

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR
EN EL CONTRATO DE SERVICIOS DENOMINADO “AUDITORIA,
ASESORÍA, CONTROL DEL CUMPLIMIENTO y CERTIFICACIÓN
DE CONFORMIDAD EN MATERIA DE SEGURIDAD DE LA
COMUNIDAD DE MADRID (2 lotes)”, A ADJUDICAR MEDIANTE
PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1018622254009916532820**



INDICE:

CLÁUSULA 1.- INTRODUCCIÓN	4
CLÁUSULA 2.- OBJETO.....	5
CLÁUSULA 3.- ÁMBITO Y ALCANCE DE APLICACIÓN	5
3.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad.	6
3.1.1 A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales y Revisiones Técnicas	6
3.1.2 B: Auditorías de seguridad de Sistemas de Información	7
3.1.3 C: Gestión de Riesgos, soporte a la Certificación y ciclo de mejora de la seguridad	8
3.2 LOTE 2: Servicio de certificación de conformidad con el esquema nacional de seguridad e ISO 27001	9
3.2.1 A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001.	9
CLÁUSULA 4.- DESCRIPCIÓN y REQUERIMIENTOS DEL SERVICIO.....	9
4.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad.	9
4.1.1 A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales de Madrid Digital y Revisiones Técnicas	11
4.1.2 B: Auditorías de seguridad de Sistemas de Información	16
4.1.3 C: Gestión de Riesgos, soporte a la certificación y ciclo de mejora de la seguridad	23
4.2 LOTE 2: Servicio de Certificación de Conformidad con el Esquema Nacional de Seguridad e ISO 27001	25
4.2.1 Entregables del Servicio de Certificación de conformidad con el ENS e ISO 27001	27
4.2.2 Auditorías extraordinarias sobre no conformidades	27
CLÁUSULA 5.- VOLUMETRÍA.....	28
5.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad	28
5.1.2 B: Auditorías de seguridad de Sistemas de Información	29
5.1.3 C: Gestión de Riesgos, soporte a la Certificación y ciclo de mejora de la seguridad	30
5.2 LOTE 2: Servicio de certificación de conformidad con el esquema nacional de seguridad e ISO 27001	30
5.2.1 A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001	30
CLÁUSULA 6.- PLAZOS DE EJECUCIÓN	31
6.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad	31
6.1.1 A1: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales: .	31
6.1.2 A2: Revisiones Técnicas.....	31
6.1.3 B: Auditorías de seguridad de Sistemas de Información	31
6.1.4 C: Servicio de Gestión de Riesgos, soporte a la certificación y ciclo de mejora de la seguridad.....	31
6.2 LOTE 2: Servicios de certificación de conformidad con el esquema nacional de seguridad e ISO 27001.	31
6.2.1 A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001	32
CLÁUSULA 7.- EQUIPO PRESTADOR DEL SERVICIO.....	32
7.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad	32
7.2 LOTE 2: Servicios de certificación de conformidad con el esquema nacional de seguridad e ISO 27001	37
CLÁUSULA 8.- MODELO DE GESTIÓN	38

8.1	Condiciones generales de los recursos del adjudicatario	39
8.1.1	Constitución inicial del equipo de trabajo	39
8.1.2	Condiciones de estabilidad del equipo de trabajo por parte de la empresa adjudicataria	39
8.1.3	Modificaciones en la composición del equipo de trabajo a petición de la Agencia	40
CLÁUSULA 9.-	CONDICIONES ADICIONALES A CUMPLIR.....	40
9.1	Disponibilidad de medios y verificación de la capacidad (Lote 1 y Lote 2).....	40
CLÁUSULA 10.-	CONTENIDO DE LAS OFERTAS	41
10.1	Contenido de las ofertas para el lote 1	41
10.1.1	Planificación y planteamiento integral del proyecto	41
10.1.2	Metodología y alcance de los servicios	42
10.1.3	Organización de los equipos de trabajo propuestos	42
10.1.4	Metodología de seguimiento y Control del Servicio	42
10.2	Contenido de las ofertas para el lote 2	43
10.2.1	Metodología y alcance del proyecto	43
10.2.2	Organización de los equipos de trabajo propuestos	43
10.2.3	Metodología de seguimiento y Control del Servicio	44
CLÁUSULA 11.-	DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS ..	44
CLÁUSULA 12.-	CALIDAD DEL SERVICIO.....	44
CLÁUSULA 13.-	CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS	44
ANEXO I :	MODELO DE CURRICULUM	46



CLÁUSULA 1.- INTRODUCCIÓN

La **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante **Madrid Digital**), según se establece en la *Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas*, modificada parcialmente por la *Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 31 de diciembre de 2015), tiene asignada, entre otras funciones, la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, mediante medios propios o ajenos, a cuyo fin le corresponde particularmente, según el Artículo 10, Tres, c:

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

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

El objeto del contrato es la prestación de los servicios **de auditoría, control, implantación y certificación de la norma ISO 27001 y certificación de conformidad con el Esquema Nacional de Seguridad 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 Prescripciones Técnicas y en los Anexos al mismo.

CLÁUSULA 3.- ÁMBITO Y ALCANCE DE APLICACIÓN

El ámbito de aplicación se circunscribe a las actividades de tratamiento de datos de carácter personal y a los Sistemas de Información, servicios e infraestructuras TIC en el ámbito de las competencias de Madrid Digital 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.

Debido a la naturaleza de los servicios a contratar, el presente pliego establece una división en dos lotes atendiendo a la tipología de los servicios requeridos, de tal forma que permita un desarrollo acorde a la estrategia de Ciberseguridad de Madrid Digital:

Lote 1: Servicios de auditoría y gestión de riesgos en materia de seguridad.

Lote 2: Servicio de Certificación de Conformidad con el Esquema Nacional de Seguridad y certificación de la norma ISO 27001.

El lote 1 tiene como objetivo la **ejecución de auditorías, revisiones técnicas y gestión de riesgos en el ámbito interno de Madrid Digital y los servicios prestados a la Comunidad de Madrid**, aplicando determinadas metodologías y procedimientos de Madrid Digital que posibilitan agilizar y homogeneizar los procesos de revisión del cumplimiento de las normativas de seguridad vigentes descritas en el presente pliego, cuyos resultados derivan en planes de acciones correctoras y mejoras de la seguridad de los sistemas en Madrid Digital y sirven como referencia para las certificaciones de conformidad con el Esquema Nacional de Seguridad del lote 2.

Por otro lado, **el lote 2** tiene como **objetivo**:

- **La expedición de Certificaciones de Conformidad con el Esquema Nacional de Seguridad**, en cumplimiento del artículo 41 del Esquema anteriormente mencionado, y desarrollado mediante la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de



Seguridad de conformidad con el Esquema Nacional de Seguridad de obligado cumplimiento por parte de las Administraciones públicas, y se requiere que la **empresa adjudicataria sea una entidad certificadora acreditada por la Entidad Nacional de Acreditación (ENAC)** para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad

- **La expedición de certificación en el cumplimiento de la norma ISO 27001**, y por tanto se requiere que **la empresa adjudicataria sea una entidad certificadora acreditada en este ámbito**.

Debido a la similitud de ambas acreditaciones y atendiendo a criterios de eficiencia y optimización de recursos, el proceso de certificación se debe abordar de manera conjunta y concurrente.

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

3.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad.

SERVICIOS DE CUOTA VARIABLE

3.1.1 A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales y Revisiones Técnicas

Se contemplan como trabajos de cuota variable los servicios referentes a auditorías en Madrid Digital para la revisión de los procedimientos e instrucciones vigentes de protección de datos personales y las revisiones técnicas, en el siguiente ámbito y alcance de actuación:

3.1.1.1 A1: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales

Auditoría de los procedimientos, procesos e instrucciones vigentes en cumplimiento de la normativa en materia de protección de datos de carácter personal, respecto al tratamiento de datos de carácter personal cuya titularidad recae en Madrid Digital, además de auditoría de Madrid Digital como Encargado del Tratamiento de las actividades de tratamiento de la Comunidad de Madrid, según la normativa legal vigente en el inicio del contrato:

- **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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.**

3.1.1.2 A2: Revisiones Técnicas

Se realizarán, las revisiones técnicas que en cada caso se estimen necesarias, durante la ejecución del contrato y hasta un máximo de horas en total indicado en el apartado correspondiente del presente pliego.



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.

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

SERVICIOS DE CUOTA FIJA

3.1.2 B: Auditorías de seguridad de Sistemas de Información

Auditoría de los Sistemas de Información, **entendiendo como Sistemas de Información las aplicaciones y sus componentes comunes (también denominados activos operacionales) utilizados**, bajo la responsabilidad de Madrid Digital.

Se tendrán en consideración las siguientes normativas y buenas prácticas para la revisión del cumplimiento legal en materia de seguridad en los Sistemas de Información:

1. **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad**, 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.
2. Norma **ISO-IEC-27002** para 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.
3. **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 Sistemas de Información al servicio de la Administración de Justicia 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, así mismo se tendrán en consideración los posibles controles derivados de las **Bases del Esquema Judicial de Interoperabilidad y Seguridad** publicado por el Comité técnico estatal de la Administración judicial electrónica (CTEAJE), de aplicación en la Administración de Justicia para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y la conservación de los datos, informaciones, documentos y servicios, utilizados por medios electrónicos que gestionen los distintos órganos judiciales en el ejercicio de sus competencias.
4. **Buenas prácticas de seguridad en el tratamiento de datos de carácter personal** adquiridas por Madrid Digital.

