PLIEGO DE PRESCRIPCIONES TÉCNICAS

Nº EXPEDIENTE: CF050-23-027

SERVICIO DE ALOJAMIENTO PARA LOS PORTALES DE LA WEB DE CITAS Y LA INTRANET CORPORATIVA DE VEIASA

ÍNDICE

1. ANTECEDENTES

VEIASA ofrece a los ciudadanos, su servicio para la solicitud de Cita Previa en cualquier Estación ITV que gestiona VEIASA. Este servicio se basa en una aplicación web que se encuentra alojada en un proveedor de servicios el cual proporciona el alojamiento, mantenimiento y soporte a la misma.

Por otro lado, VEIASA dispone de una Intranet Corporativa la cual 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 e intercambio de información.
- Combatir la dispersión geográfica abriendo un espacio común.
- Habilitar un lugar en el que poder compartir ideas, experiencias y sugerencias..
- Impulsar la creación de valor entre todo el personal.
- Ofrecer una conexión permanente con la empresa (acceso universal).
- Mejorar la comunicación entre todos los miembros de la organización.

La Intranet Corporativa ha sido impulsada por Veiasa con el claro objetivo de mejorar la comunicación interna en la empresa y mantener a toda la plantilla informada tanto de las novedades y avances que experimenta la organización como de todas aquellas cuestiones que puedan resultar de interés en nuestro ámbito de actividad.

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 proveedor contratado deberá poner a disposición de VEIASA y que serán de aplicación a ambos lotes.

3. JUSTIFICACIÓN DE LA DIVISIÓN DEL CONTRATO EN LOTES

La división en lotes se justifica debido a que el objeto del contrato corresponde a dos servicios de alojamiento independientes, en concreto:

LOTE 1: Servicio de Alojamiento para la Web de Citas de VEIASA
LOTE 2: Servicio de Alojamiento para la Intranet Corporativa de VEIASA

4. DURACIÓN

El contrato tendrá una duración de 12 meses a contar desde el día siguiente al de la puesta en marcha del servicio, y si procede, una posible prórroga de 12 meses más, dando un plazo máximo total de 24 meses. Esto es aplicable para cada uno de los lotes.

Para la duración inicial del contrato, 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. La reducción de la puesta en marcha será objeto de valoración según lo indicado en el apartado 7 del Cuadro Resumen.

El licitador deberá especificar claramente en su propuesta un plan o metodología de retorno del servicio de hosting de manera que se facilite la transferencia o traslado de la infraestructura objeto de la licitación a un nuevo proveedor.

5. REQUISITOS DEL SERVICIO

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, los soportes, 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 la aplicación web, y la intranet corporativa por separado, los elementos hardware, software y de conexión, 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 los productos anteriores:

- Sistemas operativos
- Servidores Web
- Servidores de aplicaciones
- Servidores de base de datos

Además, se necesitarán los **servicios de operación 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, a excepción de las licencias correspondientes al RAC de Oracle que serán proporcionadas por VEIASA. La instalación y configuración de estos productos en los entornos de Validación, Producción y Desarrollo será realizada por el adjudicatario bajo la supervisión de VEIASA.

El servicio de hosting incluirá las funcionalidades que se describen en los siguientes puntos. En los casos en los que se declaren dudas acerca de la arquitectura mínima descrita en este pliego y de los requisitos de los servicios demandados, se organizará una sesión técnica con los proveedores interesados. Dichos proveedores deberán solicitar la asistencia a la unidad de Contratación de VEIASA.

5.1 LOTE 1: Alojamiento para la Web de Citas de VEIASA

El Portal Web de Citas ITV, en adelante Citas ITV se encuentra desarrollada bajo tecnología multicapa J2EE y usa actualmente bases de datos Oracle.

5.1.1 Conectividad

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

- Un ancho de banda de acceso a internet garantizado al 100% de 30Mbps. De conformidad con lo dispuesto en el apartado 7 del Cuadro Resumen del PCAP, se establece como criterio de valoración la ampliación de este ancho de banda.

