PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA REALIZAR EL DESARROLLO Y EL SOPORTE A LA PUESTA EN MARCHA DE PSIS 9.0

Número de expediente: AOC-2023-44

ÍNDICE DE CLÁUSULAS Y ANEXOS

1 Objeto del contrato 4
2 Objetivos del proyecto 4
3 Descripción del servicio actual 4
3.1 Situación actual 4
3.2 Arquitectura actual del entorno productivo (PSIS 6.0) 5
3.3 Definición de la arquitectura de PSIS 8.0 5
4 Desarrollo y soporte a la puesta en marcha de PSIS 9.0 5
4.1 Alcance y duración 5
4.2 Desarrollos 5
4.2.1 Migración de la JVM a la versión estable más reciente 6
4.2.2 Migración de las librerías de Spring Framework 6
4.2.3 Migración de las librerías de BouncyCastle 7
4.2.4 Migración de las librerías de Apache Santuario 8
4.2.5 Migración de las librerías de Hibernate 8
4.2.6 Redis 9
4.2.7 Refactoring de la consola web de administración 10
4.2.8 Servidor web ligero 10
4.2.9 Estudio de refactoring de la arquitectura de código 11
4.3 Soporte a la puesta en marcha en preproducción y producción 11
4.3.1 Migración de Oracle en AWS Aurora Serverless V2 (PostgreSQL compatible) . 12
4.3.1.1 Preproducción 12
4.3.1.2 Producción 13
4.4 DevSecOps 16
4.5 Equipo de proyecto 16
4.6 Coordinación con la Oficina Técnica de mantenimiento evolutivo y correctivo 17
4.7 Requerimientos funcionales 17
4.8 Requerimientos técnicos 18
4.8.1 Infraestructura necesaria para llevar a cabo el desarrollo del proyecto 18
4.8.2 Dimensionamiento 18
4.8.3 Código fuente y propiedad intelectual 20
4.8.4 Tests unitarios y pruebas de integración 20
4.8.5 Tests de rendimiento 21
4.9 Requerimientos legales 21
4.10 Requerimientos de seguridad 21
4.10.1 Medidas de seguridad que debe incorporar PSIS 9.0 como solución 21
4.10.2 Medidas de seguridad a cumplir por parte del adjudicatario 22
4.10.2.1 Certificaciones de seguridad 22
4.10.2.2 Control de acceso al sistema 22

4.10.2.3 Control de personal 22
4.10.2.4 Protección de la información 22
4.10.2.5 Protección de los soportes 23
4.11 Requerimientos de protección de datos 23
4.12 Plan de devolución del servicio 24
4.13 Condiciones de ejecución 24
4.13.1 Obligaciones básicas 24
4.13.2 Herramientas de control 25
4.13.3 Normativa aplicable 25
4.14 Modelo de relación 25
5 Anexos 26

1 Objeto del contrato

El objeto del presente pliego es fijar las prescripciones técnicas particulares que regirán la contratación del desarrollo y el soporte a la puesta en marcha de PSIS 9.0 (Plataforma de Servicios de Identificación y Firma) del Consorci AOC.

El objetivo es continuar en la línea de modernización tecnológica de PSIS para garantizar la continuidad del servicio en un entorno de creciente consumo. El volumen actual de operaciones en PSIS es de alrededor de 28 millones de operaciones mensuales con picos de hasta más de 32 millones de operaciones mensuales.

2 Objetivos del proyecto

El objetivo es avanzar en la modernización de la solución tecnológica actual, desplegada en la nube, para utilizar las ventajas que aportan las nuevas tecnologías, para dar solución a las necesidades futuras que se prevé que el servicio tendrá a medio/largo plazo.

Este proyecto incluirá:

- Desarrollo de la solución.
- Tests unitarios.
- Tests funcionales.
- Tests de rendimiento.
- Tests de seguridad.
- Realizar tareas asociadas a la puesta en marcha del servicio en los entornos de desarrollo, preproducción y producción.

3 Descripción del servicio actual

3.1 Situación actual

El Consorci AOC ofrece a las administraciones públicas catalanas el servicio de validación. PSIS es la plataforma tecnológica desde la que se presta el servicio de validación. El servicio de validación comprende principalmente la validación de certificados y la validación y completado o preservación de firmas digitales. También permite la creación y validación de sellos de tiempo y la creación de firmas digitales de forma segura y desatendida.

El servicio de validación (en adelante PSIS) es consumido por todos los entes que forman parte de la administración pública catalana que disponen de aplicaciones informáticas donde se hace uso de certificados y firmas digitales, para dotar de seguridad a los procesos de identificación y tratamiento de documentos firmados. PSIS es un servicio transversal que se consume por prácticamente la totalidad de los servicios del Consorci AOC, así como por el resto de los entes de la administración pública catalana. Debido a esta transversalidad, es el servicio con mayor consumo del Consorci AOC: En 2022 el servicio procesó más de 300 millones de operaciones, lo que representa un incremento de unos 50 millones de operaciones respecto a 2021. Hay que tener en cuenta que el crecimiento de consumo en el resto de servicios se traduce también en un incremento del consumo de PSIS.

La solución tecnológica actual, PSIS 8.0, está desarrollada por su despliegue en el cloud en Amazon Web Services (en adelante AWS). Actualmente está desplegada en AWS sólo en el entorno de desarrollo. Los entornos de preproducción y producción todavía los tenemos en modalidad on-premises, con la versión 6.0. PSIS 6.0 es pues la modalidad on-premises; PSIS 7.0 fue una versión intermedia que no llegamos a desplegar en el entorno de preproducción y producción, y que incluía como cambio principal el despliegue en Kubernetes. Y PSIS 8.0 es Kubernetes desplegado en el Cloud de AWS con integración con servicios de AWS.

Está previsto desplegar la versión 8.0 en preproducción y producción en el segundo semestre de 2023.

La solución PSIS 8.0 es totalmente funcional. Pero es necesario actualizarla y modernizar las tecnologías empleadas. PSIS 9.0 se desarrollará a partir de PSIS 8.0.

3.2 Arquitectura actual del entorno productivo (PSIS 6.0)

Para más información consulte el documento:
Annex2_Arquitectura_PSIS6.0.pdf (para descargar vaya al punto 5 Anexos).

3.3 Definición de la arquitectura de PSIS 8.0

Para más información consulte el documento:
Annex3_AOC_Definició_Arquitectura_PSIS_8.0.pdf (para descargar vaya al punto 5 Anexos)

4 Desarrollo y soporte a la puesta en marcha de PSIS 9.0

Descripción de los servicios a prestar por el adjudicatario.

4.1 Alcance y duración

El alcance del proyecto comprende el desarrollo y apoyo a la puesta en marcha de PSIS 9.0.

La definición final del desarrollo será consensuada conjuntamente entre el adjudicatario y el Consorci AOC.

- En este contrato se continuará con el desarrollo de la solución de PSIS en la nube de AWS. PSIS ya está desplegada en AWS, y los evolutivos que se llevarán a cabo en el presente contrato están enfocados a la modernización del código fuente y la arquitectura (si procede).
- El Consorci AOC proporciona el espacio necesario en AWS para el entorno de desarrollo. La infraestructura y espacio en AWS de los entornos de preproducción y producción serán proporcionados por el Consorci AOC a lo largo de 2023.
- Construcción y desarrollo de la solución en el entorno de desarrollo.
- Se incluye el apoyo a la instalación y al despliegue del servicio en los sistemas técnicos del Consorci AOC (entornos de preproducción y producción).
- Documentación, creación de los procesos y formación detalladas de cada una de estas actividades.
- La ejecución de las tareas encomendadas deberá llevarse a cabo en las instalaciones del adjudicatario. Es posible que en alguna ocasión sea necesario el desplazamiento de alguno de los miembros del equipo a las instalaciones del Consorci AOC.

La prestación del servicio empezará el 01/07/2023 (o en la fecha de formalización del contrato), y finalizará el 31/12/2024.

4.2 Desarrollos

A continuación, describimos las tareas de desarrollo que habrá que realizar sobre la solución de PSIS desplegada en AWS.