3.1.3 C: Gestión de Riesgos, soporte a la Certificación y ciclo de mejora de la seguridad

El servicio tendrá el siguiente alcance:

- Estudio y revisión documental previa de la metodología y procesos relacionados con auditoría y gestión de riesgos en Madrid Digital.
- Análisis de la situación inicial y elaboración de guías de auditoría de sistemas de información (componentes comunes y aplicaciones).

- Definición y diseño del modelo de informe de auditoría y documentación entregable a Madrid Digital.
- Gestión documental referente a los procesos de auditoría y gestión de riesgos de los servicios del Lote 1.
- Actualización de la información referente a seguridad de la información en los sistemas de información corporativos.
- Definición de indicadores de medición de la seguridad y elaboración de informes de cumplimiento y riesgo, basados en los indicadores, con el objetivo de informar a la Dirección y a las áreas responsables de Madrid Digital de la medición de seguridad de los activos de su responsabilidad.
- Soporte y asistencia a los trabajos de pre-auditoría de Certificación y a la propia certificación de conformidad con el Esquema Nacional de Seguridad e ISO 27001 del Lote 2, y elaboración de planes de acciones correctoras derivados de las no conformidades del servicio de Certificación de Conformidad con el ENS.
- Realización de revisiones incrementales para verificar el nuevo nivel de madurez de los controles sobre los cuales Madrid Digital ha realizado mejoras o solventado deficiencias, posterior a la ejecución de las auditorías y la elaboración y ejecución de los planes de acción. Elaborar la documentación anexa que refleje el resultado de la nueva revisión, y actualizar en los sistemas Corporativos de Madrid Digital.

3.2 LOTE 2: Servicio de certificación de conformidad con el esquema nacional de seguridad e ISO 27001

SERVICIOS DE CUOTA VARIABLE

3.2.1 A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001.

Servicio de expedición de Certificaciones de Conformidad con el Esquema Nacional de Seguridad establecida en su artículo 41 y desarrollada mediante la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la **Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad** de obligado cumplimiento por parte de las Administraciones públicas, y **certificación de la norma ISO 27001**.

CLÁUSULA 4.- DESCRIPCIÓN y REQUERIMIENTOS DEL SERVICIO

4.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad.

CONSIDERACIONES GENERALES

Debido al elevado número de sistemas y tecnologías en Madrid Digital y a la confluencia de distinta normativa de seguridad, la valoración del cumplimiento en materia de seguridad objeto de este servicio se estructurará en torno a una **metodología de trabajo** que divide las revisiones de los Sistemas de Información en dos grandes bloques:

- Revisión de controles en plataformas y elementos comunes (denominados **componentes comunes o activos operacionales**)
- Revisión de controles particulares de cada Sistema de Información o aplicaciones (denominado **componente aplicación**), que en gran parte de casos están basados en frameworks de desarrollo corporativos de diferente tecnología, que permiten una homogenización y centralización de medidas de seguridad aplicables.

Los componentes comunes (o activos operacionales) son aquellos elementos de tipo organizativo (políticas, normas, procesos y procedimientos corporativos y horizontales a Madrid Digital), plataformas tecnológicas, software base, Centro de Procesamiento de Datos, servicios comunes de tramitación electrónica, etc..., sobre los cuales las aplicaciones se apoyan para poder prestar el servicio.

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 comunes o activos operacionales que le correspondan más el resultado de la revisión de los controles propios del Sistema de Información.

Madrid Digital dispone de una herramienta corporativa, denominada SENS, para la gestión de auditorías de componentes y Sistemas de Información, donde se guardan los resultados de las auditorías realizadas.

Además, la empresa adjudicataria del Lote 1, tras el análisis y revisión de la documentación proporcionada por Madrid Digital y en el transcurso del tiempo del contrato y la ejecución de las diferentes revisiones de auditoría, deberán atender los requerimientos de información referentes a las auditorías ejecutadas, y dar el soporte necesario al equipo de trabajo adjudicatario del "Lote 2: Servicios de certificación de Conformidad con el Esquema Nacional de Seguridad".



DOCUMENTACIÓN INICIAL

Al inicio de los trabajos, Madrid Digital pondrá a disposición de la empresa adjudicataria la documentación disponible referente al objeto del contrato, con el fin de facilitar el completo entendimiento de la situación actual, proporcionando entre otras, la siguiente documentación:

- Guía de componentes comunes.
- Matriz de relación de medidas de seguridad y componentes comunes o activos operacionales.
- Guía de auditoría de medidas de seguridad de Sistemas de Información.
- Documentación de referencia de los frameworks de desarrollo.
- Auditorías realizadas a componentes, Sistemas de Información y frameworks.
- Planes de Acción ejecutados y en curso.
- Etc...

SERVICIOS DE CUOTA VARIABLE

4.1.1 A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales de Madrid Digital y Revisiones Técnicas

4.1.1.1 A1: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales

Fase 1: Definición del alcance

Madrid Digital, tiene nombrado un Delegado de Protección de Datos (en adelante DPD) en cumplimiento del Reglamento General Europeo de Protección de Datos. Además, Madrid Digital es responsable de actividades de tratamiento de datos de carácter personal, las cuales se encuentran relacionadas en el Registro de Actividades de Tratamiento (RAT). Toda esta información se encuentra publicada en el portal corporativo de la Comunidad de Madrid.

A la vista de la información anteriormente indicada, el licitador deberá realizar una propuesta sobre el objeto y alcance de las auditorías de Protección de Datos en Madrid Digital, contemplando las actividades de tratamiento bajo su responsabilidad que deben ser auditadas, así como la propuesta de auditoría para la verificación del cumplimiento de Madrid Digital como encargado del tratamiento de los Centros directivos de la Comunidad de Madrid.

Fase 2: Preparación y planificación de las auditorías

Se tendrá en consideración la posibilidad de mantener reuniones iniciales con los responsables para verificar el alcance y determinar los aspectos globales y comunes que afectan a todas las actividades de tratamiento de Madrid Digital.

En esta fase el adjudicatario deberá elaborar un programa de auditoría completo que incluya todos los aspectos necesarios para la ejecución de la auditoría, en particular, y sin perjuicio de las tareas propuestas por los licitadores en sus ofertas, se incluirán las siguientes:

- Objetivo de la auditoría.

- Alcance de la auditoría, incluyendo actividades de tratamiento objeto de auditoría.
- Criterios de auditoría, incluyendo las listas de controles a verificar, objetivos de control, evidencias a solicitar en relación con la seguridad de datos personales en Madrid Digital, tales como procedimientos, registros, formación, inventarios, listas, etc., y siempre teniendo en consideración las normativas y guías publicadas por la Agencia Española de Protección de Datos. En cada uno de los controles a auditar, se deberá indicar la referencia normativa que ha dado origen a su verificación.
- Metodología y equipo de trabajo.
- Planificación detallada, con especificación de fases y actividades, calendario de hitos a alcanzar y acciones de seguimiento del proyecto.

Además, se deberá realizar el lanzamiento y presentación del programa de auditoría, que deberá iniciarse con la presentación y coordinación a las distintas áreas internas de Madrid Digital que se vean afectadas por la auditoría, y que deberá culminarse con la presentación del proyecto a la Dirección de Madrid Digital.

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.).

El adjudicatario deberá proponer, elaborar, desarrollar y entregar un modelo de gestión de evidencias para las actividades de tratamiento de Madrid Digital, que permita gestionar su acceso y gestión de manera ágil y eficiente.

Fase 3: Ejecución

Una vez elaborado y aprobado el programa de auditoría, el licitador deberá proceder a la ejecución de las actividades de auditoría previstas según la metodología propuesta, elaborando los documentos de trabajo específicos, planificando las reuniones con los interlocutores identificados.

Las reuniones de auditoría deben ser planificadas con una agenda previa que contenga los documentos de trabajo necesarios y la descripción de los objetivos y alcance de la reunión de auditoría, y a su finalización el equipo auditor deberá elaborar un acta para reflejar los acuerdos alcanzados, así como la petición de información y evidencias a los responsables.

En el transcurso de la ejecución de los trabajos, se deberán determinar los sistemas de información involucrados en las actividades de tratamiento y por tanto solicitar las evidencias asociadas a controles de las normativas de seguridad que se establecieron en la fase anterior.

En caso que así fuera requerido, el adjudicatario ofrecerá el soporte necesario para atender las observaciones o dudas planteadas por los responsables del tratamiento como resultado de las

auditorías, así como soporte a la utilización de la herramienta corporativa de Protección de datos de carácter personal, siempre y cuando la herramienta esté disponible durante el transcurso del servicio prestado.

Entregables

Informe de Auditoría

A la conclusión de la auditoría, la empresa adjudicataria deberá elaborar y facilitar los informes de auditoría resultantes de los trabajos, que dictaminará sobre el grado de adecuación de Madrid Digital a la normativa de protección de datos vigente, incluyendo un registro completo, preciso, conciso y claro de la auditoría, con referencias al objetivo de la auditoría, alcance, detalle de las actividades de tratamiento, interlocutores, fechas, ubicaciones, criterios de auditoría, metodología de trabajo, hallazgos y evidencias y conclusiones.

Atendiendo a los criterios de eficacia y optimización de recursos antes mencionados y para evitar cuestiones reiterativas en los informes, se podrá contemplar la posibilidad de elaborar un informe común junto con los informes particulares que se identifiquen.

El informe de auditoría deberá incluir un plan de acción con la descripción de las acciones correctoras y mejoras necesarias que debe implantar Madrid Digital para el cumplimiento de la normativa vigente de protección de datos personales.

