PLIEGO DE PRESCRIPCIONES TÉCNICAS

Nº EXPEDIENTE: CF050-26-011

SERVICIO DE ALOJAMIENTO PARA LOS PORTALES VEIASA.ES + DIRECTO A LÍNEA + PORTAL FORMACIÓN

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN		
FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 1/34

ÍNDICE

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 2/34

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 3/34

1. ANTECEDENTES

VEIASA dispone de diferentes aplicaciones web donde ofrece información a los cuidadanos de los servicios, utilidades y/o herramientas para facilitar el proceso de inspección técnica de vehículos, así como acciones formativas para el personal propio. Entre los portales con los que cuenta están:

- Portal corporativo veiasa.es.
- Portal de formación para empleados.
- Portal Directo a Línea.

El **Portal Corporativo de VEIASA** es una web pública que sirve de herramienta de comunicación con el ciudadano, donde se da a conocer la empresa, así como una descripción de los servicios que presta. Ha sido diseñada como punto de encuentro de los ciudadanos, con el objetivo de:

- Facilitar el acceso e intercambio de información
- Dar a conocer la dispersión geográfica de Estaciones ITV y Laboratorios
- Solicitud de Servicios de Metrología
- Solicitud de Facturas de los Servicios Prestados
- Recomendaciones sobre la inspección técnica de vehículos
- Preguntas frecuentes sobre la inspección
- Enlace a solicitud de cita previa para la inspección técnica de vehículos
- Noticias

El **Portal de Formación** es una herramienta de uso exclusivo para los trabajadores de Veiasa. Ha sido diseñada como punto de encuentro de todos los que forman parte de la empresa y, entre otros objetivos, persigue:

- Facilitar el acceso a la formación por parte de todos los trabajadores.
- Combatir la dispersión geográfica abriendo un espacio común de formación y colaboración.
- Habilitar un lugar en el que puedan impartirse acciones de formación por parte de personal externo a Veiasa.
- Impulsar la creación de valor entre todo el personal

El Portal de Formación ha sido impulsado por Veiasa con el claro objetivo de mejorar la formación continua en la empresa y mantener a toda la plantilla formada en todas aquellas cuestiones que puedan resultar de interés en nuestro ámbito de actividad.

Por último, el **Portal Directo a Línea** nace con el objetivo de minimizar los tiempos de espera del cliente en una Estación ITV, agilizando los trámites administrativos para la inspección técnica de los vehículos. Es una aplicación destinada principalmente para dispositivos móviles en la que el cliente puede realizar toda la gestión administrativa para ser llamado a la línea de inspección sin pasar por las oficinas, siempre y cuando el vehículo cumpla con las condiciones exigidas para este trámite.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 4/34

2. OBJETO

El objeto de la presente licitación es la contratación de los Servicios de Alojamiento (Hosting) y mantenimiento definidos en el presente Pliego para dar soporte a las aplicaciones descritas en el primer punto de este documento. De acuerdo con lo anterior, el presente Pliego tiene por objeto definir los requerimientos técnicos mínimos de las prestaciones que el adjudicatario deberá poner a disposición de VEIASA y que serán de aplicación a ambos lotes.

El incumplimiento de cualquiera de los requisitos indicados en el presente pliego de prescripciones técnicas, será motivo de exclusión.

Los servicios de alojamiento, sus subdominios y otros alias asociados, se llevarán a cabo mediante un servicio de hosting completo. Estos servicios deberán proporcionar el entorno, el mantenimiento, la conectividad y los servicios de soporte necesarios, de forma que quede garantizada la disponibilidad de los contenidos y servicios ofrecidos, así como la velocidad de acceso a los mismos.

Por tanto, VEIASA precisa la contratación de los **servicios de alojamiento / hosting** sobre los que se implantará y ejecutará cada una de las aplicaciones web especificadas en el punto 1, los elementos hardware, software, de conexión y de seguridad, así como el resto de herramientas necesarias para garantizar su correcto funcionamiento. Así como los **productos o componentes software** de base necesarios para el correcto funcionamiento de las aplicaciones web:

- Sistemas operativos
- Servidores Web
- Servidores de aplicaciones
- Servidores de base de datos
- Servicio firewall de aplicaciones web (WAF)

Además, se necesitarán los **servicios de operación, mantenimiento y administración** de la plataforma tecnológica resultante con el objeto de garantizar la seguridad, disponibilidad y evolución de la misma en óptimas condiciones.

Las **licencias**, soporte por parte del fabricante y derechos de acceso a parches y nuevas versiones han de ser aportados por el adjudicatario. La instalación y configuración de estos productos en los entornos de Desarrollo, Validación y Producción será realizada por el adjudicatario bajo la supervisión de VEIASA.

El servicio de hosting incluirá las funcionalidades que se describen en los siguientes puntos.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 5/34

3. DURACIÓN

El contrato tendrá una duración de **DOCE (12) MESES** a contar desde el día siguiente al de la puesta en marcha del servicio, y si procede, dos posibles prórrogas de **DOCE (12) MESES** más cada una, dando un plazo máximo total de **TREINTA Y SEIS (36) MESES**. Esto es aplicable para cada uno de los lotes.

Se establece un plazo máximo para la Puesta en Marcha que comprende el aprovisionamiento de los productos y servicios solicitados de 4 semanas a contar desde la fecha indicada en el pedido.

4. LOTE 1: PORTAL CORPORATIVO DE VEIASA (Veiasa.es) Y DIRECTO A LÍNEA

Debido a que ambas aplicaciones están desarrolladas bajo el mismo stack tecnológico, **Liferay con base de datos PostgreSQL**, la propuesta deberá contemplar el uso de la misma infraestructura para las dos aplicaciones objeto de este lote, y por lo tanto, la arquitectura propuesta debe cumplir:

- Ser **escalable** para permitir el alojamiento de hasta 5 aplicaciones del mismo stack tecnológico.
- La arquitectura debe estar diseñada para trabajar en **alta disponibilidad en todos los componentes** que forman la propuesta: balanceadores, servidores, almacenamiento, electrónica de red, WAF, etc.
- Debe permitir **realizar el mantenimiento sin afectar a la disponibilidad** de las aplicaciones alojadas.
- Debe garantizar el **aislamiento entre las aplicaciones** alojadas.

El Portal de Directo a Línea está íntimamente ligado y depende funcionalmente del Portal Web de Cita Previa de VEIASA (https://itvcita.com), por lo cual, el licitador deberá ofrecer los mecanismos necesarios para que haya conectividad y plena operatividad entre ambos portales, siendo éste un punto imprescindible del servicio. **Los licitadores deberán incluir en sus propuestas una descripción detallada de este aspecto como parte de la Solución Técnica a incluir en el sobre 2.**

4.1. Conectividad

El servicio garantizará la disponibilidad de conexión y una velocidad de acceso óptima para los usuarios. Para ello será necesario:

- Un **ancho de banda de acceso a internet garantizado al 100% de 60Mbps**. **De conformidad con lo dispuesto en el apartado 8 del Cuadro Resumen del PCAP, que establece como criterio de valoracion la ampliación de este ancho de banda.**

- La latencia debe ser inferior a 50ms.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 6/34

- El acceso a internet debe estar garantizado mediante una conexión redundante enrutadas mediante BGP.
- Conexión, de al menos, 10 Gbps en la red troncal interna.
- Proporcionar y mantener los equipos de telecomunicaciones (firewall, routers, switch, etc.).
- Control de la red de comunicaciones, vigilándose de forma permanente las conexiones de red, la infraestructura LAN de la empresa que proporciona el servicio y el Backbone.
- Gestión y administración de todos los elementos que integran la solución de comunicación, garantizando la disponibilidad e integridad de los contenidos y servicios.
- Conexiones privadas: a las aplicaciones objeto de este lote 1 se accede directamente desde internet por los usuarios, pero existen actualmente conexiones privadas (VPN) para el acceso a servicios web tanto desde las instalaciones de VEIASA como desde proveedores. Por ello será necesario la configuración de tantas conexiones VPN como VEIASA determine, así como su administración y monitorización, de modo que se garantice la disponibilidad y seguridad de las mismas.
- 5 Direcciones IP públicas.

