

SERVICIOS DE ASISTENCIA TÉCNICA PARA GOBIERNO DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

diciembre 2018



1. OBJETIVO

Metro de Madrid desea recabar soporte externo para el adecuado abordaje de un proyecto de gobierno de la Confidencialidad de la información que se maneja y trata en el seno de la Compañía. El objeto del presente documento es establecer las condiciones técnicas que regirán la prestación del citado servicio.

2. ALCANCE

2.1 ALCANCE DE LOS TRABAJOS

La información es un activo de vital importancia en cualquier empresa, y en el caso de Metro de Madrid, que además presta un servicio público esencial para los ciudadanos, la protección de la información es una tarea prioritaria en todos los ámbitos. Con este fin, Metro de Madrid se propone poner en marcha un proyecto dirigido al gobierno de la confidencialidad de la información, que analizaría el ciclo de vida de la información en todas sus fases:

- a) Creación / Recopilación de Datos
- b) Almacenamiento de Datos
- c) Uso de Datos
- d) Compartición de Datos
- e) Custodia y Expurgo

Los trabajos objeto del presente servicio se enfocarán en implementar una política de clasificación y tratamiento de la información, en la que se definan distintos niveles, cada uno de los cuales tendrá asociados procedimientos y exigencias concretas para cada una de las fases anteriores.

Por tanto, los trabajos objetos de la presente licitación, abarcan tres ámbitos distintos de acciones:

- **Ámbito Jurídico / Estratégico:** Entendiendo como tal una primera parte en la que los esfuerzos se dirigirán a establecer una clasificación (por niveles) que sea compatible con las referencias incluidas en el apartado 3.1 del presente documento.

Para cada uno de los niveles definidos se establecerán protocolos de actuación específicos, con indicaciones claras sobre qué tratamiento debe darse a la información de cada nivel, su etiquetado, acceso, almacenamiento, reproducción, distribución, destrucción, etc. También deberá definir, para cada uno de ellos, los roles y responsabilidades para el etiquetado, tratamiento, y las acciones disciplinarias derivadas del incumplimiento (ligado al Código Ético y régimen disciplinario de Metro de Madrid).

- **Ámbito de Negocio:** Metro de Madrid dispone de clasificaciones a alto nivel de la información atendiendo a iniciativas de adaptación a GDPR, implantación de un modelo de gobierno de la información, acciones de digitalización, etc.; pero que no responden específicamente a criterios de confidencialidad. Partiendo de estas clasificaciones, y tras la realización de aquellas entrevistas con personal clave de la compañía que sean necesarias, se realizará un inventario de tipologías de documentos y se definirán unos

criterios de asignación a los niveles de confidencialidad definidos, en función al menos de la tipología y el contenido de los documentos, que cubran toda la información manejada por la Compañía. Asimismo, se propondrá una organización funcional para soportar la política de clasificación y tratamiento de la información.

- **Ámbito Técnico:** Se propondrán, para cada nivel, controles a implementar para asegurar un tratamiento y custodia seguros de los documentos. Estos controles deben entenderse en sentido amplio, y siempre personalizados para cada uno de los niveles establecidos. Abarcarán desde medidas de seguridad física (archivo de papel bajo llave, control de accesos a los mismos, zonas de protección específica como servidores, CPD; análisis de la necesidad de “zonas reservadas” para el tratamiento de la información, etc.), medidas de seguridad lógica (establecimiento de servidores especiales para ciertos niveles, perfilado de usuarios, necesidad de disponer de herramientas informáticas específicas tipo DLP, etc.), medidas de tipo legal (NDA’s a firmar con terceros que deban acceder a la información), etc.

Las acciones definidas, en su conjunto, deberán además alinearse con las acciones que la compañía está dando en varios ámbitos diferentes:

- Proyecto de Gobierno del Dato
- Proyecto de Adecuación a nueva normativa GDPR
- Proyecto de Digitalización
- Proyecto de Ciberseguridad
- Proyecto Seguridad

El contratista será por tanto informado de los avances que se están haciendo en esos ámbitos para alinear las acciones llevadas a cabo en este proyecto con ellas.

