PLIEGO DE PRESCRIPCIONES TÉCNICAS

Nº EXPEDIENTE: CF050-25-033

SERVICIO DE ALOJAMIENTO WEB DE CITAS + EITV.

ÍNDICE

1. ANTECEDENTES

VEIASA dispone de diversas aplicaciones web corporativas que dan soporte a la prestación de servicios a la ciudadanía, proporcionando canales digitales seguros, accesibles y orientados a facilitar la gestión y tramitación de sus diferentes actividades. Entre los portales con los que cuenta están:

- Portal Web de Citas.
- Portal eITV.

El **Portal web de Citas** es una web pública que ofrece a los ciudadanos, su servicio para la solicitud de cita previa en cualquier Estación ITV que gestiona VEIASA. Este servicio (http://www.itvcita.com/) se basa en una aplicación web que se encuentra alojada en un proveedor de servicios que proporciona el alojamiento, mantenimiento de la infraestructura y soporte a la misma.

Por último, el **Portal eITV** nace con el objetivo de la eliminación del papel y adaptación a las nuevas tecnologías. El servicio que proporciona e-ITV está enfocado a permitir realizar solicitudes de inspecciones no periódicas de usuarios, y su posterior tramitación. Con este sistema se evita la presencia física de los usuarios para comenzar este trámite y se facilita la interacción electrónica.

Este servicio se basa en una aplicación web que se encuentra alojada en un proveedor de servicios que proporciona el alojamiento, mantenimiento de la infraestructura y soporte a la misma.

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.

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

Asimismo, se entienden incluidos en la oferta económica todos los servicios y elementos asociados para la correcta prestación del servicio en los términos y condiciones indicadas en el presente PPT , salvo que expresamente se contemple lo contrario.

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 un **servicio de alojamiento/hosting** que proporcione la infraestructura necesaria para implantar y ejecutar las aplicaciones web descritas en el punto 1. Este servicio deberá incluir los elementos hardware, software, de conectividad y de seguridad, así como todas las herramientas requeridas para garantizar su correcto funcionamiento. Asimismo, deberá suministrar los **productos y componentes software** de base indispensables para la operación de dichas aplicaciones web, entre los que se incluyen:

- Sistemas operativos.
- Servidores Web.
- Servidores de aplicaciones.
- Servidores de base de datos.
- Servicio firewall de aplicaciones web (WAF)
- Servicios de soporte a procesos de integración, mensajería, almacenamiento o búsqueda, cuando así lo requiera la arquitectura de cada aplicación.

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 especificados para cada aplicación, será realizada por el adjudicatario bajo la supervisión de VEIASA.

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

3. JUSTIFICACIÓN DE LA NO DIVISIÓN EN LA LICITACIÓN EN LOTES

La no división en lotes del presente contrato se fundamenta en la unidad funcional, técnica y operativa de los servicios requeridos. Las plataformas **Web de Citas, y eITV** comparten elementos comunes de infraestructura, seguridad, soporte técnico y gestión, por lo que su tratamiento conjunto permite una administración más eficiente, coherente y segura del entorno tecnológico.

Dividir el contrato en lotes implicaría riesgos de incompatibilidad, duplicidad de esfuerzos, aumento en los tiempos de respuesta y dificultades en la coordinación operativa, lo cual afectaría negativamente la continuidad del servicio y la experiencia del usuario. Asimismo, se considera que la naturaleza integrada del alojamiento requerido, exige una solución unificada que garantice la interoperabilidad y un único punto de responsabilidad técnica y contractual.

Por todo ello, se concluye que la no división en lotes optimiza recursos, tiempos y calidad, resultando la opción más eficiente y adecuada para cumplir los objetivos del proyecto, en línea con el artículo 99.3 de la Ley de Contratos del Sector Público.

4. 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**.

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. El licitador deberá incluir en su oferta un Plan de Puesta en marcha, **como parte de la solución técnica a incluir en el sobre 2**

5. REQUISITOS DEL SERVICIO

5.1. SERVICIO WEB DE CITAS

La web http://www.itvcita.com/, en adelante Citas ITV constituye el principal punto de acceso público para la gestión de citas previas de VEIASA, actualmente el sistema se encuentra desarrollado bajo tecnología multicapa J2EE sobre bases de datos Oracle, aunque se está realizando el desarrollo que implica la migración de la plataforma a una arquitectura orientada a componentes y microservicios que tendrá las siguientes características:

- La nueva solución se apoyará en Portal Liferay para la capa de presentación, con componentes desarrollados en React, y una capa de servicios backend implementada en NestJS (NodeJS) bajo un enfoque API First.

- El sistema integrará un bus de eventos RabbitMQ para facilitar la comunicación e integración con otros sistemas corporativos. Para la gestión de datos, la plataforma utilizará PostgreSQL para los servicios internos de Liferay, y como base de datos transaccional principal.

- El sistema integrará, además, ElasticSearch como motor de búsqueda y servicio de indexación, integrado con Liferay para proporcionar consultas eficientes y capacidades avanzadas de búsqueda dentro de la plataforma.

- La solución se debe ejecutar sobre una infraestructura en alta disponibilidad basada en una granja de nodos Liferay, un clúster de microservicios backend, y componentes de mensajería y bases de datos distribuidas.