4.2. Alojamiento

Desde el punto de vista del hardware, la arquitectura de servidores podrá ser cualquiera de las existentes en el mercado, si bien la solución técnica que se proponga deberá estar basada en los estándares de facto del mercado y precisará, al menos de:

- **Front-end (Liferay).** Se ubicará en la DMZ del proveedor, protegido por un sistema de seguridad perimetral que garantice el acceso al mismo desde Internet exclusivamente mediante protocolo HTTPS (TCP/443). Este componente albergará el portal Web de usuario.

  Para el caso concreto de los entornos de DESARROLLO y VALIDACIÓN, estos sistemas se ubicarán en una LAN privada del proveedor y no estarán publicados a Internet pero sí accesibles desde VEIASA.

- **Componente Base de datos (PostgreSQL).** Será únicamente accesible desde el front-end descrito en el punto anterior para interacción con la base de datos utilizada.

  Será necesario que se implementen los sistemas DNS propios necesarios para la correcta resolución de nombres de dominio correspondientes a la zona veiasa.es (no publicados a Internet).

- **Componente de búsqueda (ElasticSearch).** El diseño propuesto deberá contemplar HA para el motor de búsquedas ElasticSearch. Para la aceleración de las búsquedas, deberá contemplarse el uso de caché para reducir el acceso a la base de datos y agilizar los resultados.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 7/34

- **Balanceadores** para distribuir el tráfico entre los diferentes componentes que forman la solución y balancear la carga entre los nodos. Deberá permitir mantener la persistencia de la sesión de los usuarios

- **Almacenamiento compartido.** Será el repositorio donde se alojen la información y los ficheros compartidos entre los diferentes nodos de la solución.

- **Firewall** para proteger la infraestructura y para el control del tráfico entre los diferentes componentes que forman la propuesta, permitiendo sólo las conexiones que estén definidas. Aislará las diferentes redes en las que se ubiquen los componentes de la solución.

- **Servicios de monitorización.** Se encargará de monitorizar el rendimiento y la salud de los sistemas, aplicaciones y servicios que forman parte de la solución propuesta.

- **Servicio FTP seguro** accesible desde internet que permita el intercambio de ficheros entre la web y otros elementos externos (tanto de VEIASA como de los proveedores que ésta determine).

- Cada una de estas capas, podrá contar de cuantos servidores físicos o virtualizados sean necesarios en función de la propuesta de solución de alojamiento presentada por la empresa licitadora para la correcta explotación de todos los servicios ofrecidos por las aplicaciones alojadas, en función de sus desarrollos y aplicaciones.

- Adicionalmente al entorno de Producción, el adjudicatario deberá proporcionar cuantos servidores físicos o virtualizados sean necesarios en función de la propuesta de solución de alojamiento presentada, para ofrecer un **entorno de Validación** donde la empresa adjudicataria, VEIASA o ambos puedan realizar pruebas de nuevos desarrollos, revisiones, testeos etc. Estos entornos deberán de facilitar la carga de los nuevos contenidos o desarrollos, a través de un sistema en cascada de aprobaciones (del Entorno de Validación a Producción).

- Routers, switches y demás elementos en función de la solución aportada.

La propuesta presentada deberá operar en alta disponibilidad. La alta disponibilidad se entiende además del propio hardware de los servidores, para los servicios que se prestan. Cada licitador deberá proponer la solución de arquitectura que estime oportuna, y **de conformidad con lo dispuesto en el apartado 8 del Cuadro Resumen del PCAP, se valorará la propuesta de arquitectura y componentes que forman la solución para el lote 1.**

4.3. Entornos disponibles

Junto al entorno de **Producción** se proporcionará un entorno de **Validación,** con un acceso remoto y seguro (VPN, SSL y tunneling encriptado) donde la empresa adjudicataria, VEIASA o ambos puedan realizar pruebas de nuevas aplicaciones, nuevos desarrollos, revisiones, testeos etc.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 8/34

Adicionalmente, para la aplicación del portal web corporativo de veiasa.es exclusivamente, se deberá proporcionar un entorno de **Desarrollo** que contendrá tanto aplicación como base de datos.

Estos entornos deberán facilitar la carga de los nuevos contenidos o desarrollos, a través de un sistema en cascada de aprobaciones (Del Entorno de Desarrollo a Validación, y de Validación a Producción). Estos entornos pueden formar parte de un servidor dedicado, compartido o estar virtualizados.

En resumen, los entornos que deben proporcionarse por aplicación son:

- **Portal corporativo veiasa.es:**
  - Entorno de Desarrollo
  - Entorno de Validación
  - Entorno de Producción

- **Portal Directo a Línea:**
  - Entorno de Validación
  - Entorno de Producción

4.3.1 Requisitos mínimos para el Entorno de Producción

Para el entorno de Producción, se cumplirán las siguientes características:

- El servicio de hosting solicitado se debe de implementar en una arquitectura de front-end / back-end / base de datos, en la que el back-end debe conectar con los sistemas de VEIASA a través de comunicaciones debidamente securizadas de acuerdo a los requisitos de VEIASA.

- El entorno front-end debe de estar en un segmento de red aislado del back-end, y la comunicación entre ambos realizadas a través de un canal seguro.

- Dadas las características del servicio que debe soportar, con disponibilidad 24x7, la infraestructura de sistemas propuesta debe estar redundada y no presentar punto único de fallo.

- La infraestructura propuesta debe estar diseñada para proporcionar un alto rendimiento. Asimismo, debe soportar el incremento de su capacidad sin que se requiera la interrupción del servicio.

- El sistema o sistemas operativos empleados tanto para el front-end como el back-end y los componentes software que contengan deben estar bastionados. Para ello, VEIASA propone la utilización de las guías del Centro Criptológico Nacional que proceda para cada sistema o componente. El adjudicatario podrá proponer otras guías o procedimientos de bastionado alternativos cuya utilización estará supeditada a aprobación por parte de VEIASA.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 9/34

- El almacenamiento deberá operar en alta disponibilidad con redundancia de datos para evitar la pérdida de información ante una contingencia.

Se especifican a continuación los **requerimientos mínimos** para los servidores de producción:

Componente Front-end (Liferay) por cada nodo:

- 8 vCPU por aplicación
- 32 GB de Memoria RAM
- 200 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- Servidor web Apache Tomcat.
- Java JDK: OpenJDK
- Liferay CE 7.4 GA129.

Componente Base de Datos por cada nodo:

- 6 vCPU
- 32 GB de Memoria RAM
- 300 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- PostgreSQL 16.x.

Componente de búsqueda (ElasticSearch) por cada nodo:

- 6 vCPU
- 32 GB de Memoria RAM
- 200 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- ElasticSearch 8.x.

