

Expediente 58/2026

PLIEGO DE PRESCRIPCIONES TÉCNICAS

CONTRATACIÓN DEL SERVICIO DE SOPORTE Y MANTENIMIENTO DE LAS APLICACIONES SICALWIN, ACCEDE, FIRMADOC CORPORATIVO Y GAC. CONTRATACIÓN Y CONFIGURACIÓN DE AYTOS FACTURA Y MIGRACIÓN A UN ENTORNO CLOUD DE LAS APLICACIONES CONTRATADAS.

1. Antecedentes

A lo largo de los años, EUDEL ha incorporado diversas soluciones de software con el objetivo de digitalizar y optimizar sus procesos internos. En la actualidad, la organización dispone de las siguientes herramientas informáticas contratadas, operativas en modalidad *on-premise* dentro de sus instalaciones:

- SICALWin: Gestión Económico-Financiera
- GAC: Sistema de Gestión de Activos integrado con SicalWin.
- FIRMADOC CORPORATIVO. Portafirmas y gestor de expedientes.
- FIRMADOC PARA SICALWIN.
- ACCEDE: Registro de entrada / salida para EUDEL

Con la entrada en vigor de nuevas obligaciones a nivel de facturación como Batuz/ Ticketbai, se hace necesaria la contratación de un módulo nuevo de facturación que se integre con la aplicación de contabilidad existente, SicalWIN.

A su vez, es necesaria la renovación de los servidores utilizados para albergar estas aplicaciones en el CPD de EUDEL, así como la adquisición de nuevas licencias de Windows Server para su puesta en marcha. Después de una reflexión interna en EUDEL, se ha decidido por la migración de estas aplicaciones a un entorno cloud.

2. Transformación digital en la nube

EUDEL apuesta por la evolución digital con una solución en la nube que le permita gestionar las aplicaciones sin preocupaciones por servidores, actualizaciones o tareas técnicas. Permitiendo a EUDEL enfocarse en la explotación de las

aplicaciones, liberándose de la complejidad del soporte de la infraestructura tecnológica.

La transformación digital incluye las aplicaciones antes descritas y la migración de las mismas a un entorno cloud.

2.1. Alcance funcional del contrato y dimensionamiento de usuarios

El alcance funcional del contrato sería:

- Configuración y parametrización del módulo AYTOSfactura para SICALwin, así como la definición de los distintos circuitos de firma de las facturas.
- Evolución de FIRMADOC a la nueva plataforma COFIRMA
- Activación, migración y configuración de las aplicaciones a un entorno Cloud.

Durante el período de vigencia del contrato, EUDEL contará con una licencia para los siguientes usuarios.

- 5 USUARIOS SICALWin: Gestión Económico Financiera
- 22 USUARIOS FIRMADOC CORPORATIVO
- 22 usuarios para ACCEDE
- 5 USUARIOS FIRMADOC PARA SICALWIN

2.2. Migración al entorno Cloud

Las soluciones en la nube deben ofrecerse en un modelo SaaS (Software as a Service), lo que permitirá su acceso desde un entorno web o mediante un software a EUDEL. La empresa adjudicataria debe asumir las siguientes responsabilidades, eliminando la necesidad de que EUDEL invierta recursos en Mantenimiento de la infraestructura que soportan las aplicaciones.

- Mantenimiento de la infraestructura que soporta las soluciones.
- Monitorización y optimización del rendimiento de los entornos tecnológicos.
- Gestión y aprovisionamiento de servidores físicos y virtuales.
- Suministro y mantenimiento de licencias de software asociadas, como Microsoft Windows Server, Microsoft RDS CAL, SQL Server, Oracle Microsoft Office 365 (opcional).

- Mantenimiento de los centros de datos, incluyendo medidas de seguridad física y energética.
- Administración de bases de datos, con actualizaciones, copias de seguridad y restauraciones.
- Aplicación de parches de seguridad en sistemas operativos e infraestructura tecnológica.
- Implementación de seguridad perimetral, con protección frente a ataques DDoS y detección de intrusiones.
- Gestión de copias de seguridad para bases de datos, sistemas operativos y soluciones contratadas.
- Aprovisionamiento de software adicional para asistencia remota (opción disponible si se acuerda con EUDEL).
- Despliegue de mejoras y actualizaciones de las soluciones en la nube.

2.2.1. Características del Cloud

- Ubicación del Centro de Procesamiento de Datos

La infraestructura y plataformas tecnológicas necesarias para la prestación del servicio estarán alojadas en la Región España.