Debido al proceso de transición tecnológica de la Web de Citas ITV, el servicio de alojamiento deberá contemplar, desde el inicio del contrato, la coexistencia de dos infraestructuras diferenciadas:

- De inicio, el adjudicatario deberá desplegar exclusivamente la infraestructura que de soporte en Producción a la actual Web de Citas y mantenerla plenamente operativa. Adicionalmente para el entorno de Preproducción deberá desplegar de inicio tanto la infraestructura necesaria para la web actual, como la infraestructura necesaria par la nueva web en desarrollo..

- VEIASA notificará al adjudicatario, con la antelación suficiente, el inicio del despliegue de la nueva infraestructura de Producción. A partir de dicha notificación:

    - El adjudicatario deberá proceder a la creación, configuración y operación de la nueva infraestructura Liferay según el presente pliego.

    - Podrá ser necesaria la **coexistencia** simultánea de la infraestructura actual y la nueva infraestructura de Producción durante un periodo de tiempo que se determinará en el momento del despliegue de la nueva infraestructura.

Durante este periodo de transición, el adjudicatario deberá garantizar:

- La continuidad del servicio de ambos entornos,

- La disponibilidad y seguridad de los componentes descritos,

- La segregación adecuada entre ambas arquitecturas,

- Las capacidades de monitorización, backup, restauración y soporte para ambos sistemas de forma independiente.

VEIASA comunicará formalmente la fecha en la que la infraestructura de Producción correspondiente a la actual web de citas debe apagarse o ponerse fuera de servicio, una vez se certifique la estabilidad y madurez operativa de la nueva plataforma.

Ambas infraestructuras se describen de forma detallada en este documento técnico, y el adjudicatario deberá estar en condiciones de desplegar y operar cualquiera de ellas conforme a las necesidades de VEIASA.

El servicio de hosting para la web de cita previa incluirá las funcionalidades específicas que se describen en los siguientes puntos.

5.1.1 ALOJAMIENTO

Desde el punto de vista del hardware e infraestructura, 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 estándares consolidados y garantizar, en todo caso, la disponibilidad, seguridad y escalabilidad necesarias para la adecuada prestación del servicio. La solución deberá contemplar, al menos, los siguientes componentes:

Infraestructura Citas ITV actual:

- Una capa **Front-end**: El adjudicatario deberá proporcionar uno o varios componentes de front-end encargados de ejecutar la plataforma J2EE existente. Esta capa deberá operar en un entorno seguro ubicado en la DMZ del proveedor, protegido por un Sistema de Seguridad Perimetral que incluya obligatoriamente un Firewall de Aplicaciones Web (WAF)
- 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***. El adjudicatario deberá proporcionar la infraestructura necesaria para alojar la base de datos Oracle utilizada por la Web de Citas actual. Esta capa back-end deberá:
    - ubicarse en una red interna no expuesta, accesible únicamente desde la capa de aplicaciones,
    - estar protegida mediante reglas específicas de firewall y políticas de mínimo privilegio,
    - proporcionar redundancia a nivel de almacenamiento y protección frente a fallos,
    - permitir la escalabilidad necesaria para mantener el rendimiento del sistema actual.

Infraestructura nueva Citas ITV:

- **Front-end:**
    - Los nodos frontales de Liferay se ubicarán en la DMZ del proveedor, protegidos mediante un Sistema de Seguridad Perimetral que incluya obligatoriamente un Firewall de Aplicaciones Web (WAF).
    - El acceso desde Internet se realizará exclusivamente a través de HTTPS (TCP/443),
    - Estos nodos frontales deben incluir un NGINX como proxy inverso, encargado de recibir las peticiones provenientes del balanceador, aplicar reglas de seguridad HTTP adicionales y canalizarlas hacia el componente Liferay.

  Para los entornos de VALIDACIÓN y PREPRODUCCIÓN, estos sistemas se ubicarán en redes internas privadas del proveedor, no publicadas en Internet, pero accesibles

desde VEIASA a través de los mecanismos de conexión segura establecidos (VPN, RCJA, o equivalentes).

- **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.

- **Componente Base de datos (**PostgreSQL). Clúster PostgreSQL que podrá ser común para los diferentes entornos.
  Cada clúster estará configurado en HA con replicación síncrona y mecanismos automáticos de detección de fallo y conmutación (failover) sin intervención manual.

  El acceso a cada clúster quedará limitado exclusivamente a los nodos Liferay y a los componentes backend, aplicándose políticas de mínimo privilegio y controles estrictos de seguridad en las comunicaciones internas. 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.

- **Backend de microservicios** El adjudicatario deberá proporcionar y operar la capa de componentes backend destinada a la ejecución de los microservicios desarrollados en NestJS

  Estos componentes backend se ubicarán en una red interna segregada, accesible únicamente desde la capa frontal Liferay, el bus de eventos RabbitMQ y la capa de bases de datos, mediante reglas específicas y restrictivas de firewall que garanticen el principio de mínimo privilegio.

- **Bus de eventos (RabbitMQ**) La solución deberá integrar un clúster de RabbitMQ (mínimo 3 nodos en quorum queues) Este componente permitirá la publicación y consumo de eventos definidos mediante AsyncAPI, facilitando la integración con los sistemas corporativos.

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.

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 y un entorno de Preproducción 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).