Los informes correspondientes serán enviados a los responsables y al Delegado de Protección de Datos, estableciendo un plazo, acordado con Madrid Digital, y no inferior a 15 días, para la atención de alegaciones y observaciones a los informes.

Además del informe de auditoría como responsable del tratamiento, se deberá realizar un informe de auditoría específico de Madrid Digital como encargado del tratamiento de actividades de tratamiento de la Comunidad de Madrid.

Evidencias

Las evidencias recopiladas en el presente servicio deberán ser incorporadas al modelo de gestión propuesto y entregadas a Madrid Digital en formato electrónico.

Controles y evidencias de Sistemas de Información con tratamiento de datos personales

El adjudicatario deberá elaborar y entregar un documento que recoja los sistemas de información relacionados con actividades de tratamiento de datos personales, junto con la relación de evidencias recabadas y los controles y normativa de referencia, sirviendo de entrada para el servicio de auditoría de Sistemas de Información.

Presentación/informe cierre de auditoría

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 y será objeto de una presentación en las instalaciones de Madrid Digital.



En caso que estuviera disponible, los resultados de las auditorías deberán ser incorporados por parte de la empresa adjudicataria al sistema corporativo de protección de datos personales de Madrid Digital.

4.1.1.2 A2: Revisiones Técnicas

El servicio de revisiones técnicas, determinado en este apartado, se establece con carácter estimado, quedando subordinado a las necesidades de Madrid Digital, con el máximo de horas estipulado en el apartado volumetría del presente pliego.

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. 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, contemplando 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.
 - Relación de medidas de seguridad de las normativas de seguridad objeto del contrato que serán revisadas y valoradas en la revisión técnica a realizar.

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.

Cada convocatoria de reunión deberá ser planificada con antelación e ir acompañada de una **agenda** con los temas a tratar junto con la documentación necesaria y la descripción de los objetivos y alcance de la reunión, y a su finalización el equipo auditor deberá elaborar un **acta** para reflejar los acuerdos alcanzados, así como la petición de información y evidencias a los responsables.

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 y de las medidas de seguridad de la normativa de seguridad relacionada, y en cada caso, la trazabilidad y relación con las medidas de seguridad de la normativa de seguridad.

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.

SERVICIOS DE CUOTA FIJA

4.1.2 B: Auditorías de seguridad de Sistemas de Información

Para evaluar el grado de implantación de las medidas de seguridad, Madrid Digital requiere la utilización de una escala compuesta por seis (6) valores, en el rango de L0 a L5, que indica el nivel de madurez de cada uno de los controles, basado en el modelo CMM (Capability Maturity Model) y recomendado por el Centro Criptológico Nacional (CCN) para la valoración de la madurez de las medidas del Esquema Nacional de Seguridad.

B.1 Auditorías de Componentes Comunes o activos operacionales

La revisión de controles en plataformas y elementos comunes conllevará por parte del adjudicatario la evaluación del cumplimiento de cada uno de los controles de las distintas normativas de seguridad en las plataformas tecnológicas y elementos comunes a todos los Sistemas de Información de la Comunidad de Madrid, con el objetivo de agilizar y optimizar las auditorías de sistemas de información que se realicen posteriormente.

Para llevar a cabo esta actividad, Madrid Digital proporcionará al adjudicatario en el momento de inicio del contrato la documentación disponible sobre componentes comunes, incluyendo una Declaración de Aplicabilidad de medidas de seguridad, y los resultados de auditorías anteriores sobre los controles de las normativas de seguridad afectadas.

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

Fase 1: Preparación y planificación de las auditorías

En esta fase, el adjudicatario deberá revisar la información proporcionada por Madrid Digital y establecer las bases de trabajo para la ejecución de las auditorías de componentes comunes.

En particular, dentro de esta fase se incluye:

- Revisar la información proporcionada para obtener el necesario entendimiento y visión general de la organización y operativa de Madrid Digital para la ejecución del proceso de auditoría.
- Análisis de las auditorías de componentes existentes. De forma obligatoria, deberán ser objeto de una revisión de auditoría:
 - Controles no evaluados o cuya valoración del nivel de madurez es igual o inferior a L2.
 - Todos aquellos controles que, tras la revisión de los informes de auditoría ya existentes por parte del adjudicatario, no esté suficientemente claro o conforme la descripción de la implantación en Madrid Digital, el nivel de madurez y las evidencias relacionadas, así como otro tipo de cuestiones que haga necesaria una nueva revisión del control.

- Controles con un nivel de madurez L3 o superior y que Madrid Digital considere necesario realizar una nueva revisión.

En todo caso, independientemente si un determinado control es objeto de nueva auditoría o se considera conforme a auditorías anteriores, deberá ser incluido en el informe de auditoría resultante, y además, la empresa adjudicataria deberá adquirir el conocimiento suficiente sobre su implantación en Madrid Digital para abordar el proceso de auditoría del componente con garantías suficientes y permita dar el soporte necesario al prestador del Servicio de Certificación de Conformidad con el Esquema Nacional de Seguridad del Lote 2.

- Elaboración del programa de auditoría con la planificación detallada de las actuaciones, incluyendo el lanzamiento y presentación del proyecto a Madrid Digital, la coordinación con las áreas afectadas y la constitución del equipo de trabajo que llevará a cabo el proyecto.
- Elaboración del plan de auditoría, basado en las guías de auditoría elaboradas previamente, por componente detallando los controles considerados conformes a auditorías anteriores y los controles a auditar, todos ellos referenciados a su normativa de seguridad vigente, junto con el objetivo de control y detalle de las pruebas y comprobaciones previstas para la verificación de su cumplimiento.

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

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

Cada convocatoria de reunión deberá ser planificada con antelación e ir acompañada de una **agenda** con los temas a tratar junto con la documentación necesaria y la descripción de los objetivos y alcance de la reunión, y a su finalización el equipo auditor deberá elaborar un **acta** para reflejar los acuerdos alcanzados, así como la petición de información y evidencias a los responsables.

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

El equipo de trabajo elaborará un informe de auditoría por cada componente auditado donde se recojan los resultados de las revisiones efectuadas respecto al grado de adecuación y nivel de madurez de los controles de los componentes comunes bajo la responsabilidad de Madrid Digital. Los informes de auditorías deberán contener, al menos, la información indicada en el apartado "Informes de Auditoría" del presente pliego.

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

El equipo auditor estará a disposición de los responsables de los componentes para atender alegaciones y aclarar aspectos que consideren necesarios para un mayor entendimiento de los resultados obtenidos.

Fase 4 – Evidencias.

Las evidencias recopiladas a lo largo del desarrollo de los trabajos deberán ser incorporadas a un modelo de gestión de evidencias ya existente basado en la herramienta Access, o en caso que Madrid Digital así lo requiera, la empresa adjudicataria deberá elaborar y desarrollar un nuevo modelo de gestión de evidencias que facilite su tratamiento y reutilización, en cuyo caso se deberá disponer de él en las fases de preparación de las auditorías.

Fase 5 – Elaboración del Plan de Acción

A la conclusión de las auditorías, y en un plazo no superior a 30 días desde la fecha de aprobación de los informes de auditoría de todos los componentes pertenecientes al mismo bloque o agrupación de componentes de la misma naturaleza, el equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer tanto de las **Acciones Correctivas** de incumplimientos como aquellas **Acciones de Mejora o Recomendaciones** orientadas a aumentar el nivel de madurez de los controles conformes a la normativa, con el consecuente aumento de la seguridad. Estas acciones deberán tener el suficiente nivel de detalle con el objetivo de concretar y precisar a los responsables de los componentes las acciones a llevar a cabo.

Las acciones se agruparán, en función de su dimensión y ámbito de aplicación, en un plan de acción con proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - ✓ Componentes, normativa y controles afectados.
 - ✓ 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.

B.2 Auditorías de Aplicaciones

Los Sistemas de Información (aplicaciones) objeto de este servicio de auditoría deberán ser revisados según las normativas de seguridad (una o varias) de su ámbito de aplicación, descritas en la declaración de aplicabilidad 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 que no hayan sido evaluados en la revisión de controles de los componentes comunes y que corresponderán con controles asociados fundamentalmente a la funcionalidad, desarrollo, implementación e instalación en Madrid Digital, agrupados bajo la denominación de componente aplicación.

Madrid Digital proporcionará al adjudicatario una guía de auditoría con la relación de controles considerados auditables en el contexto propuesto. Esta relación deberá ser revisada por el equipo auditor y en su caso proponer las modificaciones que consideren necesarias para alcanzar el objetivo propuesto.

Las auditorías de sistemas de Información se ejecutaran a continuación de la auditoría de componentes.

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

Fase 1: Preparación y planificación de las auditorías

El objeto de esta Fase es establecer las bases de trabajo para la realización de las auditorías.

En particular dentro de esta fase se incluye:

- Revisar y analizar la documentación actual de relación de controles auditables en un Sistema de Información, y hacer una revisión de la guía de auditoría de sistemas de Información, con los objetivos de control y el detalle de las pruebas, comprobaciones y evidencias previstas para la verificación de su cumplimiento, previendo que la implantación de determinados controles vendrá determinada por la utilización de un framework de desarrollo objeto de análisis y revisión en el siguiente apartado.
- Analizar los frameworks de desarrollo en que se basa la construcción de gran número de aplicaciones en Madrid Digital, de tal forma que los controles cuya implantación sea responsabilidad del framework, se les valore con un determinado nivel de madurez común y extensible a todos los sistemas de información que lo utilizan. Se deberán analizar, al menos, los controles implementados en los frameworks de desarrollo de las siguientes tecnologías:
 - Java (framework Atlas, FW2 y Justicia)
 - Oracle Forms (versiones 4.5, 6 y 10).
 - MOVA (Framework de desarrollo de tecnologías móviles)
 - Joomla y Drupal
 - Delphi, php.

