

**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA
CONTRATACIÓN DEL SERVICIO ESPECIALIZADO DE
APOYO A LA GESTIÓN Y ADMINISTRACIÓN DE LA
PLATAFORMA DE GESTIÓN DE IDENTIDADES**



**PLIEGO DE CONDICIONES TÉCNICAS PARA LA
CONTRATACIÓN DEL SERVICIO ESPECIALIZADO DE
APOYO A LA GESTIÓN Y ADMINISTRACIÓN DE LA
PLATAFORMA DE GESTIÓN DE IDENTIDADES**

FECHA: 12 DE DICIEMBRE DE 2017



I N D I C E

1.	OBJETIVO	4
2.	ALCANCE	4
2.1	ÁMBITO DEL SERVICIO	4
2.2	HORARIOS Y LUGAR DE PRESTACIÓN DEL SERVICIO	5
3.	REQUERIMIENTOS ESPECÍFICOS	6
3.1	CARACTERÍSTICAS Y REQUISITOS DEL SERVICIO	6
3.2	PLATAFORMA TECNOLÓGICA ASOCIADA.....	11
3.3	CARACTERÍSTICAS Y REQUISITOS DEL EQUIPO DE TRABAJO.....	12
3.4	ASPECTOS TÉCNICOS A TENER EN CUENTA PARA REDACTAR LA OFERTA TÉCNICA ..	13



Dado el carácter reservado de toda la información contenida en el presente documento, la mera participación en esta licitación (que comienza con la recepción de este documento), supone que todos y cada uno de los oferentes aceptan tratar todos los datos relativos a este servicio como información privada de Metro de Madrid, S.A. En consecuencia, se deberá garantizar la confidencialidad de la misma, usándose únicamente a efectos de la redacción de una oferta para la citada licitación. Asimismo, los Oferentes se comprometen a no ceder, ni mostrar, ni transferir por medio alguno la totalidad o partes de este documento.



1. OBJETIVO

El objeto del presente documento es establecer las condiciones técnicas que regirán la presentación de ofertas para la contratación del Servicio Especializado de Apoyo a la Gestión y Administración de la Plataforma de Gestión de Identidades.

2. ALCANCE

2.1 ÁMBITO DEL SERVICIO

El Área de Sistemas de Información (ASI) tiene implementada una Plataforma de Gestión de Identidades orientada principalmente a unificar y optimizar la gestión y control de acceso de los usuarios a los diferentes sistemas de información, minimizando el riesgo de acceso indebido a recursos de información, y cumpliéndose el criterio de confidencialidad; todo ello, bajo la premisa de la necesidad de conocer para la realización de las funciones desempeñadas en la empresa, y contemplando los requisitos derivados del cumplimiento legal y normativo, y siendo de vital importancia para la función de auditoría de seguridad de la información.

La Plataforma de Gestión de Identidades implementada, está basada en la solución OpenIAM de código abierto, contándose con soporte especializado in situ para la gestión, administración y evolución del sistema de todos sus componentes, y de los desarrollos personalizados que se han realizado.

El ámbito funcional del servicio radica en la constante necesidad de evolución de los sistemas y los múltiples requisitos de éstos respecto del control de acceso, los cambios organizativos propios de la actividad normal de la empresa y aquellos de mayor impacto, pero más espaciados en el tiempo, la evolución de los propios componentes de la Plataforma de Gestión de Identidades, o su aplicación a sistemas, o aplicaciones aún no incorporados en la actualidad y las incidencias que pueden surgir en el día a día; así como, las necesidades de evolución derivadas de procesos de migración de aplicaciones y/o sistemas, o de sus plataformas tecnológicas.

Por lo anterior, es necesario contratar el servicio especializado de soporte In-situ para la gestión, administración y evolución de la plataforma de gestión de identidades para el período de un año. Es importante destacar que **no** se considera la sustitución durante el período vacacional de la(s) persona(s) que preste(n) el servicio, aunque la disponibilidad debe ser de un 100% para Metro de Madrid en relación con la gestión, administración y evolución del sistema y las tareas que ello conlleva, como se describen en el presente Pliego.

En sí, el objetivo es asegurar el correcto funcionamiento y la continuidad de la Plataforma de Gestión de Identidades, disponer de la flexibilidad y agilidad suficiente para garantizar la evolución en su alcance funcional y de sistemas.

Es importante destacar que para la prestación del servicio, Metro de Madrid permitirá el acceso a las herramientas de gestión de la Plataforma de Gestión de Identidades a las que deba accederse para realizar los trabajos objeto del servicio; sin embargo, el equipo informático a nivel de usuario y el software ofimático o de propósito específico que se requiera para la prestación del servicio deberá ser aportado por el Adjudicatario, debiéndose ajustar a los requisitos de seguridad y de configuración que Metro de Madrid establezca en cada momento durante el plazo de prestación del servicio.

