

PLIEGO DE PRESCRIPCIONES TÉCNICAS

**CONTRATO DE SERVICIO DE SUSCRIPCIÓN Y
SOPORTE INFORMÁTICO DEL SISTEMAS SAAS
DE GESTIÓN DE MANTENIMIENTO (ROSMIMAN)
IMPLANTADO EN EL CANAL DE ISABEL II, S.A.**

**PROCEDIMIENTO NEGOCIADO SIN PUBLICIDAD
NO ARMONIZADO AL PRECIO MÁS BAJO**

Nº CONTRATO: 123/2019

Área: Planificación, Control y Seguridad

Fecha: 20 de mayo de 2.019

Índice

1. Introducción y Alcance	3
1.1. Desarrollo de los servicios.....	3
1.1.1. Desarrollo del soporte y asistencia técnica	4
1.1.2. Extracción de datos del Sistema	4
1.1.3. Niveles de Servicio.....	4
1.1.4. Copia de la base de datos.....	5
1.1.5. Penalizaciones	5
1.2. Requisitos de seguridad.....	5
2. Consideraciones sociales, ambientales y de innovación.	9
3. Formato de la Oferta técnica	10

1. Introducción y Alcance

Las depuradoras de aguas residuales de Canal de Isabel II, S.A. disponen en la actualidad de un programa informático para la gestión del mantenimiento de los equipos y elementos ubicados en estas instalaciones denominado GIMDEI, basado en la aplicación ROSMIMAN, aplicación en modo SaaS (Software as a Service). Esta aplicación permite gestionar de manera sistemática el mantenimiento correctivo, preventivo y predictivo, así como generar informes adaptados a las necesidades de los servicios.

Se pretende renovar el mantenimiento de estos servicios para las estaciones depuradoras de gestión directa (operadas por Canal de Isabel II, S.A.) el cual deberá seguir realizándose como hasta la fecha.

Para el correcto funcionamiento del software es necesario el servicio de soporte y mantenimiento del mismo.

Los servicios objeto del contrato serán los siguiente:

- S1. Servicio 1: Servicios de alojamiento mensual en modo CLOUD, para la aplicación ROSMIMAN, así como alojamiento de los datos que se encuentran almacenados en la misma, en modalidad CLOUD BRONZE.

Adicionalmente Canal de Isabel II, podrá solicitar el servicio enunciado a continuación:

- S2. Servicio 2: Utilidades funcionales y colaboración para extracción de los datos contenidos actualmente en la aplicación en formato MS Access. Para ello se utilizará la bolsa de horas ofertada en este procedimiento. En ningún caso se podrá superar el importe máximo del contrato.

1.1. Desarrollo de los servicios

Se asignarán los medios humanos y materiales necesarios para garantizar en todo momento el funcionamiento de la aplicación y ejecución de la bolsa de horas en el plazo solicitado por Canal de Isabel II, S.A.

1.1.1. Desarrollo del soporte y asistencia técnica

La empresa adjudicataria deberá garantizar en todo momento el servicio de soporte y asistencia técnica, en la modalidad

El adjudicatario informará a Canal de Isabel II, S.A. sobre la funcionalidad y comunicaciones realizadas con el resto de usuarios y subsanará los errores de funcionamiento que imposibiliten el manejo de la aplicación.

1.1.2. Extracción de datos del Sistema

Se proveerá de un servicio de utilidades funcionales y colaboración para extracción de los datos contenidos actualmente en la aplicación en formato MS Access.

1.1.3. Niveles de Servicio

Se deberá garantizar la disponibilidad del programa de forma ininterrumpida (24x7).

Se fija un plazo máximo de respuesta de 24 horas ante incidencias muy graves: un sistema de la GIMDEI inoperante, comunicadas a través del servicio de soporte del proveedor.

Se fija un plazo máximo de respuesta de 48 horas ante incidencias graves: una opción del menú de un sistema de la GIMDEI inoperante, comunicadas a través del servicio de soporte del proveedor.

Se fija un plazo máximo de respuesta de 72 horas ante incidencias leves: disfunciones en alguna de las opciones del menú de un sistema de la GIMDEI, comunicadas a través del servicio de soporte del proveedor.

El personal asignado al contrato ejercerá sus tareas de atención en el periodo comprendido entre de 9 a 14.00 y de 15.00 a 17.00.

