Administració Oberta de Catalunya

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA REALIZACIÓN DE LAS TAREAS DE DESARROLLO EVOLUTIVO, MANTENIMIENTO CORRECTIVO Y SOPORTE DE TERCER NIVEL DE LOS APLICATIVOS PSIS y SIGNADOR

Número de expediente: AOC-2025-07

Generalitat de Catalunya

Localret

Índice

1. Introducción

El Consorcio AOC ofrece a las administraciones públicas catalanas el servicio de validación y sellado de tiempo. PSIS es la plataforma tecnológica desde donde se prestan estos servicios. El servicio de validación comprende principalmente la validación de certificados y la validación y completado o preservación de firmas electrónicas y documentos firmados. PSIS 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 (PSIS) es consumido por todas las entidades que forman parte de la administración pública catalana que disponen de aplicaciones informáticas donde se hace uso de certificados digitales y firma digital, con el fin de dotar de seguridad a los procesos de identificación y tratamiento de documentos firmados.

PSIS es un servicio transversal que se consume prácticamente por todos los demás servicios del Consorcio AOC, así como por el resto de las entidades de la administración pública catalana. Debido a esta transversalidad, es el servicio con el consumo más alto: en el año 2023 PSIS procesó 340 millones de operaciones.

El Signador es una herramienta de generación de firmas electrónicas basadas en certificados digitales. Las administraciones públicas catalanas lo integran en sus páginas web como herramienta de firma digital, a hacer uso tanto por parte de los empleados públicos, como cargos electos, y ciudadanos, cuando éstos deben firmar un documento administrativo o trámite.

El Signador permite firmar con certificados en local en posesión del signatario (certificado en dispositivo criptográfico o en software). Pero también ofrece la funcionalidad de firma remota mediante la integración con el servicio del Signador Centralizado del Consorcio AOC.

En el año 2023 se generaron más de 54 millones de firmas electrónicas con el Signador.

2. Objeto de la licitación

El objeto de esta contratación es la prestación de los servicios de desarrollo evolutivo, mantenimiento correctivo y soporte de tercer nivel de los aplicativos PSIS y Signador, basados ambos en tecnología Java.

Se incluye dentro del alcance de la licitación todas las tareas necesarias relativas al ciclo de vida completo de las aplicaciones, como son el análisis, el diseño técnico, el desarrollo, y el control de calidad (incluyendo tests unitarios, tests de integración, así como pruebas de rendimiento). Todas estas tareas deberán llevarse a cabo de acuerdo a la metodología de trabajo que se describe en el apartado 4.

Los principales objetivos del proyecto son, tanto para PSIS como para el Signador:

- Realización de tareas de desarrollo evolutivo sobre la arquitectura actual de cada uno de los aplicativos, en tecnología JAVA y desplegados en AWS. Estas tareas estarán enfocadas tanto en la implementación de nuevas funcionalidades como en la mejora del rendimiento.
- Realización del mantenimiento correctivo.
- Ofrecer apoyo técnico especializado en cuanto a la detección, diagnóstico y resolución de incidencias técnicas.

La duración del contrato será desde la fecha de formalización del contrato (no antes del 1 de enero de 2025) hasta el 31 de diciembre de 2025.

2.1. Desarrollo evolutivo

Desarrollo de nuevas funcionalidades o mejoras según el siguiente procedimiento (micro-proyecto):

- El Consorcio AOC proporcionará la información funcional y técnica necesaria para que el adjudicatario pueda hacer el análisis de la solución a implementar. Esta valoración se realizará en un tiempo inferior a 10 días laborables. La propuesta deberá detallar:
    - Tiempo previsto de ejecución
    - Esfuerzo por perfil
- El adjudicatario realizará el análisis detallado y el diseño técnico de la solución y el Consorcio AOC deberá validarlos.
- Una vez aprobada la propuesta por parte del Consorcio AOC y fijado el calendario de ejecución, la empresa adjudicataria asumirá el desarrollo completo de la solución y la codificación del mismo de acuerdo a la metodología que se describe en el apartado 4. Las desviaciones sobre el mismo, no imputables a cambios en la definición, podrán ser imputadas a la empresa adjudicataria, a criterio del Consorcio AOC, en función de la gravedad y el impacto.
- Gestión y control del código fuente. Esta gestión se llevará a cabo con el sistema centralizado de código fuente de que dispone el Consorcio 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 de rendimiento, en su caso, y de su ejecución en el entorno de desarrollo. En relación a las pruebas de rendimiento, el responsable de la ejecución de las mismas en el entorno de preproducción será el Consorcio AOC, con la participación del adjudicatario. El adjudicatario 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 preproducción y producción, de acuerdo al procedimiento de desarrollo definido por el Consorcio AOC.

