaciones.

5. Revisiones técnicas:

Se realizarán, las revisiones técnicas que en cada caso se estimen necesarias, hasta un máximo de 660 horas en total y durante la ejecución del contrato.

Los servicios y actividades en este epígrafe podrán realizarse sobre cualquier materia relacionada con la seguridad de la información y, entre ellos, los siguientes, sin que constituyan una relación cerrada:

- Auditorías de compromisos contractuales en materia de seguridad en la prestación de servicios TIC por terceras partes: Con la finalidad de analizar y cuantificar la consecución de los acuerdos de niveles de servicio vigentes, analizar y cuantificar el grado de madurez de los procesos de seguridad objeto de la prestación de servicio, evidenciar y valorar los riesgos efectivos del servicio, analizar y concluir sobre incidentes graves en el servicio.
- Auditorías técnicas de seguridad: Relativas a seguridad en redes y servicios de comunicaciones, seguridad en dispositivos móviles y accesos remotos, blindaje de servidores, bases de datos y servicios, accesibilidad y disponibilidad de sistemas y datos, blindaje y configuración de tecnologías de seguridad, seguridad en estaciones de trabajo, protección frente a malware y rootkits y pruebas de intrusión.
- Auditoría del cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual, en concreto de las licencias de software. En cada revisión de al menos 20 horas, deberá al menos revisarse un contrato y sus licencias derivadas, con un máximo de 4 servidores de licencias.
- Revisiones sobre el cumplimiento y adecuación de las normas y estándares en materia de seguridad establecidos en el cuerpo normativo de Madrid Digital.
- Análisis técnicos de dispositivos electrónicos: El servicio consistirá en la obtención, análisis e interpretación de las posibles evidencias digitales en los sistemas de información objeto de usos indebidos o irregulares. Podrán incluir, entre otros, memorias, ordenadores, PDA's, teléfonos móviles, soportes ópticos o magnéticos, así como otros dispositivos o soportes susceptibles de ser analizados.
- Revisiones de las reglas existentes en los firewalls que dan servicio en Madrid Digital: Se deberán identificar y analizar las reglas con el fin de determinar su eficacia en la protección segura de las redes y obtener una simplificación en su administración. En cada revisión de al menos 20 horas, se deberán revisar al menos 80 reglas de firewall.
- Auditorías de código fuente de aplicaciones: Se deberán identificar los diferentes tipos de vulnerabilidades en el código fuente de las aplicaciones, y verificar la potencial explotación de las mismas. En cada auditoría de 20 horas se deberán analizar al menos 8.000 líneas de código. Si la aplicación superara las 8.000 líneas, por cada 20 horas adicionales se analizarán 40.000 líneas.



- Informes técnico-jurídicos: Se deberá analizar el marco normativo de los servicios prestados por Madrid Digital y emitir los informes oportunos con el objeto de llevar a cabo su actividad en condiciones óptimas de seguridad jurídica.
- Auditorías del sistema de telefonía basado en voz sobre IP (VoIP): El objetivo de esta auditoría es analizar las vulnerabilidades que puedan afectar al servicio de voz sobre IP e identificar las deficiencias detectadas con el fin de mitigar los posibles riesgos. El análisis no durará más de 60 horas.

El servicio de **revisiones técnicas**, determinado en este apartado **A.5**, se establece con carácter estimado, quedando subordinado a las necesidades de Madrid Digital, abonándose, por tanto, al contratista únicamente las que efectivamente se lleven a cabo. En el caso de no realizarse todas las revisiones estimadas inicialmente, ni el número máximo de horas previsto, no se originará ningún tipo de derecho a compensación económica para el contratista.

Los servicios se realizarán mediante una comunicación de inicio por parte de Madrid Digital dirigida al adjudicatario, según necesidades del servicio, donde se expondrán las necesidades a cubrir con el proyecto concreto.

El adjudicatario acusará recibo de la solicitud del servicio, la evaluará y presentará a Madrid Digital la planificación propuesta con indicación del número de horas de dedicación al proyecto (el número máximo de horas contempladas para la realización de la totalidad de los trabajos reflejados en este apartado **A.5** es de **660 horas**).

Una vez aceptada por parte de Madrid Digital, el contratista iniciará la ejecución de los trabajos asociados al proyecto en un plazo no superior a una semana desde la comunicación de inicio por parte de Madrid Digital.

El adjudicatario elaborará una Guía de Criterios de auditoría del cumplimiento de los controles, medidas y requisitos de seguridad auditados, de tal forma que sirva de elemento común para la valoración de los controles en cada una de las auditorías y revisiones técnicas. Asimismo, deberá elaborar el modelo de gestión de las evidencias que se utilizará a lo largo del desarrollo de los trabajos, que contendrá, entre otros, las características de las evidencias, sus atributos, codificación y almacenamiento.

A lo largo de todo el servicio, el adjudicatario deberá elaborar y mantener actualizado un informe con el Plan de Acción, resultante de las no conformidades y recomendaciones identificadas en las distintas auditorías y revisiones técnicas.

Al inicio del servicio, la Dirección de Seguridad Corporativa aprobará el planteamiento y enfoque de las guías, modelos y documentos anteriores.

B) Servicio de análisis y gestión de riesgos tecnológicos

1. Medición del riesgo en los Sistemas de Información desarrollados por Madrid Digital

Con esta actividad el adjudicatario deberá mantener actualizado el Sistema de Información de riesgos de Madrid Digital (incluido dentro de la aplicación SENS), verificando cada control aplicable en los sistemas y plataformas tecnológicas y extrayendo tanto de forma global como para cada uno de los sistemas y cada una de las plataformas tecnológicas, el riesgo residual para incorporarlo de forma periódica en el cuadro de mando de seguridad.



Se deberá completar, en su caso, toda la información referida al ciclo completo de la gestión de la seguridad en los sistemas de información.

2. Gestión del riesgo que debe aplicarse en las áreas de seguridad TIC de Madrid Digital y, entre otros, los ámbitos donde deben focalizarse los mayores esfuerzos atendiendo a la naturaleza de los activos protegidos, a las amenazas a los que éstos están expuestos y la probabilidad e impacto de que alguna de ellas se materialice:

A la vista de la medición del riesgo obtenido, el adjudicatario conjuntamente con Madrid Digital fijará un determinado umbral de riesgo y elaborará los planes de acción necesarios para mitigar los riesgos identificados que superen ese determinado umbral. Asimismo, deberá mantener el inventario de los planes y el estado de su ejecución durante todo el periodo del contrato, así como prestar el apoyo y soporte necesario en la realización de los trabajos previstos en dichos planes.

3. Actualización de la información referente a seguridad de la información en los sistemas de información de seguimiento y control, así como en los repositorios corporativos:

Madrid Digital cuenta con dos sistemas corporativos de seguimiento y control de la seguridad de la información: SRPD, o sistema del Responsable de Protección de Datos y SENS, o sistema de especificación y normalización de la seguridad. En estos repositorios el adjudicatario informará de los resultados de las auditorías, revisiones técnicas que realice y mantendrá actualizada la correspondencia de normativa, control, aplicabilidad, sistema de información, ficheros y cuanta información conste y sea tratada dentro del alcance del contrato. En la fase inicial de la prestación del servicio, el adjudicatario realizará un estudio preliminar de completitud y coherencia de los catálogos existentes de normativas, controles, aplicabilidad y demás elementos que comprenden los sistemas de información mencionados.

4. Elaboración y seguimiento del plan de implantación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos en el ámbito de actuación de Madrid Digital.

El adjudicatario deberá elaborar un documento que recoja las actividades necesarias para adaptar los procesos de Madrid Digital a la nueva forma de gestión que supone la nueva normativa que permitan y faciliten la aplicación del Reglamento en el momento en que sea efectiva su aplicación.

Este documento deberá contemplar, al menos, una relación de las novedades del Reglamento, una comparativa sobre la normativa actual española, la evaluación del cumplimiento de dichas cuestiones en Madrid Digital y la propuesta de soluciones de aquellas cuestiones que así lo requieran para asegurar la adaptación de Madrid Digital al nuevo Reglamento.

Asimismo, se dará el apoyo y soporte necesarios para realizar las plantillas, cláusulas y otros documentos necesarios. Así como para definir los criterios y métodos necesarios para realizar las evaluaciones de impacto, análisis de riesgos y otros relacionados con el tratamiento de los datos personales.

Desde el momento de la aprobación de dicho documento y hasta la finalización del contrato el adjudicatario deberá realizar el seguimiento de las actividades



propuestas, de forma que el grado de implantación aparezca como una de las variables del cuadro de mando de seguridad.

5. Análisis y medición integral de cumplimiento o de control interno en materia de seguridad

Se definirá e implantará una actividad de análisis y medición integral de cumplimiento o de control interno en materia de seguridad, que se realizará mediante un sistema basado en un cuadro de mando, adaptado a la actividad de Madrid Digital, y enfocado a la gestión de la seguridad.

El objetivo de este sistema será conocer la confianza que merecen los servicios prestados por Madrid Digital en materia de seguridad, así como disponer de información de detalle de cumplimiento de las distintas regulaciones normativas en materia de seguridad por parte de Madrid Digital. Todo ello se reflejará en un cuadro de mando integral orientado a la gestión de la seguridad.