4.2.1 Migración de la JVM a la versión estable más reciente

Actualmente PSIS está funcionando con la versión de java 1.8.0_291. Java 8 ha llegado al final de las actualizaciones públicas, es decir, que no se publicarán nuevas versiones sobre Java 8. Oracle no ofrece servicio de soporte gratuito para las versiones Java 7 y Java 8.

A fecha de enero de 2023, Java 17 LTS es la última versión con soporte a largo plazo para la plataforma Java SE.

Los binarios JDK 19 y JDK 17 se distribuyen de forma gratuita y se pueden utilizar en entornos productivos, sin coste alguno, de acuerdo a la política de *No-Fee Terms and Conditions* de Oracle. JDK 19 recibirá actualizaciones de acuerdo con estas condiciones, hasta marzo de 2023, cuando será sustituida por JDK 20. JDK 17 recibirá actualizaciones según estas condiciones, al menos hasta septiembre de 2024.

La versión de Java más actual pues a fecha de enero de 2023 es la versión 19, y será sustituida por la versión 20 en marzo de 2023. Para poder disfrutar de soporte gratuito, y, sobre todo, para poder aprovechar las mejoras que nos ofrecen las versiones que se han ido introduciendo desde la versión 8 en adelante (como la resolución de bugs, vulnerabilidades de seguridad, etc.), es importante actualizar el código de PSIS a la versión estable más actual posible.

En la siguiente página web Oracle informa de las mejoras y correcciones introducidas en las diferentes releases:

https://www.oracle.com/java/technologies/javase/jdk-relnotes-index.html

Tareas a realizar por parte del adjudicatario:

- Escoger la versión más adecuada de la JVM, teniendo en cuenta las necesidades de las migraciones de las librerías de Spring (4.2.2), BouncyCastle (4.2.3) y Apache Santuario (4.2.4), e Hibernate (4.2.5).

4.2.2 Migración de las librerías de Spring Framework

Actualmente PSIS utiliza la versión 5.1.7 del framework de Spring. La versión más actual de estas librerías es la versión 6.0.x.

Las versiones que tienen soporte oficial actualmente (enero de 2023) son:

- 6.0.x es la línea de producción principal a partir de noviembre de 2022. Esta nueva generación del framework incluye una línea de base JDK 17 y Jakarta EE 9.
- 5.3.x es la rama final de la quinta generación, con soporte a largo plazo proporcionado para JDK 8, JDK 11, JDK 17 y Java EE 8.
- 4.3.x logró su EOL oficial (fin de vida útil) el 31 de diciembre de 2020. No hay previsto ningún parche de mantenimiento y seguridad en esta línea.
- 3.2.x logró su EOL oficial (fin de vida útil) el 31 de diciembre de 2016. No está previsto ningún parche de seguridad y mantenimiento en esta línea.

Las versiones de la JVM soportadas son:

- Spring Framework 6.0.x: JDK 17-21
- Spring Framework 5.3.x: JDK 8-19

Tareas a realizar por parte del adjudicatario:

- Estudio comparativo de migración en las versiones 5.3 y 6.0.
- Propuesta de diseño de los cambios que implique en PSIS la versión escogida.
- Pruebas de rendimiento para garantizar que mantenemos, como mínimo, el mismo rendimiento que con la versión actual.
- Análisis de los cambios a realizar: Revisión de los objetivos del proyecto y consenso con el Consorci AOC sobre cómo alcanzarlos.

4.2.3 Migración de las librerías de BouncyCastle

Las API Crypto de Bouncy Castle para Java consisten en lo siguiente:

- Una API de criptografía ligera.
- Un proveedor de Java Cryptography Extension (JCE) y Java Cryptography Architecture (JCA).
- Un proveedor para Java Secure Socket Extension (JSSE).
- Implementación *clean room* de JCE 1.2.1.
- Una biblioteca para leer y escribir objetos ASN.1 codificados.
- API ligeras para TLS (RFC 2246, RFC 4346) y DTLS (RFC 6347/RFC 4347).
- Generadores de certificados X.509 versión 1 y versión 3, CRL versión 2 y archivos PKCS12.
- Generadores de certificados de atributos X.509 versión 2.
- Generadores/procesadores para S/MIME y CMS (PKCS7/RFC 3852).
- Generadores/procesadores para OCSP (RFC 2560).
- Generadores/procesadores para TSP (RFC 3161 y RFC 5544).
- Generadores/procesadores para CMP y CRMF (RFC 4210 y RFC 4211).
- Generadores/procesadores para OpenPGP (RFC 4880).
- Generadores/procesadores para control de acceso extendido (EAC: *Extended Access Control*).
- Generadores/procesadores para validación de datos y servidor de certificación (DVCS: *Data Validation and Certification Server*) - RFC 3029.
- Generadores/procesadores para la autenticación de entidades con nombre basado en DNS (DANE: *DNS-based Authentication of Named Entities*).
- Generadores/procesadores para la inscripción RFC 7030 a través del transporte seguro (EST: *Enrollment over Secure Transport*).
- Versiones jar firmadas adecuadas para JDK 1.4-1.8 y Sun JCE.

PSIS utiliza esta librería para validar certificados, para crear, validar y completar firmas en formato ASN.1, y para crear y validar sellos de tiempo en formato ASN.1, etc.

En la siguiente tabla tenemos la versión de las librerías BouncyCastle que utiliza actualmente PSIS, en paralelo a la versión más reciente en enero de 2023 publicada por JDK 1.8 y superiores:

Descripción del paquete	Librería PSIS	Datos	Última versión para JDK 1.8 y superiores	Datos
PROVEEDOR	bcprov-jdk15on-1.49.jar	31/mayo/2013	bcprov-jdk18on-172.jar	25/septiembre/2022
PKIX/CMS/EAC/PKCS/ OCSP/TSP/OPENSSL	bcpkix-jdk15on-1.49.jar	31/mayo/2013	bcpkix-jdk18on-172.jar	25/septiembre/2022
SMIME	bcmail-jdk15on-1.49.jar	31/mayo/2013	bcmail-jdk18on-172.jar	25/septiembre/2022

En la siguiente página web tenemos información sobre las diferentes versiones que se han publicado de las librerías de BouncyCastle para Java:

https://www.bouncycastle.org/latest_releases.html

Debe decirse que la versión más actual de BouncyCastle no es compatible con las versiones anteriores. Por tanto, actualizarla implica rehacer el código que utiliza las APIs de BouncyCastle.

Tareas a realizar por parte del adjudicatario:

- Refactoring del código de PSIS para utilizar la versión más actual de las librerías.

4.2.4 Migración de las librerías de Apache Santuario

El proyecto Apache Santuario tiene como objetivo proporcionar la implementación de los estándares de seguridad primarios para XML:

- Sintaxis y procesamiento de la firma XML
- Sintaxis y procesamiento de cifrado XML.

La librería que proporciona las funcionalidades anteriores para Java es Apache XML Security for Java. Esta librería incluye una implementación avanzada de firma digital y cifrado. También incluye la API estándar JSR 105 (Java XML Digital Signature).

PSIS utiliza esta librería para crear, validar y completar firmas, y validar sellos de tiempo en formato XML.

En la siguiente tabla tenemos la versión de la librería Apache XML Security que utiliza actualmente PSIS, así como la versión más reciente publicada por Java:

Descripción del paquete	Librería PSIS	Fecha	Última versión para JDK 1.8 y superiores	Fecha
Seguridad Apache XML	xmlsec-2.0.6.jar	12/abril/2015	xmlsec-3.0.1.jar	12/septiembre/2022

En la siguiente página web tenemos información sobre las diferentes versiones que se han publicado de la librería de XML Security para Java:

https://santuario.apache.org/javareleasenotes.html

Hay que tener en cuenta que esta librería está modificada por su uso en PSIS, para suplir carencias que se encontraron originalmente durante el desarrollo inicial. Habrá que ver si las últimas versiones cubren estas carencias o si también es necesario modificar el código fuente.

Tareas a realizar por parte del adjudicatario:

- Refactoring del código de PSIS para utilizar la versión más actual de las librerías.

4.2.5 Migración de las librerías de Hibernate

Hibernate es una herramienta de mapeo objeto-relacional (ORM) para la plataforma Java, que facilita el mapeo de atributos entre una base de datos relacional tradicional y el modelo de objetos de una aplicación, mediante archivos declarativos (XML) o anotaciones en los beans de las entidades que permiten establecer estas relaciones. Hibernate es también una implementación de la especificación Java Persistence API (JPA).