- 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: la web de Citas ITV es accedida directamente desde internet por los usuarios, pero existen conexiones privadas (VPN StS a través de RCJA) 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.

5.1.2 Alojamiento

Desde el punto de vista del hardware, la arquitectura de servidores que se proponga para la implementación de la Web de Citas ITV deberá estar basada en los estándares de facto del mercado y precisará, al menos de:

- Una capa de aplicaciones (servidor/es web de aplicaciones) ***front-end***.
- Una capa de balanceo con las siguientes características:

    - Permitirá compensar la carga entre los nodos front-end de la aplicación asegurando que ésta se reparta de forma equitativa.
    - Permitirá añadir más nodos de front-end de forma sencilla en caso de que sea necesario.

- Podrá mantener la sesión de usuarios con persistencia tanto a nivel de IP como a nivel de sesión.
- Dispondrá de un monitor de salud de los nodos de para no enviar peticiones a uno que tenga problemas.

- Una capa de base de datos (servidor/es de Bases de datos) ***back-end***.
- 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).
- Cada una de estas capas, podrá contar, para el entorno de Producción, de cuantos servidores físicos o virtualizados 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 la Web de Citas ITV, en función de sus desarrollos y aplicaciones. En este documento se hace una propuesta de mínimos a este respecto en el punto 5.1.4 de este documento.
- 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 Preproducción y dos entornos de Validación donde la empresa adjudicataria, VEIASA o ambos puedan realizar pruebas de 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/Preproducción a Producción). Igualmente, en este documento se hace una propuesta de mínimos en los puntos 5.1.5 y 5.1.6 de este documento.

- Routers, firewalls, switches etc. en función de la solución aportada.

- Debido a la integración existente entre ambos portales, el Portal Web de Citas y el Portal de Notificaciones (no incluido en este servicio) deberán tener visibilidad entre ellos, por lo tanto, el adjudicatario deberá proporcionar todos los canales necesarios para que exista comunicación entre ambos y deberá monitorizarlos 24x7 para garantizar la operatividad. Los canales deberán ser seguros y privados por lo que se establecerán las VPN StS necesarias entre ambos alojamientos y VEIASA.

Las capas de servicios Productivos del ***front-end*** y del ***back-end*** de la Web de Citas ITV deberán de operar en alta disponibilidad, así como al menos uno de los entornos de preproducción para disponer de un entorno con exactamente las mismas características que el de producción. La alta disponibilidad se entiende además del propio hardware de los servidores, para los servicios que se prestan. De conformidad con lo dispuesto en el apartado 7 del Cuadro Resumen del PCAP, se valorará la existencia de una solución de sistema que contemple más de un nodo de comunicaciones para que en caso de caer uno pase el otro de pasivo a activo.

Los servidores destinados para alojar los servicios objeto del contrato no podrán ser compartidos con ningún otro servicio ni con otro cliente, ni ser destinados a un fin diferente al especificado en este pliego.

5.1.3 Entornos Disponibles

Junto al entorno de **Producción,** se proporcionarán dos entornos 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.

Adicionalmente, deberá proporcionarse un entorno de **Preproducción** 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 Pre Producción a Validación, y de Validación a Producción). Estos entornos pueden formar parte de un servidor dedicado, compartido o estar virtualizados.

Aunque no es objeto de este contrato, VEIASA posee un servicio WAF para proxificar el tráfico que llega a los frontales, ofreciendo una capa añadida de seguridad.

5.1.4.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.

- El componente *front-end* debe proporcionar los servicios web de Cita Previa.