El adjudicatario deberá aportar mensualmente los informes y reportes del servicio de análisis y medición integral de cumplimiento o de control interno en materia de seguridad para realizar el análisis correspondiente y la medición de los resultados obtenidos en papel y en soporte electrónico, compatible con las herramientas instaladas en Madrid Digital (MS Office 2007, Adobe Acrobat Reader 8, MS Explorer 7).

El soporte electrónico, que forma parte de los entregables del proyecto, deberá quedar a disposición de Madrid Digital con los datos de cálculo necesarios de forma que permita realizar las posteriores actividades de control interno en materia de seguridad.

En cuanto a los requisitos técnicos, el soporte electrónico deberá poder instalarse y ejecutarse en un puesto ofimático básico de la Comunidad de Madrid. Funcionalmente deberá almacenar y procesar las métricas, objetivos e indicadores de este servicio y generar los resultados correspondientes.

Las métricas, objetivos e indicadores de este servicio deberán estar orientados a la gestión de la seguridad y deberán ser una traslación de los objetivos de control, controles, criterios y medidas de seguridad correspondientes a los siguientes estándares, normas y disposiciones legales: *Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD, norma ISO-IEC-27002, los criterios generales de seguridad que han de contemplar según acuerdo del Pleno, de 13 de septiembre de 2007, del Consejo General del Poder Judicial, 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* y el cuerpo normativo vigente en Madrid Digital, así como cualquier otro que la *Dirección de Seguridad Corporativa de Madrid Digital* estime necesario para el análisis y medición de los servicios de seguridad de la Agencia.

Como mínimo, deberá relacionarse por cada uno de los controles de seguridad derivados de las normas precitadas los siguientes elementos:

1. Descripción del control.
2. Normativa/s de aplicación del control.
3. Plataformas tecnológicas de Madrid Digital sobre las que aplica el control.
4. Grado de cumplimiento del control en cada plataforma asociado a la identificación de la auditoría en la que se ha verificado y la fecha de la misma.
5. Relación de auditorías que han verificado el control.
6. Evidencias que soportan la verificación del control.



7. Relación de aplicaciones afectadas por el control.
8. Detalle del motivo del incumplimiento.
9. Relación de recomendaciones para mejorar el cumplimiento del control.
10. Plan de acción donde aparecen las recomendaciones.
11. Grado de progreso del plan de acción.

El servicio implantado deberá ser capaz de generar un archivo en formato estándar (CSV, TEXTO) con la exportación de todos los datos que se manejen.

CLÁUSULA 4.- DESCRIPCIÓN DE LOS SERVICIOS

A. Servicios de auditoría en materia de seguridad

La revisión del cumplimiento en materia de seguridad en el entorno de Madrid Digital, debido al elevado número de sistemas y a la confluencia de distinta normativa, se estructurará en dos grandes bloques: revisión de controles en plataformas y elementos comunes y revisión de controles particulares de cada Sistema de Información.

Con esta metodología se pretende una racionalización de los recursos evitando la duplicidad de los trabajos en dos niveles: primero, controles y/o medidas de seguridad comunes en las distintas normativas y, segundo, plataformas y elementos comunes que dan servicio a los distintos Sistemas de Información de la Comunidad de Madrid.

Como resultado de la aplicación de esta metodología, la auditoría de un Sistema de Información será el resultado de la revisión de los controles de los componentes y elementos comunes que le correspondan más el resultado de la revisión de los controles propios del Sistema de Información.

• REVISIÓN DE CONTROLES EN PLATAFORMAS Y ELEMENTOS COMUNES

La revisión de controles en plataformas y elementos comunes conllevará por parte del adjudicatario la revisión del cumplimiento de cada uno de los controles de las distintas normativas en las plataformas tecnológicas y elementos comunes a todos los sistemas de la Comunidad de Madrid.

El catálogo de Madrid Digital tiene 46 plataformas y elementos comunes.

Para llevar a cabo esta actividad, Madrid Digital proporcionará al adjudicatario una relación de controles y su correspondencia con las distintas plataformas tecnológicas y elementos comunes así como con cada una de las normativas de seguridad afectadas.

Para los trabajos propuestos se requiere realizar las siguientes **Fases** y actividades:

Fase 1 - Planificación y realización del programa de auditoría.

El objeto de esta Fase es establecer las bases de trabajo para la realización de la auditoría. En particular dentro de esta fase se incluye:

- Planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto, la coordinación con las áreas de Madrid Digital afectadas y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Elaboración del programa de auditoría, con especificación de los hitos a auditar (extraídos de la relación proporcionada) y el detalle de las pruebas y comprobaciones previstas para la verificación de su cumplimiento.



- Obtención de la información y documentación necesaria para poder abordar la verificación de los hitos definidos en el Programa de Auditoría. Principalmente, la información y documentación anterior se referirá a:
 - ✓ Plataformas tecnológicas bajo la responsabilidad de Madrid Digital.
 - ✓ Infraestructuras tecnológicas que componen las anteriores plataformas en el ámbito de responsabilidad de Madrid Digital:
 - Servidores donde se ubiquen los SS. II.
 - Sistemas Operativos, Sistemas Gestores de Base de Datos, etc.
 - Redes de Comunicaciones donde se ubiquen los sistemas y que permiten el acceso a los usuarios (tipos de redes disponibles, tipos de conexiones habilitadas, dispositivos y elementos de red y de comunicaciones, etc.).
 - Instalaciones o Centros de Proceso de Datos donde se ubiquen las plataformas.
 - ✓ Prestación de servicios a la Comunidad de Madrid, por parte de personal externo, en el ámbito precitado.
 - ✓ Interlocutores de las Unidades Organizativas de Madrid Digital.

Fase 2 - Trabajo de campo: Revisión y ejecución del programa de auditoría.

Durante esta fase se realizarán las entrevistas y revisiones necesarias para evaluar el grado de adecuación de las medidas y controles existentes en relación con las exigencias de las distintas normativas.

Todas las medidas y controles de cumplimiento correspondientes a cada plataforma tecnológica y elemento común han de ser objeto de auditoría y deberán estar recogidas en alguno de los hitos del programa de auditoría que se elabore al inicio del proyecto.

Fase 3 - Emisión de Informe de auditoría: Dictamen de resultados.

El equipo de trabajo elaborará un informe donde se recojan los resultados de las revisiones efectuadas respecto al grado de adecuación de las plataformas y elementos comunes bajo la responsabilidad de Madrid Digital.

Dicho informe deberá dictaminar sobre la adecuación de las medidas y controles de seguridad implantados, identificando de forma concreta las no conformidades o deficiencias respecto a las distintas normas y proponiendo las recomendaciones correctoras o complementarias que sean necesarias para subsanar las anteriores. Asimismo, el informe deberá incluir los datos, hechos y observaciones en que se hayan basado tanto el dictamen realizado como las recomendaciones emitidas.

Se elaborará además un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.

Fase 4 - Elaboración del Plan de Acción.

El equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer para implantar las recomendaciones recogidas en el Informe de Auditoría.



Las actuaciones se agruparán, en función de su dimensión y ámbito de aplicación, en proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - ✓ Descripción de los trabajos previstos.
 - ✓ Detalle de las actividades a realizar.
 - ✓ Identificación de la Unidad Organizativa de la Comunidad de Madrid responsable de su ejecución, así como de aquellas otras unidades con participación en su desarrollo.
 - Clasificación del proyecto, atendiendo a su plazo de desarrollo en función de oportunidad de ejecución (recursos humanos y económicos) y complejidad: corto, medio o largo plazo.
 - Estimación de Esfuerzos, donde se aporta un resumen estimativo del esfuerzo y duración de cada proyecto a acometer, agrupados según su plazo de realización.
 - Planificación de Proyecto, donde se muestra, mediante un cronograma, la planificación programada de cada uno de los proyectos a realizar.
- REVISIÓN DE CONTROLES PARTICULARES DE CADA SISTEMA DE INFORMACIÓN

La revisión de controles particulares de cada Sistema de Información conllevará por parte del adjudicatario la revisión del cumplimiento de cada uno de los controles de las distintas normativas en los Sistemas de Información de la Comunidad de Madrid que no hayan sido evaluados en la revisión de controles de las plataformas comunes y que corresponderán con controles asociados fundamentalmente a la funcionalidad e implementación en el propio desarrollo de las aplicaciones informáticas de la Comunidad de Madrid.

Esta revisión, junto con la realizada anteriormente, servirá para dictaminar, en su totalidad, la adecuación y el cumplimiento de cada normativa en los sistemas de la Comunidad de Madrid.

Para llevar a cabo esta actividad, Madrid Digital proporcionará al adjudicatario una relación de controles y su correspondencia con los distintos ficheros, sistemas, aplicaciones y sistemas de tratamiento.

Para los trabajos propuestos se requiere realizar las siguientes fases y actividades:

1. Auditoría de los procedimientos e instrucciones vigentes en materia de seguridad de datos personales, de conformidad con lo establecido en los Artículos 96 y 100 del 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, respecto a los ficheros de datos de carácter personal en los que Madrid Digital figura como Responsable de Fichero o Encargado del Tratamiento.