Hibernate es software libre, distribuido bajo los términos de la licencia LGPL V2.1.

La API Java Persistence (JPA), en 2019 rebautizada a Jakarta Persistence (después de que Java EE pasara a ser código abierto ofrecido por Oracle y éste diera los derechos a Eclipse Fundation, estaban legalmente obligados a cambiar el nombre de Java, ya que Oracle tiene los derechos sobre la marca Java), es una especificación de interfaz de programación de aplicaciones Java que describe la gestión de datos relacionales en aplicaciones que utilizan la plataforma Java, Standard Edition y Java Platform, Enterprise Edition/Jakarta EE.

PSIS utiliza actualmente la versión 2.1 de la JPA del Hibernate ORM 5.0. Pero Hibernate ORM 5.0 ha llegado al final de su ciclo de vida. Habría que actualizar a una versión reciente de las librerías.

En la siguiente URL tenemos información sobre las distintas versiones. A fecha de enero de 2023, la versión estable más actual es la 6.1.

https://hibernate.org/orm/releases/

En la siguiente tabla se muestra la matriz de compatibilidad entre las versiones de java, y JPA/Jakarta Persistence, más actuales:

Hibernar ORM	6.2	6.1	5.6
Java	11, 17 o 18	11, 17 o 18	8, 11, 17 o 18
JPA	N / A	N / A	2.2
Persistencia de Yakarta	3.1	3.1 y 3.0	3.0

Tareas a realizar por parte del adjudicatario:

- Estudio de los cambios que supone la migración a la versión 3.1 (o la más novedosa a la adjudicación de este concurso).
- Propuesta de diseño de cambios.
- Pruebas de rendimiento para garantizar que mantenemos, como mínimo, el mismo rendimiento que con la versión actual.
- Análisis de los cambios a realizar: Revisión de los objetivos del proyecto y consenso con el Consorci AOC sobre cómo alcanzarlos.

4.2.6 Redis

La configuración de PSIS actualmente está definida en unos archivos XML que se cargan en la base de datos. Cuando hablamos de configuración estamos haciendo referencia a la configuración interna de todos los servicios que conforman PSIS. Un despliegue en PSIS puede ser un despliegue de código, un despliegue de configuración, o ambos.

La aplicación PSIS consume la configuración de la base de datos, y la carga en la caché del servidor de aplicaciones.

Con este desarrollo se pretende migrar la configuración de la base de datos actual (AWS Aurora PostgreSQL) a Redis, y consumirla directamente desde Redis o cargarla en la caché del servidor de aplicaciones (dependerá del rendimiento y/o los costes de explotación en AWS).

Dado que PSIS 8.0 está desplegado en AWS, la migración se realizaría hacia el servicio Amazon ElastiCache for Redis. Amazon ElastiCache for Redis es un almacén de datos en memoria increíblemente rápido que ofrece una latencia inferior a un milisegundo para aplicaciones en tiempo real a escala de Internet. Creado sobre Redis de código abierto y compatible con las API de Redis, ElastiCache para Redis se puede utilizar con clientes de Redis y utiliza el formato de datos de Redis abierto para el almacenamiento. Ésto nos permitirá un desarrollo lo más agnóstico posible del cloud en el que esté desplegado PSIS.

ElastiCache proporciona la capacidad de crear y administrar usuarios y grupos de usuarios que se pueden utilizar para configurar el control de acceso basado en roles (RBAC) para las solicitudes a Redis. Es posible utilizar AWS Identity and Access Management (IAM) para conectarse a ElastiCache for Redis con identidades del IAM. Redis cumple los requisitos de PCI y HIPAA, está autorizado por FedRAMP y ofrece cifrado en tráfico y en reposo (incluida la CMK administrada por el usuario almacenada en AWS KMS), además de AUTH de Redis para las comunicaciones seguras entre nodos para proteger información confidencial, tales como la información de identificación personal (PII).

Los objetivos de la migración son:

- Poder disponer simultáneamente de más de una versión de la configuración. Ésto nos permitiría poder cambiar de versión simplemente apuntado a una u otra versión de la configuración.
- Agilizar los despliegues. Actualmente un cambio de configuración implica corte de servicio. Queremos que el cambio de configuración se pueda realizar en caliente.
- Mejorar el rendimiento.

Tareas a realizar por parte del adjudicatario:

- Propuesta de adaptación de los archivos XML de configuración actual a los requeridos para la migración a Redis.
- Propuesta de diseño de los cambios en PSIS para consumir la configuración desde Redis.
- Pruebas de rendimiento para garantizar que mantenemos, al menos, el mismo rendimiento que con el modelo actual.
- Análisis de los cambios a realizar: Revisión de los objetivos del proyecto y consenso con el Consorci AOC sobre cómo alcanzarlos.

4.2.7 Refactoring de la consola web de administración

Actualmente PSIS dispone de dos consolas:

- Una consola web que permite administrar la configuración de los servicios:
  - Carga de configuración.
  - Carga/eliminación de certificados en el Truststore.
- Una consola java que proporciona las siguientes funcionalidades:
  - Carga de bindings o claves criptográficas.
  - Carga de políticas de firma.
  - Carga de CRLs en base de datos.

  Nueva funcionalidad que deberá incluir (actualmente no se proporciona esta funcionalidad):
  - Carga de respuestas OCSP en base de datos.

Lo que queremos es unificar en una sola consola web todas estas funcionalidades. Esta nueva consola web sustituiría a las dos actuales.

Tareas a realizar por parte del adjudicatario:

- Propuesta de diseño técnico de la nueva consola web.
- Propuesta de diseño de las distintas pantallas.
- Estudio de viabilidad y coste de despliegue/explotación en EKS vs EC2 de AWS.
- Análisis de los cambios a realizar: Revisión de los objetivos del proyecto y consenso con el Consorci AOC sobre cómo alcanzarlos.

4.2.8 Servidor web ligero

Actualmente PSIS está desplegado en Kubernetes en contenedores sobre un servidor de aplicaciones Java EE. La idea es adaptar la aplicación para su despliegue en un servidor web lo más ligero posible y que al mismo tiempo proporcione el mayor rendimiento posible.

Entre los servidores Java EE open source más populares, tenemos:

- Apache Tomcat:
  - Proporciona un entorno flexible con herramientas de personalización integradas.
  - Utiliza código ligero que permite un despliegue y una carga más rápidos de las aplicaciones.
  - Es una plataforma relativamente más estable que otros servidores de aplicaciones Java EE.
- Jetty
  - Ofrece flexibilidad porque puede utilizarse como nivel web para las pilas de servidores de aplicaciones Java totales y parciales.
  - Gestiona hasta 10.000 solicitudes, por lo que es extremadamente rápido y flexible.
  - Es altamente escalable gracias a un diseño de memoria de servlet pequeño.

- Glassfish
    - Proporciona un soporte óptimo para Enterprise JavaBeans, Java Server Faces, JMS, JPA y muchos otros.
    - Fácil de desplegar código Java debido a su diseño ligero.
    - Permite crear software empresarial portátil y escalable, e integrarlo con sistemas legacy.
- JBoss Enterprise Application Platform
    - Fácil acceso a las herramientas de código abierto gracias al soporte de Red Hat.
    - Cumple con las especificaciones Java EE 7.
    - Servicios web, pilas y arquitecturas en la nube.
    - Las funciones de automatización facilitan la gestión.

Tareas a realizar por parte del adjudicatario:

- Estudio sobre la idoneidad para PSIS de los distintos servidores de aplicaciones, así como de la viabilidad de migración desde el servidor de aplicaciones actual. Comparativa entre el servidor de aplicaciones actual y el elegido para realizar la migración.
- Análisis de los cambios a realizar: Revisión de los objetivos del proyecto y consenso con el Consorci AOC sobre cómo alcanzarlos.