2.2 HORARIOS Y LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio se desarrollará en las instalaciones de Metro de Madrid principalmente en la sede principal ubicada en la calle Cavanilles 58. Sin embargo, según las propias características del servicio, es previsible que las reuniones de trabajo se realicen en diferentes ubicaciones de la empresa.

El horario de trabajo habitual de Metro de Madrid es de 7:15 a 15:30 horas de lunes a viernes. El contratista podrá establecer su propio horario de trabajo; sin embargo, todas las actuaciones que requieran participación de personal de Metro de Madrid deberán ajustarse al horario indicado, salvo casos excepcionales que serán analizados individualmente.

3. Requerimientos Específicos

Los requerimientos específicos que a continuación se detallan recogen básicamente información relativa a las características y requisitos del proyecto, así como las tareas y actividades mínimas a desarrollar.

3.1 MARCO DE REFERENCIA

Para la definición de los niveles de confidencialidad de la información, así como para la identificación de controles y procedimientos, se estará a lo dispuesto al menos en la siguiente normativa:

- 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.
- Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal de noviembre de 2017.
- Real Decreto-ley 5/2018, de 27 de Julio, de medidas urgentes para la adaptación del derecho español a la normativa de la UE en materia de protección de datos
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.
- Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales.
- Ley 48/1978, de 7 de octubre, por lo que se modifica la Ley de 5 de abril de 1968, sobre Secretos Oficiales.ISO27002:2015
- IEC/62443 2013
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. (Directiva NIS España)
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Política de seguridad de las TIC (Centro Criptológico Nacional -STIC 001). Seguridad de las tecnologías de la información y las comunicaciones que maneja información clasificada en la administración.

Adicionalmente a las referencias especificadas, cada licitador deberá detallar cualquier legislación, reglamento, estándares, códigos de buenas prácticas, así como metodologías y herramientas – principalmente de análisis de riesgos – que vayan a utilizar en el marco del proyecto.

3.2 DESCRIPCIÓN DE LOS TRABAJOS A REALIZAR

El contratista del servicio deberá realizar al menos las tareas que se indican a continuación, generando asimismo los entregables que en ellas se citan:

a) Planificación inicial del proyecto

Al inicio del proyecto, el contratista deberá elaborar, concretando ya las fechas en función del inicio efectivo de los servicios:

- Planificación detallada del proyecto (Diagrama de GANTT o similar): Dentro de la planificación se deberán identificar al menos: fases del proyecto y tareas de cada una de ellas, fechas de inicio y fin de cada tarea; hitos de entrega, validación y aceptación por parte de Metro de Madrid. Los plazos de validación de cada uno de los entregables deberán ser acordes con el volumen de información entregada.
- Plan de trabajo: Debe incluir, al menos, el objeto, alcance, y el detalle de los trabajos a desarrollar.

La planificación del proyecto y el plan de trabajo deberán ser aprobados por Metro de Madrid antes de comenzar con el trabajo de campo. Para ello se mantendrá una primera reunión de lanzamiento.

b) Entrevistas con personal clave de Metro de Madrid

Se agendarán las reuniones necesarias con miembros clave de la organización que tendrán por objeto identificar las problemáticas y requisitos de cada ámbito en lo que al objeto de los trabajos se refiere.

Se elaborará una memoria/informe con las principales conclusiones que se obtengan de esta batería de reuniones, así como un acta detallada de cada una de dichas reuniones.

c) Definición de niveles de confidencialidad

Basándose en las conclusiones y problemáticas detectadas en los trabajos antes descritos, y teniendo absolutamente presente los condicionantes en este aspecto incluidos en las normativas de referencia, se definirán niveles de confidencialidad de la información manejada en Metro de Madrid. Estos niveles deberán poder ser aplicables a toda la información que se trata en los procesos de negocio de Metro de Madrid, S.A, y la definición **de cada uno de ellos** incluirá al menos los siguientes aspectos:

- Denominación
- Definición genérica de los mismos: De forma que mediante dicha definición pueda discernirse qué nivel es el que mejor se adapta a cada uno de los documentos, en función al menos de su tipología y contenido, que Metro de Madrid genera y recibe.¹
- Definición, para cada nivel, de los controles y salvaguardas que Metro de Madrid debe implementar para el etiquetado, acceso, almacenamiento, reproducción, distribución, destrucción, etc. de la información en ellos encuadrada (ya sea verbal, visual, en papel o digitalmente). En particular, para el almacenamiento, reproducción y distribución, estos controles podrán ser de cualquiera de los siguientes tipos:
 - Controles lógicos: Relativos a tecnologías de información (almacenamiento en servidores especiales, perfilado de usuarios, etc.)
 - Controles Físicos: Aplicables sobre todo a documentación en papel (marcas de agua, custodia en armarios securizados, zonas reservadas, CPDs, etc.).
 - Controles Organizativos: Ligados principalmente a formas de organización, formas de trabajo, hábitos de conducta, etc.

¹ NOTA: No es objeto de los trabajos asignar nivel a todos los documentos en poder de Metro

- Controles legales: Principalmente necesidad de firmar acuerdos de confidencialidad (NDA's) por parte de personal de Metro de Madrid o de terceros que deban tener acceso a la documentación. Se indicará en cada nivel si la firma de estos acuerdos es pertinente y en qué casos. Cuando sean requeridos, el contratista de los servicios redactará un borrador de los mismos para cada una de las tipologías que sean requeridas.
- Definición de roles: Asignación de responsabilidades a los diferentes actores implicados en la redacción, custodia y potencial difusión de la información. Se tendrá en cuenta para este apartado el régimen disciplinario de Metro de Madrid y su Código Ético, identificando en ellos los artículos / aspectos que serían contravenidos de forma general en caso de incumplimiento de los controles definidos en el apartado anterior.

d) Plan de Acción

A la vista de lo anterior, se elaborará un plan de acción para acometer los cambios y acciones que hayan sido identificados, aportando un estudio de benchmarking sobre las mejores (o más habituales) soluciones adoptadas por otras compañías.

e) Política de Clasificación y Tratamiento de la Información

El contratista redactará la Política de Clasificación y Tratamiento de la Información, así como la Norma de Clasificación, Etiquetado y Tratamiento de la Información

f) Presentación de resultados

Al final del proyecto:

- Se realizará una sesión informativa ejecutiva dirigida a la Dirección de Metro de Madrid para informar del trabajo realizado y de sus resultados.
- Se entregará un informe ejecutivo como documento de apoyo para los asistentes a la reunión anterior.
- Se realizará una sesión informativa de detalle para informar del trabajo realizado y de sus resultados a los principales responsables designados para el despliegue de la Política de Clasificación en cada unidad organizativa de Metro de Madrid

3.3 POR SU PARTE, METRO DE MADRID DESIGNARÁ UN RESPONSABLE DEL PROYECTO QUE SERÁ EL INTERLOCUTOR PARA EL CONTRATISTA Y QUE SUPERVISARÁ LA EJECUCIÓN DE LOS TRABAJOS COMPROBANDO QUE LA REALIZACIÓN DE LOS MISMOS SE ADECUA A LOS REQUISITOS ESTABLECIDOS. DESARROLLO Y SUPERVISIÓN DE LOS TRABAJOS

Para el desarrollo de los trabajos, el Director y/o Jefe de Proyecto de la empresa contratista junto con los consultores / auditores, mantendrán la necesaria y permanente coordinación con el Responsable del Proyecto delegado por Metro de Madrid o con los técnicos designados por el mismo, quienes prestarán toda la asistencia que precisen los mismos, estableciéndose, de común acuerdo, un plan de trabajo, y de seguimiento y control del proyecto con un plan de reuniones periódicas en el caso que proceda.

4. Aspectos a Considerar para Redactar la Oferta Técnica

En la oferta técnica, además de cualquier condición especificada en el presente documento, se deberá aportar como mínimo la siguiente información:

- Enfoque y propuesta metodológica:
 - Propuesta de organización de los trabajos acorde a los planteamientos del Pliego de Prescripciones Técnicas.
 - Descripción detallada de objetivos, actividades y tareas requeridas en el ámbito del alcance del proyecto anteriormente detallado.
 - Metodología de trabajo propuesta, marco de referencia para el análisis (estándares, códigos de buenas prácticas, marco normativo y legal, etc.), así como procedimientos de seguimiento, control y calidad previstos.
- Medios humanos:
 - Perfiles del equipo de trabajo propuesto, indicando para cada uno de ellos la dedicación al proyecto en términos de porcentaje de su jornada laboral.
 - CV de los medios humanos que se asignaran al contrato. Como mínimo se aportarán los CV de los medios humanos especificados en el apartado 5 de este pliego.