El adjudicatario deberá llevar a cabo, como mínimo, los servicios que se desarrollan a continuación, organizados en las siguientes **Fases** y actividades:

Fase 1 – Requerimientos Generales:

Como cuestión previa, se desarrollarán las actuaciones necesarias para llevar a cabo los posteriores trabajos que constituirán el objeto del contrato. En particular,



y sin perjuicio de las tareas que los licitadores puedan contemplar en sus ofertas, se incluirán las siguientes:

- Planificación detallada de las actuaciones, que deberá incluir como mínimo:
 - Planificación detallada del proyecto, con especificación de fases y actividades, así como fechas de ejecución, hitos a alcanzar y acciones de seguimiento del proyecto.
 - Determinación del inventario final de los ficheros con datos de carácter personal de nivel medio o alto a auditar. Si bien en la documentación adicional al presente pliego se recoge la relación actual, durante esta actividad se determinarán de forma precisa los que constituirán el ámbito de la auditoría.
 - Actualización en los sistemas de información de Madrid Digital del inventario final de los datos referidos a los ficheros objeto del servicio de auditoría.
 - Identificación de los distintos interlocutores para coordinar las actuaciones a realizar con las Áreas de Madrid Digital y con las Consejerías y Órganos afectados.
 - Lanzamiento y presentación del proyecto, que deberá iniciarse con la presentación y coordinación de las distintas áreas internas de Madrid Digital que se vean afectadas por la auditoría, y que deberá culminarse con la presentación del proyecto a todos los centros de las Consejerías afectadas.
- Designación de la persona o de las personas de la empresa prestadora del servicio que, sin perjuicio de la responsabilidad propia de la misma, quedarán autorizados para mantener, de forma centralizada, la interlocución tanto con el personal de las áreas de Madrid Digital como con el personal de Consejerías.
- Recogida y preparación del material y documentación necesaria para ejecutar todos los trabajos previstos.

La información que no sea posible determinar en esta fase de actuaciones preparatorias deberá recabarse y/o confirmarse durante las fases posteriores de trabajo, según corresponda con la metodología planteada para la ejecución de los trabajos, aunque ello suponga un ajuste en la planificación de las actuaciones (Por ej.: sistemas de tratamiento de datos, características técnicas de los sistemas, equipos o instalaciones, etc.).
- Identificación de los componentes y elementos comunes que correspondan a cada uno de los Sistemas de Información analizados.
- Elaboración del Informe de planificación detallada de Auditoría, que deberá incluir el Programa de Auditoría con la descripción de las actividades a realizar “in situ” dentro de cada una de las actuaciones planificadas y que deberá prever los controles ya revisados en la fase inicial de plataformas y elementos comunes. Esto incluye:
 - Definición de los objetivos de control.
 - Determinación de los controles correspondientes a cada uno de los anteriores.



- Identificación de los controles revisados y elaboración de la relación final de controles a revisar.
- Identificación de las áreas o personas involucradas.
- Documentación y especificación de preparativos necesarios, incluyendo el detalle de las listas de chequeo y la relación de las pruebas a realizar en el trabajo de campo de la fase de verificación de medidas.

Fase 2 - Verificación de medidas adoptadas por Madrid Digital como Encargado del Tratamiento:

Se procederá a la revisión detallada de las políticas, normas y estándares de seguridad de Madrid Digital, de los sistemas operativos, redes, plataformas tecnológicas y herramientas de gestión institucionales que sean de aplicación en los tratamientos de datos personales de la Comunidad de Madrid y de acuerdo con lo previsto en el *R.D. 1720/2007*.

El adjudicatario, emitirá los siguientes entregables:

1. Un Informe de Auditoría para Madrid Digital del análisis de las políticas, normas y estándares de seguridad de Madrid Digital, verificación técnica de sistemas operativos, redes, plataformas tecnológicas y herramientas de gestión institucionales relacionadas con los ficheros a auditar.
2. Un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.
3. Un informe que recoja el plan de acción necesario para solventar las no conformidades recogidas en el informe de auditoría. Este Plan de Acción deberá integrarse en el Informe Global de Plan de Acción que ha de elaborarse y mantenerse actualizado a lo largo de todo el servicio.

Fase 3 - Verificación de medidas adoptadas por los Responsables de Ficheros de la Comunidad de Madrid:

Se procederá a realizar la verificación de las medidas de seguridad técnicas y organizativas llevadas a efecto en cada una de las instalaciones de los Responsables de los Ficheros que comprenda el ámbito de auditoría y en relación con los aspectos de la seguridad, en función de su nivel, previstos en el *R.D. 1720/2007*.

En función de lo anterior, para cada centro auditado, y respecto de sus ficheros automatizados correspondientes de nivel medio y alto, el adjudicatario estará obligado a elaborar y facilitar un Informe de Auditoría, que como mínimo deberá dictaminar sobre la adecuación de las medidas y controles de seguridad previstos en el desarrollo reglamentario de la LOPD, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Además, deberá incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

Para la elaboración de los respectivos informes de Auditoría, se deberá emplear el *Sistema de Información de Gestión de Madrid Digital para la Gestión de Protección de Datos de Carácter Personal*.

Asimismo, respecto a la información obtenida en cada uno de los centros y revisada en el ámbito de los ficheros auditados correspondientes, se deberá proceder a su actualización en la base de datos del Sistema de Información de



gestión de Madrid Digital para la gestión de protección de datos de carácter personal.

El prestador del servicio ofrecerá el soporte necesario para que los distintos responsables de los centros auditados accedan al Sistema de Información de gestión de Madrid Digital para la gestión de protección de datos de carácter personal y, de este modo, proceder a la consulta de los distintos informes de auditoría generados. El soporte incluirá, además, la atención de las observaciones realizadas por los Centros Directivos como resultado del análisis e interpretación realizada de los resultados obtenidos.

En el caso de los ficheros no automatizados, el prestador del servicio deberá proporcionar una guía de recomendaciones para la adecuación del tratamiento de los datos conforme a los requerimientos establecidos en el *R.D. 1720/2007*. Dicha guía, además, deberá recoger el procedimiento por el cual el Responsables o Titular de los ficheros no automatizados puede llevar a cabo la auto revisión de cumplimiento de dichas recomendaciones, mediante el uso del sistema de información de gestión de Madrid Digital para la gestión de protección de datos de carácter personal.

El adjudicatario, emitirá un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos de forma global. En el documento se plasmará las principales conclusiones segmentadas por Consejería y Centro Directivo. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.

2. Auditoría de los controles establecidos en la norma ISO-IEC-27002

Para los trabajos propuestos se requiere realizar las siguientes fases y actividades:

Fase 1 - Planificación y realización del programa de auditoría.

El objeto de esta Fase es establecer las bases de trabajo para la realización de la auditoría. En particular dentro de esta fase se incluye:

- Planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto, la coordinación con las áreas de Madrid Digital afectadas y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Identificación de los componentes y elementos comunes que correspondan a cada uno de los Sistemas de Información analizados.
- Elaboración del programa de auditoría, con especificación de los hitos a auditar (extraídos de la norma ISO-IEC-27002) y el detalle de las pruebas y comprobaciones previstas para la verificación de su cumplimiento. El programa de auditoría deberá prever los controles ya revisados en la fase inicial de plataformas y elementos comunes.
- Obtención de la información y documentación necesaria para poder abordar la verificación de los hitos definidos en el Programa de Auditoría. Principalmente, la información y documentación anterior se referirá a:
 - ✓ Sistemas de Información bajo la responsabilidad de Madrid Digital con los que se presta el servicio informático que precisa el Organismo Pagador de la Comunidad de Madrid de los gastos financiados por los fondos europeos agrícolas.



- ✓ Infraestructura tecnológica que soportan los anteriores sistemas en el ámbito de responsabilidad de Madrid Digital:
 - Servidores donde se ubiquen los SS.II.
 - Plataformas tecnológicas que soportan los SS.II. (Sistemas Operativos, Sistemas Gestores de Base de Datos, etc.)
 - Redes de Comunicaciones donde se ubiquen los sistemas y que permiten el acceso a los usuarios (tipos de redes disponibles, tipos de conexiones habilitadas, dispositivos y elementos de red y de comunicaciones, etc.).
 - Instalaciones o Centros de Proceso de Datos donde se ubiquen los servidores, dispositivos y elementos de red y de comunicaciones.
- ✓ Prestación de servicios a la Comunidad de Madrid, por parte de personal externo, en el ámbito precitado.
- ✓ Interlocutores de las Unidades Organizativas de la Comunidad de Madrid implicadas en el ámbito del organismo pagador y que tengan una necesaria participación en alguna de las fases de la auditoría.

Fase 2 - Trabajo de campo: Revisión y ejecución del programa de auditoría.

Durante esta fase se realizarán las entrevistas y revisiones necesarias para evaluar el grado de adecuación de las medidas y controles existentes en relación con las exigencias de la norma ISO-IEC 27002, todos ellos en el ámbito de los SS.II. puestos al servicio del organismo pagador de la Comunidad de Madrid y que son responsabilidad de Madrid Digital.

Todas las medidas y controles de cumplimiento han de ser objeto de auditoría y deberán estar recogidas en alguno de los hitos del programa de auditoría que se elabore al inicio del proyecto.

Fase 3 - Emisión de Informe de auditoría: Dictamen de resultados.

El equipo de trabajo elaborará un informe donde se recojan los resultados de las revisiones efectuadas respecto al grado de adecuación a la norma ISO-IEC 27002 de los sistemas de información bajo la responsabilidad de Madrid Digital, con los que se presta el servicio informático que precisa el Organismo Pagador de la Comunidad de Madrid de los gastos financiados por los fondos europeos.