4.2.9 Estudio de refactoring de la arquitectura de código

Estudio de la viabilidad técnica de alternativas de rearquitectura de la aplicación, que ofrezcan mayores ventajas y puedan ser incluidas en el alcance definido por los objetivos. Diseño técnico detallado con énfasis en diagramas de despliegue, e impacto en componentes actuales. Se podrán considerar unas alternativas principales, o combinación de ellas, con la intención de seleccionar aquélla(s) que implique(n) mayor beneficio en rendimiento y reducción de costes de explotación e infraestructura. Alternativas a considerar:

- **CaaS el servidor web** (*Container as a Service* de Web Server).
  Es la opción más sencilla, pero quizás la menos eficiente.
- **CaaS con Spring Boot** (*Container as a Service* con migración a Spring Boot)
  Spring es un framework de desarrollo de aplicaciones y contenedor de inversión de control, de código abierto, para la plataforma Java.
- **CaaS con GraalVM y Quarkus**
  GraalVM: Motor de ejecución de alto rendimiento, diseñado para acelerar la ejecución de aplicaciones escritas en Java y otros lenguajes JVM.
  Quarkus: Marco Java nativo de Kubernetes diseñado por OpenJDK HotSpot y GraalVM. Comparativamente a otros frameworks, como por ejemplo Spring, ofrece menor impacto en memoria y reducción considerable del tiempo de arranque.
- **Faas con Spring Boot** (*Function as a Service* con Spring Boot)
  En este caso es necesario asegurar la portabilidad de la solución a un cloud diferente.
  Ejemplo: AmazonWS Lambda.
- **Faas con Spring Cloud Función** (*Function as a Service* con Spring Cloud Function)
  Spring Cloud Function es un componente del stack de Spring que permite realizar aplicaciones Serverless agnósticas en el lugar donde se desplegarán.

4.3 Soporte a la puesta en marcha en preproducción y producción

Las siguientes tareas forman parte del despliegue de la solución en los entornos de preproducción y producción.

4.3.1 Migración de Oracle en AWS Aurora Serverless V2 (PostgreSQL compatible)

Los datos de los entornos productivos actuales (primario y secundario) se encuentran en una base de datos **Oracle 12c**. En la versión de PSIS en la nube, la base de datos Oracle ha sido sustituida por **AWS Aurora Serverless V2** compatible con PostgreSQL.

El esquema de datos ya lo tenemos definido en Aurora. **Es necesario migrar los datos, que habrá que convertir durante el proceso de migración al nuevo esquema compatible con PostgreSQL.**

En el entorno de desarrollo ya hemos migrado los datos necesarios.

Los datos en Oracle a migrar a Aurora Serverless V2 de AWS son datos que contienen las listas de revocación de certificados (en adelante CRL, de *Certificate Revocation Lists*) y respuestas OCSP (*Online Certificate Status Protocol*). Son datos que PSIS guarda después de utilizarlos para la validación de certificados. Cada vez que PSIS valida un certificado, guarda en base de datos la CRL (si no existe previamente) o respuesta OCSP correspondiente. No sólo como evidencia del proceso de validación, sino también para su reutilización mientras dure el tiempo de confianza (1 hora por CRLs, y 6 minutos y 40 segundos por las respuestas OCSP), así como para poder recuperarla en un futuro para la validación de firmas con sello de tiempo.

Las CRLs y respuestas OCSP están historificadas anualmente, distribuidas en distintas tablas en función del año.

4.3.1.1 Preproducción

El entorno de preproducción es único y sólo tenemos una base de datos. El volumen total de información de revocación hasta diciembre de 2022 incluido es de unos **11GB**.

En el entorno de preproducción tenemos datos desde el 2009.

Cualquier	Volumen uno MB
2009	5,25
2010	55,31
2011	69,06
2012	115,81
2013	45,94
2014	178,00
2015	244,75
2016	459,13
2017	505,06
2018	953,13
2019	1.133,13
2020	1.371,00
2021	3.776,00
2022	2.469,63
TOTAL	11.381,19 MB

En relación al número de CRLs y OCSPs, tenemos, a fecha de diciembre de 2022, unos totales de **más de 200.000 CRLS** y **más de 2 millones de respuestas OCSP**, distribuidas por año según la siguiente tabla:

Cualquier	CRL	Respuestas OCSP
2009	4.801	584
2010	15.259	12.890
2011	43.534	9.416
2012	8.688	70.098
2013	10.891	56.171
2014	11.641	98.889
2015	8.450	108.902
2016	11.764	116.456
2017	11.020	109.792
2018	11.406	199.337
2019	11.756	258.003
2020	10.785	272.020
2021	29.571	487.064
2022	16.442	344.551
TOTAL	206.008	2.144.173

4.3.1.2 Producción

El entorno productivo se ofrece en alta disponibilidad y consta de 2 entornos, llamados primario y secundario. Están dimensionados de la misma forma, y el servicio se puede ofrecer desde cualquiera de los dos en todo momento. Nunca se ofrece desde ambos a la vez. Llamamos "primario" al entorno desde el que se está ofreciendo el servicio de forma preferente en un momento dado.

En los entornos productivos, sin embargo, el volumen de datos es muy superior al del entorno de preproducción, y además necesitamos poder realizar la migración en caliente y en un tiempo lo más reducido posible.

El volumen de datos es importante. Estamos hablando de 2 entornos productivos, cada uno con un volumen de datos considerable.

En los entornos de producción tenemos datos desde el 2006.

El volumen de datos que tenemos hasta diciembre de 2022 incluido es de unos **660GB**, repartidos por entorno productivo según la siguiente tabla:

Entorno productivo	Volumen de datos con información de revocación
PSIS 1	420GB
PSIS 2	243GB
TOTAL	663GB

Los datos con información de revocación se distribuyen anualmente y por entorno productivo de la siguiente forma:

	Volumen uno MB		
Cualquier	PSIS 1	PSIS 2	MB totales
2006	1,88	1,94	3,81
2007	6,88	8,94	15,81
2008	21,56	22,44	44,00
2009	56,88	55,56	112,44
2010	1.803,06	1.862,75	3.665,81
2011	1.536,06	1.517,56	3.053,63
2012	2.031,81	1.156,06	3.187,88
2013	3.198,63	32,75	3.231,38
2014	5.645,75	169,44	5.815,19
2015	8.710,81	310,69	9.021,50
2016	16.437,06	575,31	17.012,38
2017	30.460,06	1.132,25	31.592,31
2018	57.233,06	896,63	58.129,69
2019	53.138,06	17.282,06	70.420,13
2020	18.831,06	101.338,06	120.169,13
2021	33.489,06	114.507,00	147.996,06
2022	188.035,00	2.305,75	190.340,75
TOTAL	420.636,69 MB	243.175,19 MB	663.811,88 MB

En relación al número de CRLs y OCSPs, tenemos, a fecha de diciembre de 2022, unos totales de **3,2 millones de CRLS** y **116,2 millones de respuestas OCSP**:

Entorno productivo	Nº CRL	Nº OCSP
PSIS 1	1,7 millones	78,3 millones
PSIS 2	1,5 millones	37,9 millones
TOTAL	3,2 millones	116,2 millones

Distribuidos por entorno productivo y año según la siguiente tabla:

	CRL			Respuestas OCSP		
Cualquier	PSIS 1	PSIS 2	Total	PSIS 1	PSIS 2	Total
2006	1.274	1.274	2.548	24	24	48
2007	6.420	6.483	12.903	563	560	1.123
2008	7.334	7.395	14.729	23.131	23.106	46.237
2009	9.385	9.443	18.828	86.520	86.514	173.034
2010	138.382	138.486	276.868	566.465	566.418	1.132.883
2011	107.054	107.479	214.533	519.029	518.089	1.037.118
2012	28.882	24.140	53.022	712.397	428.354	1.140.751
2013	20.571	1.813	22.384	1.132.445	51.936	1.184.381
2014	25.620	5.212	30.832	1.943.143	93.722	2.036.865
2015	28.370	4.784	33.154	3.317.155	136.933	3.454.088
2016	55.178	3.554	58.732	5.665.178	128.401	5.793.579
2017	89.938	5.792	95.730	8.054.060	299.383	8.353.443
2018	64.765	3.773	68.538	8.208.180	134.289	8.342.469
2019	302.456	145.671	448.127	7.561.047	2.464.170	10.025.217
2020	101.686	503.619	605.305	2.966.163	15.629.074	18.595.237
2021	123.618	521.260	644.878	5.361.444	17.008.281	22.369.725
2022	627.900	20.681	648.581	32.223.855	348.213	32.572.068
TOTAL	1.738.833	1.510.859	3.249.692	78.340.799	37.917.467	116.258.266

Es muy importante tener en cuenta que una misma CRL puede estar presente en ambos entornos. Las CRLs deberán consolidarse teniendo en cuenta que deben ser únicas.