Canal de Isabel II, S.A. fijará los responsables por parte de cada departamento quienes deberán estar informados de las incidencias y desarrollo de las actividades del contrato.

1.1.4. Copia de la base de datos

Se entregará una copia de la base de datos, en soporte digital y en formato estandarizado de lectura, cada mes.

1.5.4.1 El formato de entrega debe cumplir las normas de seguridad (no se considera válido un fichero ejecutable encriptado)

1.5.4.2 La entrega debe documentarse con el detalle del modelo de datos exportado; este detalle incluirá las referencias a tablas con ficheros adjuntos y los ficheros de configuración.

1.1.5. Penalizaciones

Cuando el contratista, por causas imputables al mismo, hubiere incurrido en demora respecto al cumplimiento de los plazos de resolución de avisos ante incidencias determinados en el apartado 1.5.3 Niveles de Servicio, Canal de Isabel II, S.A. se reservará el derecho de imponer penalizaciones en la proporción correspondiente a los días o fracción de día de demora respecto del total de días de la facturación mensual del esquema o esquemas afectados.

Las penalizaciones previstas en el presente apartado, tienen carácter acumulativo y no sustitutivo, a los efectos de lo dispuesto en el artículo 1.152 del Código Civil.

A los efectos de lo previsto en el artículo 1.153 del Código Civil, el adjudicatario penalizado, además de satisfacer la penalización en los términos previstos en el párrafo siguiente, deberá cumplir las obligaciones cuyo incumplimiento o retraso se penaliza.

La aplicación y el pago de las penalizaciones no excluyen la indemnización a que Canal de Isabel II, S.A. pueda tener derecho por daños y perjuicios ocasionados con motivo del incumplimiento imputable al contratista.

1.2. Requisitos de seguridad

El proveedor de servicios Cloud deberá garantizar, al menos, que para el servicio o los servicios Cloud contratados por Canal de Isabel II, S.A.:

- a) El acceso se produce exclusivamente bajo un protocolo que cifre de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad e integridad (por ejemplo, uso exclusivo de TLS 1.2 o superior, y utilizando sólo suites de cifrado robustas para evitar vulnerabilidades de tipo BEAST (RC4), Lucky13 (RC4), POODLE (SSL 3.0 y TLS 1.0), CRIME (TLS 1.0 compression), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).
- b) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.
- c) Que dicho esquema de BBDD sea accedido única y exclusivamente por el/los usuarios de aplicación que vayan a ser utilizados en la conexión del servicio Cloud a dicho esquema de BBDD.
- d) Cifrado robusto de los datos propiedad de Canal de Isabel II, S.A. en la propia BBDD y modelo (cifrado completo o cifrado del dato).
- e) Almacenamiento de los datos de autenticación de los usuarios (por ejemplo, el par usuario/contraseña) en la BBDD mediante el uso de funciones resumen (hash) robustas (al menos, SHA-256) conjuntamente con la obligación de utilizar contraseñas complejas (longitud mínima de 10 caracteres, con obligatoriedad de utilizar caracteres alfanuméricos (mezcla de mayúsculas, minúsculas y números) y no alfanuméricos (por ejemplo, signos de puntuación y ortográficos)). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (Password-Based Key Derivation Functions) para el almacenamiento de las contraseñas (por ejemplo, PBKDF2).
- f) Exista la posibilidad de uso de:
 - a. Un esquema XML para el intercambio de datos de autenticación y autorización (por ejemplo, SAML 2.0) e implementaciones de seguridad a nivel del mensaje.
 - b. OAuth 2.0 u OpenID Connect como modelos de autorización segura para consumo de servicios web.
 - c. SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.
- g) Exista la posibilidad de habilitar un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, ya sea mediante el uso de certificados electrónicos reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.
- h) Todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) han sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP) para comprobar que existen y que han sido implementadas correctamente.
- i) Se almacena de forma segura (garantía de acceso, recuperación y no modificación) y se revisa de forma regular el registro de eventos de las actividades de los usuarios (errores y eventos de seguridad). Estos registros deberán mantenerse al menos durante cinco (5) años.

j) Comunicará inmediatamente a Canal de Isabel II, S.A. acerca de todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas y de las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades.