Dicho informe deberá dictaminar sobre la adecuación de las medidas y controles de seguridad implantados, identificando de forma concreta las no conformidades o deficiencias respecto a la norma ISO-IEC 27002 y proponiendo las recomendaciones correctoras o complementarias que sean necesarias para subsanar las anteriores. Asimismo, el informe deberá incluir los datos, hechos y observaciones en que se hayan basado tanto el dictamen realizado como las recomendaciones emitidas.

Se elaborará además un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.



Fase 4 - Elaboración del Plan de Acción.

El equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer para implantar las recomendaciones recogidas en el Informe de Auditoría.

Este Plan de Acción deberá integrarse en el Informe Global de Plan de Acción que ha de elaborarse y mantenerse actualizado a lo largo de todo el servicio.

Las actuaciones se agruparán, en función de su dimensión y ámbito de aplicación, en proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - ✓ Descripción de los trabajos previstos.
 - ✓ Detalle de las actividades a realizar.
 - ✓ Identificación de la Unidad Organizativa de la Comunidad de Madrid responsable de su ejecución así como de aquellas otras unidades con participación en su desarrollo.
 - Clasificación del proyecto, atendiendo a su plazo de desarrollo en función de oportunidad de ejecución (recursos humanos y económicos) y complejidad: corto, medio o largo plazo.
 - Estimación de Esfuerzos, donde se aporta un resumen estimativo del esfuerzo y duración de cada proyecto a acometer, agrupados según su plazo de realización.
 - Planificación de Proyecto, donde se muestra, mediante un cronograma, la planificación programada de cada uno de los proyectos a realizar.
3. Auditoría de los sistemas de información al servicio de la Administración de Justicia que son responsabilidad de Madrid Digital, en cuanto a los criterios generales de seguridad que han de contemplar según acuerdo del Pleno, de 13 de septiembre de 2007, del Consejo General del Poder Judicial.

Para los trabajos propuestos en el presente documento se requiere realizar las siguientes fases y actividades:

Fase 1 - Planificación y realización del programa de auditoría.

El objeto de esta Fase es establecer las bases de trabajo para la realización de la auditoría. En particular dentro de esta fase se incluye:

- Planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto, la coordinación con los centros (Consejerías y Órganos) las áreas de Madrid Digital afectadas y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Identificación de los componentes y elementos comunes que correspondan a cada uno de los Sistemas de Información analizados.
- Elaboración del programa de auditoría, con especificación de los hitos a auditar (extraídos del documento "Criterios generales de seguridad en los sistemas de gestión procesal") y el detalle de las pruebas y comprobaciones previstas para la verificación de su cumplimiento. El programa de auditoría deberá prever los controles ya revisados en la fase inicial de plataformas y elementos comunes.



- Obtención de la información y documentación necesaria para poder abordar la verificación de los hitos definidos en el Programa de Auditoría. Principalmente, la información y documentación anterior se referirá a:
 - ✓ Sistemas de Información de gestión procesal en el ámbito de responsabilidad de Madrid Digital.
 - ✓ Infraestructura tecnológica de gestión procesal en el ámbito de responsabilidad de Madrid Digital:
 - Servidores donde se ubiquen los SS.II. de gestión procesal.
 - Plataformas tecnológicas que soportan los SS.II. de gestión procesal (Sistemas Operativos, Sistemas Gestores de Base de Datos, etc.)
 - Redes de Comunicaciones donde se ubiquen los sistemas y que permiten el acceso a los usuarios (tipos de redes disponibles, tipos de conexiones habilitadas, dispositivos y elementos de red y de comunicaciones, etc.).
 - Instalaciones o Centros de Proceso de Datos donde se ubiquen los servidores, dispositivos y elementos de red y de comunicaciones.
 - ✓ Prestación de servicios a la Comunidad de Madrid, por parte de personal externo, en el ámbito de los SS.II. de gestión procesal.
 - ✓ Interlocutores de las Unidades Organizativas de la Comunidad de Madrid implicadas en la gestión procesal y que tengan una necesaria participación en alguna de las fases de la auditoría.

Fase 2 - Trabajo de campo: Revisión y ejecución del programa de auditoría.

Durante esta fase se realizarán las entrevistas y revisiones necesarias para evaluar el grado de adecuación de las medidas y controles existentes en relación con las exigencias de los criterios generales de seguridad de los Sistemas de gestión procesal. Todos ellos en el ámbito de los SS.II. puestos al servicio de la Administración de Justicia y que son responsabilidad de Madrid Digital.

Todas las medidas y controles de cumplimiento clasificadas en: medidas técnicas, medidas organizativas, responsables de seguridad y auditorías han de ser objeto de auditoría y deberán estar recogidas en alguno de los hitos del programa de auditoría que se elabore al inicio del proyecto.

Fase 3 - Emisión de Informe de auditoría: Dictamen de resultados.

El equipo de trabajo elaborará un informe donde se recojan los resultados de las revisiones efectuadas respecto al grado de adecuación de los criterios de seguridad existentes en los Sistemas de Información de gestión procesal.

Dicho informe deberá dictaminar sobre la adecuación de las medidas y controles de seguridad implantados, identificando de forma concreta las no conformidades o deficiencias respecto a los criterios definidos por el Consejo General del Poder Judicial y proponiendo las recomendaciones correctoras o complementarias que sean necesarias para subsanar las anteriores. Asimismo, el informe deberá incluir los datos, hechos y observaciones en que se hayan basado tanto el dictamen realizado como las recomendaciones emitidas.



Se elaborará además un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.

Fase 4 - Elaboración del Plan de Acción.

El equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer para implantar las recomendaciones recogidas en el Informe Auditoría.

Este Plan de Acción deberá integrarse en el Informe Global de Plan de Acción que ha de elaborarse y mantenerse actualizado a lo largo de todo el servicio.

Las actuaciones se agruparán, en función de su dimensión y ámbito de aplicación, en proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - ✓ Descripción de los trabajos previstos.
 - ✓ Detalle de las actividades a realizar.
 - ✓ Identificación de la Unidad Organizativa de la Comunidad de Madrid responsable de su ejecución así como de aquellas otras Unidades con participación en su desarrollo.
- Clasificación del proyecto atendiendo a su plazo de desarrollo en función de oportunidad de ejecución (recursos humanos y económicos) y complejidad: corto, medio o largo plazo.
- Estimación de Esfuerzos, donde se aporta un resumen estimativo del esfuerzo y duración de cada proyecto a acometer, agrupados según su plazo de realización.
- Planificación de Proyecto, donde se muestra, mediante un cronograma, la planificación programada de cada uno de los proyectos a realizar.

4. Auditoría de la seguridad de los sistemas de información a los que se refiere 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, verificando el cumplimiento de los requisitos establecidos por el mismo en los capítulos II y III y en los Anexos I y II del citado Esquema.

Para la realización de los trabajos propuestos se seguirán las pautas establecidas en la *Guía de Auditoría del Esquema Nacional de Seguridad CCN-STIC-802 y Análisis de Riesgos en Sistemas de la Administración CCN-STIC-410 del Centro Criptológico Nacional*. Con carácter general se seguirán las siguientes fases y actividades para su ejecución:

Fase 1 - Planificación y realización del programa de trabajo.

El objeto de esta fase es establecer las bases para la realización de los trabajos. En particular dentro de esta fase se incluye:

- Planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto, la coordinación con las áreas de Madrid Digital afectadas y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Elaboración del Programa de Trabajo, con especificación de los hitos.



- Identificación de los componentes y elementos comunes que correspondan a cada uno de los Sistemas de Información analizados.
- Elaboración del Programa de Auditoría con los hitos a auditar y el detalle de las pruebas y comprobaciones previstas para la verificación de su cumplimiento. El programa de auditoría deberá prever los controles ya revisados en la fase inicial de plataformas y elementos comunes.
- Obtención de la información y documentación necesaria para poder abordar la verificación de los hitos definidos en el Programa de Trabajo. Principalmente, la información y documentación anterior se referirá a:
 - ✓ Sistemas de Información en el ámbito del Esquema Nacional de Seguridad cuya responsabilidad recaiga en Madrid Digital.
 - ✓ Identificación de los servicios a la Comunidad de Madrid e internos a Madrid Digital en el ámbito del Esquema Nacional de Seguridad.
 - ✓ Identificación de la información tratada por los sistemas en el ámbito del Esquema Nacional de Seguridad.
 - ✓ Infraestructura tecnológica de los sistemas en el ámbito del Esquema Nacional de Seguridad:
 - Servidores donde se ubiquen los SS.II.
 - Plataformas tecnológicas que soportan los SS.II. (Sistemas Operativos, Sistemas Gestores de Base de Datos, etc.)
 - Redes de Comunicaciones donde se ubiquen los sistemas y que permiten el acceso a los usuarios (tipos de redes disponibles, tipos de conexiones habilitadas, dispositivos y elementos de red y de comunicaciones, etc.).
 - Instalaciones o Centros de Proceso de Datos donde se ubiquen los servidores, dispositivos y elementos de red y de comunicaciones.

Fase 2 - Trabajo de campo: Revisión y ejecución del programa de trabajo.

Durante esta fase se realizarán las entrevistas y revisiones necesarias para evaluar el grado de adecuación de las medidas y controles existentes en relación con las exigencias de los principios básicos y requisitos mínimos de seguridad del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica para los sistemas cuya responsabilidad recaiga en Madrid Digital.