En el caso de las respuestas OCSPs, por su naturaleza, son únicas. Sin embargo, es posible que una misma respuesta OCSP esté presente en ambos entornos, porque el entorno secundario se creó inicialmente sobre una copia de los datos del entorno primario. Por tanto, también deberemos tener en cuenta que estos datos pueden estar presentes en ambos entornos y que habrá que consolidarlos eliminando duplicados y preservando la unicidad.

Dado que se trata de un entorno productivo, los datos del año en curso tendrán que migrarse en caliente. Y hasta el momento en que PSIS se ofrezca en producción desde AWS, será necesario ir migrando los nuevos datos que se vayan introduciendo en estas tablas fruto del funcionamiento normal del servicio. En este caso esto sólo aplicaría al entorno productivo que esté dando servicio en ese momento.

Como ejemplo de migración utilizando las herramientas de AWS, en la siguiente URL se expone una estrategia de migración desde Oracle hacia Aurora PostgreSQL, utilizando AWS Schema Conversion Tool (SCT) y AWS Data Migration Service (DMS):

https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/migrate-data-from-an-premises-oracle-database-to-aurora-postgresql.html

El adjudicatario deberá llevar a cabo las siguientes tareas:

- Definición del plan de migración: conversión y migración de los datos.
- Soporte a la ejecución del plan de migración para el entorno de preproducción.
- Soporte a la ejecución del plan de migración para el entorno de producción.
- Validación de los datos migrados.

4.4 DevSecOps

Se entiende por DevOps, el conjunto de prácticas que pretenden conseguir una sinergia en el ámbito del desarrollo de software (Dev) y el ámbito de operaciones (Ops). DevSecOps incorpora prácticas para que la seguridad sea parte del ciclo de desarrollo de software con mejores prácticas de codificación segura y automatización de pruebas, entre otros.

Actualmente PSIS dispone de una infraestructura DevOps basada en Git, Jenkins y CloudFormation.

El adjudicatario deberá conocer y utilizar el modelo DevOps implantado por PSIS. En caso de que sea necesario, el adjudicatario deberá ser capaz de:

- Mantener los scripts de despliegue de CloudFormation.
- Integración Continua (CI o *Continuous Integration*) / Entrega Continua (CD o *Continuous Deployment*): Mantener las pipelines de Jenkins de construcción y las pipelines de entrega/despliegue para las diferentes unidades de despliegue y sus versiones.
- Infraestructura como código (IaC o *Infrastructure as Code*) & Gestión de Configuración Integrada (CM o *Configuration Management*): Mantener las pipelines de construcción de la infraestructura en Cloud.
- Seguridad y Pruebas Integradas: Automatización de verificaciones de seguridad como SAST (*Static Application Security Testing*), DAST (*Dynamic Application Security Testing*), y ejecución de pruebas de validación del funcionamiento de la aplicación y sus diferentes partes.
- Tener en cuenta que los despliegues de cambios o nuevas versiones deben poder realizarse en caliente sin corte de servicio.

4.5 Equipo de proyecto

Para garantizar la máxima eficiencia, desarrollo, control y coordinación de las labores de este contrato, el adjudicatario deberá disponer de un equipo con conocimiento tecnológico de las aplicaciones a desarrollar.

A continuación, se indican los perfiles mínimos exigidos por el desarrollo de esta primera fase:

- 1 Jefe de Proyectos (dedicación 10%)
- 1 Arquitecto de Soluciones AWS (dedicación 25%)
- 1 Ingeniero de Software (dedicación 30%)
- 2 Desarrollador Java/J2EE (dedicación 100%)
- 1 Ingeniero Kubernetes y DevOps (dedicación 50%)

El Consorci AOC se reserva el derecho a pedir el cambio de cualquiera de los miembros del equipo sin tener que justificarlo, con una antelación de 20 días naturales a la fecha de la sustitución.

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirlo en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC. En estos casos, se fijará un tiempo de 2 semanas de formación/adaptación del nuevo miembro que correrá a cargo del adjudicatario.

Habrá que acordar el calendario de cambio con el Consorci AOC para minimizar el impacto en los desarrollos en curso.

El adjudicatario puede presentar perfiles superiores a los mínimos exigidos, pero nunca inferiores.

4.6 Coordinación con la Oficina Técnica de mantenimiento evolutivo y correctivo

La Oficina Técnica de mantenimiento evolutivo y correctivo de PSIS realiza labores de corrección de bugs y desarrollo de evolutivos, sobre el mismo código de PSIS 8.0. Será la encargada de llevar a cabo los siguientes evolutivos:

- Implementación de los nuevos estándares de firma electrónica del reglamento europeo eIDAS (electronic IDentification, Authentication and trust Services).
- Refactorización del Truststore de PSIS basado en TSLs (Trust Service status List).
- Integración de PSIS con una autoridad de sello de tiempo reconocida. Está previsto sustituir la TSA de PSIS por una TSA cualificada, es decir, que cumpla con los requerimientos del reglamento eIDAS. Habrá que integrar PSIS con la TSA cualificada para llevar a cabo las funciones de completado de firmas.

Algunos de estos evolutivos ya estarán en fase de implementación o incluso finalizados en el momento de adjudicación del presente contrato.

Será necesario que el adjudicatario trabaje conjuntamente con la oficina técnica de mantenimiento evolutivo y correctivo para coordinar los diferentes evolutivos que llevarán a cabo en paralelo ambas oficinas técnicas.

4.7 Requerimientos funcionales

Este proyecto se centrará en las siguientes actividades:

- La ejecución del contrato se iniciará en la fecha de formalización del mismo.
- La gestión y control del código fuente se llevarán a cabo con el sistema centralizado de código fuente de que dispone el Consorci AOC (basado en el sistema de control de versiones Git).
- El adjudicatario será el responsable de la definición del plan de pruebas de integración y rendimiento, y de su ejecución en los entornos de desarrollo, preproducción y producción.
- El adjudicatario por tanto será el responsable del control de calidad y de validar el buen funcionamiento de los evolutivos tanto a nivel funcional como técnico.
- El adjudicatario deberá preparar los paquetes de despliegue para los entornos de desarrollo, preproducción y producción.
- El adjudicatario tendrá que elaborar la documentación técnica y los manuales correspondientes, así como mantener actualizada la documentación existente.
- El adjudicatario deberá prestar la formación que determine el Consorci AOC cuando éste lo considere necesario.
- Para cada una de las tareas anteriores, el adjudicatario deberá proporcionar los siguientes entregables:
    - Análisis funcional.
    - Diseño técnico.
    - Planes de pruebas unitarias y de integración.
    - Manual de explotación.
    - Código fuente en el sistema centralizado del Consorci AOC.
    - Despliegue en el entorno de desarrollo.
    - Procedimiento de despliegue en los entornos de preproducción y producción del Consorci AOC.
- Aplicar controles de calidad. El adjudicatario será el responsable del control de calidad del servicio en todos aquellos desarrollos de nuevos evolutivos que realice. En particular deberá llevar a cabo las siguientes tareas:
    - Definición de los indicadores y métricas de calidad que deben cumplir los evolutivos e identificar las medidas que se utilizarán para evaluar la calidad.
    - Control de calidad de los evolutivos. Validación del correcto funcionamiento de éstos tanto a nivel funcional como técnico, mediante la ejecución de:

- Pruebas unitarias.
- Pruebas de integración.
- Pruebas funcionales.
- Pruebas de regresión.
- Pruebas de rendimiento.

- Apoyo a los equipos de desarrollo mediante la definición de los estándares y directrices que deben cumplir todos los evolutivos para ser certificados.
- Revisión y auditoría del cumplimiento de estos estándares/directrices para asegurar que se siguen los procedimientos establecidos.
- Revisión y seguimiento de la calidad de la documentación generada por los equipos de desarrollo.

4.8 Requerimientos técnicos

4.8.1 Infraestructura necesaria para llevar a cabo el desarrollo del proyecto

El adjudicatario aportará las infraestructuras informáticas, licencias de desarrollo y cualquier otro componente o medio técnico necesario para la realización de los trabajos.