Las capas de servicios Productivos de la Web de Citas ITV, tanto en la configuración actual como en la nueva configuración, deberán operar en alta disponibilidad, sin presentar puntos únicos de fallo.

El entorno de Preproducción deberá reproducir la arquitectura lógica y funcional del entorno de Producción y operar igualmente en alta disponibilidad, si bien podrá hacerlo con un dimensionamiento inferior al de dicho entorno productivo. El adjudicatario deberá garantizar que Preproducción mantiene la misma estructura de componentes, las mismas capas y los mismos mecanismos de tolerancia a fallos que Producción, salvo que VEIASA determine expresamente que algún elemento no requiere replicación por su naturaleza o criticidad.

La alta disponibilidad se entenderá tanto a nivel de hardware como de los servicios prestados en Producción. De conformidad con lo dispuesto en el Anexo 8 del Cuadro Resumen del PCAP, se valorará la existencia de una solución que contemple más de un nodo de comunicaciones en Producción para garantizar continuidad ante fallo.

5.1.2. REQUISITOS PARA EL ENTORNO DE PRODUCCIÓN

Para el entorno de Producción, tanto para la infraestructura de la web de citas actual, como para la infraestructura de la nueva web de citas, se cumplirán las siguientes características:

- El servicio de hosting solicitado se debe de implementar en una arquitectura de *front-end / back-end* (adecuándose en cada caso a la tecnología específica de la versión de la aplicación), 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 licitador deberá garantizar que todos los servicios descritos operen **sin punto único de fallo**. Para ello, deberá dimensionar las capas front-end y back-end con el número de nodos necesario para cumplir los SLA y garantizar la disponibilidad 24x7. No se aceptarán arquitecturas con un único nodo en componentes críticos

- 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.

- En ambos modelos (actual y nuevo), la capa front-end deberá proporcionar los servicios web de Cita Previa y atender el tráfico de los usuarios finales, mientras que la capa back-end albergará los sistemas gestores de bases de datos y los componentes de negocio asociados a la aplicación.

- En ambos modelos el almacenamiento deberá garantizar alta disponibilidad y ausencia de punto único de fallo. El adjudicatario deberá justificar su propuesta de dimensionamiento para cada plataforma.
  El almacenamiento de ambos entornos productivos no podrá mezclarse, debiendo mantenerse una separación lógica clara y permitir ampliación futura sin interrupción del servicio.

- Asimismo, la propuesta de arquitectura presentada por el licitador será objeto de valoración atendiendo a su adecuación técnica, coherencia, robustez, escalabilidad, eficiencia en el uso de recursos y alineamiento con los requisitos de alta disponibilidad y seguridad establecidos en este pliego.

  Esta valoración considerará especialmente la calidad del diseño planteado, la justificación técnica de las decisiones adoptadas, la capacidad de la arquitectura para soportar evolutivos y picos de carga, los mecanismos de tolerancia a fallos, la correcta segregación de componentes y redes, así como cualquier elemento que contribuya a optimizar la operación y continuidad del servicio. En todo caso, la arquitectura deberá permanecer dentro de los parámetros funcionales, tecnológicos y de seguridad definidos por VEIASA.

La propuesta del licitador deberá contemplar el despliegue de los siguientes componentes mínimos, pudiendo dimensionar libremente el número de instancias o nodos necesarios:

- Infraestructura Citas ITV actual

Front-end (servicio a usuarios)

- Oracle CentOS 7
- Apache HTTP Server (última versión estable)
- Contenedor Java: Tomcat 8.5 / JBoss EAP 7 / Wildfly 10 (a determinar por VEIASA)
- Servidor de aplicaciones configurado para funcionamiento en entorno multinodo
- Cluster JMS
- Acceso protegido a través del WAF

Front-end (servicios auxiliares: estadísticas, intercambio de ficheros)

- Oracle CentOS 7
- Contenedor Java compatible con la versión anterior.
- Tomcat 8.5 / JBOSS EAP 7 / Wildfly 10 (A determinar por VEIASA)
- Pentaho PDI C.E. 6.1
- Oracle 12g (sin RAC)
- Acceso al almacenamiento compartido del entorno

Back-end (bases de datos)

- Oracle RAC 12c
- Linux Red Hat 7 64bits (por compatibilidad con 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 dedicados, 1 CPU por nodo (6 cores mínimo)
  - Capacidad de ampliación futura si VEIASA lo requiere
  - Exclusividad de uso para VEIASA

  Sobre esta plataforma se virtualizarán los nodos de base de datos correspondientes.

Almacenamiento:

El almacenamiento deberá cubrir:

- el almacenamiento asociado a las máquinas virtuales de front-end y back-end
- el almacenamiento requerido por la arquitectura Oracle Database 12c RAC conforme a sus requisitos de certificación y operación,
- el almacenamiento necesario para los servicios auxiliares (Pentaho, logs, ficheros temporales, etc.).

En base a los datos actuales de demanda el almacenamiento neto de los entornos a implementar se estima entorno a 3TB.

Este almacenamiento deberá estar claramente segregado del utilizado por la nueva plataforma.