En relación con el número de sistemas a evaluar, se realizará el cálculo del tamaño de la muestra de los sistemas de información a auditar con un margen de error máximo del 10% y un nivel de confianza mínimo del 97%, con un mínimo de muestras de 110 sistemas de información.

Se realizará la revisión, análisis y actualización del análisis de riesgos de los sistemas de información objeto de los trabajos que identifique y valore los activos más valiosos, las amenazas, las vulnerabilidades, las salvaguardas y el riesgo residual. El análisis se realizará siguiendo la metodología MAGERIT y utilizando la herramienta PILAR, tanto en modo interactivo como en modo BATCH, todo ello en sus últimas versiones.

Deberá incluirse el estudio de los principios básicos, la valoración de cada dimensión de la seguridad, la categorización de los sistemas de Madrid Digital



en el ámbito de los trabajos, y el estudio de la aplicación de las medidas de seguridad según dichas valoraciones y categorizaciones.

Fase 3 - Emisión de Informe de los trabajos realizados: Dictamen de resultados.

Una vez confirmados los hechos y deficiencias resultados de las revisiones y pruebas de auditoría se emitirá el correspondiente informe de auditoría, que deberá dictaminar sobre la adecuación de las medidas exigidas por el *R.D. 3/2010*, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

El informe incluirá las no conformidades encontradas durante la realización de la auditoría e incluirá una opinión sobre si:

- La Política de Seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Existen procedimientos para la resolución de conflictos entre dichos responsables.
- Se han designado personas para dichos roles a la luz del principio de separación de funciones.
- Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
- Se ha realizado un análisis de riesgos, con revisión y aprobación regular, según lo establecido en las medidas aplicables del *Anexo II del R.D. 3/2010*.
- Se cumplen las medidas de seguridad descritas en el Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- Existe un sistema de gestión de mejora continua.
- En relación con la auditoría referente al *R.D. 1720/2007*, en sus artículos 96 y 110, es necesario que el informe indique con claridad cuando una deficiencia de seguridad o incumplimiento, o una mejora recomendada está, individualmente, relacionada con ambas normas, o bien con una en concreto.
- Existe una justificación de las medidas adoptadas para mitigar o suprimir los riesgos detectados, y la proporcionalidad entre las medidas y los riesgos.

Se elaborará además un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.

Fase 4 - Elaboración del Plan de Acción.

El equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer para implantar las recomendaciones recogidas en el Dictamen de Resultados. Este Plan de Acción



deberá integrarse en el Informe Global de Plan de Acción que ha de elaborarse y mantenerse actualizado a lo largo de todo el servicio.

Las actuaciones se agruparán, en función de su dimensión y ámbito de aplicación, en proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - Descripción de los trabajos previstos.
 - Detalle de las actividades a realizar.
 - Identificación de la Unidad Organizativa de la Comunidad de Madrid responsable de su ejecución así como de aquellas otras Unidades con participación en su desarrollo.
- Clasificación del proyecto atendiendo a su plazo de desarrollo en función de oportunidad de ejecución (recursos humanos y económicos) y complejidad: corto, medio o largo plazo.
- Estimación de Esfuerzos, donde se aportará un resumen estimativo del esfuerzo y duración de cada proyecto a acometer, agrupados según su plazo de realización.
- Planificación de Proyecto, donde se mostrará, mediante un cronograma, la planificación programada de cada uno de los proyectos a realizar.

5. Revisiones técnicas

Se realizarán, las revisiones técnicas que en cada caso se estimen necesarias, hasta un máximo de 660 horas en total y durante la ejecución del contrato. Para cada uno de los trabajos propuestos se requiere realizar las siguientes fases y actividades:

Fase 1 - Planificación y realización del programa de trabajo.

El objeto de esta Fase es establecer las bases para la realización de cada uno de los trabajos. En particular dentro de esta fase se incluye:

- Planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Elaboración del Programa de Trabajo, con especificación de los hitos.
- Obtención de la información y documentación necesaria para poder abordar la verificación de los hitos definidos en el Programa de Trabajo. Principalmente, la información y documentación anterior se referirá a:
 - ✓ Sistemas de información sobre los que versarán los trabajos.
 - ✓ Identificación de las posibles evidencias digitales que se deberán obtener como resultado de los trabajos.
 - ✓ Identificación de las materias y cuestiones sobre las que versará el dictamen de resultados de las revisiones practicadas.

Fase 2 - Trabajo de campo: Revisión y ejecución del programa de trabajo.

Durante esta fase se realizarán las entrevistas y revisiones necesarias para evaluar el grado de adecuación de las medidas y controles existentes en relación con las exigencias del programa de trabajo.



Fase 3 - Emisión de Informe de los trabajos realizados: Dictamen de resultados y entrega de las evidencias obtenidas.

En esta fase se pondrá a disposición de Madrid Digital las evidencias obtenidas como resultado del trabajo, en formato digital y compatible con los sistemas de Madrid Digital así como un informe resultado del análisis e interpretación de las evidencias obtenidas.

El informe deberá incluir un dictamen de resultados que versará sobre las materias o cuestiones objeto de la revisión practicada.

Se elaborará además un documento en formato PowerPoint que recoja un resumen de los resultados obtenidos. Este documento será objeto de una presentación en las instalaciones de Madrid Digital.

Fase 4 - Elaboración del Plan de Acción.

El equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer para implantar las recomendaciones recogidas en el Dictamen de Resultados. Este Plan de Acción deberá integrarse en el Informe Global de Plan de Acción que ha de elaborarse y mantenerse actualizado a lo largo de todo el servicio.

Las actuaciones se agruparán, en función de su dimensión y ámbito de aplicación, en proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - Descripción de los trabajos previstos.
 - Detalle de las actividades a realizar.
 - Identificación de la Unidad Organizativa de la Comunidad de Madrid responsable de su ejecución así como de aquellas otras Unidades con participación en su desarrollo.
- Clasificación del proyecto atendiendo a su plazo de desarrollo en función de oportunidad de ejecución (recursos humanos y económicos) y complejidad: corto, medio o largo plazo.
- Estimación de Esfuerzos, donde se aportará un resumen estimativo del esfuerzo y duración de cada proyecto a acometer, agrupados según su plazo de realización.
- Planificación de Proyecto, donde se mostrará, mediante un cronograma, la planificación programada de cada uno de los proyectos a realizar.

B. Servicio de análisis y gestión de riesgos tecnológicos

Las actividades de este servicio se realizarán de forma continua a lo largo de todo el contrato, e irán orientadas a realizar el análisis y la gestión del riesgo de los Sistemas de Información de Madrid Digital en base a los resultados obtenidos en las distintas auditorías realizadas durante el servicio y en las que se hayan realizado hasta fecha en Madrid Digital. Asimismo contemplará mantener actualizada la información obtenida en los Sistemas de Información de seguridad de Madrid Digital y a realizar la explotación de la misma para realizar los análisis que sean necesarios.

Dentro de estas tareas se encuentran las siguientes:

- Elaborar y dar soporte al desarrollo de políticas, normativas, procedimientos, guías protocolos, estándares, buenas prácticas, etc... en el ámbito de la



seguridad TIC. Definir, implantar y adecuar los controles de seguridad derivados de las normativas de seguridad objeto del contrato al ámbito de los sistemas, infraestructura y tecnología de Madrid Digital, especialmente los controles resultantes del nuevo reglamento europeo de protección de datos.

- Concretar el alcance que los requerimientos de seguridad de la normativa vigente aplican a cada una de las fases del ciclo de vida de los Sistemas de Información y a los servicios y plataformas existentes en Madrid Digital que los soportan, estableciendo un marco de seguridad integral.
- Identificar en los Sistemas de Información la existencia de datos de carácter personal a los que haya que aplicar la legislación de Protección de Datos.
- Soporte a la categorización de Sistemas de Información establecidos en el ENS, siguiendo criterios de proporcionalidad razonables y mensurables basados en el RD que regula el Esquema Nacional de Seguridad.
- Verificar el cumplimiento de los controles y requerimientos de seguridad de los Sistemas de Información y efectuar los análisis de riesgos pertinentes, generando tanto los informes correspondientes como su grabación en las herramientas corporativas de Madrid Digital.
- Establecer recomendaciones como resultado de las auditorías y el análisis de riesgos realizados, con el objetivo de adecuarse a los niveles de cumplimiento de la normativa de seguridad existente.
- Formalizar las recomendaciones en los planes de acción, adecuación y mejora necesarios.

En cuanto a la actividad concreta de análisis y medición integral de cumplimiento o de control interno en materia de seguridad, los trabajos se realizarán conforme a las siguientes fases:

Fase 1 – Precarga inicial del sistema de medición del cumplimiento

El equipo de trabajo deberá introducir en el sistema propuesto todos los resultados de los que Madrid Digital disponga respecto de las revisiones que en materia de seguridad haya realizado hasta la fecha de inicio de los trabajos que son objeto del presente pliego.

Fase 2 – Diseño del modelo de relación de controles de seguridad, aplicaciones, plataformas tecnológicas, auditorías, evidencias y cumplimiento.

El equipo de trabajo deberá elaborar el modelo de relación entre las entidades propuestas, de tal forma que durante la ejecución del servicio se puedan ofrecer los informes y resultados establecidos en el apartado B de la Cláusula 3 del presente pliego.

Fase 3 – Mantenimiento del servicio del sistema de medición de cumplimiento o de control interno en materia de seguridad

El adjudicatario alimentará el sistema mediante los resultados que se obtengan a lo largo del servicio de auditoría que es objeto de este contrato.