- Exclusividad y dedicación de recursos

Las bases de datos serán dedicadas, garantizando que ninguna otra entidad ni organismo tendrá acceso compartido a las mismas, reforzando así la seguridad y confidencialidad de la información.

- Plataforma Tecnológica y Seguridad

La plataforma tecnológica se desplegará en alta disponibilidad, garantizando continuidad operativa ante incidencias. Incluirá un núcleo común que incorporará funcionalidades de Autenticación, Autorización y Auditoría, permitiendo el cumplimiento de los requisitos establecidos por la LOPDGDD en materia de protección de datos. Se integrarán controles de acceso y mecanismos de autenticación, así como herramientas de monitorización, registro de actividad, bloqueo de sesiones y control de calidad del código fuente en cumplimiento del Esquema Nacional de Seguridad.

El sistema asegurará un rendimiento eficiente y estable, optimizando el uso de recursos para garantizar una experiencia de usuario adecuada. Se establece el compromiso de que todas las transacciones se ejecutarán en tiempos compatibles con una correcta usabilidad, excluyéndose de dicha medición los retardos atribuibles a servicios externos al sistema.

- **Medidas de Seguridad**

La implementación de medidas de seguridad resulta esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos, así como para prevenir accesos no autorizados y asegurar la recuperación de la información ante posibles incidentes. Para ello, se aplicarán las medidas técnicas y organizativas necesarias, en función del estado de la tecnología, la sensibilidad de los datos tratados y los riesgos a los que puedan estar expuestos, ya sean derivados de acciones humanas o de causas físicas o naturales. Estas medidas tienen como objetivo evitar la alteración, pérdida, acceso o tratamiento no autorizado de los datos, y se alinearán con los estándares internacionales aplicables, como la ISO/IEC 27001 y el Esquema Nacional de Seguridad (ENS), garantizando así un enfoque integral y conforme a las mejores prácticas de seguridad.

- **Medidas de Seguridad Física Diseño seguro**

Los emplazamientos de los centros de datos deben elegirse con sumo cuidado para mitigar los riesgos medioambientales, como inundaciones, condiciones climáticas extremas y actividad sísmica. Las zonas de disponibilidad deben estar construidas de forma que sean independientes y estén físicamente separadas entre sí.

Los centros de datos deben estar diseñados para prever y tolerar errores mientras se mantienen los niveles de servicio. En caso de error, los procesos automatizados deben desviar el tráfico de la zona afectada. Las aplicaciones principales deben implementarse en un estándar N+1, de forma que en caso de que se produzca un error en un centro de datos, haya capacidad suficiente para poder equilibrar la carga del tráfico entre los demás sitios.

Cada zona de disponibilidad debe estar diseñada para que funcione de forma independiente con una alta fiabilidad. Las zonas de disponibilidad estarán conectadas, lo que le permitirá diseñar aplicaciones con facilidad que conmuten por error entre las zonas de disponibilidad sin interrupciones. Los sistemas de alta resistencia y, por tanto, la disponibilidad de los servicios, serán una función del diseño del sistema.

Se monitorizará en todo momento el uso de los servicios para implementar infraestructura con el fin de respaldar los compromisos y requisitos de disponibilidad de la empresa adjudicataria.

- Acceso de los empleados al centro de datos

Se proporcionará acceso físico al centro de datos solo a los empleados autorizados. Todos los empleados que necesiten tener acceso al centro de datos primero deberán solicitar el acceso y proporcionar una justificación empresarial válida. Estas solicitudes se concederán en función del principio de privilegios mínimos

El acceso de terceros lo solicitarán empleados autorizados, que deberán rellenar una solicitud de acceso de terceros y proporcionar una justificación empresarial válida. Estas solicitudes se concederán en función del principio de privilegios mínimos.

El acceso físico a los centros de datos se registrará, se monitorizará y se mantendrá.

Los puntos de acceso físico a las salas de servidores se grabarán con cámaras de televisión de circuito cerrado (CCTV). Las imágenes se conservarán de acuerdo con los requisitos legales y de conformidad.

El acceso físico estará controlado en los puntos de acceso del edificio por personal de seguridad profesional mediante videovigilancia, sistemas de detección de intrusiones y otros recursos electrónicos.

Se instalarán sistemas de detección de intrusiones electrónicos en la capa de datos para monitorizar, detectar y alertar automáticamente al personal acerca de los incidentes de seguridad.

- Administración de recursos

Los activos se administrarán centralmente a través de un sistema de administración del inventario que almacenará y realizará un seguimiento del propietario, la ubicación, el estado, el mantenimiento e información descriptiva de los recursos.