- El adjudicatario deberá elaborar la documentación técnica y los manuales de usuarios correspondientes, así como mantener actualizada la documentación existente.
- El adjudicatario deberá prestar la formación a los usuarios que determine el Consorcio AOC cuando éste lo considere necesario.

Los evolutivos a implementar podrán responder a diferentes necesidades:

- Evolutivos funcionales: Modificación de funcionalidades existentes o incorporación de nuevas.
- Evolutivos de carácter legal y/o normativo: Relacionados con el cumplimiento de la normativa vigente (p. ej. Reglamento General de Protección de Datos, Esquema Nacional de Seguridad, etc.).
- Evolutivos de carácter técnico: Relacionados con necesidades de carácter tecnológico (mejoras en la arquitectura base, actualización del software base y/o de librerías de terceros, mejoras de rendimiento en determinadas funcionalidades, etc.).
- Evolutivos de seguridad: Su propósito es mejorar el nivel de seguridad del servicio en aspectos como pueden ser las políticas de control de acceso y los métodos de autenticación, las políticas de cifrado de datos en reposo y en tráfico, el plan de continuidad y la recuperación de datos, el procedimiento de gestión de parches de seguridad y actualizaciones, el procedimiento de gestión de incidentes de seguridad, etc.

Es muy importante destacar que el adjudicatario deberá tener un papel especialmente proactivo con los evolutivos tanto con los de carácter técnico como de carácter legal o normativo, proponiendo al Consorcio AOC todas aquellas mejoras que ayuden al cumplimiento de la normativa vigente, a mejorar el rendimiento del servicio o a fortalecer la seguridad. El adjudicatario por tanto deberá presentar recurrentemente, y de forma proactiva, al Consorcio AOC, todas aquellas propuestas de mejora que considere adecuadas con el correspondiente análisis y estimación de costes, y será decisión unilateral del Consorcio AOC decidir cuáles de estas propuestas finalmente se acaban aceptando y ejecutando (de acuerdo al mismo formato de micro-proyecto como cualquier otro evolutivo que hubiera propuesto el propio Consorcio AOC).

Para cada uno de estos micro-proyectos el adjudicatario deberá proporcionar los siguientes entregables:

- Diseño funcional
- Diseño técnico
- Planes de pruebas unitarias y de integración
- Manual de explotación
- Documentación para el CAU

2.1.1. Evolutivos previstos

A continuación, se exponen evolutivos previstos a realizar durante 2025. No serán exclusivos, y en función de las necesidades del servicio se llevarán a cabo éstos y/o habrá que desarrollar nuevos.

PSIS

1. Implementación de los **nuevos estándares de firma electrónica del reglamento europeo eIDAS (*electronic IDentification, Authentication and trust Services*)**:
    a. *Perfil de referencia de XAdES (XML Advanced Electronic Signatures)*
    ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES)
        - Parte 1*: Bloques de construcción y firmas de referencia XAdES*
        - Parte 2*: Firmas XAdES extendidas*

    b. *Perfil de referencia CAdES (Firma electrónica avanzada de CMS)*
    - ***ETSI EN 319 122 CMS Advanced Electronic Firmas (CAdES)***
        - Parte 1*: Bloques de construcción y firmas de referencia CAdES*
        - Parte 2*: Firmas CAdES extendidas*

    c. *Perfil de referencia de PAdES (PDF Firma Electrónica Avanzada)*
    ETSI EN 319 142 PDF Perfiles Avanzados de Firma Electrónica (PAdES)
        - Parte 1*: Bloques de construcción y firmas de referencia de PAdES*
        - Parte 2*: Perfiles de firmas PAdES adicionales*

2. Implementación **del estándar de firma electrónica JAdES (*JSON for Advanced Electronic Signatures*)**
    a. *Firma web JSON (JWS)*
        - RFC7515
    b. *Perfil de referencia de JAdES (JSON for Advanced Electronic Singatures)*
    ETSI TS 119 182-1 JAdES digital firmas
        - Parte 1: Bloques *de construcción y firmas de referencia de JAdES*

3. Integración de PSIS con una **autoridad de sellado de tiempo reconocida**. Está previsto sustituir la TSA de PSIS por una TSA calificada, es decir, que cumpla con los requerimientos del reglamento eIDAS. Habrá que integrar PSIS con la TSA calificada para llevar a cabo las funciones de completado de firmas.