El adjudicatario deberá proporcionar a Madrid Digital, con una periodicidad mínima mensual, un informe que plasme los resultados del estado de cumplimiento en materia de seguridad, de acuerdo con la metodología adoptada y los requisitos establecidos en el Apartado B de la Cláusula 3 del presente pliego. Este informe adicionalmente



también se emitirá y proporcionará a Madrid Digital cada vez que existan cambios significativos, y como mínimo cada vez que se finalice un servicio de auditoría.

En el momento en el que Madrid Digital lo solicite, el adjudicatario deberá entregar toda la información del sistema de medición en un soporte en formato electrónico estándar (texto, CSV, Excel o Access), de acuerdo con las especificaciones y campos establecidos por Madrid Digital en el momento de la solicitud.

CLÁUSULA 5.- EQUIPO PRESTADOR DEL SERVICIO

Para la prestación de los trabajos objeto del contrato, el adjudicatario pondrá a disposición de Madrid Digital un equipo mínimo, con la cualificación y el perfil técnico mínimos, que a continuación se detallan:

- Requisitos en cuanto al **NÚMERO MÍNIMO DE RECURSOS Y CATEGORÍA PROFESIONAL MÍNIMA** exigida al personal prestador del servicio:
 - **2 Consultores**
 - **2 Analistas**
- Requisitos en cuanto a **TITULACIÓN MÍNIMA** exigida a cada uno de los miembros del equipo prestador del servicio:
 - Titulación Universitaria de Grado, Arquitecto, Ingeniero, Licenciado o equivalente.
- Requisitos en cuanto a **CONOCIMIENTOS Y EXPERIENCIA PROFESIONAL MINIMA** exigida a cada uno de los miembros del equipo prestador del servicio:

Perfil Consultor:

- Al menos una de las certificaciones reconocidas en el ámbito de auditorías y gestión de la seguridad, como CISA y CISM de ISACA. Las certificaciones deberán estar vigentes en el momento del inicio de los trabajos y mantenerse en vigor hasta la finalización de los mismos.
- Experiencia de al menos 4 años en proyectos de ciclo de vida del desarrollo software de sistemas de información y/o en operación de infraestructuras y sistemas, con conocimiento en planificación de proyectos de desarrollo, diseño y programación en diversas tecnologías, lenguajes y bases de datos, con especial relevancia en las siguientes tecnologías: java, Oracle, directorio Activo, LDAP, Oracle forms, Delphi, Joomla, fatwire, Unix, Windows.
- Conocimientos de protección de datos (a nivel técnico y jurídico) y, en especial, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Conocimientos de ISO 27000, Esquema Nacional de Seguridad.
- Haber participado en proyectos de auditoría de tecnologías de la información durante al menos siete años como Auditor, y especialmente en las normas de seguridad que son objeto del contrato.

Perfil Analista:

- Certificación CISA de ISACA.
- Experiencia de al menos 3 años en proyectos de ciclo de vida del desarrollo software de sistemas de información y/o en operación de infraestructuras y



sistemas, con conocimiento en planificación de proyectos de desarrollo, diseño y programación en diversas tecnologías, lenguajes y bases de datos, con especial relevancia en las siguientes tecnologías: java, Oracle, directorio Activo, LDAP, Oracle forms, Delphi, Joomla, fatwire, Unix, Windows.

- Conocimientos de protección de datos (a nivel técnico y jurídico) y, en especial, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Conocimientos de ISO 27000, Esquema Nacional de Seguridad.
- Haber participado en proyectos de auditoría de tecnologías de la información durante al menos cuatro años como Auditor.
- Haber participado en proyectos de auditoría de seguridad en materia de protección de datos personales durante al menos cuatro años como Auditor.
- Haber participado en proyectos de auditoría de seguridad en ISO27000 y/o Esquema Nacional de Seguridad durante al menos cuatro años como Auditor.

Al efecto, el licitador propuesto como adjudicatario, con carácter previo a la adjudicación del contrato, deberá aportar el *currículum vitae* de las personas asignadas a la ejecución del contrato, que deberá presentar debidamente cumplimentado y firmado por la persona que ostente la representación, especificando la cualificación profesional de cada uno de los miembros del equipo propuesto (con detalle de categoría, titulación, formación y actividad profesional) según Anexo II del presente Pliego de Cláusulas Técnicas.

CLÁUSULA 6.- VERIFICACIÓN DE LA CAPACIDAD DE LOS COMPONENTES DEL EQUIPO PRESTADOR DEL SERVICIO Y SUSTITUCIÓN DE LOS COMPONENTES DE DICHO EQUIPO
--

6.1. Condicionantes del equipo de trabajo:

El contratista responderá siempre de la adecuación del personal encargado de la realización de los servicios objeto del contrato, que responderá siempre a los *requisitos mínimos* que en el presente Pliego de Cláusulas Técnicas se señalan.

La falsedad en el nivel de conocimientos técnicos del equipo adscrito al servicio, facultará a esta Agencia para instar la **resolución** del contrato.

6.2. Constitución inicial del equipo de trabajo

El equipo técnico inicialmente propuesto por el adjudicatario, una vez aprobado por la Agencia, se incorporará al contrato para la ejecución de los trabajos objeto del mismo.

Dicho equipo responderá a los requisitos mínimos que en el presente pliego se señalan y a las mejoras que sobre dichos requisitos mínimos haya ofertado el licitador que resultare adjudicatario.

El contratista responderá de la permanente adecuación del personal encargado de la realización de los servicios objeto del contrato. A tal efecto, durante la ejecución de los trabajos, la Agencia podrá comprobar y verificar su capacidad en cualquier momento, pudiendo solicitar la sustitución de los profesionales que considere no idóneos para la prestación del servicio.

No obstante, la falsedad en el nivel de cualificación profesional del personal asignado, 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 el apartado siguiente, facultará a esta Agencia para instar la **resolución** del contrato.

Serán de exclusiva responsabilidad del adjudicatario tanto las cargas sociales y salariales del personal, como los impuestos y gastos derivados de la prestación del servicio.

6.3. Modificaciones en el equipo de trabajo propuestas por la empresa

Si el contratista propusiera la sustitución de algún componente del equipo de trabajo, deberá comunicarlo por escrito a la Agencia con quince días naturales de antelación.

La autorización de cambios puntuales en la composición del equipo requerirá de las siguientes condiciones:

- Justificación escrita, detallada y suficiente, explicando el motivo que suscita el cambio.
- Presentación de un candidato 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 alguno de los candidatos propuestos.

En el supuesto de que se produzcan sustituciones de miembros del equipo adscrito a la ejecución del servicio, se requiere un solapamiento de los recursos, sin coste adicional para la Agencia, durante un periodo mínimo de tres días laborables.

El número máximo de sustituciones permitidas será de un recurso por semestre.

6.4. Modificaciones en la composición del equipo de trabajo a petición de la Agencia

La valoración final de la calidad de los trabajos desarrollados 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 diez días naturales, por otro de igual categoría, si existen razones justificadas que lo aconsejen.

Toda nueva incorporación al equipo prestador del servicio deberá cumplir los requisitos mínimos, en cuanto a titulación, formación y actividad profesional establecidos en el presente pliego para cada uno de los recursos.

El adjudicatario se compromete a facilitar la incorporación de los profesionales requeridos en el plazo de diez días naturales desde la comunicación por parte de esta Agencia.

Estos cambios propuestos por la Agencia no se tendrán en consideración para el cómputo del número máximo de sustituciones permitidas en el apartado anterior (6.3.).

6.5. Penalizaciones

El adjudicatario asumirá las **penalizaciones** correspondientes, según el procedimiento establecido en el Anexo I al Pliego de Cláusulas Jurídicas.

Las **penalizaciones** aplicables, en el caso de incumplimiento de las obligaciones asumidas por el contratista en virtud del presente contrato, y detalladas en los apartados anteriores, son las que se indican a continuación:

- El incumplimiento por el adjudicatario del período mínimo de solapamiento de personal, establecido para cada nueva incorporación al equipo prestador a



propuesta de la empresa, dará lugar a la imposición de una penalización de **400 euros/día/recurso**.

- En caso de que el adjudicatario supere el número máximo de sustituciones permitido dará lugar a la imposición de una penalización de **2.000 euros/recurso**.
- El incumplimiento por el adjudicatario del plazo máximo establecido para una nueva incorporación, en caso de sustitución de componentes del equipo prestador a petición de la Agencia, dará lugar a la imposición de una penalización de **600 euros/día/recurso**.

Los importes de penalizaciones son sin incluir IVA.

CLÁUSULA 7.- CONDICIONES ADICIONALES A CUMPLIR

7.1. Disponibilidad de medios y verificación de la capacidad.

El adjudicatario deberá contar con los medios propios, personales y materiales, necesarios de cara al soporte técnico que pueda necesitar, para llevar a cabo con éxito todos los servicios objeto del contrato, teniendo en cuenta que, en todo caso, el equipo prestador del servicio se ubicará en las instalaciones que Madrid Digital determine.

Los empleados de la empresa contratista, que ejecuten por cuenta de ésta trabajos directamente relacionados con el objeto del contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por la propia empresa contratista. No obstante, si fuese necesario por razones operativas asociadas a la naturaleza del servicio a prestar, Madrid Digital proporcionaría a los miembros del equipo adscrito a la ejecución del servicio los medios que estime oportunos para la ejecución de los trabajos y obligaciones demandadas.