Se clasificará como Críticos los dispositivos de almacenamiento de contenido multimedia usados para almacenar los datos de los EUDEL y, por ello, los tratará como de alto impacto a lo largo de su ciclo de vida. Cuando un dispositivo de almacenamiento llegue al final de su vida útil, se dará de baja mediante las técnicas detalladas en NIST 800-88.

- Energía

Los sistemas de suministro eléctrico de los centros de datos estarán diseñados para que puedan duplicarse y mantenerse por completo sin que ello repercuta en las operaciones, 24 horas al día. Se garantizará que los centros de datos estén equipados con sistemas de suministro eléctrico de reserva para garantizar el suministro a las operaciones en casos de cortes eléctricos para cubrir las cargas más importantes y esenciales de la instalación.

- Condiciones climáticas y temperatura

Los centros de datos usarán mecanismos para controlar las condiciones climáticas y mantener una temperatura de funcionamiento constante para los servidores y otro hardware y, así, impedir el sobrecalentamiento y reducir la posibilidad de que se produzcan interrupciones del servicio

- Detección y extinción de incendios

Los centros de datos estarán equipados con sistemas de detección y de extinción de incendios. Los sistemas de detección de incendios utilizarán sensores de detección de humo en los espacios de redes, mecánicos y de infraestructura.

- Medidas de Seguridad Lógica

El servicio en la nube incorporará los controles de seguridad lógica que garanticen la seguridad de los datos almacenados y proporcionen un acceso seguro y controlado a las aplicaciones publicadas.

Todos los servidores que conformen la plataforma en la nube incorporarán un antivirus que combina protección EDR y EPP en un único agente ligero para endpoints, ofreciendo una defensa avanzada y automatizada.

- Parcheado de sistemas

Los sistemas operativos que conformen la plataforma en la nube estarán actualizados según las recomendaciones del fabricante.

Las actualizaciones se instalarán en entornos controlados de validación y una vez certificados se instalan en los entornos de Producción.

- Monitorización

La monitorización en sistemas aportará visibilidad, control y capacidad de reacción ante el comportamiento de los recursos de TI. Permitirá supervisar en tiempo real el estado, rendimiento y disponibilidad de servidores, aplicaciones, redes y servicios, detectando fallos o anomalías antes de que afecten al usuario final.

La plataforma en la nube estará controlada por una solución integral de monitorización disponible en todo momento (24x7x365). Este sistema de control será operado por un equipo dedicado y especialista en la monitorización de las aplicaciones.

- Copias de Seguridad

La política de Backup de los datos almacenados en la nube se establecerá según la criticidad del recurso y los datos almacenados.

- Backup completo de los últimos 7 días: Se aplica a Servidores de Aplicaciones que no contienen datos tan solo binarios de las aplicaciones y son fácilmente recreables desde una plantilla.

- Backup completo de los últimos 14 días más una foto semanal con rotación de 4 semanas: Servidores de infraestructura que contienen configuración, pero no contienen datos
- Backup completo de los últimos 14 días más una foto semanal con rotación de 54 semanas (1 año): Servidores y repositorios que contienen datos. Se externalizan diariamente a una segunda región geográfica (Irlanda) con una retención de 14 días en esta segunda región.

Adicionalmente, para las bases de datos, se realizará una copia mediante un plan de mantenimiento de SQL Server hacia un Bucket S3 cuya política es la siguiente:

- Backup Full Semanal
 - Backup Diferencial Diario
 - Backup del Log de Transacciones cada 10 minutos
 - Retención 15 días en disco
 - Retención de 14 días y 52 semanas en copia de seguridad en repositorio de copia.
- Requerimientos de conectividad

La conexión a las aplicaciones en la nube será optimizada para usar el mínimo ancho de banda necesario mediante la compresión de datos y optimización del tráfico.

Con el objetivo de reforzar la seguridad y reducir el riesgo de sufrir un ciberataque, el acceso a las aplicaciones en la nube se limitará exclusivamente a direcciones IP ubicadas en territorio español. Para acceder desde el extranjero, será necesario establecer una conexión VPN con la infraestructura on-premise de EUDEL ubicado en España, asegurando que todo el tráfico se redirija a través del túnel VPN para que el acceso a la nube se realice con una IP declarada en España.

3. Cumplimiento Normativo

Los sistemas de información y los servicios de la empresa adjudicataria deben haber sido auditados y encontrados conforme a las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para CATEGORÍA ALTA.