- Infraestructura nueva Citas ITV

Front-end (servicio a usuarios)

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación).
- NGINX como proxy inverso y servidor web
- Liferay CE/DXP (versión indicada por VEIASA)
- Acceso al almacenamiento compartido del entorno
- Acceso protegido a través del WAF

Capa de búsqueda (ElasticSearch)

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación).
- ElasticSearch en modo clúster (versión compatible con Liferay CE/DXP)
- Mecanismos de tolerancia a fallos.
- Almacenamiento de alto rendimiento para índices
- Acceso restringido desde la capa front-end y servicios autorizados
- Configuración alineada con las recomendaciones de Liferay para integraciones de búsqueda

Capa de microservicios (back-end funcional)

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación).
- NodeJS (versión LTS)
- Framework NestJS
- Acceso seguro a PostgreSQL y RabbitMQ

Capa de mensajería

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación).
- RabbitMQ en modo clúster con soporte para quorum queues
- Almacenamiento persistente de baja latencia
- Configuración tolerante a fallos y conmutación automática

Capa de base de datos

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación).
- PostgreSQL en alta disponibilidad mediante replicación síncrona
- Mecanismo automático de failover
- Almacenamiento tipo NVMe o SSD empresarial
- Acceso exclusivo desde front-end y back-end

Almacenamiento:

El almacenamiento deberá cubrir:

- el repositorio de contenidos/document library de Liferay,
- los índices del clúster de ElasticSearch,
- la base de datos PostgreSQL (datos y WAL),
- los microservicios (logs, artefactos temporales y configuraciones),
- y cualquier servicio transversal asociado al funcionamiento de la nueva arquitectura.

El adjudicatario deberá dimensionar el almacenamiento en función de las necesidades declaradas en su propuesta técnica y de las buenas prácticas de los productos incluidos.

5.1.3. REQUISITOS PARA EL ENTORNO DE VALIDACIÓN

El entorno de Validación tendrá como finalidad permitir a VEIASA la revisión, prueba y aceptación formal de los entregables correspondientes a la **nueva Web de Citas ITV** antes de su paso a Preproducción y Producción. Este entorno deberá estar plenamente aislado del entorno de Producción, garantizando que su actividad no tenga impacto alguno sobre los servicios productivos. No obstante, podrá compartir con el entorno de Preproducción determinados componentes de infraestructura no productiva siempre que se mantenga el aislamiento lógico mediante mecanismos de segregación (por ejemplo, virtual hosts, bases de datos separadas, roles independientes y políticas de acceso estrictas).

El entorno de validación deberá **reproducir de forma fiel la arquitectura funcional** del entorno productivo, sin necesidad de replicar sus capacidades de alta disponibilidad o escalabilidad horizontal. Deberá por tanto incluir las mismas capas funcionales y los mismos componentes software que el entorno de producción.

5.1.4. REQUISITOS PARA LOS ENTORNOS DE PREPRODUCCIÓN

Durante el periodo de transición entre la arquitectura actual de la Web de Citas ITV y la nueva solución basada en Liferay y microservicios, el adjudicatario deberá proporcionar dos entornos de Preproducción independientes, plenamente operativos y accesibles para VEIASA, con el fin de permitir pruebas funcionales, diagnósticos, validaciones urgentes y la resolución de incidencias en cualquiera de las dos plataformas.

Los entornos de Preproducción serán:

- Preproducción Web de Citas actual (arquitectura J2EE / Oracle 12c)
- Preproducción Nueva Web de Citas (Liferay + NGINX + NestJS + RabbitMQ + Elastic Search+ PostgreSQL)

Cada entorno deberá mantener su propia infraestructura lógica, plenamente segregada, sin interferencias entre aplicaciones y con acceso seguro desde VEIASA mediante VPN/RCJA. Ambos entornos deberán estar protegidos por el WAF corporativo.

Preproducción – Web de Citas actual (Tecnología J2EE)

El entorno de Preproducción de la Web de Citas actual servirá como plataforma de soporte durante el tiempo de convivencia, únicamente para resolución de incidencias, refactorizaciones puntuales o comprobaciones necesarias hasta la desactivación completa de esta versión.

Este entorno deberá contar con, al menos, las siguientes capas y componentes software obligatorios, quedando el dimensionamiento físico o número de instancias a propuesta del licitador:

1. Capa front-end (J2EE)

- Sistema operativo Oracle CentOS 7
- Servidor web Apache HTTPD (última versión estable)
- Contenedor Java: Tomcat 8.5 / JBoss EAP 7 / Wildfly 10 (según indique VEIASA)
- Soporte a JMS
- Pentaho PDI CE 6.1 cuando así lo requiera la aplicación
- Acceso al almacenamiento compartido del entorno
- Acceso protegido a través del WAF

2. Capa back-end (Oracle Database)

- Linux Red Hat 7 64bits
- Oracle Database 12c (instancia única; sin RAC)
- Almacenamiento redundado con RAID o tecnología equivalente
- Acceso permitido exclusivamente desde la capa front-end y redes autorizadas

Preproducción – Nueva Web de Citas (Liferay + Microservicios)

Este entorno reproducirá la arquitectura funcional y lógica del entorno de Producción y deberá operar igualmente en alta disponibilidad, si bien podrá hacerlo con un dimensionamiento inferior al de dicho entorno productivo. La estructura de componentes, capas y mecanismos de tolerancia a fallos será equivalente a la de Producción, salvo que VEIASA determine expresamente que algún elemento no requiere replicación completa. De este modo se garantiza la representatividad total de las pruebas, despliegues e integraciones previas al paso a Producción.