La dotación de dichos medios tiene naturaleza transitoria, ya que se utilizarán únicamente durante la ejecución del contrato, además su uso estará limitado exclusivamente al desarrollo de los trabajos que constituyen el objeto del contrato. En todo caso, Madrid Digital adoptará las medidas necesarias para que estas herramientas tengan una identificación diferenciada respecto de las asignadas al personal al servicio de Madrid Digital.

En el caso de que, por razones ajenas a Madrid Digital, los trabajos contratados puedan implicar para el contratista la decisión de ejecución de los mismos en régimen de turnos, en sábados o festivos, o en horario nocturno, esta Agencia no aceptará sobrecostes adicionales por estas circunstancias, que deberán ser asumidos siempre por el contratista.

7.2. Certificación de un Sistema de Gestión de Seguridad de la Información.

Para acreditar su solvencia las empresas licitadoras deberán aportar certificación vigente acreditativa de disponer y mantener operativo un *Sistema de Gestión de Seguridad de la Información*, de acuerdo a la norma internacional ISO 27001, emitido por una entidad acreditada por ENAC o equivalente, según lo especificado en el Anexo I del Pliego de Cláusulas Jurídicas.

7.3. Responsable del Servicio.

El contratista designará a un **Responsable del Servicio**, que será el responsable máximo del contrato ante Madrid Digital y distinto del Responsable o Jefe de Equipo designado de entre los miembros del mismo.



Este responsable será el interlocutor único con el Responsable del Contrato por parte de Madrid Digital y se encontrará en permanente contacto con el personal que la Dirección de Madrid Digital designe a los efectos que se señalan en la Cláusula 19 del Pliego de Cláusulas Jurídicas.

El adjudicatario, a través del *Responsable del Servicio*, y con la periodicidad que Madrid Digital 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 será el interlocutor único entre el adjudicatario e Madrid Digital. Coordinará todo el proyecto y será el responsable, en último término, de la buena marcha de los trabajos. Entre sus **tareas** principales cabe destacar las siguientes:

- Coordinar la ejecución de los trabajos.
- Realizar la planificación general de los trabajos y de las tareas asociadas.
- Supervisar y controlar la calidad de las actividades desarrolladas por su equipo.
- Hacer entrega a Madrid Digital de los documentos desarrollados por su equipo.

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

7.4. Ubicación de los integrantes del servicio.

La prestación del Servicio de análisis y gestión de riesgos tecnológicos requerirá la permanencia continua en las instalaciones de la Agencia y la dedicación completa y exclusiva al mismo de, al menos, 1 Analista.

CLÁUSULA 8.- SEGUIMIENTO Y CONTROL DEL CONTRATO

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

Seguimiento continuo de la evolución de los trabajos entre el *Responsable del Servicio* por parte del adjudicatario y el *Responsable del Contrato* que Madrid Digital designe.

Madrid Digital determinará los procedimientos y herramientas a utilizar para poder llevar a cabo el seguimiento y control de los trabajos. En todo caso, el Responsable del Servicio por parte del adjudicatario designará un Responsable o Jefe de Equipo.

El Jefe del Equipo deberá asistir obligatoriamente a todas las reuniones de seguimiento del contrato siendo el interlocutor único con el equipo de proyecto de Madrid Digital, ya sea a nivel técnico, táctico u operativo. Asimismo, deberá conocer en todo momento todos los detalles relativos a la planificación, ejecución y seguimiento de los trabajos (incluyendo todos los detalles técnicos de las auditorías, revisiones técnicas o trabajos que están en el alcance del presente pliego).

CLÁUSULA 9.- PLAZO DE GARANTÍA

Se establece un plazo de garantía del contrato de **UN AÑO** cuyo cómputo se iniciará desde la fecha de recepción o conformidad de los trabajos.

Hasta que no tenga lugar la finalización del periodo de garantía, 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 Madrid Digital 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, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados.

CLÁUSULA 10.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Normativa aplicable.

1. 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)*.
 - Y las 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.

Medidas de seguridad de carácter mínimo.

2. 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*):
 - 2.1 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.
 - 2.2 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 Madrid Digital, y en concreto:
 - 2.2.1 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.
 - 2.2.2 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.
 - 2.2.3 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 Madrid Digital. La salida de soportes y documentos fuera de los locales deberá ser también autorizada por Madrid Digital. 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.

- 2.2.4 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.
- 2.2.5 Solo con el consentimiento expreso y escrito de Madrid Digital, 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.
- 2.2.6 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.
- 2.2.7 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.
- 2.2.8 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.
- 2.2.9 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
- 2.3 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:
 - 2.3.1 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.

2.3.2 Exclusivamente el personal autorizado por Madrid Digital podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

2.3.3 Será necesaria la autorización de Madrid Digital para la ejecución de los procedimientos de recuperación de los datos.

2.4 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 **finés policiales**; o aquéllos que contengan datos derivados de actos de **violencia de género**, deberán observar las siguientes medidas:

2.4.1 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 Madrid Digital.

2.4.2 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.

2.4.3 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.

2.4.5 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.

2.4.6 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.

3. 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 dentro del equipo prestador del servicio a un miembro como **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.

4. 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 Madrid Digital, aunque sea para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
5. 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 Madrid Digital, el equipo prestador del servicio procederá a destruir o a devolver a Madrid Digital 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.

6. 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*, Madrid Digital, 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**

Derecho de información en la recogida de datos.

- 8 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 para Madrid Digital como por la C.M., inscrito en el Registro General de Ficheros de Datos Personales de la Agencia Española de Protección de Datos, y no podrán ser cedidos salvo por los supuestos previstos en la Ley. El Órgano responsable del fichero es el *Consejero-Delegado de Madrid Digital*, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es la *calle Embajadores Nº 181, de Madrid*, todo lo cual se informa en cumplimiento del *Artículo 5 de la LOPD*.

CLÁUSULA 11.- SEGURIDAD DE LA INFORMACIÓN TRATADA

La empresa adjudicataria, así como todos los componentes del equipo adscrito a la ejecución de los trabajos objeto del presente contrato, asumen las siguientes obligaciones:

11.1. Sigilo y confidencialidad de la información tratada.

Cada uno de los componentes del Equipo prestador del servicio se compromete a proteger la confidencialidad de cualquier información tratada como consecuencia de la ejecución de los trabajos derivados del contrato.

Todos los componentes del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información dimanante de la ejecución del contrato.

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, ceder o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución.

Esta obligación no se limita al tiempo de ejecución del presente contrato, 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 Madrid Digital, la Comunidad de Madrid o cualquier tercero que tenga relaciones contractuales con la misma, en relación con el objeto del presente contrato, será considerada como



«Información Confidencial», incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

El Equipo prestador del servicio deberá:

- 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 prestador del servicio.
- Utilizar o transmitir la Información Confidencial exclusivamente para los fines del contrato.
- No realizar copia de la Información Confidencial sin el previo consentimiento escrito de Madrid Digital, excepto aquellas copias que sean necesarias por el Equipo prestador del servicio.
- Restringir el acceso a la Información Confidencial únicamente a aquellas personas que necesiten conocerla para los fines del Contrato.

Cualquier publicidad o información a los medios de comunicación referida a la simple existencia del presente Contrato o a su contenido, deberá ser previamente aprobada por escrito por Madrid Digital.

El Equipo prestador del servicio procederá a destruir o a devolver a Madrid Digital toda la Información Confidencial a la finalización del contrato, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida. La destrucción o devolución de la Información Confidencial 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.

11.2. Modificaciones en la composición del Equipo prestador del servicio.

En el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en el presente documento.

A tal efecto, el firmante del presente documento, se compromete a formar e informar al nuevo personal de tales obligaciones, asumiendo, en caso contrario, las responsabilidades que pudieran derivarse por su incumplimiento.

CLÁUSULA 12.- PROPIEDAD DE LOS TRABAJOS

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

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



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

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

El contratista no podrá utilizar la información obtenida en la actividad desarrollada como consecuencia del contrato, no pudiendo transmitir dicho conocimiento, sin el consentimiento expreso y por escrito de Madrid Digital.

CLÁUSULA 14.- CALIDAD

Durante el periodo de ejecución del contrato, el adjudicatario propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada.

No obstante, Madrid Digital podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, la Agencia podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

CLÁUSULA 15.- CONTENIDO MÍNIMO DE LAS OFERTAS

En el presente apartado se describe la estructura según la cual deberán elaborarse las ofertas presentadas por cada uno de los licitadores. Para la elaboración de la citada propuesta los licitadores deberán basarse en los requerimientos recogidos en este Pliego. La oferta debe incorporar la totalidad de los trabajos solicitados en el Pliego, de manera que no se admitirán ofertas parciales por actividad.

Con carácter obligatorio, la memoria deberá presentarse en papel y en soporte electrónico, compatible con las herramientas instaladas en Madrid Digital (MS Word 2007, Adobe Acrobat Reader 8, MS Explorer 7).

Los licitadores deberán evitar descripciones genéricas o excesivamente prolijas que puedan perjudicar la comprensión de la oferta técnica directamente diseñada y ofrecida a Madrid Digital. El licitador deberá ajustarse especialmente a lo indicado en este punto, y circunscribir su propuesta exclusivamente a lo demandado en el pliego.