El entorno de desarrollo basado en los servicios de AWS será proporcionado por el Consorci AOC.

El adjudicatario mantendrá en todo momento la actualización del código fuente en el sistema de control de versiones del Consorci AOC.

La ejecución de las tareas encomendadas deberá poder llevarse a cabo en las instalaciones del adjudicatario, pero es posible que en alguna ocasión sea necesario el desplazamiento de alguno de los miembros del equipo del adjudicatario a las instalaciones del Consorci AOC.

4.8.2 Dimensionamiento

La nueva solución debe estar dimensionada para poder absorber sin degradación del servicio los volúmenes de operaciones previstos. Por tanto, la infraestructura y la arquitectura deben estar diseñadas para poder escalar las necesidades puntuales de un aumento de peticiones al servicio.

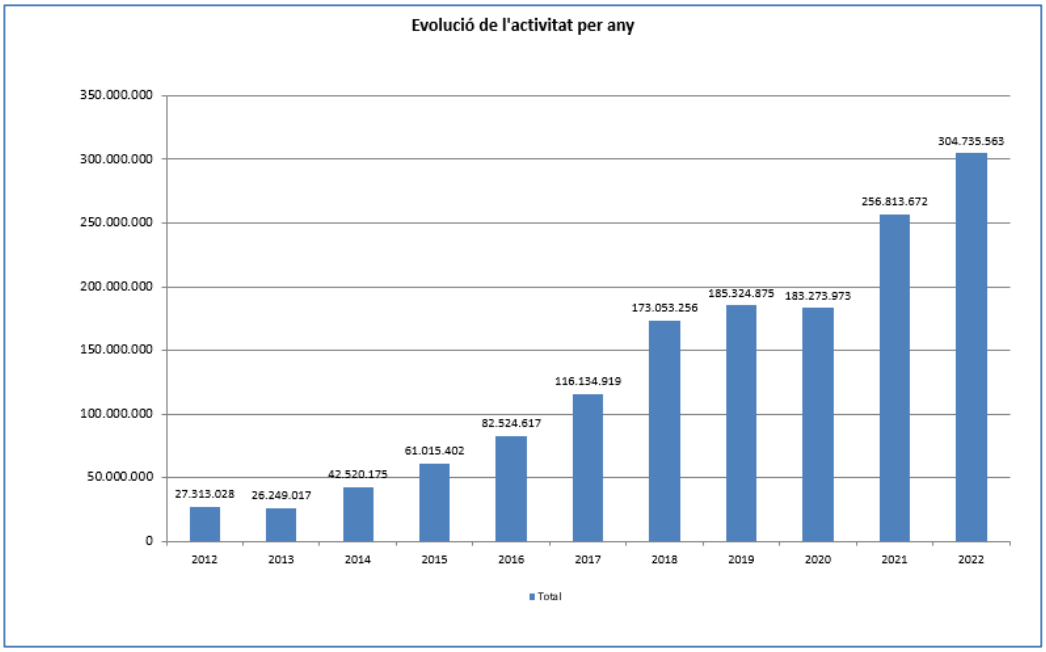
La nueva arquitectura debe dar respuesta a los siguientes requerimientos técnicos:

- ANS

  El servicio de PSIS es **24x7**. No podemos permitirnos paradas del servicio en ningún momento. Es indispensable garantizar el mayor rendimiento posible para seguir ofreciendo un **SLA por encima del 99.5%**.

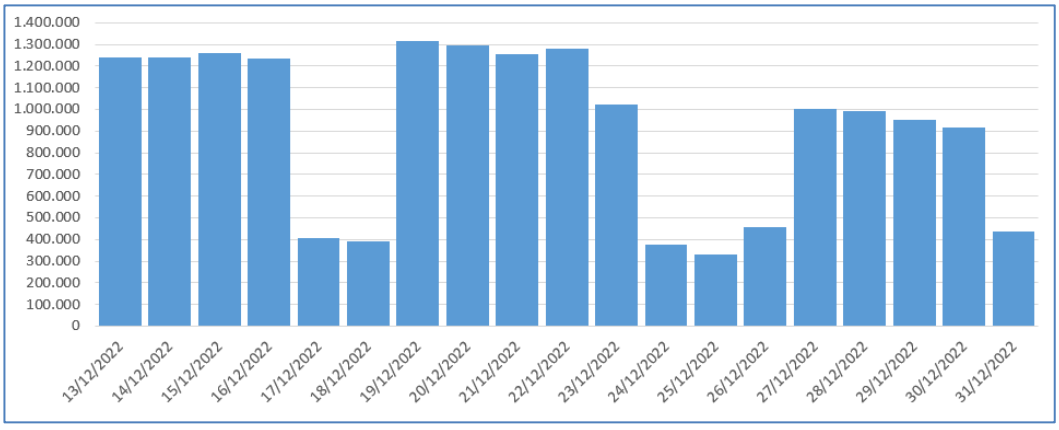
- Volumetrías

  PSIS es un servicio transversal al resto de servicios del Consorci AOC y en general de las AAPP catalanas. Tiene por tanto un consumo muy elevado, con **más de 300 millones de operaciones anuales**. El volumen de operaciones crece a medida que las administraciones digitalizan sus procesos, con lo que se prevé un incremento importante a medio/largo plazo. El crecimiento desde 2012 ha sido el siguiente:

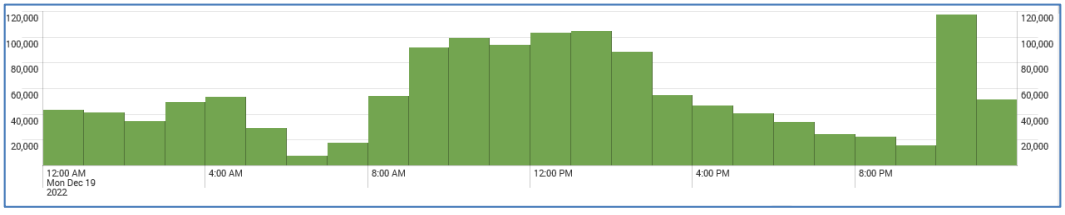


La volumetría actual en operaciones de cliente es:

- El número total en 2022 fue de más de 300 millones de operaciones.
- El volumen mensual actualmente es del orden de **28 millones de operaciones mensuales de media**. Este número oscila entre 20 y más de 32 millones de operaciones mensuales.
- El **volumen de peticiones diarias** puede oscilar **entre 300.000 y 1,3 millones**.
  Por ejemplo, en el siguiente gráfico tenemos el volumen de peticiones diarias durante las dos últimas semanas del mes de diciembre de 2022:



El tráfico de peticiones en PSIS es continuo. Sin embargo, este tráfico no se distribuye de manera uniforme durante el día, sino que en ciertas franjas el volumen de peticiones es más concentrado. Por ejemplo:



La solución debe poder absorber, en el entorno productivo, sin degradación de los tiempos de respuesta, como mínimo:

- **3.000 operaciones de cliente por minuto**.
- **50 operaciones concurrentes** con tiempos medios de respuesta inferiores a 1 segundo.

- Tiempo de respuesta

Los tiempos de respuesta de PSIS deben ser de **milisegundos**. Sólo las operaciones de validación y completado de firmas o documentos pueden tener puntualmente tiempo de respuesta del orden de pocos segundos dependiendo de la antigüedad y complejidad de la firma.
Obviamente los tiempos de respuesta de PSIS pueden verse comprometidos por la fuerte dependencia de éstos frente a los servicios de revocación de terceros.
El tiempo medio de respuesta por los diferentes tipos de operaciones deben ser del orden de:

- Validación de certificados: **inferior a 100 mseg**
- Validación y completado de firmas y documentos firmados: **inferior a 300 mseg**
- Creación de sellos de tiempo: **inferior a 100 mseg**
- Creación de firma: **inferiores a 2 segundos** (hay que decir que este valor corresponde a las firmas de iArxiu, que son especialmente complejas).
- Guardado de evidencias legales: **inferior a 50 mseg**

El Consorci AOC valorará muy positivamente cualquier reducción de los tiempos de respuesta.