1. Capa front-end (Liferay + NGINX)

- Sistema operativo Oracle Linux (la última versión estable a fecha de adjudicación)
- Servidor web/proxy inverso NGINX

- Liferay CE/DXP con el servidor de aplicaciones correspondiente (Tomcat)
- Integración con ElasticSearch
- Acceso al almacenamiento compartido del entorno
- Acceso protegido a través del WAF

2. Capa de microservicios (NodeJS + NestJS)

- NodeJS LTS
- NestJS, siguiendo los arquetipos corporativos
- Configuración estricta de firewall (mínimo privilegio)
- Acceso exclusivamente desde front-end, RabbitMQ y PostgreSQL

3. Capa de mensajería (RabbitMQ)

El entorno de Preproducción deberá contar con:

- un despliegue de RabbitMQ compatible con Producción.
- o acceso aislado mediante virtual hosts a un clúster no productivo compartido con Validación.

4. Capa de base de datos (PostgreSQL)

- PostgreSQL versión igual a la utilizada en Producción
- Recursos suficientes para pruebas de integración
- Replicación opcional (no obligatoria para Preproducción)
- Acceso estrictamente restringido mediante firewall

Requisitos comunes de ambos entornos de Preproducción

- Bastionado según guías CCN-STIC (ENS – Nivel Medio).
- Protección mediante el WAF corporativo.
- Monitorización completa del estado de los sistemas.
- Soporte a Servicios Transversales: FTP/S, logging, monitorización y backup (según Capítulo 6).
- Registro y envío de logs a los colectores corporativos de VEIASA.
- Conectividad segura con VEIASA mediante VPN, RCJA o los mecanismos que esta determine.
- Posibilidad de realizar refrescos periódicos de bases de datos desde Producción, según calendario y procedimiento aprobado por VEIASA.
- Aislamiento completo entre los entornos de Preproducción de la Web de Citas actual y la nueva.

5.2. SERVICIO PORTAL eITV

El Portal eITV (https://portaleitv.veiasa.es/) es una aplicación corporativa orientada a la tramitación electrónica de los procedimientos asociados a las inspecciones no periódicas de vehículos, permitiendo a los usuarios aportar documentación, realizar gestiones previas y consultar el estado de sus expedientes de manera telemática

El portal e-ITV se encuentra desarrollada bajo tecnología ReactJS, apoyándose de servicios web desarrollados en Python que deberán alojarse en el mismo sistema que el Portal e-ITV.

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

5.2.1 ALOJAMIENTO

Desde el punto de vista del hardware la arquitectura de servidores que se proponga para la implementación del Portal e-ITV deberá estar basada en los estándares de facto del mercado. Dicha arquitectura deberá sustentar un entorno de PRODUCCIÓN con su equivalente de PREPRODUCCIÓN, basados en servidores virtuales independientes por cada entorno a modo de front-end que deberán cumplir con las siguientes condiciones:

1. Servidor front-end. Se ubicará en la DMZ del proveedor, protegido mediante un Sistema de Seguridad Perimetral que deberá incluir obligatoriamente un Firewall de Aplicaciones Web (WAF).
   Dicho WAF inspeccionará el tráfico entrante al Portal eITV conforme a las recomendaciones, garantizando que el acceso desde Internet se realice exclusivamente mediante protocolo HTTPS (TCP/443) y bloqueando cualquier patrón de tráfico considerado indebido o malicioso.

   Este servidor albergará tanto el portal Web de usuario desarrollado bajo tecnología React como los servicios web o webservices de usuario desarrollados sobre lenguaje Python.

   Para el caso concreto del entorno de PREPRODUCCIÓN, este sistema se ubicará en una LAN privada del proveedor y no estará publicado a Internet.

2. Con la finalidad de evitar la subida de documentos infectados a través del Portal e-ITV por parte de los usuarios, ambos entornos deberán incluir un motor de escaneo antimalware, basado en tecnologías como Kaspersky Scan Engine o soluciones equivalentes, alojado en las infraestructuras del adjudicatario. No serán válidas las propuestas que utilicen este servicio en modalidad cloud pública externa.

   Este servicio deberá estar disponible para su integración con el Portal eITV con el fin de analizar los archivos y contenidos que puedan ser cargados o procesados por el sistema.

La solución deberá cumplir, como mínimo, las siguientes características:

- Arquitectura escalable.
- Integración mediante API para detección de amenazas desde las aplicaciones.
- Integración con aplicaciones, portales web, gateways de correo, NAS y proxies mediante HTTP o ICAP.
- Capacidad de escaneo de archivos y URLs.
- Detección de malware, phishing, rootkits, spyware, adware y otras amenazas.
- Debe permitir funcionar como servicio REST, en modo clúster o dentro de contenedores Docker/kubernetes, con panel web de gestión.

El adjudicatario será responsable de la instalación, configuración, actualización y mantenimiento operativo de este servicio durante toda la duración del contrato.

3. 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).

4. 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 adjudicataria para la correcta explotación de todos los servicios ofrecidos por el Portal e-ITV, en función de sus desarrollos y aplicaciones. En este documento se hace una propuesta de mínimos a este respecto en el apartado 5.2.2.

