CONTR_2025_499992 : CONTRATACIÓN DE SERVICIOS IAAS DE COMPUTACIÓN GPU PARA LA AGENCIA DE MEDIO AMBIENTE Y AGUA DE ANDALUCÍA, M.P.

PLIEGO DE PRESCRIPCIONES TÉCNICAS

JOSE RAMON MARTINEZ ALVAREZ		04/12/2025 10:49:28	PÁGINA: 1 / 17
VERIFICACIÓN	NJyGw0veIk8l58MuhQZCS4I630BTx4	https://ws050.juntadeandalucia.es/verificarFirma/	

Índice

1 Antecedentes....3
2 Objeto....3
3 Requerimientos del servicio....4
3.1 Infraestructura IaaS y recursos a demanda....4
3.1.1 Requisitos de capacidad y rendimiento....4
3.1.2 Requisitos mínimos de disponibilidad y consumo garantizado de recursos....4
3.1.3 Almacenamiento....5
3.1.4 Entorno de trabajo....5
3.1.5 Ejecución de procesos personalizados (jobs)....5
3.1.6 Red y conectividad....6
3.1.7 Escalabilidad y uso bajo demanda....7
3.1.8 Transferencia de archivos....7
3.1.9 Gestión de identidades y accesos....8
3.1.10 Monitorización del consumo....8
3.1.11 Acuerdo de Nivel de Servicio (ANS)....8
3.1.12 Soporte técnico....8
4 Lugar de ejecución....9
5 Plazo de ejecución....9
6 Puesta en marcha del servicio....9
7 Condiciones generales....9
7.1 Información de base y herramientas de soporte al servicio....9
7.2 Confidencialidad de la información....10
7.3 Lugar de trabajo y medios necesarios....11
7.4 Propiedad intelectual de los trabajos....11
7.5 Seguridad....11
7.6 Rediseño funcional y simplificación de procedimientos administrativos....12
7.7 Definición de procedimientos administrativos por medios electrónicos....12
7.8 Uso de certificados y firma electrónica....13
7.9 Verificación de documentos firmados electrónicamente....13
7.10 Interoperabilidad....13
7.11 Disponibilidad pública del software....14
7.12 Gestión de usuarios y el control de accesos....14
7.13 Uso de infraestructura tic y herramientas corporativas....15
7.14 Conformidad con los marcos metodológicos de desarrollo de software de la junta de andalucía....15
7.15 Accesibilidad....16
7.16 Normalización de fuentes y registros administrativos....16
7.17 Cláusula sobre apertura de datos....16
7.18 Cláusula sobre apertura de servicios....16
7.19 Prevención de riesgos laborales....17

1 Antecedentes

Actualmente la Agencia de Medio Ambiente y Agua de Andalucía (en adelante la Agencia) no cuenta capacidad para procesamiento GPU (Unidades de Procesamiento Gráfico) necesaria para el desarrollo y entrenamiento de modelos de aprendizaje automático y Deep Learning (Aprendizaje Profundo), basados en imágenes satelitales multiespectrales.

El presente pliego de prescripciones técnicas tiene como objetivo establecer los requisitos para la contratación por parte de la Agencia de servicios de procesamiento GPU en la nube, concretamente mediante el acceso a servicios Iaas (Infrastructure as a Service). El propósito de este contrato es brindar el soporte necesario para el desarrollo de una línea de trabajo centrada en la explotación y análisis de datos ambientales e imágenes satelitales utilizando técnicas de Ciencia de Datos, en particular Aprendizaje Automático y Deep Learning. Esto permitirá automatizar la identificación y análisis, a partir de imágenes satelitales, de entidades con características ambientales de interés (hábitats, usos del suelo, datos climáticos, tipos de vegetación, áreas incendiadas, etc).para la gestión ambiental y para la ayuda a la toma de decisiones informadas.

Estos modelos, adaptados a la adquisición de imágenes a las características espaciales y temporales específicas de cada temática, podrán llegar a permitir actualizaciones semanales de las entidades identificadas.

Por tanto, para lograr este objetivo, es fundamental contar con una capacidad de una infraestructura procesamiento GPU adecuada que permita automatizar el entrenamiento de modelos de Deep Learning a partir de imágenes satelitales y posteriormente seleccionar aquel que ofrezca el mejor rendimiento en términos de precisión y eficiencia de acuerdo a las necesidades.