4.8.3 Código fuente y propiedad intelectual

La gestión y control del código fuente se llevará a cabo con el sistema centralizado de código fuente de que dispone el Consorci AOC (basado en el sistema de control de versiones Git).

El adjudicatario acepta expresamente que la propiedad de todos los entregables, independientemente de su naturaleza, así como de los resultados de los trabajos realizados, y en particular los productos y servicios objeto del contrato, corresponde únicamente al Consorci AOC con exclusividad y con carácter general, sin que el adjudicatario pueda conservar, ni obtener copia de los mismos o facilitarlo a terceros.

El adjudicatario no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados como resultado de la prestación del servicio objeto del contrato, bien sea en forma total o parcial, original o reproducida, sin autorización expresa del Consorci AOC, que la daría, en su caso, previa petición formal del adjudicatario con indicación expresa de la finalidad.

4.8.4 Tests unitarios y pruebas de integración

El adjudicatario tendrá que implementar un juego exhaustivo de pruebas unitarias y de integración para validar todos y cada uno de los servicios implementados a lo largo del desarrollo de PSIS 9.0.

El adjudicatario deberá ejecutar estos juegos de pruebas en los entornos de desarrollo, preproducción y producción del Consorci AOC una vez se haya ejecutado la puesta en marcha y explotación, y se haya realizado el despliegue de la nueva solución en los entornos AWS del Consorci AOC.

4.8.5 Tests de rendimiento

Durante el desarrollo y al final del proyecto, el adjudicatario deberá proporcionar juegos de pruebas de carga y test de estrés para validar que PSIS 9.0 cumple con los requerimientos técnicos y funcionales.

4.9 Requerimientos legales

PSIS 9.0 debe ser un servicio cualificable, es decir:

- La solución propuesta deberá cumplir con los requisitos que establece la norma **ETSI EN 319.401** " *General Policy Requirements for Trust Service Providers* ", en relación a la gestión y operación del servicio.
- La solución deberá cumplir con la especificación técnica **ETSI TS 119.441** " *Policy requirements for TSP providing signature validation services* ", la cual establece requisitos específicos de gestión y operación de un servicio específico de validación.
- PSIS está catalogado como servicio de **nivel alto** según el **Esquema Nacional de Seguridad** (ENS). La valoración de PSIS para cada dimensión de seguridad es la que se expone en la siguiente tabla. La solución deberá aplicar todos los controles que aparecen en el Anexo II del ENS de acuerdo con la valoración de cada dimensión de seguridad.

	RGPD	ENS					
SERVICIO	Datos Personales	Confidencialidad	Disponibilidad	Autenticidad	Integridad	Trazabilidad	RTO
Definiciones	Las consecuencias que tendría sobre las personas la revelación a personas no autorizadas o que no necesitan conocer la información.	Las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.	Las consecuencias que tendría el no poder comprobar a posteriori quién ha accedido a, o modificado, cierta información.	Las consecuencias que tendría que la información no fuera auténtica.	Las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.	Las consecuencias que tendría el no poder comprobar a posteriori quién ha accedido a, o modificado, cierta información.	Tiempo máximo de recuperación del servicio en caso de Indisponibilidad.
Validador - PSIS	Media	Media	Alta	Alta	Media	Alta	<4 horas

RGDP: Reglamento General de Protección de Datos
ENTE: Esquema Nacional de Seguridad
RTO: Objetivo de Tiempo de Recuperación

4.10 Requerimientos de seguridad

4.10.1 Medidas de seguridad que debe incorporar PSIS 9.0 como solución

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad de nivel alto del Esquema Nacional de Seguridad que afectan directamente a PSIS 9.0 como solución y plataforma tecnológica. Concretamente son las descritas en:

- ***Annex4_Taula aplicabilitat_ENS_PSIS.xlsx*** (para descargar vaya al punto 5 Anexos)

4.10.2 Medidas de seguridad a cumplir por parte del adjudicatario

4.10.2.1 Certificaciones de seguridad

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad de nivel medio del Esquema Nacional de Seguridad. Concretamente son las descritas en:

- ***Annex5_Requeriment_de_seguretat_(ENS)_pels_proveidors_de_software.pdf*** y que son las que afectan al adjudicatario como parte del sistema PSIS 9.0. (para descargar vaya al punto 5 Anexos)

El Consorci AOC auditará en un plazo no superior a 6 meses, que el adjudicatario cumple con los requerimientos que se detallan en el documento anexo *Annex5_Requeriment_de_seguretat_(ENS)_pels_proveidors_de_software.pdf*. La auditoría se realizará mediante la entrega de las evidencias indicadas en el anexo al Consorcio AOC para que éste determine el grado de cumplimiento.

El adjudicatario estará exento de la auditoría si aporta una certificación vigente del Esquema Nacional de Seguridad de nivel bajo expedido por una empresa certificadora independiente y homologada.

En caso de auditoría externa de PSIS, el adjudicatario deberá participar en la auditoría en las tareas que le correspondan, entregando las evidencias que el auditor reclame y haciendo las adecuaciones necesarias que les correspondan.

4.10.2.2 Control de acceso al sistema

El adjudicatario deberá adaptarse en todo momento a los mecanismos de control de acceso a los sistemas de información que imponga el Consorci AOC para acceder a sus sistemas.

4.10.2.3 Control de personal

El adjudicatario deberá informar en todo momento de las altas y bajas del personal interno o subcontratado que en su nombre acceda a los sistemas del Consorci AOC.

En caso de baja de un usuario, de forma inmediata el adjudicatario deberá informar al Consorci AOC para revocar sus derechos de acceso a los sistemas.

4.10.2.4 Protección de la información

El adjudicatario no podrá utilizar los datos reales de los sistemas de producción en los sistemas de desarrollo.

El adjudicatario no podrá descargar información del Consorci AOC en sus sistemas o en soportes portátiles como USBs, DVDs, portátiles, tabletas, etc. En caso de tener que hacerlo deberá solicitar la autorización del Consorci AOC y el soporte deberá estar cifrado.

Los ficheros temporales que se hubieran creado exclusivamente por la realización de trabajos temporales auxiliares deberán cumplir con las medidas establecidas que se apliquen a los ficheros considerados definitivos.

Todo archivo temporal así creado será borrado una vez haya dejado de ser necesario por la finalidad que motivó su creación.

Al finalizar la relación laboral entre el Consorci AOC y el adjudicatario, éste deberá entregar toda la información propiedad del Consorci AOC (procedimientos, código fuente, etc.) y realizar un borrado seguro de los soportes donde ésta esté almacenada.

El contrato debe determinar la propiedad de la información a la que tendrá acceso el adjudicatario, ya sea de la parte contratante o de terceras partes.

El adjudicatario debe comprometerse en el contrato a mantener la confidencialidad en el tratamiento de la información del cliente, comprometerse por contrato a no divulgar o acceder indebidamente a la información sin la autorización expresa de su propietario. El adjudicatario queda obligado a no acceder ni utilizar la información a la que tenga acceso para cualquier fin que no esté explicitado en el contrato o se autorice expresamente por escrito con posterioridad a la firma del contrato.

4.10.2.5 Protección de los soportes

El adjudicatario no puede descargar información del Consorci AOC en sus sistemas. En caso de tener que hacerlo habrá que pedir la autorización del Consorci AOC, y si ésta es concedida los soportes se protegerán de la siguiente manera:

- Los soportes de información con datos del Consorci AOC deben identificarse mediante etiquetado o mecanismo equivalente de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor cualificación.
- Las etiquetas o mecanismos equivalentes deberán ser fácilmente identificables. Se informará a los usuarios sobre estos mecanismos de identificación para que, bien mediante simple inspección, bien mediante el recurso a un repositorio, puedan entender el significado.
- Se podrá excluir, por previsión a la normativa, la obligación de etiquetado en caso de soportes en que no se pudiera cumplir por sus características físicas, estableciendo medidas alternativas para asegurar su identificación y localización.
- Los soportes de información que deban reutilizarse para otra información o entregar a otra organización deben ser objeto de un borrado seguro de su contenido.

Se destruirán de forma segura los soportes de información, en los siguientes casos:

- Cuando la naturaleza del soporte no permita un borrado seguro.
- Cuando así lo requiera el procedimiento asociado al tipo de información contenida.