Se tomará como punto de partida la documentación de arquitectura de los diferentes frameworks y el resultado de las auditorías realizadas sobre los mismos.

Fruto de este análisis, se podrá determinar que es necesario mantener reuniones y entrevistas con los responsables de arquitectura para adecuar la valoración del nivel de madurez de los controles a la situación del momento.

Los resultados de la revisión deberán ser documentados por la empresa adjudicataria y trasladados a la guía de auditoría de Sistemas de Información.

- Elaborar el Plan de auditoría anual con la relación de sistemas de información auditables.
- Elaborar el programa de auditoría con la 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.
- Determinar los sistemas de Información objeto de auditoría y elaborar el plan de auditoría para cada uno de ellos, identificando a los responsables, interlocutores, tecnologías, componentes comunes asignados y toda la información necesaria para la auditoría, con especificación de los controles a auditar, objetivos de control y el detalle de las pruebas, comprobaciones y evidencias previstas para la verificación de su cumplimiento.

La empresa adjudicataria deberá proponer, diseñar, elaborar y desarrollar un modelo de gestión de evidencias de Sistemas de Información, ya sea basado en el modelo de evidencias de componentes o en un nuevo modelo, que facilite su gestión y un acceso ágil, eficiente y relacional.

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

Durante esta fase se realizarán las entrevistas, reuniones y en general las acciones necesarias para evaluar el grado de adecuación de las medidas y controles objeto de auditoría en relación con las exigencias de las distintas normativas aplicables a cada Sistema de Información.

Cada convocatoria de reunión deberá ser planificada con antelación e ir acompañada de una **agenda** con los temas a tratar junto con la documentación necesaria y la descripción de los objetivos y alcance de la reunión, y a su finalización el equipo auditor deberá elaborar un **acta** para reflejar los acuerdos alcanzados así como la petición de información y evidencias a los responsables.

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

El equipo de trabajo elaborará un informe individual por cada Sistema de Información auditado donde se recojan los resultados de las revisiones efectuadas respecto al grado de adecuación de las medidas y controles de las normativas aplicables.



Dicho informe deberá dictaminar sobre los niveles de madurez de las medidas de seguridad auditadas, según la metodología propuesta, y recogerá indicadores de madurez y cumplimiento.

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

El equipo auditor estará a disposición de los responsables de cada uno de los Sistemas de Información para atender alegaciones y aclarar aspectos que consideren necesarios para un mayor entendimiento de los resultados obtenidos.

Fase 4 – Evidencias.

Las evidencias recopiladas a lo largo de la auditoría de Sistemas de Información deberán ser entregadas a Madrid Digital de manera organizada y normalizada, de forma que permita relacionar los controles o medidas de seguridad con sus respectivas evidencias, e incorporadas al modelo de gestión de evidencias de Sistemas de Información.

Fase 5 – Elaboración del Plan de Acción

A la conclusión de las auditorías de los Sistemas de Información pertenecientes al mismo ámbito de negocio, y en un plazo no superior a 30 días, el equipo de trabajo elaborará un documento con el Plan de Acción en el que se desarrollará las actuaciones que se precisan acometer tanto de las **Acciones Correctivas** de incumplimientos como aquellas **Acciones de Mejora o Recomendaciones** orientadas a aumentar el nivel de madurez de los controles conformes a la normativa, con el consecuente aumento de la seguridad. Estas acciones deberán tener el suficiente nivel de detalle con el objetivo de concretar y precisar a los responsables de los componentes las acciones a llevar a cabo.

Las acciones se agruparán, en función de su dimensión y ámbito de aplicación, en un plan de acción con proyectos concretos. Para cada uno de ellos se especificará:

- Descripción del Proyecto, que incluirá como mínimo:
 - ✓ Componentes, normativa y controles afectados.
 - ✓ 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.

B.3 Informes generales por normativa de seguridad

A la finalización de las auditorías de componentes comunes y Sistemas de Información, la empresa adjudicataria deberá elaborar un informe de auditoría por cada una de las normativas de seguridad indicadas a continuación.

Los informes generales de normativa deberán determinar el valor promedio de la madurez de cada uno de los controles que la componen, todo ello basado en los resultados obtenidos en las auditorías, contemplando los componentes y sistemas de información donde aplica la normativa y sus resultados de auditoría, y describiendo la metodología utilizada para determinar el resultado de los niveles de madurez.

- Informe general de auditoría del **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad**, considerando todos aquellos datos necesarios para realizar el **informe del Estado de la Seguridad** de Madrid Digital a través de la herramienta **INES del Centro Criptológico Nacional**, en cumplimiento de la Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la **Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad**, y las guías de Seguridad CCN-STIC relacionadas con la elaboración de dicho informe, y teniendo en consideración los aspectos descritos en la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la **Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información**.
- Informe general de auditoría de la **Norma ISO-IEC-27002** para 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.
- Informe general de auditoría de **Gestión Procesal**, referentes 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 Sistemas de Información al servicio de la Administración de Justicia.



B.4 Contenido de los informes de auditoría

Los informes de auditoría deberán dictaminar sobre la adecuación de las medidas y controles de seguridad implantados, proporcionando al menos la siguiente información:

- Datos referentes a la empresa y equipo auditor participante, junto con la validación y firma de aprobación por parte del auditor jefe.
- Participantes en la auditoría
- Fecha de emisión del informe junto con un control de cambios para la gestión de la entrega de diferentes versiones del documento.
- Datos propios de la auditoría realizada, tales como **objetivo** y **alcance** de la auditoría, **metodología** empleada, normativa y medidas de seguridad aplicables, **criterios** de auditoría, **hechos observados y hallazgos**, **evidencias**, **nivel de madurez**, **conclusiones y recomendaciones correctoras o de mejora**, así como toda aquella información que permita una mayor comprensión del proceso de auditoría.
- El informe de auditoría deberá incluir un resumen ejecutivo que incluya el índice madurez total e índice de cumplimiento respecto a un determinado nivel de seguridad, para cada una de las normativas de seguridad aplicables, en consonancia con la metodología propuesta por el Centro Criptológico Nacional en sus guías de referencia.
- La empresa adjudicataria deberá proporcionar a Madrid Digital ficheros de carga en el formato acordado (excel, csv o similar), que permitan cargar de manera automática el resultado de los informes de auditoría en la herramienta corporativa de Madrid Digital, SENS. En caso contrario, la carga de la información de las auditorías deberá ser realizada de forma manual por la empresa adjudicataria.

Durante las fases de preparación y planificación de las auditorías, el adjudicatario deberá presentar un modelo o plantilla de informe de auditoría y, si así lo requiere Madrid Digital, planificar una auditoría piloto de un determinado componente y Sistema de Información, y tras la entrega de su informe, valorar la idoneidad del entregable y realizar los ajustes necesarios.

4.1.3 C: Gestión de Riesgos, soporte a la certificación y ciclo de mejora de la seguridad

Las actividades de este servicio serán gestionado de forma continua por la empresa adjudicataria a lo largo del tiempo de duración del contrato, debiendo realizar, entre otras, las siguientes tareas y actividades:

- Estudio y revisión documental previa de la metodología y de los procesos de auditoría y gestión de riesgos de Madrid Digital. Entendimiento de la actividad y competencias de Madrid Digital, procesos, estructura, activos y funcionamiento.
- Análisis de la situación actual y elaboración de las guías de auditoría de los sistemas de información (componentes comunes y aplicaciones):
 - Análisis y revisión de las declaraciones de aplicabilidad y matriz de relaciones componentes-medidas de seguridad

- Guías de auditoría detallando los criterios de evaluación, controles, objetivos de control, y evidencias necesarias.
- Definición y diseño del modelo de informe de auditoría y documentación entregable a Madrid Digital: Elaboración del modelo y plantilla del informe de auditoría de sistemas de información y resto de entregables.
- Gestión documental referente a los procesos de auditoría y gestión de riesgos de la documentación generada durante el desarrollo de los trabajos del Lote 1 del presente pliego.
- Soporte y asistencia, en coordinación y colaboración con la Oficina del Gobierno de la seguridad (OGS) de Madrid Digital, en la realización de los análisis de riesgos de sistemas de información y la elaboración de los documentos de declaración de aplicabilidad según la metodología existente.
- Mantener actualizados los sistemas de gestión de auditoría y riesgos (incluido dentro de la aplicación SENS) y del sistema de gestión del Reglamento General de Protección de Datos. 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.
- Identificar indicadores y métricas de seguridad asociados a los procesos de auditoría y gestión de riesgos, que permitan medir el cumplimiento, el riesgo y por tanto el estado de la seguridad en Madrid Digital, y alineados entre otras, con las métricas propuestas por el Centro Criptológico Nacional. Además, se deberá proponer una metodología y trasladar los resultados de los trabajos realizados a los indicadores requeridos en la herramienta INES del Centro Criptológico Nacional, en referencia al informe anual del estado de la seguridad de Madrid Digital.
- A petición de Madrid Digital, elaborar informes y presentaciones de cumplimiento, riesgos y estado de la seguridad tanto a nivel de Dirección como a cada una de sus unidades organizativas, como resultado de las auditorías y análisis de riesgos de cumplimiento realizados, y basados en los indicadores y métricas de seguridad definidas y utilizados.
- Proponer, modelizar y desarrollar procesos y/o herramientas que permitan la recogida de información de las aplicaciones corporativas de Madrid Digital y automaticen la generación de informes del estado de cumplimiento de seguridad en Madrid digital basados en los indicadores y métricas definidas.
- Elaborar presentaciones y recomendaciones sobre el resultado de los diferentes servicios del Lote 1 y proporcionar el soporte necesario tras su finalización.
- Dar soporte y asistencia a las pre-auditorías de certificación y a las certificaciones del servicio de certificación de conformidad con el Esquema Nacional de Seguridad e ISO



27001 del Lote 2, atendiendo las peticiones de información y documentación, y obteniendo las evidencias requeridas. Elaborar los planes de mejora y de acciones correctoras derivados de las no conformidades del servicio de Certificación de Conformidad con el ENS, alineándolos con los planes de acción derivados de las auditorías de sistemas de información realizadas.