La contratación mediante IaaS permite la configuración de equipos personalizados de acuerdo a las necesidades de procesamiento, almacenaje y memoria que se requieran en cada momento.

2 Objeto

El objeto del presente Pliego de Prescripciones Técnicas es establecer los requisitos y regular la contratación de una solución de Infraestructura como Servicio (IaaS) que permita el aprovisionamiento y gestión de recursos de cómputo, incluidas instancias con GPU de alto rendimiento, almacenamiento escalable y red segura. Se deberá incluir, ade-

más, la habilitación de un sistema que permita un consumo de recursos flexible y bajo demanda, así como las condiciones de soporte, Acuerdos a Nivel de Servicio (ANS) y seguridad exigidas para la prestación del servicio.

3 Requerimientos del servicio

3.1 Infraestructura IaaS y recursos a demanda

El adjudicatario deberá garantizar que el servicio ofertado cumpla, como mínimo, con los siguientes requisitos técnicos de capacidad, escalabilidad y personalización en los recursos de cómputo ofrecidos a través de su plataforma de infraestructura como servicio (IaaS):

3.1.1 Requisitos de capacidad y rendimiento

1. **Disponibilidad de instancias con GPU de alto rendimiento** (NVIDIA, AMD u otras), adecuadas para cargas intensivas de entrenamiento de modelos deep learning y/o análisis y masivo de datos.

2. **Configuraciones escalables** en CPU, GPU, RAM y almacenamiento, ajustables según demanda.

3. **Instancias con arquitectura avanzada** de 1 a 8 GPUs, con memoria por GPU entre 24 y 96 GB, orientadas a cargas de IA intensiva.

4. **Instancias generales con** 1 a 96 vCPU y 64 a 512 GB de RAM

5. **Capacidad para iniciar instancias personalizadas** dentro de los rangos definidos en los puntos anteriores.

6. A fin de acreditar el cumplimiento de los requisitos técnicos establecidos en este apartado, el licitador deberá disponer de un catálogo de instancias que cubra, como mínimo, los rangos especificados. Este catálogo deberá reflejar la variedad de configuraciones disponibles en su plataforma de IaaS.

3.1.2 Requisitos mínimos de disponibilidad y consumo garantizado de recursos

7. Durante la vigencia del servicio contratado, el adjudicatario deberá garantizar, como mínimo, la disponibilidad y posibilidad de uso efectivo de los siguientes recursos computacionales.

    - **Instancia de referencia 1:** Al menos 2000 horas de uso efectivo de una instancia con las

siguientes características mínimas: 48 vCPUs, 192 GB de RAM, 4 GPUs con 24 GB de memoria cada una, y al menos 2 TB de almacenamiento SSD/M.2 o equivalente por instancia. Deberá ser posible el uso simultáneo de al menos 3 instancias de estas características. En caso de utilizarse instancias con diferentes capacidades, las horas computadas se ajustarán proporcionalmente al diferencial de características respecto a esta instancia patrón. Las horas de uso serán ajustables proporcionalmente si se usan instancias con diferentes capacidades dentro los rangos de características especificados en el apartado 4.1.1.

- **Instancia de referencia 2:** garantía uso de instancias con un mínimo de 48 vCPUs, 512 GB de RAM (sin GPU) y 2 TB de almacenamiento SSD/M.2 o equivalente. Se deberá permitir el uso simultáneo de al menos 3 instancias de estas características.

- **Instancia de referencia 3:** garantía uso de instancias con 48 vCPUs, 192 GB de RAM, 8 GPUs con 80 GB de memoria cada una, y al menos 2 TB de almacenamiento SSD/M.2 o equivalente por instancia.

3.1.3 Almacenamiento

8. Almacenamiento SSD escalable, mínimo 30 TB independiente del almacenamiento local de las instancias.

9. Opciones de backup, snapshots o almacenamiento redundante.

3.1.4 Entorno de trabajo

El entorno ofertado deberá incluir herramientas que faciliten a los usuarios trabajar con datos, desarrollar y ejecutar código personalizado, y gestionar sus cargas de trabajo. En particular, se deberán cumplir los siguientes requisitos:

10. El servicio deberá permitir lanzar instancias con Jupyter Lab preinstalado y funcional desde el primer uso.

11. Los usuarios deberán poder instalar librerías propias, ejecutar terminales de sistema, y trabajar con múltiples kernels.