Almacenamiento compartido:

- 200 GB de espacio en disco neto SSD/NVMe

Los requisitos anteriores son mínimos, y deberán adaptarse en función a la propuesta realizada por el licitador.

Para el **sistema operativo** se partirá de una instalación mínima de la subversión más reciente disponible en repositorios oficiales. Se dispondrá de una partición de 20GB específica para logs, que VEIASA podrá solicitar que se redimensione, dentro del espacio disponible, si lo considera necesario.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 10/34

En relación a la instalación mínima, VEIASA podrá solicitar la instalación de determinados paquetes RPM existentes en repositorios oficiales o autorizados (como por ejemplo EPEL).

Se implementará la **configuración de firewall del sistema** indicada por VEIASA al adjudicatario, así como las configuraciones y políticas de **SELINUX** (que deberá estar siempre habilitado) que ésta entienda necesarias para garantizar la seguridad y correcto funcionamiento de los sistemas. Estas configuraciones atenderán siempre al principio de mínimo privilegio/acceso necesario.

Para los **FQDNs y las URLs públicas**, VEIASA será responsable de la configuración DNS necesaria en los servidores públicos correspondientes a la zona veiasa.es, de forma que garantice que apuntan a las direcciones IP públicas que indique el adjudicatario.

Para todos los **FQDNs y las URLs privadas**, será el adjudicatario quien establezca en sus sistemas DNS la configuración necesaria para el correcto funcionamiento de los sistemas.

Todas las versiones de software anteriormente citadas son estimativas y se concretarán al inicio del contrato. Igualmente, las versiones serán actualizadas a petición de VEIASA para mantener la continuidad del soporte de la misma y estarán incluidas en el servicio de hosting sin coste adicional para VEIASA.

4.3.2 Requisitos mínimos para el Entorno de Validación

Se debe proveer un entorno de Validación similar al de Producción, que permita:

- Simular el entorno de producción.
- Realizar pruebas sin impacto.
- Garantizar la compatibilidad.

Se especifican a continuación los **requerimientos mínimos** para los servidores de producción:

Componente Front-end (Liferay) por cada nodo:

- 4 vCPU por aplicación
- 16 GB de Memoria RAM
- 100 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- Servidor web Apache Tomcat.
- Java JDK: OpenJDK
- Liferay CE 7.4 GA129.

Componente Base de Datos por cada nodo:

- 2 vCPU

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 11/34

- 8 GB de Memoria RAM
- 100 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- PostgreSQL 16.x.

Componente de búsqueda (ElasticSearch) por cada nodo:

- 2 vCPU
- 8 GB de Memoria RAM
- 100 GB de espacio en disco neto SSD/NVMe
- 2 Tarjetas de Red 10Gbps
- Oracle Linux 9 64bits (la última versión estable a fecha de adjudicación).
- ElasticSearch 8.x.

Almacenamiento compartido:

- 100 GB de espacio en disco neto SSD/NVMe

Los requisitos anteriores son mínimos, y deberán adaptarse en función a la propuesta realizada por el licitador pero deberá contener los mismos componentes que en el entorno de Producción.

Las versiones del sistema como del resto de los componentes software, así como las configuraciones deberán ser los mismos que los del entorno de Producción.

4.3.3 Requisitos mínimos para el Entorno de Desarrollo

Se deberá facilitar un entorno de Desarrollo que contará con los mismos componentes que los entornos de Producción y Validación pero adaptando los requisitos a los objetivos de un entorno de desarrollo, que permita principalmente:

- Realizar correctivos y evolutivos de las aplicaciones.
- Integrar herramientas de desarrollo y depuración de código.
- Permitir la instalación de herramientas de test.
- Simular comportamiento del entorno de Producción con los nuevos evolutivos y correctivos.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 12/34

4.4. Acuerdos de Nivel de Servicio

A continuación, se especifican los requisitos mínimos exigidos por VEIASA en cuanto a los niveles de servicio para el lote 1, que se medirán de forma mensual:

INDICADOR	DESCRIPCIÓN	UNIDAD DE MEDIDA	VALOR
Puesta en Marcha	Tiempo de puesta en marcha de la plataforma en las infraestructuras del adjudicatario	SEMANAS	<=**CUATRO (4) SEMANAS**
Disponibilidad	Disponibilidad de todos los servicios de la plataforma	%	>= 99,95%
Incidencias	Tiempo de resolución ante incidencias en el servicio	MINUTOS	< **SESENTA (60) MINUTOS**
Caudal	Ancho de banda asignado al servicio	Mbps	>=60 o el valor ofertado por el licitador si es superior
Despliegue de versiones	Pasos a producción	HORAS	<**CUATRO (4) HORAS**
	Pasos a validación	HORAS	<**VEINTICUATRO (24) HORAS**
	Refresco de entornos	HORAS	<**CUARENTA Y OCHO (48) HORAS**

El adjudicatario pondrá a disposición de VEIASA un acceso a un panel de control para extraer de manera autónoma las estadísticas medidas en este apartado.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 13/34

5. LOTE 2: PORTAL DE FORMACIÓN

El portal de formación está soportado bajo LMS de Moodle y soportado con una base de datos MariaDB. La propuesta presentada deberá cumplir:

- Ser **escalable** para permitir el crecimiento de la aplicación.
- La arquitectura debe estar diseñada para trabajar en **alta disponibilidad en todos los componentes** que forman la propuesta: balanceadores, servidores, almacenamiento, electrónica de red, WAF, etc.
- Debe permitir **realizar el mantenimiento sin afectar a la disponibilidad** de las aplicaciones alojadas.

5.1. Conectividad

El servicio garantizará la disponibilidad de conexión y una velocidad de acceso óptima para el Portal de Formación. Para ello será necesario:

- Un ancho de banda de acceso a internet garantizado al 100% de 100Mbps. **De conformidad con lo dispuesto en el apartado 8 del Cuadro Resumen del PCAP, se establece como criterio de valoración la ampliación de este ancho de banda.**
- La latencia debe ser inferior a 50ms.
- El acceso a internet debe estar garantizado mediante una conexión redundante enrutadas mediante BGP.
- Conexión, de al menos, 10 Gbps en la red troncal de interna.
- Proporcionar y mantener los equipos de telecomunicaciones (firewall, routers, switches, etc.).
- Control de la red de comunicaciones, vigilándose de forma permanente las conexiones de red, la infraestructura LAN de la empresa que proporciona el servicio y el Backbone.
- Gestión y administración de todos los elementos que integran la solución de comunicación, garantizando la disponibilidad e integridad de los contenidos y servicios.
- Conexiones privadas: el Portal de Formación es accedido directamente desde internet por los usuarios, pero existen conexiones privadas (VPN StS a través de RCJA) para el acceso a servicios web desde las instalaciones de VEIASA. Por ello, será necesario la configuración de tantas conexiones VPN como VEIASA determine, así como su administración y monitorización de modo que se garantice la disponibilidad y seguridad de las mismas.
- 2 Direcciones IP públicas.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 14/34

5.2. Alojamiento

Desde el punto de vista del hardware, la arquitectura de servidores podrá ser cualquiera de las existentes en el mercado, si bien la solución técnica que se proponga deberá estar basada en los estándares de facto del mercado y contará con, al menos, las siguientes características:

- Una capa de aplicaciones (servidor/es web de aplicaciones) ***front-end***.
- Una capa de base de datos (servidor/es de Bases de datos) ***back-end***.
- **Balanceadores** para distribuir el tráfico entre los diferentes componentes que forman la solución y balancear la carga entre los nodos. Deberá permitir mantener la persistencia de la sesión de los usuarios
- **Almacenamiento compartido.** Será el repositorio donde se alojen la información y los ficheros compartidos entre los diferentes nodos de la solución.
- **Firewall** para proteger la infraestructura y para el control del tráfico entre los diferentes componentes que forman la propuesta, permitiendo sólo las conexiones que estén definidas. Aislará las diferentes redes en las que se ubiquen los componentes de la solución.
- **Servicios de monitorización.** Se encargará de monitorizar el rendimiento y la salud de los sistemas, aplicaciones y servicios que forman parte de la solución propuesta.
- **Servicio FTP** accesible desde internet que permita el intercambio de ficheros entre la web y otros elementos externos (tanto de VEIASA como de los proveedores que ésta determine).
- De cuantos servidores compartidos sean necesarios en función de la propuesta de solución de alojamiento presentada por la empresa adjudicataria para la correcta explotación de todos los servicios ofrecidos por el Portal de Formación en función de sus desarrollos y aplicaciones como el alojamiento de documentos, envío de notificaciones por correo electrónico, contenido multimedia (vídeos e imágenes), foros y blogs. En este documento se hace una propuesta de mínimos a este respecto en el apartado 6.3.
- De cuantos servidores compartidos o virtualizados sean necesarios en función de la propuesta de solución de alojamiento presentada por la empresa adjudicataria para ofrecer un entorno de Validación, además del de Producción. Estos entornos deberán facilitar la carga de los nuevos contenidos o desarrollos, a través de un sistema en cascada de aprobaciones (del Entorno de Validación a Producción).
- Routers, firewall, switches etc. en función de la solución aportada.

Las capas de servicios Productivos del ***front-end*** y del ***back-end*** que soporten el Portal de Formación deberán operar en alta disponibilidad, y pueden ser un único componente o componentes independientes, según la propuesta del licitador. La alta disponibilidad se entiende además del propio hardware de los servidores, el de los servicios que se prestan.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 15/34

La propuesta presentada deberá operar en alta disponibilidad. La alta disponibilidad se entiende además del propio hardware de los servidores, para los servicios que se prestan. Cada licitador deberá proponer la solución de arquitectura que estime oportuna, y **de conformidad con lo dispuesto en el apartado 8 del Cuadro Resumen del PCAP, se valorará la propuesta de arquitectura y componentes que forman la solución para el lote 2.**

5.3. Entornos disponibles

Junto al entorno de **Producción,** se proporcionará un entorno de **Validación,** con un acceso remoto y seguro (VPN, SSL y tunneling encriptado) donde la empresa adjudicataria, VEIASA o ambos puedan realizar pruebas de nuevas aplicaciones, nuevos desarrollos, revisiones, testeos etc.

Estos entornos deberán facilitar la carga de los nuevos contenidos o desarrollos, a través de un sistema en cascada de aprobaciones (del Entorno de Validación a Producción). Estos entornos pueden formar parte de un servidor dedicado, compartido o estar virtualizados.

5.3.1 Requisitos mínimos para el Entorno de Producción

El entorno de Producción, debe de cumplir las siguientes características:

- El servicio de hosting solicitado se debe de implementar en una arquitectura de front-end / back-end, en la que el back-end debe conectar con los sistemas de VEIASA a través de comunicaciones debidamente securizadas de acuerdo a los requisitos de VEIASA.

- El entorno front-end debe de estar en un segmento de red aislado del back-end, y la comunicación entre ambos realizadas a través de un canal seguro.

- Dadas las características del servicio que debe soportar, con disponibilidad 24x7, la infraestructura de sistemas propuesta debe estar redundada y no presentar punto único de fallo.

- La infraestructura propuesta debe estar diseñada para proporcionar un alto rendimiento. Asimismo, debe soportar el incremento de su capacidad sin que se requiera la interrupción del servicio ni aumento de costes.

- El sistema o sistemas operativos empleados tanto para el front-end como el back-end y los componentes software que contengan deben estar bastionados. Para ello, VEIASA propone la utilización de las guías del Centro Criptológico Nacional que proceda para cada sistema o componente. El adjudicatario podrá proponer otras guías o procedimientos de bastionado alternativos cuya utilización estará supeditada a aprobación por parte de VEIASA.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 16/34

- El componente back-end deberá albergar un sistema gestor de bases de datos en el que se desplegarán las bases de datos, que contendrán la información utilizada por la aplicación de Formación.

Se especifican a continuación los requerimientos **mínimos** para el servidor de producción:

- Al menos 16 vCPU.
- 64 Gb de RAM.
- Discos de tecnología SSD/NVMe (mínimo 5.000 IOPS) con capacidad para 8TB netos configurados en alta disponibilidad.
- Sistema operativo Oracle Linux 64 bits (versión a determinar por VEIASA en el momento de la instalación).
- Red de backbone a 10 Gbps.
- Servidor Web: Apache + Php (versiones a determinar por VEIASA en el momento de la instalación).
- Bases de datos: MariaDB (versión a determinar por VEIASA en el momento de la instalación)
- LMS Moodle (versión a determinar por VEIASA en el momento de la instalación)
- Servicio FTP accesible desde VEIASA.
- Servicio de notificaciones mediante envío de correos.

5.3.2 Requisitos mínimos para el Entorno de Validación

El **entorno de Validación** se utilizará principalmente, para lo siguiente:

- Actualizaciones de Moodle.
- Instalación de plugins.
- Pruebas de rendimiento.
- Testing de funcionalidades.

Para el entorno de Validación se establecen los siguientes requisitos **mínimos**:

- Al menos 8 vCPU con 6 cores a 2.6 Ghz.
- 32 Gb de RAM.
- Discos de tecnología SSD/NVMe (mínimo 5.000 IOPS) con capacidad para 4TB netos configurados en alta disponibilidad.
- Sistema operativo Oracle Linux 64 bits (versión a determinar por VEIASA en el momento de la instalación).
- Red de backbone a 1 Gbps.
- Servidor Web: Apache + Php (versiones a determinar por VEIASA en el momento de la instalación).
- Bases de datos: MariaDB(versión a determinar por VEIASA en el momento de la instalación)
- LMS Moodle (versión a determinar por VEIASA en el momento de la instalación)
- Servicio FTP accesible desde VEIASA.
- Servicio de notificaciones mediante envío de correos.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 17/34

5.4. Acuerdos de Nivel de Servicio

A continuación, se especifican los requisitos mínimos exigidos por VEIASA en cuanto a niveles de servicio, que se medirán de forma mensual:

INDICADOR	DESCRIPCIÓN	UNIDAD DE MEDIDA	VALOR
Puesta en Marcha	Tiempo de puesta en marcha de la plataforma en las infraestructuras del adjudicatario	SEMANAS	<=**CUATRO (4) SEMANAS**
Disponibilidad	Disponibilidad de todos los servicios de la plataforma	%	>= 99,95%
Incidencias	Tiempo de resolución ante incidencias en el servicio	MINUTOS	<= **SESENTA (60) MINUTOS**
Caudal	Ancho de banda asignado al servicio	Mbps	>=100 o el valor ofertado por el licitador si es superior
Actualizaciones	Versiones de Moodle	SEMANAS	<=**UNA (1) SEMANA**
	Nuevos plugins	HORAS	<=**VEINTICUATRO (24) HORAS**
	Refresco de entornos	HORAS	<=**CUARENTA Y OCHO (48) HORAS**

6. CARACTERÍSTICAS COMUNES A AMBOS LOTES

6.1. Seguridad del Alojamiento (WAF)

El alojamiento, para ambos lotes, deberá contar con una solución de seguridad (WAF) que supervisará el tráfico para proteger las aplicaciones web de ataques.