Queda expresamente fuera del alcance de la licitación cualquier adquisición de software o de los mantenimientos de productos que constituyen la Plataforma de Gestión de Identidades.

Cualquier dato enumerativo que se ofrece a lo largo de este documento se hace de forma que facilite la confección de las ofertas, de modo que cada oferente tenga una idea lo más aproximada del entorno de trabajo. Se publica con carácter meramente informativo, lo cual, significa que durante la prestación del servicio, los datos podrían variar o podrían no ser exactos al 100%, principalmente por razones derivadas de la normal evolución de la base tecnológica de Metro de Madrid.

La información que se facilita no eximirá al Adjudicatario de comprobar o cotejar los datos con la realidad, la discrepancia entre la realidad, y esta información no dará derecho a incremento alguno del precio establecido en el Contrato, ni a indemnización de ningún tipo.

2.2 HORARIOS Y LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio se prestará desde las instalaciones del Centro de Tecnologías de la Información de Metro de Madrid, sito en Avenida del Partenón 5, Campo de las Naciones. Sin embargo, según las necesidades específicas que surjan durante la prestación del servicio y la disponibilidad de sitios de trabajo en cada momento, podrá realizarse desde cualquiera de los sitios de trabajo adscritos al Área de sistemas de Información.

El horario de trabajo será de 7:15 a 15:30 horas de lunes a viernes; no obstante, el horario habitual de prestación de servicio podrá verse modificado de forma temporal en situaciones excepcionales.

3. REQUERIMIENTOS ESPECÍFICOS

Los requerimientos específicos que a continuación se detallan recogen básicamente información relativa a las características y requisitos del servicio, casuística que constituye la base del mismo y plataforma tecnológica base para el servicio.

3.1 CARACTERÍSTICAS Y REQUISITOS DEL SERVICIO

Las actividades de gestión, administración, mantenimiento y evolución de la Plataforma de Gestión de Identidades y sus desarrollos a medida que constituyen la base del servicio incluyen:

1. Gestión y administración de la plataforma y todos sus componentes que supone la administración del sistema en producción, desglosándose en las siguientes tareas por componente:

Admin Console (webconsole)

- Revisión del funcionamiento global del sistema mediante revisión ficheros logs y trazas de auditoría.
- Mantenimiento y creación de tareas batch.
- Mantenimiento y creación de metadatos.
- Localización y personalización de la interfaz.
- Mantenimiento de políticas de atributos para el aprovisionamiento a los sistemas finales (Managed System).
- Mantenimiento de diferentes vistas/permisos para administración delegada.
- Mantenimiento y definición de conectores y Managed Systems.
- Configuración y mantenimiento de los procesos de reconciliación.
- Configuración y mantenimiento de los procesos de sincronización.
- Adaptación de los scripts de preprocesado y postprocesado del proceso Provisioning de OpenIAM a los requerimientos y reglas de negocio definidas por Metro de Madrid.
- Generación y creación de nuevos informes a través de BIRT.
- Creación y mantenimiento de estructura organizativa y sus tipos.
- Establecimiento y mantenimiento de políticas de contraseñas y autenticación.
- Generación de operaciones de cambio masivas.

- Mantenimiento de tipos de recursos, recursos, roles y grupos para cada sistema gestionado.
- Personalización y mantenimiento del motor de notificaciones.

Almacén Central de Identidades

Gestión del repositorio centralizado de la herramienta que almacena toda la información de las identidades digitales de los empleados y colaboradores. El modelo de datos incluye toda la información relativa a la identidad requerida por los aplicativos (identidad, cuentas asociadas, estructura organizativa, roles, etc.).

Fuente Autoritativa, Ciclo de Vida y Aprovisionamiento

Gestión de la integración con la fuente de identidades (módulo HR de SAP R/3), y la sincronización con la gestión de identidades. Debe gestionar el ciclo de vida completo de las identidades (incorporación, modificaciones, traslados y bajas). Estas operaciones serán realizadas de forma automática en base a la información recibida desde RRHH.

Gestión manual a través de formularios y actualización en todos los repositorios finales.

Carga masivas a partir de ficheros de carga en cuanto a:

- Alta, Baja Modificación de Identidades.
- Conexión de roles.
- Desconexión de roles.

Conexión a Sistemas Gestionados

Gestión de las conexiones con los sistemas finales integrados a partir de los agentes propios de la herramienta o desarrollados a medida.