12. Cuando las instancias dispongan de GPU, Jupyter Lab deberá estar configurado para aprovechar su capacidad.

3.1.5 Ejecución de procesos personalizados (jobs)

El entorno deberá soportar la ejecución de **jobs definidos por el cliente**, permitiendo el procesamiento autónomo de cargas computacionales diversas, mediante los siguientes mecanismos:

13. **Lanzamiento de jobs personalizados**: El sistema deberá permitir la ejecución de scripts, contenedores, binarios o notebooks definidos por el cliente, sin necesidad de ajustarse a flujos de trabajo predefinidos por el proveedor.

14. **Ejecución aislada, programable y escalable**: Cada job deberá ejecutarse en un entorno aislado y podrá ser configurado para lanzarse manualmente, de forma programada, o como respuesta a eventos. Se valorará el soporte para ejecución en lote, planificación periódica o colas de trabajos.

15. **Asignación dinámica de recursos**: El sistema deberá permitir que cada job especifique los recursos necesarios (CPU, GPU, RAM, almacenamiento), y aprovisionar automáticamente los recursos correspondientes. Una vez finalizada la ejecución, los recursos deberán ser liberados de forma automática para optimizar el uso de la infraestructura.

16. **Interfaces de control abiertas**: El lanzamiento y gestión de los jobs deberá ser posible a través de interfaces estándar como CLI, API o SDK, facilitando la integración con herramientas propias del cliente o terceros.

17. **Soporte para contenedores e imágenes personalizadas**: El sistema deberá admitir la ejecución de jobs sobre contenedores o imágenes previamente definidas por el cliente, garantizando la portabilidad y la replicabilidad de entornos.

18. **Asistencia técnica especializada**: El adjudicatario deberá proporcionar asistencia técnica específica para la definición, despliegue y optimización de jobs, incluyendo:

    - Apoyo en la configuración de entornos de ejecución.
    - Asesoramiento sobre buenas prácticas en la preparación y lanzamiento de cargas de trabajo.
    - Resolución de incidencias en la ejecución de procesos.
    - Acompañamiento en el diseño de cargas complejas, distribuidas o de alto volumen.

3.1.6 Red y conectividad

El servicio ofertado deberá garantizar unas condiciones de red y conectividad adecuadas para el tipo de cargas intensivas previstas, así como unos niveles de seguridad y disponibilidad acordes a un entorno de misión crítica.

19. **Alta disponibilidad y ancho de banda garantizado**: La infraestructura deberá disponer de conectividad redundante y mecanismos de alta disponibilidad para garantizar el flujo continuo de datos. El ancho de banda deberá permitir la transferencia sostenida de grandes volúmenes de información sin cuellos de botella, tanto en operaciones de entrada como de salida.

20. **Red interna segura**: Se deberá garantizar la existencia de una red privada lógica (por ejemplo, mediante VPC o segmentación equivalente), de uso exclusivo por el adjudicatario para la ejecución de sus cargas de trabajo. Esta red deberá contar con cortafuegos configurables, reglas de acceso granulares, y herramientas de control de tráfico que permitan prevenir accesos no autorizados, ataques de red o movimientos laterales no deseados.
21. **Redundancia geográfica y tolerancia a fallos**: El sistema deberá contar con mecanismos de conmutación automática entre regiones o zonas de disponibilidad en caso de incidente mayor. Se deberá garantizar que ante la caída de una zona, los servicios pueden ser restaurados sin intervención manual y sin pérdida de datos o interrupción prolongada.
22. **Baja latencia y fiabilidad**: Se deberá asegurar una latencia mínima en las comunicaciones internas (entre instancias y servicios de almacenamiento/red) y una fiabilidad suficiente para operaciones en tiempo real o cuasi tiempo real.
23. **Cumplimiento normativo**: El entorno de red y seguridad deberá estar certificado, o demostrar conformidad, con estándares reconocidos internacionalmente en materia de seguridad de la información y gestión de servicios, tales como ISO/IEC 27001, el Esquema Nacional de Seguridad (ENS), o equivalentes.