- Cuando Madrid Digital así lo requiera, el adjudicatario deberá realizar revisiones incrementales para verificar el nuevo nivel de madurez de los controles sobre los cuales Madrid Digital ha realizado mejoras o solventado deficiencias como resultado de las auditorías y la ejecución de los planes de acción. Como resultado de estas revisiones incrementales, deberá elaborar la documentación anexa que refleje el resultado, y actualizar en los sistemas Corporativos de Madrid Digital.

4.2 LOTE 2: Servicio de Certificación de Conformidad con el Esquema Nacional de Seguridad e ISO 27001

SERVICIOS DE CUOTA VARIABLE

Debido al alto grado de similitud entre el Esquema Nacional de Seguridad y la norma ISO 27001, este servicio tendrá la capacidad para evaluar de manera conjunta y concurrente:

- El cumplimiento del Esquema Nacional de Seguridad de Sistemas de Información (componentes comunes incluidos) bajo el ámbito de responsabilidad de Madrid Digital, y su prestador deberá disponer de la acreditación necesaria para expedir las **Certificaciones de Conformidad con el Esquema Nacional de Seguridad**, en los términos establecidos en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la **Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad**, así como las guías CCN-STIC de referencia en la materia.
- El cumplimiento de la norma ISO 27001 en materia de seguridad de la información de Madrid Digital.

La empresa adjudicataria deberá proponer la metodología de trabajo, criterios y medidas de seguridad a verificar según el esquema de acreditación para la expedición de la certificación de conformidad. Previo al inicio de cada certificación del ENS e ISO 27001, Madrid Digital proporcionará la categoría del sistema en los términos establecidos en el Esquema Nacional de Seguridad.

Previo al inicio de las certificaciones propuestas por Madrid Digital, se requerirá a la empresa adjudicataria la ejecución de gap análisis y pre-auditorías que permitan conocer con carácter previo, las brechas existentes entre Madrid Digital y los requisitos mínimos e imprescindibles para afrontar el proceso de certificación de conformidad, y poder establecer las líneas de actuación necesarias para el inicio de la certificación de conformidad.

Los sistemas sometidos al proceso de certificación de conformidad con el ENS e ISO 27001 podrán ser de diferente naturaleza y condición:

- Componentes comunes, agrupados por su naturaleza y servicio prestado, tales como:
 - Organización de la Seguridad
 - Procesos horizontales (Certificación del software, Paso a Producción, Gestión de incidentes...)
 - Centro de Procesamiento de Datos (CPD)
 - Tecnología y Software Base (Sistemas operativos, Bases de Datos, Servidores web, Servidores de aplicaciones, Gestores de Contenidos...)
 - Servicios Comunes de Tramitación Electrónica.
- Sistemas de Información desarrollados a medida en Madrid Digital en diferentes lenguajes y tecnologías (java, forms, Delphi, php, drupal, joomla, SAP...).
- Instalaciones o implantaciones en las infraestructuras de Madrid Digital de software o productos de terceros, ya sean del ámbito privado o de otras administraciones públicas, en cuyo caso se requerirá la existencia del Certificado de Conformidad proporcionado por el sistema instalado en Madrid Digital.

En el caso que el sistema a verificar disponga de una auditoría o revisión de seguridad realizada previamente, Madrid Digital pondrá a disposición de la empresa adjudicataria toda la documentación existente (informes, hallazgos, evidencias...) con el objetivo de minimizar los tiempos de la certificación y recopilación de evidencias.

La volumetría del servicio de certificación de conformidad con el ENS e ISO 27001 será el previsto en las cláusulas correspondientes del presente pliego, y su ejecución se prevé dentro de los últimos 16 meses de duración del contrato, salvo el gap análisis y pre-auditorías, cuyo alcance, valoración y ejecución podrán ser solicitados desde el inicio del contrato, con el objetivo de identificar y acometer con tiempo las líneas de actuación previas al inicio de las certificaciones. La empresa adjudicataria deberá poner en marcha cada uno de los trabajos y las certificaciones de conformidad propuestas por Madrid Digital en el plazo máximo de 10 días naturales desde la aceptación por parte de Madrid Digital del inicio de una Certificación de Conformidad, dentro del plazo de ejecución del Lote 2.

Las tareas más significativas a realizar en una certificación serán, entre otras:

- Definición del alcance de la certificación de conformidad
- Revisión documental
- Reuniones de auditoría
- Elaboración de la documentación post-auditoría (actas, solicitud de evidencias, etc...)
- Elaboración de informes de auditoría
- Presentación de resultados a las áreas involucradas y a la Dirección de Madrid Digital.

Cada convocatoria de reunión deberá ser planificada con antelación e ir acompañada de una **agenda** con los temas a tratar junto con la documentación necesaria y la descripción de los objetivos y alcance de la reunión, y a su finalización el equipo auditor deberá elaborar un **acta**

para reflejar los acuerdos alcanzados así como la petición de información y evidencias a los responsables.

4.2.1 Entregables del Servicio de Certificación de conformidad con el ENS e ISO 27001

Tras la verificación realizada, el servicio de Certificación de Conformidad hará entrega a Madrid Digital del correspondiente **Informe de auditoría** del sistema evaluado, dictaminando sobre el grado de cumplimiento de la norma ISO 27001 con las garantías y cumpliendo lo establecido en la citada normativa y el grado de cumplimiento con el ENS, con las garantías metodológicas requeridas y cumpliendo con lo establecido en la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública por la que se aprueba la Instrucción Técnica de Seguridad (ITS) denominada "Auditoría de la Seguridad de los Sistemas de Información", así como cumplir con lo establecido en las guías CCN-STIC de referencia en la materia.

Cuando el resultado de la auditoría sea favorable:

- Se expedirá la correspondiente Certificación de Conformidad con el Esquema Nacional de Seguridad en los términos establecidos en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Se expedirá el correspondiente certificado de conformidad con la norma ISO 27001.

En caso que el dictamen de la auditoría indique la existencia de no conformidades, en el informe de auditoría debe reflejarse de manera clara, precisa y concreta los hallazgos de no conformidad evidenciados, con el objetivo de elaborar el Plan de Acciones Correctivas que permita solventar los hallazgos de no conformidades evidenciadas y someter al sistema a una nueva revisión una vez hayan sido solventados.

A la finalización de las auditorías, se deberá entregar un informe ejecutivo y realizar su presentación a la Dirección de Madrid Digital.

4.2.2 Auditorías extraordinarias sobre no conformidades

El Servicio de Certificación de Conformidad con el ENS e ISO 27001 tendrá la obligación de realizar en los sistemas en los que no haya sido posible expedir la Certificación de Conformidad debido a un dictamen desfavorable, al menos una **nueva revisión exclusivamente sobre los hallazgos de no conformidad**, una vez Madrid Digital considere que se han producido las correcciones y se dan las circunstancias adecuadas para cambiar el dictamen a favorable.



CLÁUSULA 5.- VOLUMETRÍA

5.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad

SERVICIOS DE CUOTA VARIABLE

5.1.1.1 A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales y Revisiones Técnicas

Se destinarán a los trabajos relacionados con servicios de cuota variable el siguiente volumen de horas de trabajo:

- 300 horas de Auditor Senior
- 700 horas de auditor de seguridad
- 660 horas de arquitecto de sistemas

Por otra parte, se valorará la aportación de horas adicionales del perfil de auditor de seguridad y de arquitecto de sistemas conforme a los criterios de valoración establecidos por Madrid Digital para el presente pliego.

Se realizarán los servicios de cuota variable que en cada caso se estimen necesarios por parte de Madrid Digital, abonándose, por tanto, al contratista únicamente las que efectivamente se lleven a cabo, y con las siguientes características:

5.1.1.2 A1: Auditorías de los procedimientos e instrucciones vigentes de protección de datos personales

Los trabajos relacionados con las auditorías de procedimientos e instrucciones vigentes de protección de datos personales de Madrid Digital para este servicio se realizarán con un porcentaje de las horas correspondientes a los perfiles auditor senior y auditor de seguridad, según el alcance acordado entre el licitador y Madrid Digital en la fase de definición del alcance del servicio.

Para la elaboración de la propuesta se deben tener en cuenta las siguientes consideraciones:

- Se deben considerar la totalidad de las actividades de tratamiento de Madrid Digital indicadas en el RAT, con la agrupación que se considere necesaria por similitud entre actividades, y además del informe como **responsable del tratamiento**, se debe realizar un informe de auditoría específico de verificación de sus obligaciones como **encargado del tratamiento** de Centros Directivos de la Comunidad de Madrid.

Se encuentra disponible en el Registro de Actividades de Tratamiento (RAT) del portal de la Comunidad de Madrid (<http://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos>), las Actividades de Tratamiento existentes en Madrid Digital.



5.1.1.3 A2: Revisiones Técnicas

Las revisiones técnicas se realizarán con horas correspondientes a los perfiles profesionales auditor senior, auditor de seguridad (del porcentaje restante del servicio A1) y al perfil profesional correspondiente a arquitecto de sistemas.