5. 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 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 Preproducción a Producción). Igualmente, en este documento se hace una propuesta de mínimos en el apartado 5.2.3.

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

5.2.2 REQUISITOS PARA EL ENTORNO DE PRODUCCION

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 y un servicio de análisis de malware a demanda con las características expuestas en el punto 5.2.1.

- 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 licitador deberá garantizar que todos los servicios descritos operen **sin punto único de fallo**. Para ello, deberá dimensionar las capas front-end y back-end con el número de nodos necesario para cumplir los SLA y garantizar la disponibilidad 24x7. No se aceptarán arquitecturas con un único nodo en componentes críticos

- El sistema operativo empleado para el front-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 adjudicatario deberá disponer de las capacidades de almacenamiento necesarias para garantizar alta disponibilidad y ausencia de punto único de fallo.

- Asimismo, la propuesta de arquitectura presentada por el licitador será objeto de valoración atendiendo a su adecuación técnica, coherencia, robustez, escalabilidad, eficiencia en el uso de recursos y alineamiento con los requisitos de alta disponibilidad y seguridad establecidos en este pliego.
  Esta valoración considerará especialmente la calidad del diseño planteado, la justificación técnica de las decisiones adoptadas, la capacidad de la arquitectura para soportar evolutivos y picos de carga, los mecanismos de tolerancia a fallos, la correcta segregación de componentes y redes, así como cualquier elemento que contribuya a optimizar la operación y continuidad del servicio. En todo caso, la arquitectura deberá permanecer dentro de los parámetros funcionales, tecnológicos y de seguridad definidos por VEIASA.

La propuesta del licitador deberá contemplar el despliegue de los siguientes componentes mínimos, pudiendo dimensionar libremente el número de instancias o nodos necesarios:

Servidor front-end (Portal eITV)

- 30 GB de almacenamiento en sistema redundado
- Sistema operativo Oracle Linux 8 , instalación mínima con particiones dedicadas para /var y /var/log.
- SELinux en modo Enforcing y firewall configurado según directrices de VEIASA.
- Servidor web Apache HTTP Server 2.4.x con soporte SSL, configurado con los certificados proporcionados por VEIASA.
- Middleware mod_wsgi 4.9.0 para la ejecución de servicios Python.
- Intérprete Python 3.9. Las librerías y dependencias necesarias para la ejecución del Portal eITV y de sus servicios backend se instalarán mediante el gestor de paquetes estándar de Python (pip o equivalente), a partir de los ficheros de definición de dependencias que serán facilitados por VEIASA.
  El adjudicatario será responsable de mantener dichas dependencias en versiones soportadas y compatibles entre sí, sin alterar el correcto funcionamiento de la aplicación.
- Acceso protegido a través del WAF.

Servidor de colas y servicios asociados

- RabbitMQ 3.9.14 (sobre Erlang/OTP 24), con la configuración de virtual hosts, usuarios y colas proporcionada por VEIASA.
- Configuración del planificador Celery según instrucciones de VEIASA.

Full Qualified Domain Names (FQDNs) / URLs: los sistemas implementados serán accesibles mediante los siguientes FQDNs/URLs:

- Servidor front-end: https://portaleitv.veiasa.es/

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.

5.2.3 REQUISITOS PARA EL ENTORNO DE PREPRODUCCIÓN

Este entorno reproducirá la arquitectura funcional y lógica del entorno de Producción. La estructura de componentes, capas y mecanismos de tolerancia a fallos será equivalente a la de Producción, salvo que VEIASA determine expresamente que algún elemento no requiere replicación completa. De este modo se garantiza la representatividad total de las pruebas, despliegues e integraciones previas al paso a Producción.

Servidor front-end (Preproducción eITV)

- 30 GB de almacenamiento en sistema redundado
- Sistema operativo Oracle Linux 8, con instalación mínima y particiones dedicadas para /var y /var/log.
- SELinux en modo Enforcing y firewall configurado según directrices de VEIASA.
- Servidor web Apache HTTP Server 2.4.x con soporte SSL; los certificados serán proporcionados por VEIASA.
- Middleware mod_wsgi 4.9.0 para ejecución de servicios Python.
- Intérprete Python 3.9. Las librerías y dependencias necesarias para la ejecución del Portal eITV y de sus servicios backend se instalarán mediante el gestor de paquetes estándar de Python (pip o equivalente), a partir de los ficheros de definición de dependencias que serán facilitados por VEIASA.
  El adjudicatario será responsable de mantener dichas dependencias en versiones soportadas y compatibles entre sí, sin alterar el correcto funcionamiento de la aplicación.
- Acceso a través del WAF si el entorno se expone externamente (o mediante VPN/RCJA en caso contrario).

Servidor de colas y servicios asociados

- RabbitMQ 3.9.14 (sobre Erlang/OTP 24), con virtual hosts, usuarios y colas configurados según instrucciones de VEIASA.
- Configuración del planificador Celery según los servicios definidos por VEIASA.