Signador

1. Integración del Signador con la nueva solución del Consorcio AOC por **firma remota**. Actualmente el Signador está integrado con el Signador Centralizado del Consorcio

AOC. Pero esta solución de firma remota será sustituida por una nueva y habrá que sustituir la integración actual por la integración con la nueva solución.

2. Integración del Signador con una **autoridad de sellado de tiempo reconocida**. Habrá que integrar el Signador con la TSA calificada para añadir sellos de tiempo a las firmas generadas.

2.2. Mantenimiento correctivo

- Se entiende por mantenimiento correctivo la resolución de incidencias de carácter funcional y/o técnico que impidan el normal funcionamiento del servicio. Se incluyen tanto incidencias a nivel funcional, como de rendimiento.
- Las tareas de mantenimiento correctivo que el Consorcio AOC determine que hay que implementar con carácter urgente, se priorizarán por delante de los trabajos de mantenimiento evolutivo que se estén realizando en el momento de la incidencia. Estas tareas se someterán al control del Acuerdo Nivel de Servicio derivado de la categoría de la incidencia que ha originado el correctivo, y las penalizaciones asociadas se tratarán siguiendo estos criterios.
- Los informes de seguimiento semanal deberán reflejar estos correctivos realizados, y los Niveles de Servicio conseguidos para cada uno de ellos. Se contemplará finalizado el correctivo cuando las pruebas en torno a preproducción determinen la validez del mismo. El equipo responsable de realizar el correctivo, deberá realizar la documentación necesaria para la subida al entorno de preproducción y su correspondiente validación.

2.3. Gestión del cambio de configuración

El servicio de gestión de cambio de configuraciones consiste en realizar todas aquellas tareas necesarias para que la aplicación PSIS incorpore los cambios de configuraciones solicitados por el Consorcio AOC.

Los tipos de cambios de configuraciones pueden ser diversos, pero como mínimo, el servicio deberá cubrir las siguientes solicitudes:

- Carga de nuevas entidades de certificación (CA's).
- Carga / Renovación de certificados de entidades de respuesta OCSP.
- Carga de nuevos perfiles de certificados (que habrán sido emitidos por una entidad de certificación cargada a PSIS).

- Cambios en el parseo de los perfiles de certificados para obtener los diferentes atributos de los certificados en función de su perfil (política de certificado).
- Carga de políticas de firma.
- Configuración para cargar nuevas llaves dentro de la aplicación PSIS para poder firmar de manera centralizada (funcionalidad ASC).
- Configuración de permisos de autorizaciones de uso de una llave (privada) cargada a PSIS por parte de otra clave (pública).

2.4. Apoyo de tercer nivel

El servicio de apoyo avanzado consiste en realizar todas aquellas tareas necesarias con el fin de dar respuesta a todas aquellas consultas que plantee el Consorcio AOC . Los tipos de consultas pueden ser diversas:

- Consultas relacionadas con cualquier funcionalidad del servicio.
- Consultas relacionadas con el diseño de cualquiera de los módulos de la aplicación.
- Consultas relacionadas con la manera en que se utiliza de cualquiera de las funcionalidades de la aplicación.
- Consultas relacionadas con respuestas que el Consorcio AOC considere inesperadas del servicio.
- Consultas relacionadas con los mensajes de error obtenidos del servicio.
- Consultas relacionadas con la configuración vigente del servicio.
- Consultas relacionadas con los estándares y normativas en los que se basa el servicio.

2.5. Control de calidad

El adjudicatario será el responsable del control de calidad del servicio en todos aquellos desarrollos de nuevos evolutivos y correctivos que realice. En particular tendrán que llevar a cabo las siguientes tareas:

- Definición de los indicadores y métricas de calidad que deben cumplir los evolutivos/correctivos e identificar las medidas que se utilizarán para evaluar la calidad.
- Creación de un modelo de gestión de la calidad que asegure y garantice los acuerdos de nivel de servicio (ANS) definidos.