Se ejecutaran las revisiones técnicas que en cada caso se estimen necesarias por parte de Madrid Digital, a realizar durante la ejecución del contrato, abonándose, por tanto, al contratista únicamente las que efectivamente se lleven a cabo con la estimación de horas que se realice en cada revisión.

SERVICIOS DE CUOTA FIJA

5.1.2 B: Auditorías de seguridad de Sistemas de Información

Se han establecido la siguiente volumetría de componentes y aplicaciones objeto de auditoría para el presente contrato, indicando aquellos que ya han sido objeto de una auditoría anterior:

ELEMENTO A AUDITAR	Nº DE ELEMENTOS A AUDITAR	AUDITADOS PREVIAMENTE
Componentes comunes/ Activos operacionales	45	45

ELEMENTO A AUDITAR	Nº DE ELEMENTOS A AUDITAR	AUDITADOS PREVIAMENTE
Aplicaciones de Organismo Pagador	Entre 5 y 10 (*)	5
Aplicaciones de Gestión Procesal	Entre 20 y 25 (*)	19
Resto de Aplicaciones (desarrollados con framework corporativos y otras tecnologías como por ejemplo SAP o productos comerciales)	100	Inicialmente, no se contempla que las aplicaciones de este apartado dispongan de auditoría previa.
TOTAL Aplicaciones	135	24

(*) En caso de no alcanzar el número máximo previsto, el número de aplicaciones restantes se contabilizará en el apartado "Resto de Aplicaciones", hasta alcanzar el número total de aplicaciones.

El responsable del contrato de Madrid Digital, por razones internas de disponibilidad de medios y recursos, podrá reducir el número de aplicaciones objeto de auditoría si no se pudieran atender de manera eficiente los inicialmente previstos.

Además, previo a la auditoría de aplicaciones, se auditarán los frameworks o kits de desarrollo más relevantes de Madrid Digital:

Con al menos una auditoría realizada:

- Java (framework Atlas, FW2 y Justicia)
- Oracle Forms (versiones 4.5, 6 y 10).

Sin auditoría realizada:

- MOVA (Framework de desarrollo de tecnologías móviles)
- Joomla y Drupal
- Delphi, php, SAP, etc...

5.1.3 C: Gestión de Riesgos, soporte a la Certificación y ciclo de mejora de la seguridad

Se establece como servicio continuo a lo largo de 22 meses, con inicio en el tercer mes del contrato y hasta el fin del mismo, con el alcance y descripción de los trabajos indicado en el presente pliego, y devengando en cada uno de los meses de trabajo una cantidad económica determinada, según se indica en el modelo económico del presente pliego.

5.2 **LOTE 2: Servicio de certificación de conformidad con el esquema nacional de seguridad e ISO 27001**

SERVICIOS DE CUOTA VARIABLE

5.2.1 **A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001**

Se realizarán los gap análisis, pre-auditorías y certificaciones de conformidad con el ENS y de la *ISO 27001* de sistemas que en cada caso estimen necesarias Madrid Digital, hasta alcanzar **un máximo de 1084 horas en total**. Inicialmente, se estima que las certificaciones de conformidad se ejecuten durante los últimos 16 meses de contrato, no así los gap análisis y pre-auditorías, que podrán contemplarse desde el inicio del contrato a petición de Madrid Digital.

Madrid Digital propondrá el inicio de los trabajos al adjudicatario según los términos que a continuación se indican.

- Madrid Digital requerirá a la empresa adjudicataria el inicio de los gap análisis, pre-auditorías y de las Certificaciones de Conformidad que estime necesaria, y tras acordar de manera conjunta el alcance propuesto, el adjudicatario deberá entregar la valoración de las jornadas de trabajo previstas en un plazo no superior a 5 días hábiles. Madrid Digital deberá formalizar la aceptación de los trabajos, y en un plazo no superior a 10 días hábiles de la aceptación, el adjudicatario deberá estar en disposición de iniciar la certificación.

- En el caso que la realización de la auditoría de certificación supere o requiera mayor número de horas que el previsto en la valoración aceptada por Madrid Digital, el exceso de horas será asumido por parte de la empresa adjudicataria.

CLÁUSULA 6.- PLAZOS DE EJECUCIÓN

El plazo de ejecución del contrato será de VEINTICUATRO MESES, y según los siguientes plazos parciales:

6.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad

SERVICIOS DE CUOTA VARIABLE

6.1.1 A1: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales:

Se estima un plazo máximo de ejecución de 3 meses a realizar durante el año 2022.

6.1.2 A2: Revisiones Técnicas

Se realizarán las revisiones técnicas que en cada caso se estimen necesarias por parte de Madrid Digital, y a lo largo del tiempo de ejecución del contrato (24 meses).

SERVICIOS DE CUOTA FIJA

6.1.3 B: Auditorías de seguridad de Sistemas de Información

El plazo de ejecución de las auditorías de componentes comunes (servicio B1) se estima entre 6 y 8 meses a realizar durante los años 2021 y 2022.

Tras la finalización de la auditoría de componentes, el plazo de ejecución de las auditorías de las aplicaciones (servicio B2) y la elaboración de los informes generales de cada una de las normativas de seguridad (servicio B3) se realizará durante un tiempo estimado de entre 10 y 12 meses, a realizar durante los años 2022 y 2023.

6.1.4 C: Servicio de Gestión de Riesgos, soporte a la certificación y ciclo de mejora de la seguridad

El plazo de ejecución de este servicio continuo será desde el tercer mes de contrato hasta su finalización, 22 meses en total. Se deberá tener en cuenta lo expuesto en la cláusula "Equipo prestador del servicio".

6.2 LOTE 2: Servicios de certificación de conformidad con el esquema nacional de seguridad e ISO 27001.

SERVICIOS DE CUOTA VARIABLE



6.2.1 A: Servicio de Certificaciones de Conformidad con el Esquema Nacional de Seguridad e ISO 27001

Se realizarán las pre-auditorías y certificaciones de conformidad con el ENS de los componentes o sistemas que en cada caso estimen necesarias Madrid Digital, hasta alcanzar **un máximo de 1084 horas en total**, a ejecutar a lo largo de los 24 meses de contrato.

Madrid Digital requerirá a la empresa adjudicataria el inicio de la Certificación de Conformidad con el ENS e *ISO 27001* que estime necesaria, y tras acordar de manera conjunta el alcance propuesto, el adjudicatario deberá entregar la valoración de las jornadas de trabajo previstas. Madrid digital deberá formalizar la aceptación de los trabajos, y en un plazo no superior a 10 días de la aceptación, el adjudicatario deberá estar en disposición de iniciar la certificación.

En el caso que la realización de la auditoría de certificación supere o requiera mayor número de horas que el previsto en la valoración aceptada por Madrid Digital, el exceso de horas será asumido por parte de la empresa adjudicataria.

CLÁUSULA 7.- EQUIPO PRESTADOR DEL SERVICIO

7.1 LOTE 1: Servicios de auditoría y gestión de riesgos en materia de seguridad

Para la ejecución de los trabajos del Lote 1, el adjudicatario pondrá a disposición de Madrid Digital un equipo mínimo que garantice el nivel de conocimiento requerido para cada uno de los servicios.

El adjudicatario garantizará en todo momento la permanencia y transferencia del conocimiento a lo largo de la duración del contrato, tanto del conocimiento transferido inicialmente por la Agencia, como del propio adquirido por el equipo de trabajo durante la prestación de los servicios.

Equipo de trabajo mínimo para la ejecución del Lote 1:

- 1 Auditor Senior de Seguridad
- 2 Auditores de seguridad
- 1 Arquitecto de Sistemas, cuyo perfil deberá variar dependiendo de la materia objeto de las auditorías y revisiones técnicas.

Todo el equipo de trabajo deberá ser partícipe del análisis y revisión de la documentación proporcionada por Madrid Digital así como del proceso de elaboración de los entregables requeridos, y en cada caso, asistencia y soporte a las entrevistas y reuniones de auditorías en su ámbito de responsabilidad en el equipo, además de prestar el apoyo y soporte necesario al equipo del servicio de certificación con el Esquema Nacional de Seguridad.

El **auditor Senior** de Seguridad tendrá, entre otras, las siguientes funciones y obligaciones:

- Representante e interlocutor principal del equipo auditor ante Madrid Digital de todos los servicios del Lote 1.

- Planificación de actividades. Organización, dirección y coordinación del equipo auditor de todos los servicios del Lote 1.
- Coordinación, planificación e interlocución de todas las sesiones de auditoría con los responsables e interlocutores asignados.

Deberá ser el responsable del equipo auditor y Jefe del Proyecto, siendo parte activa en la gestión, coordinación, ejecución y seguimiento del contrato, y por defecto, será obligatoria su presencia:

- En todas las reuniones y entrevistas de auditoría que se produzcan en el ámbito de los servicios correspondientes al Lote 1, salvo en las reuniones y entrevistas donde Madrid Digital indique de manera expresa que no considera necesario su asistencia
- En las reuniones de seguimiento requeridas por Madrid Digital, excepto en aquellos casos que coincidan con otras reuniones o entrevistas de auditoría objeto del contrato y que previamente se hayan acordado con Madrid Digital.

La ausencia del auditor senior en las reuniones y entrevistas donde es obligada su presencia, hará que las sesiones sean canceladas, procediendo a la penalización prevista en el apartado correspondiente del presente pliego.