El acceso a un servicio proporcionado por un proveedor de servicios Cloud será siempre a través del software dispuesto en la maqueta corporativa instalada en un equipo corporativo (fijo o portátil). No se accederá a través de clientes pesados proporcionados por terceros, incluyendo el software proporcionado por el propio proveedor de servicios Cloud.

Canal de Isabel II, S.A. realizará las siguientes gestiones, a través de la correspondiente solicitud de acceso cursada en la aplicación corporativa de solicitudes e incidencias, para garantizar a los usuarios de Canal de Isabel II, S.A. autorizados el acceso al servicio Cloud a través de:

1. El control de acceso a través de pertenencia a grupos de usuarios en el Directorio Activo.
2. Los permisos que sean necesarios en los sistemas corporativos de control de acceso existentes.

En este punto, el proveedor de servicios Cloud deberá proporcionar, al menos, la siguiente información:

1. Requisitos técnicos para el acceso al servicio o servicios Cloud que proporciona y que hayan sido contratados por Canal de Isabel II, S.A.
2. Requisitos de ancho de banda de acceso a Internet para la parte cliente.
3. Usuarios de prueba con las autorizaciones estrictamente necesarias, para poder realizar correctamente las verificaciones que correspondan (funcionales, técnicas, de seguridad, etc.).

El servicio prestado por el proveedor de servicios Cloud, por defecto, no se integrará de ninguna manera con los Sistemas de Información de Canal de Isabel II, S.A. En caso de que desde la Subdirección de Sistemas Informáticos se estime la viabilidad de una posible integración, con objeto de poder evaluar la dimensión y el alcance de la misma, se revisarán, al menos, los siguientes puntos:

- Funcionamiento del proveedor de servicios Cloud (certificaciones, niveles de madurez, procesos, etc.).
- Posibilidades técnicas y costes de integración con los sistemas de información de Canal de Isabel II, S.A. (tecnologías, seguridad, etc.), teniendo en cuenta la infraestructura tecnológica y de comunicaciones de Canal de Isabel II, S.A.
- Nivel de control que el negocio tendrá sobre los servicios Cloud proporcionados.
- Nivel de seguridad implementado por el proveedor de servicios Cloud.
- Nivel de dependencia y requisitos del servicio corporativo de Internet.

Dicha evaluación se recogerá en un informe que será entregado al Comité de Coordinación de Seguridad de la Información (en adelante, CCSI) para su conocimiento y correspondiente evaluación. Sólo en caso de aceptación por parte del CCSI se procederá a informar cumplidamente al dueño de los datos para su autorización final y, sólo entonces, se iniciarán las tareas de la

Empresa
Canal de Isabel II, S.A.

Servicio de suscripción y soporte informático del
sistema SaaS de Gestión de Mantenimiento
(Rosmiman) implantado en Canal de Isabel II, S.A

Fecha
20/05/2019

Elaborado por
Área de Planificación, Control y
Seguridad

Documento
Pliego de Prescripciones Técnicas

Versión
V01

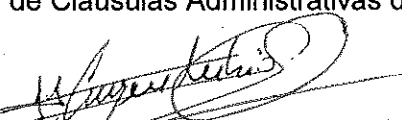
integración, que se englobarán dentro de un proyecto y serán gestionadas como tal, siguiendo la metodología de gestión de proyectos adoptada por Canal de Isabel II, S.A.

2. Consideraciones sociales, ambientales y de innovación.

Debido a la naturaleza del contrato (suministro de nuevas licencias y actualización, soporte y mantenimiento de licencias existentes de software), no aplican como requerimientos específicos las consideraciones sociales, ambientales y de innovación, más allá de lo establecido como condiciones especiales de ejecución en el apartado 9.3 del Anexo I del Pliego de Cláusulas Administrativas Particulares.

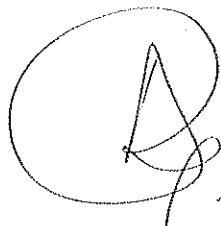
3. Formato de la Oferta técnica

La oferta técnica se atenderá al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.



Firma: Enrique Rubio Donis

AREA PLANIFICACIÓN, CONTROL Y SEGURIDAD



Firma: Ángel Rodríguez García

SUBDIRECCIÓN DE SISTEMAS INFORMÁTICOS



Firma: Pablo Galán González

DIRECCIÓN RECURSOS