El **WAF** (Web Application Firewall) deberá **proteger las aplicaciones web frente a ataques a nivel de capa 7 (HTTP/HTTPS)**. El WAF debe incluir:

- Filtrado y análisis del tráfico HTTP/S.
- Detección y prevención de ataques.
- Definición de reglas personalizadas por aplicación.
- Identificación y gestión del tráfico generado por bots.
- Mantenimiento y actualización periódica.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 18/34

- Debe estar lo suficientemente dimensionado para no afectar al rendimiento de las aplicaciones.
- Permitir la integración con balanceadores y monitorización.
- Permitir la trazabilidad de las conexiones.

Deberá cubrir como mínimo:

- **Protección HTTP.** Detección y bloqueo de ataques tipo XSS, SQLi, CSRF, RFI, LFI, etc.
- **Protección contra DoS/DDoS.**
- **OWASP.** Protección frente a las 10 vulnerabilidades OWASP más críticas.
- **Reglas.** Debe permitir la definición de reglas personalizadas.
- **Soporte HTTPS.** Inspección de tráfico cifrado.
- **Gestión de firmas.** Actualización automática y manual de firmas y patrones de ataque.
- **Tolerancia a fallos.** Debe permitir la continuidad del tráfico en caso de cualquier fallo del WAF.
- **Alertas.** Debe permitir el registro de logs de eventos con acceso a alertas en tiempo real y estadísticas.
- **Informes.** Debe permitir la generación de informes bajo demanda sobre la actividad.
- **Granularidad.** Debe tener capacidad para habilitar/deshabilitar reglas por aplicación y/o URL.
- **Alta disponibilidad.** El servicio debe estar en alta disponibilidad.

El servicio WAF deberá estar dimensionado para permitir inspeccionar y procesar en tiempo real el tráfico generado sin que se produzca degradación en el rendimiento de las aplicaciones.

6.2. Servicio de Logs

Ambos lotes deberán contar con un **servicio de logs** donde se habilitarán las configuraciones y comunicaciones necesarias para garantizar el reenvío de logs de los sistemas implementados a los colectores de logs que VEIASA implemente en su infraestructura propia.

6.3. Licencias

En lo relativo a las licencias, la empresa adjudicataria deberá disponer de cuantas licencias sean necesarias para el correcto funcionamiento de la totalidad del servicio objeto del presente pliego, soporte vigente por parte del fabricante y derechos de acceso a parches y nuevas versiones, durante el periodo de duración del contrato y sin coste añadido para VEIASA.

6.4. Redundancia, Dimensionamiento y Escalabilidad

A continuación, se indican los requisitos en cuanto a redundancia, dimensionamiento y escalabilidad para **ambos lotes**:

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 19/34

- La propuesta de solución de alojamiento, contemplará la **redundancia** para los elementos vitales de los servidores (fuentes de alimentación, ventiladores, RAID en disco, etc.) que alberguen los servicios.

- La solución propuesta estará lo suficientemente **dimensionada** para garantizar su buen rendimiento y tiempos de respuesta de la aplicación.

- La solución propuesta se diseñará teniendo en cuenta la **escalabilidad** de la misma en caso de necesitar, a tenor de un mayor número de usuarios, tráfico etc. ampliaciones o reestructuraciones de la solución inicial aportada **sin coste adicional para VEIASA**.

Si durante la vigencia del servicio se identificasen problemas relacionados con la redundancia, escalabilidad y dimensionamiento, en cualquiera de los componentes que forman la solución, el adjudicatario se compromete a aumentar los recursos asignados, sin coste añadido para VEIASA, para cumplir con los niveles de calidad requeridos.

6.5. Centro de Proceso de Datos

Los servidores asignados al servicio deberán estar ubicados físicamente en locales especialmente acondicionados y seguros (CPDs) diseñados en base a una arquitectura redundante y tolerante a fallos tanto en la infraestructura de red, como en el suministro eléctrico y control de entorno. Estos CPDs tendrán las siguientes características:

- Sistemas redundantes de alimentación ininterrumpida de Energía.

- Garantizar el suministro eléctrico con una garantía de disponibilidad del 100%.

- Sistema de climatización asegurada con equipos redundantes de funcionamiento alterno.

- Suelo técnico.

- Control medioambiental.

- Cámara Ignifuga, sistemas de detección y extinción de Incendios.

- Seguridad 24x7 (control de acceso seguro, personal de seguridad, circuitos cerrados de tv, etc.).

- Monitorización y soporte de todas las características referidas.

- Ventanas planificadas de mantenimiento: La empresa adjudicataria avisará con una antelación de, al menos, 3 días de cualquier trabajo de mantenimiento y actualización de su red si afecta a la disponibilidad del servicio. En casos de fuerza mayor el plazo podrá reducirse, en todo caso, VEIASA deberá estar convenientemente informada.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 20/34

- Estar ubicado dentro del territorio nacional. La ubicación de la infraestructura de hosting en territorio nacional garantiza el control técnico y, operativo sobre los sistemas y datos, reforzando la capacidad de respuesta ante incidentes y la trazabilidad exigida por el Esquema Nacional de Seguridad (RD 311/2022). El propuesto como adjudicatario deberá cumplimentar al efecto el anexo 10 del CR.

6.6. Soporte Técnico

Se proporcionará un mantenimiento continuado y seguro, habilitándose los mecanismos pertinentes (stock de hardware, etc.) **de manera que no se produzcan interrupciones del servicio superiores a los Acuerdos de Nivel de Servicio establecidos**. En este mantenimiento se incluyen todas las acciones necesarias para la correcta explotación de los equipos instalados:

- El adjudicatario deberá asignar un gestor del servicio y ofrecerá sus datos de contacto a VEIASA para poder comunicar asuntos de máxima urgencia que, o bien impidan la prestación del servicio, o bien, se encuentre en riesgo de parada. Este gestor del servicio deberá tener capacidad para poder escalar y priorizar internamente en el adjudicatario las acciones necesarias para su resolución a la mayor brevedad.

- **Atención de incidencias:** el adjudicatario deberá realizar las actuaciones que sean necesarias frente a averías o incidencias sobre el sistema, en unos tiempos de respuesta definidos que garanticen un tiempo de impacto mínimo. Estas actuaciones pueden implicar desde correcciones pequeñas hasta la reinstalación y recuperación completa del sistema. **Este servicio de atención de incidencias estará disponible de forma permanente (24x7, 365 días al año)**.

- **Despliegue de versiones:** mediante un soporte programado disponible, según se coordine con VEIASA, para el despliegue de nuevas versiones de software. En los casos de pasos a producción se harán de forma general en horario de mínimo impacto, que será acordado con VEIASA previamente en cada pase, para el sistema mientras que los pasos a preproducción se acordarán en cada caso según las necesidades de VEIASA.