Este certificado aplica a la provisión, migración, administración, mantenimiento y soporte de software, en la modalidad Software como Servicio (SaaS) e instalaciones en EUDEL (On-Premise), necesario para la adecuada prestación de servicios a EUDEL.

4. Continuidad del servicio

4.1. Plan de Recuperación ante Desastres.

La empresa adjudicataria garantizará la continuidad del servicio ante una caída crítica del sistema mediante su Plan de Recuperación ante Desastres. Este plan contemplará varios escenarios evaluados y su objetivo será el de garantizar la continuidad operativa del servicio en la nube en caso de un incidente grave que afecte su infraestructura tecnológica o sus servicios críticos. Esto incluye eventos como fallos de hardware, ciberataques, desastres naturales, errores humanos u otros eventos imprevistos.

- Minimizar el tiempo de inactividad (downtime).
- Recuperar sistemas, datos y servicios esenciales lo más rápido posible.
- Reducir la pérdida de datos mediante copias de seguridad y réplicas.
- Proteger la integridad y confidencialidad de la información.
- Mantener la continuidad del negocio mientras se restauran los servicios.
- Asignar roles y responsabilidades claras en situaciones de crisis.
- Cumplir con normativas legales o contractuales sobre continuidad del negocio.

El RTO (Recovery Time Objective) comprometido en los escenarios evaluados será de 2 horas, mientras que el RPO (Recovery Point Objective) será de 1 hora.

La empresa adjudicataria se compromete a realizar una prueba anual del plan para comprobar su funcionalidad. Una vez completada la prueba, la empresa adjudicataria proporcionará a EUDEL una evidencia de la ejecución de las pruebas de continuidad y contingencia.

5. Protección de Datos y Confidencialidad

5.1. RGDP

En cumplimiento del Reglamento (UE) 2016/679, de 27 de abril (RGPD), y de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), la empresa adjudicataria dispondrá de un Sistema de Gestión de Protección de Datos auditado por una entidad independiente, que garantiza el adecuado cumplimiento de los requisitos legales vigentes. En este marco, se habrán desarrollado acciones de revisión y auditoría orientadas a verificar el cumplimiento íntegro de las obligaciones aplicables, incluyendo la evaluación periódica de las medidas técnicas y organizativas implantadas, la revisión del Registro de Actividades de Tratamiento, la comprobación de la correcta gestión de consentimientos y bases jurídicas, la supervisión de los procedimientos de respuesta ante incidentes de seguridad y la verificación de los acuerdos formalizados con encargados del tratamiento. Asimismo, el Sistema contemplará la adecuada gestión y atención de los derechos de los interesados —acceso, rectificación, supresión, oposición, limitación, portabilidad y demás derechos reconocidos— garantizando su tramitación en los plazos y condiciones previstos por la normativa. Todo ello permitirá asegurar un marco de cumplimiento sólido, actualizado y alineado con los principios de responsabilidad proactiva y mejora continua establecidos por la normativa vigente

5.2. Confidencialidad

La empresa adjudicataria estará obligado a mantener la plena confidencialidad y secreto, con respecto a la información manejada durante la ejecución del contrato. Esta obligación tendrá una duración de 5 años desde el conocimiento de esa información, salvo que en el presente pliego o en el contrato correspondiente, se determine un plazo mayor.

La empresa adjudicataria tratará con la máxima reserva todos y cada uno de los aspectos de la información implicada, no pudiendo comunicarlos o cederlos a terceros salvo que este previamente autorizado por EUDEL.

Todas las personas que intervengan en cualquier fase del proceso de contratación estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

La empresa adjudicataria dispondrá de acuerdos con todos los proveedores implicados, y específicamente mantendrá encargos y contratos de confidencialidad, y exigirá que sus usuarios con acceso a los datos, formalicen contratos de confidencialidad, los cuales son requeridos y revisados.

Todos los procesos asociados a la obligación de confidencialidad serán revisados, en base al proceso de verificación de medidas de seguridad del Esquema Nacional de Seguridad – Real Decreto 311/2022.

La empresa adjudicataria no copiará, ni reproducirá, ni comunicará o exhibirá, ningún elemento, información, documento y análogos, que le haya sido entregados para la prestación o que debiera generar para la ejecución del servicio.

A todos los efectos quedan sometidos a confidencialidad, los datos personales de los que es responsable EUDEL y cuanta información institucional y de carácter interno y organizativo, no sometida a publicidad actividad, se vea implicada.