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

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

2 Servidores virtualizados de front-end de servicio a usuarios (sujetos a balanceo de carga):

- 8 núcleos de 2.8Ghz, 8MB cache
- 32 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux CentOS (última versión estable) 64bits.
- Tomcat 8.5 / JBOSS EAP 7 / Wildfly 10 en cluster (A determinar por VEIASA)
- Cluster JMS (Java Message Service)
- Servidor web Apache (última versión estable)

2 Servidores virtualizados de front-end de servicio a estadísticas e intercambio de ficheros (no sujetos a balaceo de carga):

- 8 núcleos de 2.8Ghz , 8MB cache
- 32 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux CentOS (última versión estable) 64bits.
- Tomcat 8.5 / JBOSS EAP 7 / Wildfly 10 (A determinar por VEIASA)
- Pentaho PDI C.E. 6.1
- Oracle 12g (sin RAC)

2 Servidores virtualizados de back-end*:

- 4 núcleos 2.8Ghz , 8MB cache
- 32 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux Red Hat 7 64bits.
- Oracle RAC 12c

* Debido a los requisitos de licenciamiento del sistema gestor de base de datos, el **hardware físico** donde se ejecuten las máquinas virtuales del back-end deberá tener obligatoriamente, las siguientes características:

- 2 nodos físicos con 1 CPU cada uno, pero con capacidad para instalar más en el futuro si VEIASA lo estima necesario.
- Cada CPU tendrá 6 cores
- Sobre esta plataforma física se virtualizarán los nodos de back-end
- Será de uso exclusivo para VEIASA

Almacenamiento:

- El almacenamiento neto de los entornos a implementar se estima entorno a 3TB.
- El adjudicatario deberá disponer de las capacidades de almacenamiento necesarias para implementar diferentes niveles de RAID según los requerimientos funcionales/uso del almacenamiento (Sistema Operativo/aplicaciones/BBDD/logs/etc) para lo que deberá disponer de la capacidad de ofrecer los niveles RAID 0,1,10,5,6.

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.

5.1.5 Requisitos mínimos para el Entorno de Preproducción

2 Servidores virtualizados con los productos de front-end y back-end:

- 4 núcleos de 2.8Ghz , 15MB cache
- 16 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux CentOS (última versión estable) 64bits.
- Tomcat 8.5 / JBOSS EAP 7 / Wildfly 10 (A determinar por VEIASA)
- Cluster JMS (Java Message Service)
- Pentaho PDI C.E. 6.1
- Oracle RAC 12c

*Debido a los requisitos de licenciamiento del sistema gestor de base de base de datos, **estas máquinas virtuales deberán estar en el mismo entorno físico donde están los nodos de producción** (descrito en el apartado anterior).

5.1.6 Requisitos mínimos para el Entorno de Validación

El alojamiento deberá contar con 2 entornos de Validación, adicionales al entorno de Producción y Preproducción, con las siguientes características cada uno de ellos:

1 Servidor virtualizado front-end (sujetos a balanceo de carga):

- 4 núcleos de 2.8Ghz, 8MB cache
- 16 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux CentOS (última versión estable) 64bits.
- Tomcat 8.5 / JBOSS EAP 7 / Wildfly 10 en cluster (A determinar por VEIASA)
- Cluster JMS (Java Message Service)
- Servidor web Apache (última versión estable)
- Pentaho PDI C.E. 6.1

1 Servidor virtualizado de back-end*:

- 2 núcleos 2.8Ghz, 8MB cache
- 16 GB de Memoria RAM
- 2 Tarjetas de Red 10/100/1000
- Linux Red Hat 7 64bits.
- Oracle Standard 12c

5.1.7 Resto de Servicios para la Web de Cita Previa

Además de los entornos de producción, validación y preproducción serán necesarias los siguientes servidores y servicios:

- **Servicio FTP/S:** se precisa de un espacio de al menos 100GB en un servidor FTP/S (no tiene porqué ser dedicado) al que accederán los servidores de front-end y back-end para el intercambio de datos con sistemas externos.

- **Servicio de correo:** dentro de los servicios ofertados, es necesario incluir el servicio de correo para el dominio itvcita.com para el envío de notificaciones.