- **Soporte y mantenimiento del software y hardware instalado.** Esto incluye la instalación de parches y actualizaciones del sistema operativo y paquetes software instalados. El adjudicatario se comprometerá a mantener los sistemas en las últimas versiones estables, propondrá a VEIASA estas actualizaciones y elaborará el plan de acción de cada actuación, incluyendo el estudio de contingencias y procedimientos de recuperación para el caso de eventuales incidencias. El plan de intervención contendrá las tareas previstas, con sus tiempos, posibles efectos laterales y previsión de incidencia para el servicio. El plan de contingencia describirá las acciones que se realizarán en caso de incidencias al aplicar el plan de intervención. Debe incluir las medidas para devolver los sistemas a su situación original.

- **Corrección de vulnerabilidades.** Las vulnerabilidades detectadas en cualquier elemento hardware y/o software que forma parte de la solución, deberán ser corregidas por el adjudicatario, elaborando previamente un plan de actuación para la ejecución de las medidas y consensuando con VEIASA las actuaciones y ventanas horarias. Estas

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 21/34

vulnerabilidades podrán ser identificadas por el propio adjudicatario o bien, comunicadas por VEIASA.

- **Gestión y mantenimiento de la seguridad del entorno:**

  - ✓ Cambio de contraseñas de acceso de los usuarios de administración.
  - ✓ Control de los niveles de privilegio de las cuentas.
  - ✓ Control de servicios abiertos
  - ✓ Seguimiento de debilidades de aplicaciones y sistemas operativos, así como su corrección.
  - ✓ Auditorías periódicas de seguridad, al menos, una cada 6 meses.

- **Servicio de copias de seguridad diarias (backups)** ubicadas en lugar seguro dentro de las instalaciones durante al menos un mes. Estas copias se realizarán sin parada de los sistemas para maximizar la disponibilidad de los mismos. Así mismo, con la periodicidad que VEIASA considere oportuna se entregará copia en un plazo no superior a una semana, a contar desde la petición por parte de VEIASA de la copia.

- **Acceso remoto y seguro** (VPN, SSL, tunneling encriptado) a los servidores desde las instalaciones de VEIASA o desde los proveedores que VEIASA considere.

- **Monitorización 24x7** que incluirá como mínimo:

  - ✓ Estado y conectividad de todos los elementos necesarios para el correcto funcionamiento de los servicios: servidores, routers, switches, balanceadores, firewalls, sistemas, almacenamiento... etc.
  - ✓ Nivel de uso de los diferentes elementos de los sistemas: discos, CPU, memoria, red, ancho de banda, etc.
  - ✓ Comprobación de los servicios desplegados en los sistemas: procesos corriendo, puertos abiertos, etc.
  - ✓ Chequeo del estado de servicios estándar publicados a internet: PING, HTTP, HTTPS, SFTP, SMTP, POP, DNS, con emisión de alertas.
  - ✓ Chequeo del estado de servicios estándar internos: Conexiones activas, PostgreSQL, Tomcat, Salud de ElasticSearch, Java, Moodle, etc.
  - ✓ Chequeo del estado de otros servicios o procesos no estándar para lo que se hayan desarrollado previamente los scripts adecuados. Por ejemplo:

    - Exportación de ficheros.
    - Importación de datos.
    - Estadísticas.
    - Otros procesos de control.

  - ✓ Seguimiento y control de las comunicaciones, el ancho de banda consumido y latencia.

  En base a esta monitorización el proveedor deberá proponer acciones preventivas que vayan orientadas a mejorar la estabilidad y disponibilidad de los entornos.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 22/34

- **Informes mensuales de seguimiento** donde se resumirá el estado de los sistemas, principales acciones realizadas y el estado de las actividades programadas. Se incluirá, además, un apartado resumen de los incidentes de seguridad detectados durante el periodo. Se deberá incluir, como mínimo, lo siguiente:

  - ✓ Resumen de actividad del periodo:
    - ➢ Recursos asignados a la infraestructura: procesadores, memoria, almacenamiento, etc.
    - ➢ Ancho de banda asignado al servicio con gráficas de medición del mes en curso.
    - ➢ Incidentes atendidos, estado y soluciones aplicadas.
    - ➢ Tareas ejecutadas en el periodo.
    - ➢ Tareas pendientes y fechas comprometidas.
    - ➢ Estado de los backup y pruebas de restauración

  - ✓ Informes personalizados de la base de datos que incluyan:
    - ➢ Datos de Auditoría de configuración de Bases de Datos: revisión de configuración, parámetros, almacenamiento, entorno, etc.
    - ➢ Ajuste de Rendimiento, Monitorización, Capacity Planning: análisis de estadísticas, detección de cuellos de botella, reconfiguraciones, planes de contingencia, monitorización proactiva...
    - ➢ Ajuste SQL: ajuste de consultas, propuesta de planes de ejecución alternativos, recodificación, creación de índices, cambios paramétricos, vistas materializadas, etc.
    - ➢ Ajuste PL/SQL, análisis, recodificación eficiente, análisis de vulnerabilidades, mejoras funcionales, …
    - ➢ Revisión copias de seguridad realizadas

  - ✓ Resultado de las auditorías de seguridad si las hubiere.
  - ✓ Informe de seguimiento de los cumplimientos de ANS.
  - ✓ Apartado de posibles mejoras en caso que se detectaran.

6.7. Copias de Seguridad

El servicio ofertado deberá contemplar la gestión de copias de seguridad con la siguiente distribución:

- Una copia completa una vez a la semana, el domingo, con retención de 1 mes.
- Copias diarias 6 días a la semana, de lunes a sábados, incrementales o diferenciales. Estas copias tendrán una retención de 1 semana.
- Copias mensuales con retención de 1 año o fin de contrato.
- Copias anuales con retención hasta finalización de contrato.
- El tiempo de restauración de una copia completa no debe superar las 3 horas.

Semestralmente, el adjudicatario verificará la restauración de las copias de seguridad con el objeto de certificar su validez por parte de VEIASA.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 23/34

6.8. Auditorías de Seguridad

La empresa adjudicataria realizará semestralmente auditorías de seguridad de vulnerabilidades y presentará a VEIASA un plan detallado para solucionarles. Igualmente, VEIASA tendrá acceso en cualquier momento, a la realización de auditorías sobre los sistemas y comunicaciones que albergan el servicio. Se deberá por tanto permitir el acceso a los administradores de sistemas de VEIASA o del proveedor que VEIASA indique en los casos en los que se considere necesario.

6.9. Plan de Continuidad

El adjudicatario debe contemplar el diseño e implantación de un plan de continuidad del servicio, así como los mecanismos lógicos y físicos para garantizar la continuidad del servicio en el menor tiempo posible. Este plan de continuidad deberá ser testeado al menos 1 vez al año y deberá de entregarse junto con la oferta, junto con la documentación preadjudicación.

6.10. Plan de Retorno del Servicio

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por VEIASA a tales efectos, toda la información y documentación que estas soliciten para disponer de un pleno conocimiento técnico de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

El licitador deberá colaborar con VEIASA en el proceso de finalización del contrato y transición de salida, asegurando el traspaso del servicio a VEIASA o la empresa que VEIASA determine, colaborando activamente durante este proceso, para facilitar la transición de los servicios sin causar perjuicios.

El licitador deberá incluir en su oferta, junto con la documentación preadjudicación, un **Plan de Retorno del Servicio**, cuya ejecución deberá realizarse durante el último mes de servicio y con una duración máxima de 30 días para garantizar un traspaso de conocimiento óptimo para la posible continuidad del servicio por parte de otro licitador a la finalización del contrato. En dicho Plan de Retorno del Servicio, el licitador deberá especificar con el mayor nivel de detalle las siguientes acciones a realizar:

- El licitador, previamente a la finalización de su relación contractual, deberá transferir el conocimiento y toda la documentación y herramientas utilizadas durante el contrato a VEIASA o la empresa que VEIASA determine.