6. Garantía de acceso a la información

Cuando EUDEL lo requiera, la empresa adjudicataria quedará obligado a garantizar el ejercicio de los derechos de acceso por parte de los ciudadanos o empresas, mediante el uso de formatos estandarizados de datos que cumplan los requisitos establecidos en el Esquema Nacional de Interoperabilidad:

- Los documentos y servicios de administración electrónica que se pongan a disposición de los ciudadanos o de otras Administraciones Públicas deben ser visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos o empresas por razón de su elección Tecnológica
- Se adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida.
- Los documentos electrónicos se conservarán en el formato en el que hayan sido elaborados, enviados o recibidos, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido de los documentos, de la firma electrónica y de los metadatos que lo acompañan. Así mismo, la empresa adjudicataria garantizará la capacidad de integración del sistema objeto del presente contrato sobre aquellos otros sistemas de gestión y producción administrativa con los que el EUDEL pueda operar, tales como el Gestor Documental, para lo que tendrá en consideración los webservices (propios y ajenos) que permitan esta integración de forma coherente, sencilla y transparente, garantizando esta integración

7. Portabilidad de la información. Reversión del sistema

La empresa adjudicataria dispondrá de una política alineada con el Esquema Nacional de Seguridad y la normativa vigente en materia de protección de datos, que regula la devolución, transferencia y/o eliminación de la información gestionada en sus sistemas.

Los datos almacenados en la plataforma en la nube son y seguirán siendo en todo momento propiedad exclusiva del EUDEL. En el momento de la resolución del contrato o finalización del Servicio, La empresa adjudicataria entregará a EUDEL, o a la persona o entidad que éste designe, la totalidad de los datos, junto con la información técnica y de configuración del Sistema, en un formato exportable y estructurado, que permita a EUDEL su conservación en sus propios sistemas o, en su caso, la migración a un nuevo proveedor sin pérdida de información.

La empresa adjudicataria garantizará que la transferencia de los datos y el control del Sistema se realicen en un plazo máximo de un mes desde la solicitud de EUDEL.

Asimismo, EUDEL se reserva el derecho a exigir la transferencia de los servicios a un nuevo proveedor cuando considere que la prestación no cumple los niveles de servicio (SLA) o condiciones funcionales y operativas acordadas, basándose en los informes o incidencias comunicadas durante la ejecución del Servicio.

8. Actualización Continua y Cumplimiento Normativo

La suscripción en la nube garantizará que la plataforma esté siempre actualizada y en óptimas condiciones de funcionamiento, sin necesidad de intervención por parte de EUDEL.

Funcional: La plataforma se actualizará de forma continua y automática para mejorar su rendimiento, eficiencia y usabilidad. Estas mejoras se implementarán directamente en el entorno de producción de manera transparente, asegurando siempre el acceso a la versión más avanzada de la solución.

Legal: Ante cualquier cambio en normativas de obligado cumplimiento, la plataforma se adaptará de forma automática, garantizando que siempre esté alineada con la legislación vigente sin requerir instalaciones adicionales ni intervenciones manuales.

Correctivo: Cualquier incidencia o error detectado se corregirá con prioridad según su impacto. Gracias a la arquitectura en la nube, las correcciones se aplicarán de forma remota, minimizando el impacto en el servicio y asegurando su disponibilidad constante.

9. Espacio de clientes y soporte al usuario en la nube

La empresa adjudicataria pondrá a disposición de EUDEL un espacio de clientes con los siguientes servicios:

- Registro y seguimiento de solicitudes a través de tickets
- Permitirá registrar consultas o incidencias aportando la máxima información para poder solucionar las peticiones.
- Este modelo permitirá un soporte disponible las 24 horas.
- Cualquier consulta o incidencia se registrará a través de la apertura de un ticket en el sistema que permitirá hacer seguimiento y trazabilidad.
- Cualquier cambio en la gestión de los asuntos reportados se comunicará vía correo electrónico y en caso de ser necesario, se contactará con la entidad por teléfono.
- EUDEL, a través del Espacio de Clientes podrá modificar y actualizar sus datos en cualquier momento. Solo el/los Administrador/es de EUDEL podrán cambiar o eliminar datos de todos los usuarios registrados para su organización, además de gestionar las altas y bajas de usuarios.
- EUDEL será el responsable de solicitar las altas y bajas de usuarios a través del Espacio Clientes, siguiendo los procedimientos y canales establecidos para tal fin.
- El Espacio de Clientes integrará un Centro de Recursos con información actualizada y autogestionable, que complementará la formación continua y la comunicación con las entidades.

Contendrá:

- Comunicaciones oficiales sobre el servicio y las actualizaciones.
- FAQs, manuales de usuario y boletines informativos.
- Materiales formativos y documentación técnica de referencia.