3.1.7 Escalabilidad y uso bajo demanda

El sistema deberá permitir que el usuario final tenga un control directo y autónomo sobre los recursos computacionales que utiliza. Esto incluye la capacidad de:

24. Iniciar o detener instancias en cualquier momento, sin intervención del proveedor.
25. Escalar verticalmente o redimensionar las instancias en términos de CPU, GPU, RAM y almacenamiento, según las necesidades del momento.
26. Programar dichas acciones o realizarlas bajo demanda, utilizando mecanismos nativos de la plataforma o herramientas complementarias proporcionadas por el adjudicatario.
27. Las funcionalidades indicadas deberán estar accesibles mediante una interfaz de usuario (panel de control) y mediante interfaces programables (CLI/API/SDK).

3.1.8 Transferencia de archivos

El servicio deberá proporcionar medios seguros y eficientes para la transferencia de archivos hacia y desde el entorno IaaS. En concreto:

28. Se deberán habilitar protocolos como SFTP o alternativas equivalentes, que permitan la subida y descarga de grandes volúmenes de datos.
29. Todas las transferencias deberán estar cifradas en tránsito mediante mecanismos robustos como TLS o SSH.
30. Se valorará positivamente el soporte para montajes de almacenamiento remoto o compartido entre instancias.

3.1.9 Gestión de identidades y accesos

El sistema deberá incorporar mecanismos avanzados de

31. **Gestión centralizada de identidades**: creación, modificación y revocación de cuentas y roles de usuario.
32. **Control de acceso basado en roles (RBAC)**: asignación granular de permisos a usuarios, grupos o servicios.
33. **Autenticación multifactor (MFA)** obligatoria para cuentas con privilegios administrativos.
34. **Registro de actividad (auditoría)**: trazabilidad completa de accesos, acciones administrativas y operaciones críticas.
35. **Delegación de administración**: posibilidad de otorgar permisos administrativos limitados.
36. **Gestión de sesiones**: políticas configurables de expiración por inactividad o tiempo.
37. **Sistema de alertas**: notificaciones en caso de accesos no autorizados, errores repetidos de autenticación u otros eventos críticos.

3.1.10 Monitorización del consumo

38. El sistema deberá contar con un panel de control donde se visualicen, en tiempo real o con refrescos frecuentes, los consumos de recursos (CPU, GPU, almacenamiento, red).
39. Los datos deben ser accesibles al menos al administrador del sistema y exportables a formatos estándar.
40. Deberán establecerse umbrales configurables de consumo, que generen alertas (correo electrónico, SMS o panel).
41. Se valorará la existencia de mecanismos automáticos de restricción o suspensión del servicio al superar ciertos límites, previa configuración por parte del cliente.

3.1.11 Acuerdo de Nivel de Servicio (ANS)

42. El adjudicatario deberá garantizar un ANS mínimo del **99,9% mensual** de disponibilidad del servicio para los componentes críticos del sistema: infraestructura IaaS, panel de gestión, servicios de red y almacenamiento.
43. En caso de incumplimiento del ANS, se deberán establecer **mecanismos compensatorios automáticos**: descuentos en facturación, extensión del servicio, entre otros.

3.1.12 Soporte técnico.

El adjudicatario deberá proporcionar un soporte técnico acorde al nivel de criticidad de la infraestructura:

44. Se establecerán reuniones periódicas (al menos una semanalmente de aproximadamente una hora) entre la dirección técnica de la entidad contratante y el equipo asignado por el adjudicatario, con el fin de revisar la evolución del servicio y tratar puntos relacionados con:
    - La orientación activa en el uso eficiente de los recursos, incluyendo recomendaciones para optimi-

zar el consumo de instancias o evitar costes innecesarios.

- Soporte técnico específico para la resolución de incidencias, configuraciones avanzadas o personalizadas, y asistencia en la puesta en marcha de proyectos concretos dentro de la plataforma

45. El soporte estará disponible mediante múltiples canales (teléfono, sistema de tickets, chat) diferenciando niveles de prioridad y urgencia.
46. Se ofrecerá atención 8x5 para incidencias críticas que afecten la disponibilidad o integridad del servicio.

4Lugar de ejecución

A los efectos de la presente licitación, se entenderá que el lugar de ejecución del servicio de infraestructura como servicio (IaaS) será el territorio donde el contratante reciba y utilice efectivamente los servicios de infraestructura tecnológica con independencia del lugar donde se ubiquen físicamente los recursos técnicos del adjudicatario. La prestación se considerará ejecutada en el lugar en que el poder adjudicador reciba efectivamente el servicio.