- Elaboración de informes y documentos entregables. Será el responsable último de todas las fases del proyecto y de la documentación entregable correspondiente a todos los servicios del Lote 1. Deberá figurar como responsable en todos los informes de auditoría y resto de entregables, sin menoscabo de cualquier otra firma por parte de los representantes oportunos del adjudicatario.
- Atender las posibles dudas o alegaciones de los interlocutores sobre los resultados de los análisis de riesgo y de las auditorías.
- Soporte al servicio de certificación de conformidad con el ENS.
- Asistencia e interlocución en las reuniones de seguimiento del contrato propuestas por Madrid Digital.

Los auditores de seguridad tendrán, entre otras, las siguientes funciones y obligaciones:

- Análisis y revisión de la documentación actual.
- Asistencia a reuniones y entrevistas de auditoría.
- Realización de los análisis de riesgos y elaboración de los documentos de declaración de aplicabilidad.
- Elaboración de documentos de trabajo (checklist, actas, agendas, informes, hallazgos, evidencias...) y entregables finales.
- Realización de revisiones técnicas, informes y presentaciones.
- Atender las posibles dudas o alegaciones de los interlocutores sobre los resultados de la auditoría.



- Soporte al servicio de certificación de conformidad con el ENS, atendiendo las solicitudes de información y documentación.

El arquitecto de Sistemas formará parte del equipo auditor, dando el soporte necesario a los aspectos más técnicos del ámbito de las auditorías, y deberá estar presente al menos en las reuniones de auditoría de los componentes tecnológicos y aquellas de aplicaciones donde se traten aspectos técnicos y de arquitectura.

Los arquitectos de Sistemas tendrán, entre otras, las siguientes funciones y obligaciones:

- Análisis y revisión de la documentación técnica proporcionada por Madrid Digital
- Asistencia a reuniones y entrevistas de auditoría de su ámbito de responsabilidad y conocimiento, dando el soporte técnico necesario al equipo auditor.
- Elaboración de informes de auditoría y revisiones técnicas.

SERVICIOS DE CUOTA VARIABLE

Servicio "A: Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales y Revisiones Técnicas"

Los trabajos relacionados con las auditorías de los procedimientos e instrucciones vigentes de protección de datos personales, se ejecutarán con el perfil de auditor senior y como mínimo de 1 auditor de seguridad durante todo su plazo de ejecución. El auditor senior deberá planificar, gestionar y coordinar el proceso de auditoría, siendo el responsable último de los trabajos realizados y entregados.

Para las revisiones técnicas, los trabajos se realizarán con la estimación de horas según la materia y necesidades de la revisión solicitada por Madrid Digital, si bien deberán ser planificados y coordinados por el auditor senior de seguridad responsable del Lote 1.

SERVICIOS DE CUOTA FIJA

Servicio "B: Auditorías de seguridad de Sistemas de Información".

Será obligatoria la presencia al menos del siguiente equipo de trabajo:

- 1 auditor senior seguridad con las funciones indicadas anteriormente.
- 2 auditores de seguridad, con las siguientes consideraciones:
 - Auditor de seguridad 1: Su dedicación será completa, y será obligatoria su disponibilidad en las instalaciones de Madrid Digital o en remoto, según determine en cada momento Madrid Digital, y hasta la emisión del último informe de auditoría y plan de acción.
 - Auditor de seguridad 2: Disponibilidad durante el tiempo de ejecución de las auditorías a tiempo parcial, pudiendo ser compatible y complementaria con la prestación del servicio "C. Gestión de Riesgos", con el objetivo de optimizar los

recursos del contrato y el reaprovechamiento del conocimiento adquirido y de los trabajos realizados.

- 1 arquitecto de sistemas con las funciones indicadas anteriormente, y cuyo perfil podrá variar según los conocimientos técnicos requeridos en cada auditoría.

Servicio "C. Gestión de Riesgos, soporte a la Certificación y ciclo de mejora de la seguridad".

Además de la gestión y coordinación por parte del auditor senior de seguridad, se asignará un auditor de seguridad durante todo el plazo de ejecución de este servicio. La **dedicación mínima** será la siguiente:

- **Desde el inicio de este servicio, en el tercer mes del contrato, durante los 4 meses siguientes (del tercer mes al sexto del contrato, ambos inclusive)**, con jornada de trabajo con horario de 9:30 a 14:00, donde será obligatoria su presencia en las instalaciones de Madrid Digital o en remoto, según determine Madrid Digital en cada caso. Su actividad será incompatible con la ejecución de los trabajos del servicio "A. auditoría de los procedimientos e instrucciones vigentes de protección de datos personales", si bien deberá estar integrado y colaborar con el equipo auditor para la planificación, coordinación y compartición de la información y el conocimiento necesario para la correcta ejecución de los servicios de auditoría posteriores.
- **Desde el séptimo mes de contrato, y durante los siguientes 15 meses**, la dedicación será de 5 jornadas al mes, con jornada de trabajo de 9:30 a 14:00, donde será obligada su presencia en las instalaciones de Madrid Digital o en remoto, según determine Madrid Digital en cada caso. Para optimizar los recursos del contrato en este periodo, este recurso podrá ser también el auditor de seguridad 2 del servicio "B: Auditorías de seguridad de Sistemas de Información", compatibilizando ambas funciones como se ha indicado en los puntos anteriores.
- **Los tres últimos meses de contrato**, jornada de trabajo con horario de 9:30 a 14:00, donde será obligatoria su presencia en las instalaciones de Madrid Digital o en remoto, según determine Madrid Digital en cada caso.

Requisitos mínimos en cuanto al perfil profesional requerido para el personal prestador del servicio:

PERFIL	AUDITOR SENIOR
EXPERIENCIA	<p>Al menos 5 años de experiencia como auditor de tecnologías de la información, de los cuales mínimo tres años auditando el Esquema Nacional de Seguridad y 2 años auditando Protección de Datos Personales.</p> <p>Al menos de 4 años como responsable de equipos de trabajo de Seguridad de la Información y/o Ciberseguridad para organizaciones, públicas o privadas, de</p>

PERFIL	AUDITOR SENIOR
	<p>tamaño igual o superior a Madrid Digital y cuya actividad sea equivalente en naturaleza, volumen y alcance a la de la Agencia.</p> <p>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, Drupal, Unix, Windows.</p>
TITULACIÓN	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente
FORMACIÓN COMPLEMENTARIA	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.
OTROS	<p>Conocimientos de protección de datos (a nivel técnico y jurídico) y, en especial, del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.</p> <p>Conocimientos de Esquema Nacional de Seguridad y ISO 27002.</p>

PERFIL	AUDITOR DE SEGURIDAD
EXPERIENCIA	<p>Haber participado al menos 4 años como auditor de seguridad en proyectos de auditoría de tecnologías de la información, de los cuales mínimo 2 años auditando el Esquema Nacional de Seguridad y 1 año auditando Protección de Datos Personales.</p> <p>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, php, Joomla, Drupal, Unix, Windows.</p>
TITULACIÓN	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente
FORMACIÓN COMPLEMENTARIA	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.
OTROS	<p>Conocimientos de Esquema Nacional de Seguridad y ISO 27002.</p> <p>Conocimientos de protección de datos (a nivel técnico y jurídico) y, en especial, del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.</p>



PERFIL	ARQUITECTO DE SISTEMAS
EXPERIENCIA	Experiencia de al menos 4 años en proyectos de arquitectura de software, diseño y desarrollo de sistemas de información y/o en operación de infraestructuras y sistemas, con conocimiento en diversas tecnologías, lenguajes y bases de datos, con especial relevancia en las siguientes: java, Oracle, directorio Activo, LDAP, Oracle forms, Delphi, php, Joomla, Drupal, Unix, Windows, desarrollo de aplicaciones móviles, etc...
TITULACIÓN	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente
FORMACIÓN COMPLEMENTARIA	Se valorará disponer de alguna certificación de seguridad en sistemas, entornos web, bases de datos.
OTROS	Conocimientos de ISO 27002, Esquema Nacional de Seguridad

Al efecto, el licitador propuesto como adjudicatario en cada uno de los lotes, 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 I.

7.2 LOTE 2: Servicios de certificación de conformidad con el esquema nacional de seguridad e ISO 27001

SERVICIOS DE CUOTA VARIABLE

Para la ejecución de los trabajos del Lote 2, la empresa adjudicataria deberá ser una **entidad certificadora acreditada por la Entidad Nacional de Acreditación, ENAC, conforme a la norma UNE-EN ISO/IEC 17065:2012, para expedir certificaciones tanto del Esquema Nacional de Seguridad como de la norma ISO 27001.**

Además, pondrá a disposición de Madrid Digital un equipo auditor formado por personal propio de la entidad de certificación y con experiencia previa en certificaciones de conformidad en el Esquema Nacional de Seguridad y en norma ISO 27001 en organismos públicos o privados. El equipo auditor deberá estar compuesto al menos por un auditor senior con las siguientes funciones:

- Representante e interlocutor principal del equipo auditor ante Madrid Digital de los trabajos del Lote 2.
- Planificación de actividades. Organización, dirección y coordinación del equipo auditor del Lote 2.
- Coordinación, planificación e interlocución de todas las sesiones de auditoría con los responsables e interlocutores asignados.

Requisitos mínimos en cuanto al perfil profesional requerido para el personal prestador del servicio:

PERFIL	AUDITOR SENIOR
EXPERIENCIA	8 años de experiencia como auditor de tecnologías de la información, de los cuales al menos 4 años realizando certificaciones de conformidad en ENS y/o ISO 27001, (y de esos 4 años, mínimo 2 años de ellos realizando certificaciones de ENS).
TITULACIÓN	Titulación Universitaria de Grado, Ingeniero, Licenciado o equivalente
FORMACIÓN COMPLEMENTARIA	Auditor con doble cualificación para la obtención de la certificación del Esquema Nacional de Seguridad y la norma ISO 27001. Al menos una de las certificaciones reconocidas en el ámbito de auditorías y gestión de la seguridad, como CISA 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.
OTROS	Conocimientos de Esquema Nacional de Seguridad e ISO 27001.