- **Servicio de logs:** El adjudicatario deberá proporcionar los mecanismos necesarios para que los logs generados en el servicio de Web de Citas se integre con las herramientas corporativas de VEIASA, concretamente con Graylog.

- **Servidores/servicios de monitorización de rendimiento de aplicaciones**: VEIASA se reserva el derecho de instalar aplicativos o servicios en las instalaciones del adjudicatario para extraer datos de rendimiento de la web de citas. En caso de ser necesario alojamiento específico para estas herramientas se tratará como modificación del contrato.

5.1.8. Licencias

En lo relativo a las licencias de software, la empresa adjudicataria deberá disponer de cuantas licencias sean necesarias para el correcto funcionamiento de la totalidad del sistema 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, **exceptuando** las licencias de **Base de datos ORACLE** (y RAC) que sean necesarias implementar, las cuales serán proporcionadas por VEIASA.

5.1.9 Acuerdos de Nivel de Servicio

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

SERVICIO	INDICADOR	DESCRIPCION	VALOR
Puesta en Marcha	P1	Tiempo puesta en marcha de la plataforma en las infraestructuras del adjudicatario	<=4 semanas o el plazo ofertado por el licitador si es menor
Disponibilidad	D1	Disponibilidad de todos los servicios de la plataforma	>= 99,95%
Incidencias	I1	Tiempo de resolución ante incidencias en el servicio	< 60 minutos o el tiempo ofertado por el licitador si es menor
Tareas	T1	Tiempo en dar estimación de comienzo y duración de trabajos ante peticiones de tareas no incluidas en el alcance (bolsa de horas)	4 días
Despliegue de versiones	V1	Pasos a producción*	<4h
	V2	Pasos a preproducción	<24h
	V3	Refresco de bases de datos	<24h

*Se realizan a las 21h con lo que si pidieran con un margen superior a las 4h no implicaría incumplimiento (ej: si a las 9 am se pide un paso a producción estándar, éste se realizará a las 21h sin implicar incumplimiento por superar las 4h).

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.

5.2 LOTE 2: Alojamiento para la Intranet Corporativa de VEIASA

5.2.1 Conectividad

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

- Un ancho de banda de acceso a internet garantizado al 100% de 30Mbps. De conformidad con lo dispuesto en el apartado 7 del Cuadro Resumen del PCAP, establece como criterio de valoracion la ampliación de este ancho de banda.

- 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 la Intranet corporativa se accede directamente desde internet por los usuarios, pero existen actualmente conexiones privadas (VPN) 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.

5.2.2 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:

- Un servidor web de aplicaciones (***front-end***) dedicado.

- Un servidor de base de datos (***back-end***) dedicado.

- 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 la intranet en función de sus desarrollos y aplicaciones como el alojamiento de documentos, envío de noticias 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.

- 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 Producción, Validación y otro de Desarrollo.

- Routers, firewall, switches etc. en función de la solución aportada.

Las capas de servicios Productivos del ***front-end*** y del ***back-end*** que soporten la Intranet corporativa deberán de operar en alta disponibilidad. La alta disponibilidad se entiende además del propio hardware de los servidores, para los servicios que se prestan. De conformidad con lo dispuesto en el apartado 7 del Cuadro Resumen del PCAP, se valorará la existencia de una solución de sistema que contemple más de un nodo de comunicaciones para que, en caso de caer uno, pase el otro de pasivo a activo.

Los servidores destinados para alojar los servicios objeto del contrato no podrán ser compartidos con ningún otro servicio con otro cliente, ni ser destinados a un fin diferente al especificado en este pliego.

5.2.3 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.

Adicionalmente deberá proporcionarse 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.

5.2.4. 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.

- 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.