5 Plazo de ejecución

La duración del contrato será de 18 meses a partir de la firma de la Orden de Inicio.

6Puesta en marcha del servicio

El servicio deberá estar perfectamente funcional bajo los requisitos establecidos en este pliego en el plazo de un mes desde la firma del contrato.

7 Condiciones generales

7.1 Información de base y herramientas de soporte al servicio

LA AGENCIA facilitará al contratista cuanta información disponga relacionada con las materias objeto del presente trabajo.

Toda la información que se proporcione, es propiedad de LA AGENCIA y no podrá ser utilizada en futuros trabajos ya sea como referencia o como base de los mismos, a menos que se cuente con la autorización expresa por escrito de LA AGENCIA.

El contratista podrá hacer propuestas sobre cualquiera de las herramientas de soporte al servicio mencionadas, siempre y cuando supongan una mejora en la productividad y calidad del servicio. Para que los cambios propuestos se lleven a efecto, previamente deben ser aprobados por LA AGENCIA.

7.2 Confidencialidad de la información

Sin perjuicio de lo indicado en el pliego de cláusulas administrativas que rige al contrato, la información a la que tenga acceso el contratista como consecuencia del contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de LA AGENCIA.

El contratista además, en cumplimiento de la “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”, únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones de LA AGENCIA, y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas.

Además, tendrá que cumplir las medidas técnicas y organizativas estipuladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el "Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal". En el caso de que la empresa, o cualquiera de sus miembros, destinen los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas.

7.3 Lugar de trabajo y medios necesarios

La prestación del servicio se realizará preferentemente desde las instalaciones del contratista, salvo en determinadas circunstancias donde se aconseje la actuación presencial a requerimiento del Director de Proyecto de LA AGENCIA. Los medios físicos (cualquier equipo físico que se requiera para la prestación del servicio) y lógicos (licencias de desarrollo, sistemas operativos u ofimáticos, etc.) correrán por cuenta del contratista.

La infraestructura de comunicaciones necesaria para la prestación del servicio será la que recomiende la Red Corporativa de la Junta de Andalucía. En todo caso, el coste de estos servicios de comunicaciones será por cuenta del contratista.

Para facilitar la comunicación entre el Equipo de Trabajo del contratista y el de LA AGENCIA, será imprescindible el uso de un sistema de videoconferencia que será provisto por LA AGENCIA. El coste de estos servicios podrá ser repercutido al contratista.

7.4 Propiedad intelectual de los trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de LA AGENCIA, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el contratista autor material de los trabajos. El contratista renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de LA AGENCIA, específicamente todos los derechos de explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente a LA AGENCIA.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

7.5 Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el 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. En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes, considerando que el sistema de información recae en la categoría de seguridad de nivel BAJO.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

Se atenderá también a la normativa interna de LA AGENCIA en materia de Seguridad TIC.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccncert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.

7.6 Rediseño funcional y simplificación de procedimientos administrativos

Con carácter general se deberá tener en consideración que la aplicación de medios electrónicos a la gestión de los procedimientos será precedida de la realización de un análisis de rediseño funcional y simplificación, en el marco del objetivo de simplificación de los procedimientos administrativos que persigue la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y lo dispuesto en su artículo 75.2, y de la promoción de la aplicación del principio de simplificación en la presentación de escritos y documentos y en la tramitación de los expedientes que se realicen a través de redes abiertas de telecomunicación, de acuerdo con el artículo 5.4 del Decreto 183/2003, de 24 de junio, por el que se regula la información y atención al ciudadano y la tramitación de procedimientos administrativos por medios electrónicos (Internet).

Para ello se considerará el Manual de Simplificación Administrativa y Agilización de Trámites de la Administración de la Junta de Andalucía, aprobado por Orden de 22 de febrero de 2010 (BOJA núm. 52 de 17 de marzo) disponible en la siguiente dirección:

https://ws024.juntadeandalucia.es/ae/extra/manualdesimplificacion

7.7 Definición de procedimientos administrativos por medios electrónicos

La definición de los procedimientos deberá realizarse conforme a los conceptos y términos expresados en el documento Dominio Semántico del Proyecto w@ndA (ISBN 84-688-7845-6) disponible en la web de soporte de administración electrónica de la Junta de Andalucía. La citada web está accesible en la siguiente dirección:

http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

7.8 Uso de certificados y firma electrónica

Para la identificación y firma electrónica mediante certificados electrónicos se atenderán las guías y directrices indicadas en el apartado correspondiente a la plataforma @firma en la web de soporte de administración electrónica de la Junta de Andalucía, en particular en lo relativo a la no utilización de servicios y componentes obsoletos, de custodia de documentos en la plataforma o cuya desaparición esté prevista para futuras versiones, a formatos de firma electrónica y la realización de firmas electrónicas diferenciadas y verificables para cada documento, realizándose en su caso las oportunas actuaciones de adecuación de las funcionalidades actualmente existentes en los sistemas incorporados en el objeto de la contratación. La citada web está accesible en la siguiente dirección:

http://www.juntadeandalucia.es/haciendayadministracionpublica/ae

Se utilizarán los servicios provistos por la implantación corporativa de la plataforma @firma gestionada por la Consejería competente en materia de administración electrónica.

7.9 Verificación de documentos firmados electrónicamente

Para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad, en el marco del artículo 27.3.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el artículo 42.b) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y el apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico, se utilizará la Herramienta Centralizada de Verificación, de acuerdo con el protocolo técnico disponible en el apartado correspondiente de la web de soporte de administración electrónica de la Junta de Andalucía.

7.10 Interoperabilidad

El presente contrato cumplirá con lo indicado en la normativa que sobre el Marco de Interoperabilidad digital haya dictado la Junta de Andalucía y por la que se pretende la normalización de los formatos, protocolos e interfaces que permitan garantizar el principio de neutralidad tecnológica, la interoperabilidad de los servicios y Sistemas de Información entre administraciones, así como la preservación del conocimiento general y la gestión eficaz y eficiente del uso de las TIC.

El sistema implantará los protocolos ENIDOCWS y ENIEXPWS para que los documentos y expedientes electrónicos que se gestionen en el mismo puedan, a partir de sus códigos seguros de verificación, ser puestos a disposición e interoperar de manera estandarizada con otros sistemas y repositorios electrónicos de la Junta de Andalucía, así como remitirse a otras Administraciones si procede.

También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio de información con la ciudadanía, otras Administraciones Públicas y entidades, publicados en el Centro de Interoperabilidad Semántica de la Administración (CISE) que resulten de aplicación.

7.11 Disponibilidad pública del software

De conformidad con lo establecido en la orden de 21 de febrero de 2005, sobre disponibilidad pública de los programas informáticos de la administración de la Junta de Andalucía y de sus organismos autónomos, el sistema de información desarrollado pasará a formar parte del repositorio de software libre de la Junta de Andalucía, en las condiciones especificadas en la citada orden. La empresa adjudicataria deberá entregar el código fuente del sistema de información desarrollado, así como la documentación asociada y la información adicional necesaria, en un formato directamente integrable en el repositorio de software libre de la Junta de Andalucía. De esta obligación quedarán exentos todos aquellos componentes, productos y herra-

mientas que no habiéndose producido como consecuencia de la ejecución del contrato, estén protegidos por derechos de propiedad intelectual o industrial que no permitan la libre distribución o el acceso al código fuente.

La aplicación desarrollada será publicada en el repositorio de software libre de la Junta de Andalucía; viniendo acompañada además, junto con el software, de la documentación completa, en formato electrónico, referente tanto al análisis y descripción de la solución así como del correspondiente manual de usuario, con objeto de que este software pueda fácilmente ser usable.

7.12 Gestión de usuarios y el control de accesos

A. En el caso de que el sistema realice el tratamiento de datos personales.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar, se tendrán en cuenta las estipulaciones que sobre seguridad hace la legislación vigente en materia de tratamiento de datos personales (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) así como de la legislación nacional vigente en materia de protección de datos, y el Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre. En particular, se perseguirá:

- La correcta identificación de los usuarios (medida op.acc.1 del anexo II del ENS).
- La adecuada gestión de derechos de acceso (medida op.acc.4).
- La correcta selección e implantación de los mecanismos de autenticación (medida op.acc.5).

B. En cualquier caso.

En virtud de lo establecido en el artículo 14.4 del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del 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, para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso y de qué tipo son éstos. El certificado electrónico podrá utilizarse como medio de autenticación de usuarios, si bien no de modo exclusivo, debiéndose disponer de un medio de autenticación alternativo a su utilización, de acuerdo a las consideraciones establecidas en el anexo II del ENS.