Nombres de dominio y DNS

- El entorno será accesible mediante la URL:
  https://portaleitv-val.veiasa.es

6. REQUERIMIENTOS COMUNES

6.1 SERVICIOS TRANSVERSALES APLICABLES A TODAS LAS APLICACIONES

Además de los entornos específicos definidos para cada una de las aplicaciones incluidas en este pliego, el adjudicatario deberá proporcionar los siguientes servicios comunes para garantizar la correcta operatividad, integración y supervisión de los sistemas:

- Servicio de almacenamiento de ficheros compartido

  El adjudicatario deberá proporcionar un sistema de almacenamiento persistente y compartido, accesible desde los distintos nodos que conforman los entornos de Producción, Preproducción y Validación de las aplicaciones objeto de este contrato.

  Dicho almacenamiento se empleará para:
  - la gestión documental y los repositorios de contenidos de aquellas aplicaciones que lo requieran (p.ej., Liferay en la nueva Web de Citas),
  - el almacenamiento temporal o permanente de ficheros subidos por los usuarios finales en el Portal eITV u otras aplicaciones con funcionalidad equivalente,
  - el acceso compartido a recursos comunes entre nodos de front-end y back-end cuando sea necesario para garantizar la coherencia del servicio.

  El sistema de almacenamiento deberá estar diseñado sin punto único de fallo, ofreciendo alta disponibilidad y mecanismos de redundancia adecuados al volumen y criticidad del servicio.

  La tecnología de almacenamiento (NFS, NAS, almacenamiento distribuido o equivalente) será propuesta por el licitador, y deberá garantizar la integridad, disponibilidad y consistencia de los datos, así como su compatibilidad con los requisitos específicos de cada aplicación.

- Servicio FTP/S

  El adjudicatario deberá habilitar un servicio FTP/S accesible de forma segura desde los servidores alojados, con un espacio mínimo de 50 GB, destinado al intercambio de datos con sistemas externos. Este servicio podrá ser compartido entre aplicaciones, garantizando siempre la existencia de espacios lógicamente segregados, controles de acceso independientes y trazabilidad de las operaciones.

- Servicio de correo

  El adjudicatario deberá proporcionar un servicio de correo electrónico destinado al envío de notificaciones generadas por las aplicaciones alojadas. El servicio deberá operar en modalidad multidominio, permitiendo el envío seguro desde los dominios que VEIASA determine (incluyendo, como mínimo, itvcita.com).

Deberá garantizar autenticación y reputación mediante SPF, DKIM y DMARC, así como disponibilidad 24x7, mecanismos de reintento, monitorización y registro de envíos. VEIASA facilitará la configuración DNS necesaria para la correcta operación del servicio.

- Servicios de monitorización y rendimiento

  Se habilitarán las soluciones de monitorización necesarias para supervisar la disponibilidad, rendimiento, uso de recursos y estado de los sistemas que soportan las aplicaciones.
  VEIASA podrá instalar o integrar herramientas propias de diagnóstico o extracción de métricas en las instalaciones del adjudicatario, quien deberá proporcionar el acceso seguro necesario, así como los agentes o conectores requeridos.

- Servicio de registro y envío de logs

  El adjudicatario deberá habilitar las configuraciones y comunicaciones necesarias para el correcto reenvío de logs (sistema, aplicación, auditoría y seguridad) hacia los colectores corporativos definidos por VEIASA.
  Los logs deberán enviarse en tiempo real o con la frecuencia indicada por VEIASA y cumplir con las recomendaciones del Esquema Nacional de Seguridad.

- Compatibilidad con herramientas corporativas

  Los servicios indicados deberán garantizar la compatibilidad con las plataformas de análisis de VEIASA, tanto actuales como futuras, incluyendo sistemas SIEM, Graylog o soluciones equivalentes de observabilidad.

6.2 REDUNDANCIA, DIMENSIONAMIENTO Y ESCALABILIDAD

- La solución general propuesta para deberá garantizar la ausencia de puntos únicos de fallo, contemplando la redundancia de los elementos críticos de los servidores que alberguen los servicios. y de la infraestructura asociada, tales como fuentes de alimentación, ventiladores, sistemas de almacenamiento (RAID), hipervisores y elementos de red que alberguen los servicios.

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

- 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.

- La infraestructura deberá cumplir con los siguientes objetivos de continuidad del servicio aplicables a **todas** las aplicaciones web:

- RTO (Recovery Time Objective) ≤ 60 minutos
- RPO (Recovery Point Objective) ≤ 15 minutos, alcanzables mediante mecanismos de replicación y/o copias de seguridad continuas.

Sera objeto de valoracion conforme a lo indicado en el apartado 8 del CR la reducción del tiempo de recuperación del servicio (RTO) por debajdo del máximo permitido (60 minutos), con un valor mínimo admisible de RTO de **15 minutos**.

- El adjudicatario deberá elaborar y mantener un Plan de Capacidad que contemple la evolución previsible de los recursos y que será revisado con periodicidad trimestral, aportando evidencias del uso real de CPU, memoria, almacenamiento, entrada/salida y red, así como las recomendaciones de ajuste o ampliación que procedan para mantener los niveles de servicio comprometidos.

6.3 SEGURIDAD PERIMETRAL Y WAF

El adjudicatario deberá proporcionar un servicio de Firewall de Aplicaciones Web (WAF) en alta disponibilidad, destinado a proteger los entornos de Producción y Preproducción de todas las aplicaciones incluidas en el presente pliego.