Sincronización de Contraseñas y Autoservicio de Usuarios

Gestión de los procesos de sincronización de contraseñas en todas las cuentas de los sistemas asociados a una identidad, incluyendo el procedimiento de autenticación alternativo basado en un mecanismo de desafíos-respuestas. Igualmente, debe considerarse lo siguiente:

- Definición y mantenimiento de preguntas utilizadas para los desafíos/respuestas.
- Definición de vistas y capacidades para el autoservicio.
- Creación y mantenimiento de flujos de workflow.
- Localización y personalización de la interfaz del portal.

Modelo RBAC y Perfilado

Gestión y mantenimiento del modelo de roles definido en Metro de Madrid, que se podrá asignar de forma automática en el alta y modificación de identidades, asignando los accesos básicos a los sistemas de información.

La plataforma debe contemplar la creación y asociación de roles/perfiles que de forma automática genere cuentas y conecte estas cuentas a grupos de sistemas finales.

2. De forma general deberán realizarse las siguientes tareas:

Directorios

En función de los diferentes directorios o repositorios sobre los que se realizan tareas de aprovisionamiento, deben contemplar las siguientes actividades:

- Directorio Activo
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, definición de permisos sobre unidades de red, sistema de captura de cambios de contraseñas, etc.
- Microsoft Exchange
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, límites de buzones, cambios de contenedores, etc.
 - Tratamiento de solicitudes de modificación y casos especiales.
- LDAP
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios.
 - Mantenimiento y réplica de la estructura de ramas de los sistemas LDAP.
 - Creación y mantenimiento del funcionamiento de los grupos de aplicación-perfil.
 - Mantenimiento del sistema de notificaciones de aviso de caducidad de cuentas.

- DOCUMENTUM
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios.
- IBM Domino
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios.
 - Creación, asignación y mantenimiento de grupos de permisos de nivel de acceso, lectura y administración del Gestor Documental Platón, adaptándolos a los cambios en la estructura organizativa de la empresa.
- AUAC¹
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, procesos de prejubilación y renombrado, etc.
 - Creación y mantenimiento de los grupos de asignación aplicación perfil.
- SAP (Incluye SAP R/3, SAP Portal y SAP Netweaver)
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, procesos de prejubilación y renombrado, etc.
 - Mantenimiento de informes necesarios para auditorías.
 - Mantenimiento de matrices de relación de grupos de usuarios en SAP Portal, con unidades organizativas y grupos colectivos.
- MOBILE Y MOBILE ALARMAS
 - Mantenimiento y mejoras de los procesos relacionados con los aplicativos de Incimov y de envíos de alertas SMS en cuanto a altas, bajas y modificación de cuentas de usuarios, procesos de prejubilación y renombrado, etc.
 - Mantenimiento y evolución de la estructura de tablas intermedias a medida necesarias para la correcta gestión de estas aplicaciones.

¹ AUAC es un conjunto de aplicaciones desarrolladas en PowerBuilder por Metro de Madrid. El repositorio de usuario está basado en una base de datos Oracle.

- ZIMBRA Open Source Edition
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, procesos de prejubilación y renombrado, etc.
 - Inclusión en las herramientas de gestión de contraseñas (consola COMMIT y autorreseteo de contraseñas).
 - MOODLE
 - Mantenimiento y mejoras de los procesos relacionados con altas, bajas y modificación de cuentas de usuarios, procesos de prejubilación y renombrado, etc.
 - Inclusión en las herramientas de gestión de contraseñas (consola COMMIT y autorreseteo de contraseñas).
3. Análisis In-Situ de posibles incidencias, resolución mediante desarrollo y/o implementación de correctivos, o en su caso, canalizando las incidencias y apoyándose en el servicio de soporte que ofrezcan los fabricantes.
 4. Evolución de la plataforma que incluye actividades de explotación y ampliación de la plataforma, mejoras del servicio, inclusión de nuevas funcionalidades o ampliación del alcance de sistemas integrados, ayuda en la migración a nuevas versiones del producto, migraciones en la infraestructura del sistema y actuación frente a cambios en los sistemas integrados, siempre y cuando estas actividades no impliquen desarrollos a medida.
 5. Monitorización de la plataforma, realización de estadísticas y medición para la continua mejora del servicio.
 6. Propuestas de mejora del servicio y dimensionamiento para su planificación.

Deben tenerse en cuenta que pueden surgir necesidades específicas adicionales a los entornos descritos, o bien, la plataforma informática puede evolucionar durante el período de vigencia del servicio, requiriéndose la adecuación del equipo de trabajo a dichos cambios, incluyendo procesos de migración de los productos.