Se aplicarán mecanismos de cifrado que garanticen la confidencialidad y la integridad de la información contenida en todos los soportes.

4.11 Requerimientos de protección de datos

Por cada ámbito objeto de análisis que comporte el tratamiento de datos de carácter personal será necesario realizar un informe de las medidas a adoptar para implantar las medidas de privacidad desde el diseño y por defecto para dar cumplimiento a los requerimientos establecidos en el Reglamento (UE) 2016/ 679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales y a la libre circulación de estos datos, y a la Ley orgánica 3/2018, de 5 de diciembre , de protección de datos personales y garantía de los derechos digitales. El informe deberá contener el análisis de los principios del Reglamento a los que se da cumplimiento con cada una de las medidas aportadas, justificándolo también en base a la normativa específica que regula el ámbito de actuación de las administraciones usuarias del servicio, y a la adecuación de cada medida propuesta en relación a su propósito de cumplir los principios de protección de datos y reducir el riesgo por los derechos y las libertades.

Habrá que tener en cuenta como mínimo las Guías publicadas tanto por el Comité Europeo de Protección de Datos como por la Agencia Española de Protección de Datos y las que pueda publicar la Autoridad Catalana de Protección de datos.

4.12 Plan de devolución del servicio

Al final del servicio el adjudicatario tendrá que planificar y ejecutar el plan de devolución del servicio al Consorci AOC.

Este plan constará como mínimo del manual detallado de instalación y puesta en marcha, y de los paquetes de despliegue para los entornos de desarrollo, preproducción y producción. En caso de que a lo largo del proyecto PSIS 9.0 no esté desplegado en los entornos de preproducción y producción, el adjudicatario deberá dar posteriormente apoyo a la puesta en marcha en estos entornos.

El adjudicatario entregará al Consorci AOC las fuentes de los programas informáticos, manuales, estudios, informes, análisis y otros productos, en buen estado de conservación y funcionamiento.

4.13 Condiciones de ejecución

4.13.1 Obligaciones básicas

El adjudicatario deberá cumplir las siguientes obligaciones básicas:

- El Consorci AOC se hará cargo de las dos primeras semanas de formación en la aplicación PSIS. Todo el tiempo que exceda de estas dos semanas y hasta que se empiecen los trabajos, correrá a cargo de la empresa licitadora.
- Gestionar cualquier alteración del servicio en las condiciones expresadas en este pliego.
- El adjudicatario tendrá que calcular el esfuerzo necesario para llevar a cabo cada uno de los evolutivos pactados. Periódicamente el adjudicatario enviará al Consorci AOC las horas dedicadas a cada uno de los evolutivos en curso. Se establecerán controles entre el volumen de horas ejecutadas y los objetivos alcanzados. En caso de que algún desarrollo se desvíe en gran medida de las previsiones iniciales y este desvío no se corresponda a un cambio de requerimientos por parte del Consorci AOC ni sea técnicamente justificable, el adjudicatario deberá asumir parte de los costes extra, siempre que el Consorci AOC así lo considere.
- Realizar reuniones periódicas con el Consorci AOC para exponer el cumplimiento del servicio y tratar los posibles problemas o mejoras del servicio.
- Realizar la formación de los técnicos designados, en todos aquellos aspectos que el Consorci AOC crea oportunos y que sean de directa aplicación a los servicios requeridos.
- Toda la documentación generada por el equipo será en catalán y en el formato propuesto por el Consorci AOC.
- Presentación de informes mensuales de presentación del servicio de acuerdo con los indicadores que el Consorci AOC considere apropiados:
    - Informe resumen de las actuaciones ya resueltas (micro proyectos) y horas realizadas.
    - Informe del estado de las actuaciones en curso y horas realizadas.
    - Informe resumen de las actuaciones pendientes y horas estimadas.
    - Planificación de las actuaciones a realizar.
    - Detalle del total de horas realizadas durante el mes.
- Definir una forma de trabajo basada en metodologías del tipo Agile o basada en micro proyectos.

4.13.2 Herramientas de control

Las herramientas de control corporativas del Consorci AOC son, principalmente, Jira y Microsoft Teams. Y son las que se utilizarán para llevar a cabo la gestión del proyecto.

El adjudicatario será responsable de:

- Proponer las herramientas adicionales a las herramientas corporativas del Consorci AOC, que deben permitir el seguimiento y el control global del contrato.
- El Consorci AOC se reserva el derecho a validar, y en su caso a definir, las herramientas que deban utilizarse para la gestión y el control del servicio.

4.13.3 Normativa aplicable

El adjudicatario se compromete a cumplir los requerimientos de seguridad, calidad y continuidad aplicables al objeto del contrato especificados en:

- La legislación vigente en general y, en particular, cuando se traten datos de carácter personal, el Reglamento UE 2106/679 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. Además de lo establecido en el Pliego de cláusulas administrativas particulares, por cada módulo funcional que implique el tratamiento de datos de carácter personal, se deberá aportar un informe justificativo del análisis del impacto del mismo sobre los datos afectados y la justificación de medidas implantadas para dar cumplimiento a la normativa vigente.
- ISO/IEC 27001 de seguridad de la información o el Esquema Nacional de Seguridad.

4.14 Modelo de relación

El adjudicatario tendrá que explicar en su propuesta cuál es el modelo de relación que propone para garantizar el éxito del proyecto.

Sin embargo, como mínimo, habrá que establecer los siguientes niveles de interlocución:

- Reuniones de estrategia y dirección con las siguientes características:
    - Interlocutores: Responsable del servicio por parte del adjudicatario, Jefe de Servicio por parte del Consorci AOC.
    - Periodicidad: Mensual
    - Objetivo: Realizar el seguimiento del contrato, analizando diversos aspectos: productividad, control de horas, temas de facturación, seguimiento de metas (a alto nivel), etc.
    - Entregables: Actas de las reuniones, informes ejecutivos, informes con control de horas (hechas y pendientes), etc.
- Reuniones de seguimiento con las siguientes características:
    - Interlocutores: Las personas asignadas por el adjudicatario para llevar a cabo el servicio. Por parte del Consorci AOC será el Jefe de Proyectos o alguno de los técnicos asignados al proyecto.
    - Periodicidad: Semanal
    - Objetivo: Seguimiento detallado de las metas y del plan de proyecto y gestión de las incidencias o desvíos más destacables.
    - Entregables:
        - Informe resumen de las actuaciones ya resueltas y horas realizadas.
        - Informe resumen de las actuaciones en curso y horas realizadas.
        - Informe resumen de las actuaciones pendientes y horas estimadas.
        - Planificación de las actuaciones a realizar.
        - Detalle de las horas totales realizadas durante el mes el curso.

- Reuniones de coordinación con la actual oficina técnica de mantenimiento evolutivo y correctivo de PSIS:
    - Interlocutores: Las personas asignadas por el adjudicatario. Por parte de la Oficina Técnica actual será el Jefe de Proyectos o alguno de los técnicos asignados al proyecto.
    - Periodicidad: Semanal como mínimo; a determinar en función de las necesidades.
    - Objetivo: Coordinación de ambas oficinas técnicas en relación con los evolutivos que se estén llevando a cabo en paralelo por cada una de ellas.
- Reuniones de trabajo para avanzar y concretar los aspectos del proyecto mediante una metodología del tipo ágil.

5 Anexos

En este apartado encontrará documentos de referencia que explican cómo es el actual PSIS 6.0, así como la definición de la arquitectura de PSIS 8.0.

Todos estos anexos se pueden consultar en el siguiente enlace:

https://llicenciesaoc.sharepoint.com/:f:/s/Tecnologia/EjI50ow4XrxJgGwgqK92AjwBDGlkjNJt1RpDkntYZq7Hbw?e=n3ydo7

- Anexo 1 - Descripción tecnológica de PSIS 6.0
- Anexo 2 - Arquitectura de PSIS 6.0
- Anexo 3 - Definición de la arquitectura de PSIS 8.0
- Anexo 4 - Tabla aplicabilidad ENS PSIS
- Anexo 5 - Requerimiento de seguridad (ENS) para los proveedores de software

Barcelona

Fecha: 2023.04.25
09:09:27 +02'00'

Áurea Alcaide Izquierdo

Área de Tecnología del Consorci AOC