La **estructura** según la cual deberán elaborarse las ofertas a presentar por los licitadores es la siguiente:

1. Planificación, metodología y alcance del proyecto.

- Planificación detallada del proyecto, con especificación de fases y actividades asociadas, incluyendo dedicación esperada de Madrid Digital.
- Descripción detallada de la metodología de trabajo y de las actividades para desarrollar las tareas objeto del servicio, con la garantía de calidad requerida.

Se prestará una especial atención a aquellos aspectos de la propuesta para los que el presente pliego requiere la máxima precisión y el mayor detalle posible de desarrollo.
- Descripción detallada de la solución propuesta para el servicio de análisis y medición integral de cumplimiento así como del sistema aportado para la



obtención de la información respecto del análisis y medición del cumplimiento de las distintas regulaciones normativas en materia de seguridad.

- Descripción de la documentación y de los entregables comprometidos para cada una de las líneas de servicio definidas.

2. Organización de los equipos de trabajo propuestos.

Propuesta y descripción de la estructura de los equipos de trabajo, especialmente en lo que se refiere a:

- Composición, organización y dedicación del equipo de trabajo propuesto, para cada uno de los trabajos y de las fases correspondientes: Debe quedar claro el número total de recursos que van a estar involucrados en cada uno de los servicios definidos, los perfiles que tienen, las fases de las auditorías en las que participarán y las horas de dedicación de cada recurso en cada uno de los servicios y, cuando proceda, en cada fase de las auditorías.
- Asegurar la estabilidad del equipo.
- Comprometer la implicación de los equipos de trabajo en situaciones de crisis, en las que prima la continuidad del servicio objeto de contratación.
- Propuestas de valor cuya aplicación sea factible, de manera que permitan a Madrid Digital obtener la flexibilidad en la gestión de las capacidades necesaria ante picos de trabajo.

3. Metodología de Seguimiento y Control del Servicio.

Descripción del modelo de seguimiento del servicio:

- Propuesta detallada de cada uno de los Informes a elaborar para el seguimiento de los periodos definidos.
- Métricas adicionales, así como cualquier otro aspecto de valor para el seguimiento y control del servicio que el licitador comprometa, que permita afianzar y mejorar el modelo de servicio de Madrid Digital.

4. Gestión del Conocimiento.

Propuesta del *Plan de Gestión del Conocimiento* a implementar durante la ejecución del contrato, el cual deberá contemplar:

- Método para asegurar la calidad y grado de actualización de la documentación.
- Despersonalización del conocimiento de las aplicaciones y sistemas objeto del contrato.
- Gestión de la devolución del conocimiento a Madrid Digital.

5. Análisis de Riesgos del Servicio.

Se anticiparán los principales riesgos que pueden afectar al desarrollo del servicio objeto del contrato, estableciendo las medidas preventivas y paliativas que se considere necesario establecer tanto por parte del contratista como de Madrid Digital.

Los licitadores adjuntarán en el Sobre nº 2, junto a la documentación anteriormente citada, un **resumen ejecutivo**, de un máximo de **dos páginas**, en el que de forma esquemática y comprensible recojan el contenido técnico de este sobre.



Con la finalidad de garantizar el cumplimiento de lo exigido en el *Artículo 140 del TRLCSP*, que impone a los Órganos de Contratación la obligación de no divulgar la información facilitada por los empresarios que éstos hayan designado como confidencial, el licitador deberán identificar qué aspectos concretos de su oferta técnica se han de considerar confidenciales, señalando expresamente los párrafos que contengan dicha información confidencial. A este respecto se ha de tener en cuenta que la declaración de confidencialidad no puede afectar a toda la documentación técnica presentada.

CLÁUSULA 16.- PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **VEINTICUATRO MESES**, comprendidos entre el **16 de septiembre de 2017 y el 15 de septiembre de 2019**, y según los siguientes plazos parciales:

A) Servicios de auditoría en materia de seguridad:

SERVICIO DE AUDITORÍA DE CONTROLES DE PLATAFORMAS COMUNES: El plazo de ejecución será como máximo de cuatro meses. Esta auditoría se realizará al inicio del servicio.

SERVICIO DE AUDITORÍA DE CONTROLES PARTICULARES DE CADA SISTEMA DE INFORMACIÓN:

1. **Auditoría LOPD:** El plazo de ejecución será como máximo de cinco meses. Esta auditoría se realizará en 2018.
2. **Auditoría 27002:** El plazo de ejecución será como máximo de dos meses. Esta auditoría se realizará en 2019.
3. **Auditoría SSII Administración de Justicia:** El plazo de ejecución será como máximo de dos meses. Esta auditoría se realizará en 2019.
4. **Auditoría ENS:** El plazo de ejecución será como máximo de cuatro meses. Esta auditoría se realizará en 2018.
5. **Revisiones técnicas:** Se realizarán, las revisiones técnicas que en cada caso se estimen necesarias, hasta un máximo de 660 horas en total y durante la ejecución del contrato. Estos análisis se podrán realizar en cualquier momento a lo largo de la ejecución del contrato.

B) Servicio de análisis y gestión de riesgos tecnológicos:

1. **Análisis y Gestión del Riesgo,** se realizará a lo largo de todo el servicio de manera continua.
2. **Análisis de cumplimiento del Reglamento UE 2016/679,** se realizará a lo largo de todo el servicio.
3. **Precarga inicial del sistema de medición del cumplimiento:** El plazo de ejecución será de un mes, a contar desde el día de inicio del contrato.
4. **Resto de trabajos:** los contemplados en la Cláusula 3 Apartado B del presente Pliego, el plazo de ejecución será de veinticuatro meses.

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 ejecución de los mismos, Madrid Digital quedará facultada para instar la **resolución** del contrato.



CLÁUSULA 17.- 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, los licitadores podrán dirigirse a:

Madrid Digital

Dirección de Seguridad Corporativa.

Área de Seguridad de la Información y Protección de Datos

C/ Embajadores, 181. 28045 Madrid

Tel.: 91 580 50 00. Horario de consultas: de 9 a 14 horas, de lunes a viernes



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **0907656939089738880572**

ANEXO I

Volumetría

- A. Auditoría de los procedimientos e instrucciones vigentes en materia de seguridad de datos personales: Volumetría de ficheros de datos de carácter personal

VOLUMETRÍA DE FICHEROS ASOCIADOS:

Ficheros nivel medio	Ficheros nivel alto	Total ficheros
123	135	258

- B. Auditoría del Sistema de Gestión de la Seguridad de la Información (SGSI) del Organismo Pagador de la Comunidad de Madrid: Volumetría del número de Sistemas de Información

Para la realización de los trabajos se han definido dieciséis (16) Sistemas de Información que serán auditados.

- C. Auditoría de los sistemas de información al servicio de la Administración de Justicia: Volumetría del número de sistemas de información

Para la realización de los trabajos se han definido trece (13) Sistemas de Información que serán auditados.

- D. Auditoría de la seguridad de los sistemas de información relativos al Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Volumetría del número de sistemas

El cálculo del tamaño de la muestra de los Sistemas de Información a auditar se realizará, conforme a lo descrito en la cláusula 4 "Descripción de los Servicios", sobre el total de los Sistemas de Información que son responsabilidad de la Agencia, aproximadamente 1.200.

Todos los centros directivos objeto de los trabajos objeto del contrato se encuentran dentro del territorio de la Comunidad de Madrid.



ANEXO II
Experiencia profesional

Por cada una de las personas componentes del equipo de trabajo, incluir la siguiente información:

TITULACIÓN ACADÉMICA UNIVERSITARIA

TÍTULO ACADÉMICO	CENTRO	AÑOS	FECHA EXPEDICIÓN	TIC

AÑOS: duración oficial del título académico

TIC: si/no según pertenezca o no a tecnologías de la información

FORMACIÓN Y CERTIFICADOS OFICIALES (ÁMBITO DE AUDITORÍA, SEGURIDAD Y TIC)

CURSO/CERTIFICACIÓN	CENTRO/ENTIDAD	HORAS	FECHA EXPEDICIÓN

EXPERIENCIA PROFESIONAL

EMPRESA	CATEGORÍA	FECHA INICIO	FECHA FIN	ACTIVIDAD DE LA EMPRESA

CATEGORÍA: En caso de haber ocupado puestos de diversas categorías dentro de la misma empresa, indicarlo en filas diferentes.

DATOS RELATIVOS A PROYECTOS

NOMBRE PROYECTO	ROL/ CATEGORÍA	FECHA INICIO	FECHA FIN	CLIENTE	FUNCIONALIDAD

FUNCIONALIDAD: Breve descripción del objeto y funcionalidad del proyecto

EXPERIENCIA EN ENTORNOS TECNOLÓGICOS

CATEGORÍA	MESES	BASES DE DATOS	SISTEMAS OPERATIVOS	LENGUAJES DE PROGRAMACIÓN	OTROS

CATEGORÍA: La ejercida en el proyecto

LENGUAJES DE PROGRAMACIÓN: Indicar el entorno concreto de BBDD, S.O, lenguaje de programación o cualquier otro entorno tecnológico en los proyectos en que ha participado y dispone de experiencia.

ELABORADO Y PROPUESTO POR: <i>El Director de Seguridad Corporativa</i> Fdo.: Fernando Ledrado Gómez	APROBADO POR: <i>El Consejero Delegado de la Agencia para la Administración Digital de la C.M.</i> Fdo.: Blas Labrador Román
---	--