El WAF podrá implementarse sobre una plataforma común, siempre que se garantice:

- la existencia de políticas diferenciadas por aplicación y por entorno,
- la segregación lógica del tráfico,
- la capacidad de inspección en tiempo real para todo el tráfico entrante y saliente,
- la aplicación de reglas basadas en OWASP Top 10 y guías CCN-STIC,
- la disponibilidad y rendimiento suficiente para absorber la carga agregada de todos los entornos.

El WAF deberá estar en funcionamiento tanto para los entornos de Producción como para los entornos de Preproducción, incluso cuando estos últimos no estén expuestos a Internet de forma directa, debiendo inspeccionar el tráfico HTTP/HTTPS que acceda a los servicios web de las aplicaciones objeto de este contrato, independientemente de que su origen sea Internet, redes internas de VEIASA, conexiones procedentes de VPN, RCJA o cualquier otro mecanismo de acceso remoto autorizado por VEIASA.

Sin perjuicio del cumplimiento de los requisitos mínimos establecidos en el presente apartado, la incorporación de medidas adicionales de seguridad perimetral podrá ser objeto de valoración conforme a lo dispuesto en el PCAP.

6.4 CONECTIVIDAD

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

- Un ancho de banda de acceso a internet garantizado al 100% de, como mínimo, **100Mbps**. **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.**

- Doble enlace de acceso a Internet con balanceo automático (active-active) y convergencia mediante BGP

- Proporcionar y mantener los equipos de telecomunicaciones: routers, firewalls, switches, balanceadores y WAF, asegurando su disponibilidad en HA.

- 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: Tanto la web de Citas ITV como el portal eITV son accedidas directamente desde internet por los usuarios, pero existen actualmente 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.

6.5. 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.

- 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. 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 CPD deberá disponer de conectividad redundante a Internet y estar integrado en una red troncal (Backbone) de alta capacidad, gestionada por el adjudicatario, que asegure la disponibilidad e integridad del tráfico hacia los servidores alojados.

6.6 CENTRO DE RESPALDO

Para garantizar la continuidad del servicio, se requiere que el adjudicatario disponga de un Centro de Respaldo donde poder ofrecer continuidad ante una contingencia desde el inicio de la prestación de los servicios. Las características que debe cumplir el Centro de Respaldo son las mismas que para el CPD principal. Concretamente debe tener:

- Sistemas redundantes de alimentación ininterrumpida de Energía.

- 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.
- 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)

6.7. SOPORTE

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**. Este mantenimiento incluirá:

- **Atención de incidencias:** la empresa adjudicataria 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 para el sistema mientras que los pasos a otros entornos 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: la empresa adjudicataria 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.

- **Otras peticiones de servicio**: el servicio deberá contemplar una bolsa de horas de tareas adicionales de, al menos, 240 horas al año, para realizar tareas no contempladas inicialmente para cualquiera de las aplicaciones, por ejemplo:

    - ✓ Pruebas con nuevas tecnologías.
    - ✓ Integración de nuevos sistemas.
    - ✓ Instalación de nuevo software
    - ✓ Pruebas funcionales.

- **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.
- Chequeo del estado de otros servicios o procesos no estándar para lo que se hayan desarrollado previamente los scripts adecuados.

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

En base a esta monitorización, la empresa adjudicataria 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 de consultas, propuesta de planes de ejecución alternativos, recodificación, cambios paramétricos, etc.
- 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.

El servicio deberá contar con una organización adecuada que garantice la correcta operación, mantenimiento y soporte de la plataforma durante toda la vigencia del contrato.

La estructura organizativa y el modelo de gestión del servicio deberán permitir:

- una adecuada interlocución con VEIASA,

- la gestión eficaz de incidencias y peticiones de servicio,
- el cumplimiento de los niveles de servicio establecidos,
- y la continuidad operativa en caso de contingencias.

La organización del servicio deberá describirse en la propuesta técnica y podrá ser objeto de valoración conforme a los criterios establecidos en el PCAP, sin que el presente requisito implique la exigencia de adscripción de medios personales específicos.

6.8. 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 por parte del fabricante y derechos de acceso a parches y nuevas versiones, durante el periodo de duración del contrato, sin coste alguno para VEIASA, **exceptuando** las licencias de **Base de datos ORACLE** (y RAC) que sean necesarias implementar, las cuales serán proporcionadas por VEIASA.

6.9. DOCUMENTACIÓN TÉCNICA

El adjudicatario generará los documentos e informes, tanto en formato papel como en soporte 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.

6.10. 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.

6.11. ACUERDO 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
Disponibilidad	D1	Disponibilidad de todos los servicios de la plataforma	>= 99,95%
Incidencias	I1	Tiempo de resolución ante incidencias en el servicio	< 60 minutos
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 lasa 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.

6.12 AUDITORÍAS

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.

6.13. 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, como parte de la solución técnica a incluir en el sobre 2**

6.14. 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, **como parte de la solución técnica a incluir en el sobre 2** cuya ejecución debe 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.

6.15. SISTEMAS DE GESTIÓN DEL SERVICIO

Las empresas licitadoras deberán acreditar, antes de la adjudicación , mediante copia de las mismas, 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.

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 o superior 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.

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. 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

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.

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.

7.5. 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.

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 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 apartado específico de protección de datos del Pliego de Cláusulas Administrativas Particulares y el contrato que se firme al efecto.

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