5. Medios humanos

La empresa licitadora que resulte adjudicataria asignará un equipo especializado y con experiencia que será responsable de la ejecución de los servicios objeto de la licitación, es decir, de todos y cada uno de los aspectos recogidos en el alcance del proyecto y de las tareas técnicas y de gestión que se han especificado en el presente documento.

El equipo estará compuesto por perfiles tanto legales como técnicos, es decir, los integrantes del equipo deberán acreditar formación y experiencia en los aspectos legales y técnicos que constituyen el ámbito de los servicios a prestar.

En concreto, el equipo deberá contemplar al menos cuatro perfiles profesionales a saber:

- **Consultor / Auditor / Especialista 1:**

Deberá contar con:

- Titulación universitaria de grado medio o superior.
- Experiencia mínima de cinco (5) años en la realización de trabajos similares en los ámbitos de consultoría y/o auditoría en seguridad de la información.
- Conocimientos demostrables en:
 - Metodologías de análisis y gestión de riesgos tecnológicos.
 - Auditorías de seguridad de la información.

- **Consultor / Auditor / Especialista 2:**

Deberá contar con:

- Titulación universitaria de grado medio o superior.
- Experiencia mínima de cinco (5) años en el ámbito de la seguridad física.

- **Especialista Legal:**

Deberá contar con:

- Titulación universitaria en Derecho.
- Experiencia mínima de cinco (5) años en labores legales (Asesor Jurídico o abogado de empresa).

- **Director y/o Jefe del Proyecto:**

Deberá con:

- Titulación universitaria de grado medio o superior.
- Experiencia mínima de cinco (5) años en la realización de trabajos similares en los ámbitos de consultoría y/o auditoría en seguridad de la información, cumplimiento legal y normativo o consultoría estratégica o de negocio.

Tendrá como principal cometido asegurar la eficaz y eficiente ejecución del proyecto y la satisfacción de Metro de Madrid en relación con el servicio prestado, así como, identificar las necesidades de Metro de Madrid para asegurar que el servicio dado coincide con sus expectativas.

Para cada uno de los perfiles, al menos dos (2) años de la experiencia solicitada deberán estar dentro de los últimos 5 años para asegurar que el conocimiento del personal se adecua al marco legal, normativo y regulatorio actual. La experiencia mínima requerida se especificará mediante una relación de los proyectos más relevantes en los que hayan participado indicando cliente, descripción de los trabajos realizados, perfil desempeñado, duración y fechas de ejecución.

Los perfiles mencionados anteriormente podrán ser cubiertos por una o más personas.

Los citados medios personales deberán ser acreditados mediante la presentación del Curriculum Vitae de cada una de las personas asignadas, tanto del personal técnico como mandos intermedios, en el que se indique la experiencia, titulaciones, etc. y/o Títulos académicos que habrán de ser, necesariamente, españolas, o estar homologadas en el ámbito de la Unión Europea.

6. Obligaciones del Contratista

Los medios humanos aportados por el adjudicatario para la ejecución del contrato estarán sometidos al poder de dirección y organización (retribuciones, horarios, instrucciones, etc.) del contratista adjudicatario en todo ámbito y orden legalmente establecido. Será, por tanto, éste el único responsable y estará obligado al cumplimiento de cuantas disposiciones legales resulten aplicables al caso, en especial en materia de contratación, Seguridad Social, prevención de riesgos laborales y tributarios, por cuanto dicho personal en ningún caso tendrá vinculación jurídico-laboral con Metro de Madrid. Todo ello con independencia de las facultades de control e inspección que legal y /o contractualmente correspondan a Metro de Madrid.

7. Medios Materiales

El adjudicatario del contrato pondrá los medios materiales necesarios para llevar a cabo los servicios objeto del contrato.