C. En relación con las directrices corporativas que se creen en materia de gestión de identidades.

En todo lo relativo a la implementación de la funcionalidad de gestión de usuarios y control de accesos del sistema de información a desarrollar(roles, gestión de login y password,....) se deberán respetar las directrices que la Junta de Andalucía elabore en lo referente a la gestión de identidades y en su caso, adaptándose a la solución de single sign-on que la Junta haya provisto. Dichas Directrices se proporcionarán con la suficiente antelación, aportando la documentación técnica existente para tal fin.

7.13 Uso de infraestructura tic y herramientas corporativas

Se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la Junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización. Se considerarán, entre otras, las siguientes:

- Para el modelado y tramitación de los flujos de trabajo ligados a procedimientos administrativos se deberá utilizar el tramitador TREW@ y herramientas asociadas (eximiéndose de esta obligación en El certifiel caso de flujos de trabajo que no estén ligados a procedimientos).
- @firma: la plataforma corporativa de autenticación y firma electrónica para los procedimientos administrativos, trámites y servicios de la Administración de la Junta de Andalucía.
- Autoridad de Sellado de Tiempo de la Junta de Andalucía.
- @ries: el registro unificado de entrada/salida.
- notific@: prestador de servicios de notificación.
- LDAP del correo corporativo para la identificación y autenticación de usuarios, hasta que se produzca la implantación definitiva del Directorio Corporativo de la Junta de Andalucía.
- port@firma: gestor de firma electrónica interna, etc.

7.14 Conformidad con los marcos metodológicos de desarrollo de software de la junta de andalucía.

Durante la realización de los trabajos se tendrán en cuenta los recursos proporcionados por los marcos metodológicos vigentes de desarrollo de software en la Junta de Andalucía, así como las pautas y procedimientos definidos en éstos.

7.15 Accesibilidad

Todos los sitios webs y aplicaciones para dispositivos móviles desarrollados o que sean mejorados de manera significativa en el marco del presente contrato deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

En este ámbito se deberán cumplir lo establecido por el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. En particular, se deberán cumplir los requisitos pertinentes de la norma EN 301 549 V1.1.2 (2015-04) o de las actualizaciones de dicha norma, así como de las normas armonizadas y especificaciones técnicas en la materia que se publiquen en el Diario Oficial de la Unión Europea y/o hayan sido adoptadas mediante actos de ejecución de la Comisión Europea.

7.16 Normalización de fuentes y registros administrativos

Con la finalidad de asegurar la compatibilidad e interoperabilidad con otras fuentes y registros administrativos, el tratamiento de variables demográficas (sexo, edad, pais de nacimiento, nacionalidad, estado civil, composición del hogar), geográficas (país, región y provincia, municipio y entidad de población, dirección, coordenadas) o socioeconómicas (situación laboral, situación profesional, ocupación, sector de actividad en el empleo, nivel más alto de estudios terminado) que se haga en el sistema seguirá las reglas para la normalización en la codificación de variables publicadas por el Instituto de Estadística y Cartografía de Andalucía accesibles a través de la URL: http://www.juntadeandalucia.es/institutodeestadisticaycartografia/ieagen/sea/normalizacion/ ManNormalizacion.pd

7.17 Cláusula sobre apertura de datos

El diseño y desarrollo informático deberá facilitar el acceso y descarga de todos los datos existentes en la aplicación, así como posibilitar su publicación en el Portal de Datos Abiertos de la Junta de Andalucía. Los datos se proporcionarán en formatos estructurados, abiertos e interoperables, de acuerdo con la normativa vigente de publicidad y reutilización de información pública Los sistemas de información desarrollados deberán permitir la descarga de todos los datos en bruto y desagregados en varios formatos no propietarios como, por ejemplo, CSV, JSON, XML o también un estándar de facto como EXCEL (de las tablas que constituyan el núcleo de la aplicación, así como las tablas auxiliares para su interpretación) preferiblemente mediante API REST (interfaz de programación de aplicaciones), basado en estándares abiertos que permitirá el acceso automático a los datos y en tiempo real. Si los anteriores conjuntos de datos contienen información de carácter personal, se realizarán la extracción de datos mediante un proceso de disociación o anonimización que garantice el cumplimiento de la Ley de Protección de Datos.