- El licitador debe definir en el Plan de Retorno del Servicio todos los aspectos necesarios, como pueden ser:
    - Planificación
    - Procedimientos y metodologías para el traspaso del conocimiento

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 24/34

- Entregables
- Cualquier otro aspecto que se considere relevante para la correcta continuidad del servicio.

Tras la finalización del contrato, el licitador deberá haber entregado todo el material e información adquirida durante la prestación del servicio, independientemente del formato y/o soporte, quedando obligado a mantener la estricta confidencialidad de toda la información y datos manejados durante la prestación del servicio. Dicha obligación deberá trasladarse a todo el personal participante en dicho servicio.

6.11. Documentación del Servicio

El adjudicatario generará los documentos e informes, en formato electrónico, necesarios y suficientes para la adecuada prestación y documentación de cada uno de los servicios anteriormente indicados.

Los documentos e informes deberán ser actualizados en la medida que se vayan realizando tareas de configuración y/o instalación de nuevos productos y servicios y serán en todo momento un fiel reflejo de la infraestructura Hardware/Software desplegada en las instalaciones del adjudicatario.

Los documentos e informes generados estarán en todo momento accesibles por el personal designado por VEIASA, quien podrá solicitar la modificación y/o ampliación del alcance de los mismos.

Como mínimo se exige la elaboración y actualización a lo largo de la prestación del servicio de los siguientes entregables:

- Documento de instalación y configuración de la infraestructura Hardware.
- Documento de instalación y configuración de la infraestructura Software de base.
- Documento de instalación y configuración de las herramientas empleadas para la prestación de los servicios que garanticen la disponibilidad, seguridad y evolución de la plataforma solicitadas
- Actuaciones y cambios realizados en la infraestructura a nivel hardware, software y comunicaciones.
- Niveles de cumplimiento de calidad de servicio.
- Incidencias operativas y de seguridad producidas en el servicio, con fecha y hora de comienzo y fin.
- Disponibilidad y rendimiento de las comunicaciones.
- Disponibilidad y rendimiento del hardware sobre el que están montados los servicios.
- Informe de Copias de seguridad y Pruebas de Restauración.
- Propuestas de mejoras.

6.12. Sistemas de Gestión del Servicio

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 25/34

Las empresas licitadoras deberán acreditar, antes de la adjudicación , mediante copia del certificado, que disponen de las certificaciones indicadas en el apartado de solvencia, así como del:

- **ENS nivel MEDIO o SUPERIOR** en el ámbito del objeto del contrato.

7. CLÁUSULAS ESPECÍFICAS

7.1. Ciberseguridad

Cumplimiento del Esquema Nacional de Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información dictados por el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

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 adoptarán las medidas de seguridad indicadas en el anexo II del ENS aplicables a la categoría del sistema y a los niveles de seguridad requeridos para el mismo, en las dimensiones de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad, que se detallan a continuación:

NIVEL MEDIO

A estas medidas se sumarán aquellas medidas adicionales que se definan por el Responsable de Seguridad (artículo 28 del ENS) y aquellas que se añadan en base a análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, a la evaluación de impacto en la protección de datos (artículo 3.3 del ENS).

El Responsable de Seguridad trasladará las medidas aplicables a través del Responsable del Contrato durante la ejecución de este.

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 del organismo contratante en materia de ciberseguridad.

El organismo contratante desplegará los medios necesarios para auditar el cumplimiento de la política de seguridad y de los niveles de servicio acordados por parte del contratista, según lo expresado en los documentos de contratación.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 26/34

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.ccn-cert.cni.es/), así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía y a las indicaciones del Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía.

Colaboración en la gestión de la seguridad del sistema

El adjudicatario colaborará con la realización de los análisis de riesgos que se realicen, que tendrán en cuenta los siguientes aspectos:

- Identificación de los activos relevantes dentro del alcance considerado del Sistema de Información.
- Valoración cualitativa de los activos más valiosos del sistema. La valoración de los activos corresponde a los responsables designados en la política de seguridad del organismo. Para ello se tendrá en cuenta el perjuicio que supondría su degradación.
- Identificación y cuantificación de las amenazas más probables.
- Identificación y valoración de las salvaguardas que protegen de dichas amenazas.
- Identificación y valoración del riesgo residual.
- El adjudicatario deberá prestar al organismo la colaboración necesaria durante la realización de auditorías técnicas y de cumplimiento normativo.

Certificación ENS de la empresa

En cumplimiento de la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad aprobada por Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, el adjudicatario deberá disponer de Declaración o Certificación de Conformidad con el ENS categoría MEDIA para la prestación de los servicios o provisión de las soluciones contempladas en este expediente, en caso de existir en el alcance de esta contratación servicios no prestados desde las instalaciones de la Junta de Andalucía (por ejemplo, servicios prestados desde una nube). Esta Certificación de Conformidad con el ENS debe versar sobre soluciones proporcionadas o servicios prestados por el operador del sector privado que estén relacionadas con las soluciones y servicios que son objeto de contratación del presente expediente, según apartado VII.1 de la Instrucción Técnica de Seguridad citada.

Interlocución y roles en materia de ciberseguridad

Se asignarán los roles relacionados con la seguridad de los sistemas de información, reflejados en el Esquema Nacional de Seguridad y detallados en la guía CCN-STIC 801 (Responsabilidades y Funciones en el ENS).

La interlocución con el adjudicatario en aspectos de seguridad corresponderá al Responsable del Contrato, con la colaboración y con la orientación del Responsable de Seguridad.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 27/34

Todos estos roles serán identificados e informados, dentro del marco normativo de seguridad establecido en la Junta de Andalucía, desde el inicio del desarrollo del sistema.

Punto de contacto (PoC) de seguridad

En cumplimiento del artículo 13 del Real Decreto 311/2022 (Esquema Nacional de Seguridad), el adjudicatario deberá designar un PoC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de ciberseguridad y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El adjudicatario deberá comunicar cualquier cambio o sustitución de dicho POC a lo largo de la vida del contrato.

Dicho PoC de seguridad será el propio responsable de Ciberseguridad del contratista, formará parte de su área o tendrá comunicación directa con la misma, y su identificación se comunicará al SOC de la Junta de Andalucía a través del Responsable de Seguridad asignado al sistema.

La comunicación de este PoC incluirá la referencia al contrato en el cual se realiza, su duración estimada, las actividades principales a realizar y los accesos remotos que se prevén.

Gestión de incidentes

El adjudicatario comunicará al personal de ciberseguridad del organismo, en primera instancia, o al Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía cualquier ciberincidente que detecte o del que tenga conocimiento.

Para la gestión de los incidentes de seguridad se seguirá lo dictado en la vigente Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC (https://juntadeandalucia.es/boja/2018/141/29). En especial, en el punto 6 (comunicación de incidentes), 8 (comunicación entre organismos y entidades de incidentes y medidas adoptadas), 9 (colaboración con AndalucíaCERT) y 11 (denuncias).