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

Servidor front-end:

- 2 Procesadores Quad Core 2.8Ghz
- 16 GB de Memoria RAM
- 200 GB de espacio en disco neto en RAID5
- 2 Tarjetas de Red 10/100/1000

- CentOS 64bits (la última versión estable a fecha de adjudicación).
- Servidor web Apache2 versión 2.4.6.
- PHP 7.3.29
- Drupal 8
- Librerias Auxiliares

Servidor back-end Veinet:

- 2 Procesadores Quad Core 2.8Ghz
- 16 GB de Memoria RAM
- 200 GB de espacio en disco neto en RAID10
- 2 Tarjetas de Red 10/100/1000
- CentOS 64bits (la última versión estable a fecha de adjudicación).
- MariaDB 10.4.8.
- Librerías Auxiliares

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.

5.2.5 Requisitos mínimos para el Entorno de Validación

Para el entorno de Validación se establecen los mismos requisitos expresados para el entorno de producción en el punto 5.2.4 del presente documento, con la salvedad de aquellos referidos a la alta disponibilidad y alto rendimiento.

5.2.6 Requisitos para el Entorno de Desarrollo

- 2 núcleos de al menos 2,8 GHz.
- 16 GBytes de memoria RAM dedicada.
- Espacio de 200 Gbytes en el sistema de almacenamiento
- Tarjetas de Red duplicadas 10/100/1000
- Sistema Operativo Linux CentOs 64 bits (la última versión estable a fecha de adjudicación)
- Servidor web Apache 2 versión 2.4.6
- PHP 7.3.29
- Servidor de BBDD MariaDB 10.4.8

5.2.7 Acuerdos de Nivel de Servicio

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

SERVICIO	INDICADOR	DESCRIPCION	VALOR
Puesta en Marcha	P1	Tiempo puesta en marcha de la plataforma en las infraestructuras del adjudicatario	<=4 semanas o el plazo ofertado por el licitador si es menor
Disponibilidad	D1	Disponibilidad de todos los servicios de la plataforma	>= 99,95%
Incidencias	I1	Tiempo de resolución ante incidencias en el servicio	< 60 minutos o el tiempo ofertado por el licitador si es menor

*Se realizan a las 21h, con lo que si pidieran con un margen superior a las 4h no implicaría incumplimiento (ej: si a las 9 am se pide un paso a producción estándar, éste se realizará a las 21h sin implicar incumplimiento por superar las 4h).

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.

6. REDUNDANCIA, DIMENSIONAMIENTO Y ESCALABILIDAD

- La propuesta de solución de alojamiento, en ambos lotes, 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.

7. CENTRO DE PROCESO DE DATOS

Los servidores 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.
- Estar ubicado dentro del territorio nacional.
- Ser propiedad del licitador, no pudiendo ser compartido y siendo gestionado por el mismo.

8. 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 60 minutos**. 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. Como datos de referencia se realizan:
    - ✓ 1 paso a Producción semanal.

- ✓ 1 paso a Preproducción semanal (en cada uno de los entornos).
- ✓ 52 refrescos de base de datos anuales en preproducción con los datos de producción (1 a la semana).

- 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 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.

- 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… 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: Oracle, Jboss/Tomcat, Apache, 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 cualificaciones
  - Exportación de cliente
  - Importación de datos inspecciones
  - Importación de datos de matrículas desde tráfico
  - 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.

- 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:
    - 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.

9. DOCUMENTACIÓN TÉCNICA

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.

10. 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 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 sobre los entornos de validación/preproducción con el objeto de certificar su validez por parte de VEIASA. Este proceso se coordinará con VEIASA en todo momento.

11. AUDITORIAS

La empresa adjudicataria realizará mensualmente auditorías de seguridad de vulnerabilidades y presentará a VEIASA un plan detallado para solucionarles. Igualmente, VEIASA tendrá acceso en cualquier momento y sin previo aviso al adjudicatario, 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.

12. 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.

13. TRANSFERENCIA TECNOLÓGICA

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 un Plan de Retorno del Servicio, cuya ejecución deberá realizarse durante el último mes de servicio y con una duración 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 Devolución, 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 devolución del servicio todos los aspectos necesarios, como pueden ser:
    - Planificación

- Procedimientos y metodologías para el traspaso del conocimiento
- 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.