Al efecto, el licitador propuesto como adjudicatario en cada uno de los lotes, 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 I.

CLÁUSULA 8.- MODELO DE GESTIÓN

La prestación de los servicios solicitados en el presente pliego precisa de un estrecho seguimiento en su desarrollo por parte de Madrid Digital, con objeto de garantizar la correcta ejecución de los mismos, y el cumplimiento por tanto de los objetivos del proyecto.

El contratista designará un **Responsable del Servicio** que será el responsable máximo del contrato ante Madrid Digital.

Madrid Digital determinará la periodicidad, 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 como Responsable o Jefe de Equipo al auditor Jefe, que 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).

Se levantará **acta** de cada una de las reuniones de seguimiento mantenidas. El adjudicatario será responsable de la elaboración de las actas, y su paso a revisión por los asistentes en las cuarenta y ocho (48) horas siguientes de su finalización.

8.1 Condiciones generales de los recursos del adjudicatario

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 Prescripciones Técnicas se señalan.

8.1.1 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.

Los empleados del adjudicatario que ejecuten por cuenta de éste trabajos directamente relacionados con el objeto del presente contrato, utilizarán los medios de producción físicos y lógicos de que hayan sido provistos por su propia organización, entendiendo como tal ordenador portátil personal, teléfonos móviles, tablets, licencias software ofimático, ...etc.

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.

Madrid Digital podrá exigir la ampliación inmediata del número de estos efectivos si no resultaran suficientes para la realización de todas las tareas previstas para la prestación del servicio descrito en este documento.

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.

8.1.2 Condiciones de estabilidad del equipo de trabajo por parte de la empresa adjudicataria

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 ocasionales 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 requerirá un solapamiento de los recursos, sin coste adicional para la Agencia, durante un periodo mínimo de **diez días laborables**.

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

8.1.3 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. El adjudicatario se comprometerá a facilitar la incorporación de los profesionales requeridos en este plazo, desde la comunicación formal por parte de esta Agencia.

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.

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

CLÁUSULA 9.-	CONDICIONES ADICIONALES A CUMPLIR
---------------------	--

9.1 Disponibilidad de medios y verificación de la capacidad (Lote 1 y Lote 2)

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.

CLÁUSULA 10.- CONTENIDO DE LAS OFERTAS

En el presente apartado se describe la estructura y contenido a incluir dentro del sobre correspondiente a la oferta técnica. 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. **En la oferta técnica no se debe incluir información ni referencia alguna a los criterios cualitativos evaluables de forma automática por aplicación de fórmulas.**

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.

Resulta obligatorio, para facilitar la valoración de las ofertas, que la documentación presentada se ajuste a lo especificado en esta cláusula. Los licitadores podrán incluir documentación adicional en anexos si lo consideran necesario. Con carácter obligatorio, la propuesta deberá presentarse en soporte digital compatible con las herramientas instaladas en Madrid Digital.

Dentro de ésta propuesta técnica no se deberá incluir ninguna información sobre precios, la cual deberá entregarse exclusivamente en el sobre correspondiente, según se especifica en el pliego de cláusulas administrativas.

10.1 Contenido de las ofertas para el lote 1

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, con una visión integral de los diferentes servicios de auditoría propuestos.

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos.

NOTA: En la oferta técnica no se debe incluir información referente a ningún criterio cualitativo evaluable de forma automática por aplicación de fórmulas.

10.1.1 Planificación y planteamiento integral del proyecto

- Planificación detallada e integral del proyecto, con especificación de fases, tareas y actividades asociadas.



10.1.2 Metodología y alcance de los servicios

- Descripción detallada del alcance, metodología de trabajo y actividades para desarrollar las tareas objeto de cada uno de los servicios de auditoría propuestos:

- Servicios de Cuota variable:
 - Auditoría de los procedimientos e instrucciones vigentes de protección de datos personales.
 - Revisiones Técnicas.
- Servicio B: Auditoría de Sistemas de Información (componentes y aplicaciones)
- Servicio C: Gestión de Riesgos, soporte a la certificación y ciclo de mejora continua, y en especial las actividades correspondientes a análisis de riesgos y la elaboración del documento de declaración de aplicabilidad.

- Descripción de la documentación y de los entregables mínimos comprometidos para cada una de las líneas de servicio definidas, con especial atención y relevancia a los modelos de documentación propuestos de todos los servicios.

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.

10.1.3 Organización de los equipos de trabajo propuestos

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

- Composición, organización y dedicación del equipo de trabajo propuesto, para cada uno de los trabajos planificados 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, y los perfiles profesionales, rol y las horas de dedicación de cada recurso en cada uno de los servicios y, más específicamente y cuando proceda, en cada fase.

- 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.

10.1.4 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.

10.2 Contenido de las ofertas para el lote 2

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, con una visión integral de los diferentes servicios de auditoría propuestos.

La oferta técnica a presentar por cada licitador deberá ajustarse al siguiente orden de exposición y contenidos.

NOTA: En la oferta técnica no se debe incluir información referente a ningún criterio cualitativo evaluable de forma automática por aplicación de fórmulas.

10.2.1 Metodología y alcance del proyecto

- Descripción detallada del alcance, metodología de trabajo y actividades para desarrollar las tareas objeto del servicio propuesto:

- Gap análisis y pre-auditorías para conocer con carácter previo, las brechas existentes entre Madrid Digital y los requisitos mínimos e imprescindibles para afrontar el proceso de certificación de conformidad.
- Auditorías de certificación de ISO 27001 y Esquema Nacional de Seguridad de manera conjunta y concurrente.

- Descripción de la documentación y de los entregables comprometidos para cada una de las actividades, con especial atención y relevancia a los modelos de documentación propuestos.

10.2.2 Organización de los equipos de trabajo propuestos

Propuesta y descripción de la estructura de los equipos de trabajo acorde al alcance y servicios propuestos, especialmente en lo que se refiere a:

- Composición y organización del equipo de trabajo. Debe quedar claro el número total de recursos que van a estar involucrados en el proceso de auditoría, los roles y perfiles profesionales, así como los años de experiencia y las empresas y/o sector, ya sea del ámbito público o privado en los cuales se ha adquirido la experiencia requerida.
- Asegurar la estabilidad del equipo y su continuidad a lo largo de las diferentes certificaciones.
- 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.



10.2.3 Metodología de seguimiento y Control del Servicio

Descripción del modelo de seguimiento del servicio propuesto:

- Propuesta de seguimiento del servicio y entregables propuestos.
- 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.

CLÁUSULA 11.- DERECHOS SOBRE EL HARDWARE, SOFTWARE E INFRAESTRUCTURAS

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

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

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

CLÁUSULA 12.- CALIDAD DEL SERVICIO

Durante el periodo de ejecución del contrato, el adjudicatario propondrá las mejoras de calidad que estime oportunas, para optimizar la actividad desarrollada. No obstante, Madrid Digital podrá establecer acciones de aseguramiento de la calidad sobre las tareas realizadas y los productos obtenidos. A tal fin, Madrid Digital podrá incorporar los recursos que considere oportunos para garantizar la correcta puesta en marcha y prestación del servicio objeto del contrato.

CLÁUSULA 13.- CONSULTAS SOBRE EL PLIEGO DE PRESCRIPCIONES TÉCNICAS

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

Agencia para la Administración Digital de la Comunidad de Madrid

Dirección de Ciberseguridad, Protección de Datos y Privacidad

E-mail: SEGURIDAD_DE_LA_INFORMACION@madrid.org

Los licitadores deberán identificar, a un único responsable de la oferta, que será durante el periodo de licitación, el interlocutor único con Madrid Digital, para cualquier tipo de consulta o

aclaración sobre los términos expuestos en el presente pliego, no admitiéndose ninguna consulta o aclaración de persona distinta a la señalada.

Por su parte la Agencia se compromete a responder en los términos indicados en la Cláusula 10 del Pliego de Cláusulas Administrativas Particulares.

La Directora de Ciberseguridad, Protección de Datos y Privacidad

Fdo.: Esther Muñoz Fuentes



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **1018622254009916532820**

ANEXO I : MODELO DE CURRICULUM

MODELO DE CURRÍCULUM VITAE DEL EQUIPO PRESTADOR DEL SERVICIO (A aportar para cada miembro del equipo propuesto)

APELLIDOS:	
NOMBRE:	
CATEGORÍA PROFESIONAL:	
TTITULACIÓN / UNIVERSIDAD o CENTRO / HOMOLOGACIÓN (en caso de haberse obtenido la titulación fuera de España):	
FORMACIÓN:	
ACTIVIDAD PROFESIONAL (Especificando como mínimo: Empresa, duración del proyecto, descripción del mismo y actividades desarrolladas y cliente para el que se ejecuta):	

Las empresa propuesta como adjudicataria en cada uno de los lotes, **con carácter previo a la adjudicación**, deberá aportar este documento, debidamente cumplimentado y firmado por la persona que ostente la representación de la empresa, para cada uno de los miembros del equipo propuesto del Equipo, indicando el perfil al que se adscribe, así como toda aquella documentación que Madrid Digital estime necesaria para la acreditación de los datos contenidos en dichos currículos.

□ FIN DEL ANEXO I -