Accesos remotos

El acceso remoto de los técnicos del equipo del proyecto, en el marco del contrato, a los servicios o sistemas de información de la entidad contratante Verificaciones Industriales de Andalucía, se realizará nominalmente mediante el procedimiento aprobado por la Red Corporativa de la Junta de Andalucía (que podrá incluir, a modo de ejemplo, la opción de cliente VPN y/o soluciones de tipo SASE) sin necesidad de disponer de una conexión permanente al Nodo de Interconexión de la Red Corporativa de la Junta de Andalucía (funcionamiento en modo cliente de servicios internos, esto es, conectividad no simétrica), previa autorización por parte del Responsable del Contrato.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 28/34

Caso de que algún software necesario por el adjudicatario para el acceso remoto requiera de suscripción, el adjudicatario se deberá hacer cargo de estos posibles gastos ocasionados.

El modo de acceso será tal que garantice la seguridad de operación y explotación del sistema, así como el objetivo de almacenar y gestionar las solicitudes de servicio e incidencias que se produzcan durante la ejecución del contrato.

El adjudicatario debe realizar las solicitudes de forma individual para cada uno de los técnicos que requieran el acceso remoto, debiendo ser validada cada solicitud por el Responsable del Contrato. Asimismo, deberá comunicar en su caso las bajas eventuales que pudiera producirse durante la vida del contrato.

El adjudicatario debe cumplir con la política de acceso remoto que aplique en el organismo durante todo el periodo de vigencia del contrato, que puede incluir, entre otros aspectos: alta del usuario en el Directorio Corporativo de la Junta de Andalucía, mecanismo de identificación y autenticación robusto empleando el certificado digital de la FNMT, software de la red privada virtual a utilizar, funciones permitidas y datos accesibles desde acceso remoto, tiempo máximo para cerrar sesiones inactivas, activación de los registros de actividad, etc.

Igualmente, el adjudicatario asegurará que la comunicación esté limpia de malware, virus y/o cualquier otro tipo de tráfico malicioso o no deseado.

Requisitos de seguridad en el desarrollo de aplicaciones

Se deberán considerar al menos los siguientes requisitos de seguridad, en el caso de que el objeto del contrato implique trabajos de desarrollo:

- Defensa en profundidad, estableciéndose distintos puntos de control de seguridad en las distintas capas de una aplicación.
- Confidencialidad en las comunicaciones.
- Avisos legales sobre deberes y obligaciones.
- Prevención ante la obtención de credenciales de usuarios.
- Posibilidad de inhabilitación de cuentas de usuario.
- Se garantizará el principio de mínimo privilegio, tanto en el acceso a los datos como a las funciones. La gestión de estos permisos se realizará a través de roles, evitando la posibilidad de asignar permisos o privilegios directos.
- Identificación unívoca de usuario registrado.
- Autenticación y gestión de sesiones de forma segura con objeto de evitar el robo o la manipulación de sesión.
- Trazabilidad.
- Validación de datos de entrada y salida.
- Gestión correcta de mensajes de error.
- Gestión segura de archivos.
- Limpieza de documentos creados o publicados por el aplicativo.

7.2. Gestión de Usuarios y Control de Acceso

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 29/34

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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. 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).

a) 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.

b) En el caso de que, en alguno de los sistemas, aplicaciones, herramientas, etc. objeto de contratación se gestionen trámites y actuaciones que se realizan con la Administración de la Junta de Andalucía por razón de la condición de empleado público.

El sistema deberá admitir, para los trámites y actuaciones que su personal realice con ella por razón de su condición de empleado público, el sistema de identificación de la plataforma de Gestión Unificada de Identidades de Andalucía (GUIA) de acuerdo con el artículo 25.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

7.3. Interoperabilidad

Las ofertas garantizarán un adecuado nivel de inteoperabilidad técnica, semántica y organizativa, conforme a las estipulaciones del Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI). En concreto, se cumplirán las Normas Técnicas de Interoperabilidad establecidas por dicho esquema. Se cuidarán especialmente los aspectos de interoperabilidad orientados a la ciudadanía, de tal forma que se evite la discriminación a los ciudadanos por razón de sus elecciones tecnológicas.

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.

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 30/34

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.

En relación con el desarrollo de soluciones para la tramitación electrónica de los procedimientos, en todo caso se garantizará la plena interoperabilidad de las soluciones implantadas, de acuerdo con el art. 37.4 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

7.4. Uso de Infraestructuras TIC y Herramientas Corporativas

En el marco de lo dispuesto sobre el impulso de los medios electrónicos en el art. 36.1 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía, 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.

7.5. Accesibilidad

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 31/34

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 UNE-EN 301-549:2019, de Requisitos de accesibilidad de productos y servicios TIC, 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.

Por último, como obliga la normativa se deberá realizar al menos una revisión anual de la accesibilidad de los sitios web y sistemas desarrollados o mejorados de manera significativa en el marco del contrato, así como actualizar y en su caso, elaborar, la correspondiente Declaración de accesibilidad de conformidad con el modelo europeo establecido Decisión de Ejecución (UE) 2018/1523 de la Comisión de 11 de octubre de 2018 por la que se establece un modelo de declaración de accesibilidad de conformidad con la Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

7.6. 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, país 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.pdf

7.7. 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 Junta de Andalucía, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 32/34

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 Junta de Andalucía, 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 Junta de Andalucía.

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.

7.8. Confidencialidad y datos de carácter personal

La información a la que tenga acceso la empresa como consecuencia del contrato tendrá un carácter confidencial. Se considera expresamente como información confidencial toda la información a la que tenga acceso, vea, escuche o pueda deducir durante los trabajos a realizar o estancias en áreas seguras de VEIASA (centros de proceso de datos, almacenes, etc.).

El personal de la empresa adjudicataria debe asumir el compromiso de confidencialidad y salvaguarda de toda esta información confidencial.

La empresa adjudicataria no podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de VEIASA.

La empresa adjudicataria, en calidad de encargado de tratamiento, podrá tener acceso a los datos de carácter personal necesarios para la ejecución de los trabajos definidos en este pliego, correspondientes a aquellos tratamientos de datos personales de los que es responsable VEISA y que se incluyan en el anexo específico de protección de datos del Pliego de Cláusulas Administrativas Particulares.

Ese anexo incluirá sus obligaciones como encargado de tratamientos y el destino de los datos a la finalización del contrato, el alcance de las actuaciones a realizar por la empresa adjudicataria en relación a dichos tratamientos y las medidas técnicas y organizativas que deberá implantar para garantizar la seguridad de su tratamiento.

La empresa adjudicataria se obliga a respetar todas las obligaciones que pudieran corresponderle como encargado de tratamientos de datos de carácter personal con arreglo a las disposiciones del Reglamento General de Protección de Datos (RGPD), Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales y cualquier otra disposición o regulación complementaria que le fuera igualmente aplicable.

La empresa adjudicataria únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones del Responsable del Tratamiento, y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el caso de que la empresa adjudicataria destine los datos personales a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones de esta licitación, será considerada

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 33/34

Responsable del Tratamiento, respondiendo de las infracciones en que hubiere incurrido personalmente.

7.9. Transferencia Tecnológica

Durante la ejecución de los trabajos objeto del contrato la empresa adjudicataria se compromete, en todo momento, a facilitar a las personas designadas por VEIASA a tales efectos, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos.

David Pelayo Cruz
Jefe de la Unidad de Mantenimiento de Sistemas de Información

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	06/03/2026
VERIFICACIÓN	Pk2jmRAKQCPQ2FTK7UNLWQL5NL7CPC	PÁG. 34/34