14. SISTEMAS DE GESTIÓN DEL SERVICIO

Las empresas licitadoras deberán acreditarque disponen de los siguientes sistemas imprescindibles para poder continuar en el proceso de selección, tanto para el lote 1 como para el lote 2:

- Un sistema de gestión del servicio TI tal como viene detallado en la norma ISO 20000. Las empresas licitadoras podrán acreditar el sistema de gestión requerido mediante la aportación de la certificación ISO 20000, certificación equivalente o cualquier sistema propio del licitador donde se acredite dicha gestión de servicio.

- Un sistema de seguridad de la Información tal como viene detallado en la norma ISO 27001. Las empresas licitadoras podrán acreditar el sistema de seguridad de la información requerido mediante la aportación de a certificación ISO 27001, certificación equivalente o cualquier sistema propio del licitador donde se acredite dicho sistema de seguridad de la información.

- Los licitadores deberán disponer y aportar, **con la oferta técnica**, la certificación en el Esquema Nacional de Seguridad (ENS) de, al menos, nivel medio. El cumplimiento del ENS deberá acreditarse mediante declaraciones o certificados de conformidad con el ENS, según se indica en presente PPT.

Además, exclusivamente para el lote 1, será necesario disponer también del siguiente sistema de calidad:

- Un sistema de calidad de servicios de desarrollo software, tal como viene detallado en la certificación CMMI. Para la acreditación de este sistema se permitirá presentar la certificación CMMI (nivel 3 mínimo), certificación equivalente o cualquier sistema propio del licitador donde se acredite dicho sistema de calidad de servicios de desarrollo software.

15. CLÁUSULAS ESPECÍFICAS

<u>Interoperabilidad</u>

Las ofertas garantizarán un adecuado nivel de interoperabilidad 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.

También se atenderá a los modelos de datos sectoriales relativos a materias sujetas a intercambio deinformación 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.

Tratamiento de datos de carácter personal
Tal y como se indica en el apartado 12 del PCAP

Gestión de Usuarios
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 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.

Directrices coroporativas en materia de gestion de identidades
Se establece la misma clausula tipo que para la de gestión de usuarios.

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 Verificaciones Industriales de Andalucia 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 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 Verificaciones Industriales de Andalucia, 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 Verificaciones Industriales de Andalucia.

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.

Garantía
Tal y como se indica en el apartado 5.9 del PCAP

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 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.

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 311/2022, de 3 de mayo, 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 de nivel medio, en función de los tipos de activos presentes y las dimensiones de información relevantes, considerando las categorías de seguridad en las que recaen los sistemas de información objeto de la contratación según los criterios establecidos en el anexo I del ENS de nivel medio. 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 Verificaciones Industriales de Andalucía en materia de Seguridad TIC.

Según la normativa vigente sobre el ENS, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad:

La arquitectura del servicio deberá adaptarse a la arquitectura de seguridad de los Nodos de Interconexión Avanzados de la Red Corporativa de Telecomunicaciones de la Junta de Andalucía (en adelante, RCJA), de tipo APP-6 (según la guía CCN-STIC 811), compuesto por una doble barrera de cortafuegos y por un sistema de proxys para la navegación y publicación.
En caso de que se requiera de interconexión con Internet u otras redes externas, ya sea en navegación o en publicación, se deberá hacer uso de los siguientes servicios ofrecidos por la RCJA:

- La interconexión con redes externas se realizará utilizando bien el servicio de accesos externos o el servicio VPN sede contra sede o bien mediante el servicio VPN de usuario corporativo.
- Servicio de proxy inverso externo para la publicación.
- Servicio de proxy socks para la navegación por puertos especiales distintos al 80 o al 443.

Propuesta de redacción elaborada por:

28764181J DAVID PELAYO (C:A41398645)

Firmado digitalmente por 28764181J DAVID PELAYO (C:A41398645)
Fecha: 2024.01.24 13:16:44 +01'00'