3.2 PLATAFORMA TECNOLÓGICA ASOCIADA

En cuanto a la infraestructura tecnológica y los sistemas que se asocian a las actividades a realizar en el marco de la prestación del servicio cabe destacar²:

Plataforma de Gestión de Identidades

- En cuanto a la herramienta OpenIAM se contará, al menos, con los siguientes componentes:
 - Servidor de Aplicaciones³ con los siguientes componentes principales:
 - OpenIAM Services (Enterprise Service Bus)
 - OpenIAM Connectors⁴
 - Consolas de Gestión:
 - OpenIAM Admin Console
 - OpenIAM SelfService
 - OpenIAM Active Directory Password Filter
 - OpenIAM Credential Provider

Directorios y Sistemas⁵

- Directorio Activo de Microsoft.
- Microsoft Exchange.
- Aplicación de Seguridad propietaria para la gestión de los usuarios de las aplicaciones corporativas de Metro⁶.
- OpenDJ 2.6 y SUN OpenSSO 8.x.
- Directorios de SAP R/3 y SAP Enterprise Portal.
- Directorio de SAP Netweaver.
- IBM Domino.
- Mobile y Mobile Alarmas
- Zimbra Open Source Edition
- Moodle

Nota: En la mayoría de los casos, cada uno de estos directorios y sistemas disponen de tres entornos diferenciados: desarrollo, preproducción y producción, sobre los que se realizan actividades desde la Plataforma

² La infraestructura puede variar en función de la evolución tecnológica que experimente Metro de Madrid y los propios sistemas objetos de la gestión y administración.

³ Desplegada sobre tecnología JBoss y Tomcat.

⁴ Aunque los conectores estarán implementados en el servidor de aplicaciones, habrá que tener en cuenta la posible existencia de conectores remotos para los Directorio Activo y Exchange.

⁵ Referido a los principales entornos sobre los que interactúa la Plataforma de Gestión de Identidades como parte de los procesos de aprovisionamiento de usuarios.

⁶ La aplicación está desarrollada en PowerBuilder y el repositorio de usuarios está basado en Oracle.

de Gestión de Identidades. Sin embargo, en algunos casos, como puede ser SAP R/3, el número de entornos gestionados llega a catorce.

3.3 CARACTERÍSTICAS Y REQUISITOS DEL EQUIPO DE TRABAJO

El equipo de trabajo que se encargará de la prestación del servicio deberá adecuarse a los siguientes requisitos:

- Deberán poseer formación académica y profesional, y experiencia en servicios similares relativos a sistemas de Gestión de Identidades, así como conocimientos técnicos en los sistemas y/o productos incluidos en los servicios objeto del contrato con los mínimos exigidos en el apartado 20 del Pliego de Condiciones Particulares.
- Se requieren conocimientos de:
 - Solución OpenIAM
 - Suite BMC Identity Management
 - Programación en lenguaje C
 - Programación en Java y Java EE (Jsp, Beans, ...)
 - Scripting (shell bash, python, perl, groovy y powershell)
 - Weblogic
 - Jsp
 - Javascript
 - Html
 - Powershell
 - Vbscript
 - Administración de base de datos Oracle 10g y 11g
 - Administración y lenguaje de consultas SQL
 - S.O. Solaris 10
 - Lotus notes
 - Gestor documental Platon
 - Generador de informes BIRT
 - Gestor de WorkFlows Activiti
 - S.O. Windows: 2003 y 2008 a nivel de servidores, y WXP y W7 a nivel de cliente
 - Administración de Directorio Activo
 - Administración de Microsoft Exchange.
 - Administración LDAP
 - En cuanto a sistemas SAP, conocimiento de los modelos de control de acceso de SAP R3, SAP Netweaver y SAP Enterprise Portal



- En cuanto a la integración del aprovisionamiento, conocimiento de las API de SAP y Documentum.

3.4 ASPECTOS TÉCNICOS A TENER EN CUENTA PARA REDACTAR LA OFERTA TÉCNICA

En la oferta técnica se deberá aportar la siguiente información:

- Un plan descriptivo del servicio, donde se incluye la planificación detallada con el desglose de tareas, recursos y productos. Dicho plan será la base para la constitución del programa de trabajo conjunto y detallado, que unificará, realizará y gestionará el gestor o responsable del servicio por parte del adjudicatario. El plan deberá ser validado por Metro de Madrid, y servirá de guía para el control y seguimiento de los trabajos durante todo el tiempo que estos duren, hasta la finalización de la prestación del servicio.

Descripción de la organización y de los medios técnicos que prevé dedicar específicamente, es decir, del plan de servicio completo a ofrecer.