7.18 Cláusula sobre apertura de servicios

Las ofertas presentadas deberán estar orientadas a la estrategia “API First”, teniéndose en cuenta la necesidad de definir y publicar servicios comunes que puedan ser consumidos desde varios canales, sistemas u organismos. Este enfoque está basado en definir en la fase inicial una API de servicios externos e internos de la organización o sistema, para que los distintos interlocutores y canales puedan utilizar los servicios de la API en cuanto se publique. La especificación OpenAPI (OAS) define un estándar para la descripción de APIs REST, que permite tanto a humanos como a servicios de integración descubrir y entender las capacidades y características de un servicio sin necesidad de acceder a los detalles de implementación del código fuente, documentación técnica, o detalles del tráfico de mensajes. Los servicios definidos apropiadamente a partir del estándar OpenAPI, permiten que un consumidor pueda entender e interactuar con un servicio remoto a partir de una implementación mínima. En concreto, la definición de los servicios de la API se realizará cumpliendo las especificaciones OpenAPI establecidas por dicha organización (OAS). En relación a los estándares a emplear en el marco del presente contrato, las ofertas deben garantizar el cumplimiento y utilización del estándar y normas establecidas por OpenAPI, en los casos que fuese necesario.

7.19 PRevención de riesgos laborales

La empresa adjudicataria estará obligada a cumplir los requisitos y obligaciones exigidos en materia de Seguridad y Salud Laboral establecidos en la normativa vigente de prevención de riesgos laborales, y en especial en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales y en el Real Decreto 171/2004,

de 30 de enero, por el que se desarrolla el artículo 24 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, en materia de coordinación de actividades empresariales.

Antes del inicio de la actividad contratada, el contratista deberá acreditar a través de una declaración responsable (ver anexo), el cumplimiento de las siguientes obligaciones:

- Acreditación del modelo de organización de la prevención de riesgos laborales adoptado para el desarrollo de las actividades preventivas (constitución de Servicio de Prevención Propio, Ajeno, Mancomunado, etc).
- Evaluación de riesgos y planificación de actividades preventivas de la actividad contratada.
- Todos los trabajadores de la citada empresa así como los de sus subcontratas y trabajadores autónomos que vayan a trabajar en el centro de trabajo de La Agencia:
    - Se encuentran afiliados y dados de alta en el Régimen General de la Seguridad Social, encontrándose la empresa al corriente en el pago de las cuotas empresariales de dichos trabajadores.
    - Disponen del correspondiente certificado de aptitud médica para su puesto trabajo a desarrollar en el centro de trabajo de la Agencia.
    - Han recibido información sobre los riesgos laborales y pautas de actuación en caso de emergencia del centro de trabajo de la Agencia en el que van a realizar su actividad.
    - Han recibido información de los riesgos y medidas de prevención inherentes a su puesto de trabajo.
    - Disponen de la formación teórico-práctica específica del puesto de trabajo que van a desarrollar.
    - Han recibido los EPIs (equipos de protección individual) correspondientes, conforme a lo previsto en el documento preventivo correspondiente (Plan de seguridad y salud, Evaluación de riesgos, etc), y han sido formados para su correcto uso y mantenimiento.
    - En el caso de usar un equipo de trabajo, han recibido formación teórico-práctica para el manejo de dichos equipos y están autorizados por escrito para ello.
- Los equipos de trabajo que se vayan a utilizar en la ejecución de los trabajos disponen de marcado CE, declaración de conformidad o cumplen con las disposiciones mínimas de seguridad y salud para su utilización conforme a lo dispuesto en el Real Decreto 1215/1997, de 18 de julio, por el que se establecen las disposiciones mínimas de seguridad y salud para la utilización por los trabajadores de los equipos de trabajo, se encuentran en perfecto estado, han pasado las revisiones correspondientes y disponen de manual de instrucciones en castellano.
- La empresa dispone de seguro de responsabilidad civil y la maquinaria o vehículos que circulen por carretera y estén matriculados cuentan con el seguro obligatorio, en vigor

En caso de accidente o incidente, la empresa adjudicataria deberá notificarlo inmediatamente a la Agencia a través del Responsable del contrato, remitiendo en el plazo máximo de 7 días el informe de investigación del accidente o incidente.