- Control de calidad de los evolutivos. Facturación del funcionamiento correcto de los mismos tanto a nivel funcional como técnico. Ejecución de pruebas unitarias y de integración. Ejecución de pruebas funcionales y de regresión. Ejecución de pruebas de rendimiento, en su caso.
- 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
- Comunicación y formación a los usuarios que determine el Consorcio AOC.

Todas estas actividades estarán dirigidas por el Consorcio AOC y deberán estar coordinadas por el Responsable del Servicio asignado por el adjudicatario. Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afecten a la solicitud de los evolutivos y correctivos.

2.6. Estándares de firma electrónica

Se valorará también positivamente la acreditación de conocimiento y/o experiencia en el ámbito de la firma electrónica, así como en los estándares de firma electrónica y de las librerías java que los implementan.

Estándares de firma electrónica:

- Protocolo DSS d'OASIS
- Estándares de firma XAdES, CAdES, y PAdES
- Estándares eIDAS de firma
- Protocolo RFC3161
- Electronic Signature Policies
- Public Key Infrastructure
- Etc.

Librerías java:

- BouncyCastle
- Apache XML Security

3. Equipo de trabajo

Para garantizar la máxima eficiencia, control y coordinación del servicio objeto de este contrato, la empresa adjudicataria deberá disponer en el momento de iniciar el contrato de un equipo con un amplio conocimiento tecnológico de los servicios a gestionar y con una fuerte experiencia en tareas similares a las descritas en este pliego.

La empresa adjudicataria deberá conformar el equipo de trabajo necesario al momento de iniciar el contrato. El proveedor podrá proponer unos perfiles y roles de personal superiores a los descritos a continuación para garantizar la ejecución satisfactoria del alcance de este contrato, pero en ningún caso podrá presentar unos perfiles inferiores a los mínimos exigidos en los criterios de adscripción de medios materiales y/o personales a la ejecución del contrato indicados en el apartado ***G4.*** del Cuadro de Características. El Consorcio AOC considera necesaria la participación mínima de los siguientes perfiles y roles:

Jefe de proyectos

Funciones:

- Seguimiento detallado del plan derivado del contrato, e interlocución con el Consorcio AOC por temas derivados de la ejecución del contrato.
- Dirección del servicio y coordinación de los recursos asignados al servicio, tanto materiales como personales.

Requisitos:

- Titulación: Ingeniería técnica o titulación superior.
- Experiencia mínima de 5 años en funciones de gestión de equipos responsables del desarrollo, testeo, mantenimiento correctivo y evolutivo de aplicaciones Java, y en especial de aplicaciones críticas en entornos productivos.
- Experiencia mínima de 5 años liderando equipos de como mínimo 4 integrantes.
- Experiencia mínima de 3 años en gestión de proyectos de aplicaciones java en la nube AWS e integración con servicios AWS.
- Experiencia mínima de 3 años en gestión de proyectos con contenedores.

Ingeniero de Software (dedicación 100%)

Funciones:

- Hacer la recopilación de los requerimientos de los nuevos evolutivos y correctivos a desarrollar, y asegurarse de que son completos, correctos y consistentes desde el punto de vista funcional.

- Establecer las planificaciones de los diferentes evolutivos y correctivos encomendados al adjudicatario, velando para que cada una de estas tareas se realicen de forma diligente y dentro de la planificación acordada. Informar al Consorcio AOC de las desviaciones tan pronto como se detecten.
- Generar la documentación asociada al servicio (análisis funcional, manuales de usuario, informes de seguimiento, etc.).
- Supervisión del trabajo del resto de personas del equipo con el objetivo de maximizar la calidad de los entregables.
- Proporcionar formación y apoyo al resto de miembros del equipo y también al personal del Consorcio AOC que éste determine. Proporcionar mentoría y orientación al resto de desarrolladores del equipo en cuestiones de arquitectura y diseño.
- Confección del diseño técnico y de la documentación de la arquitectura ligada a cada evolutivo y correctivo.
- Tomar las decisiones de diseño/arquitectura relativas a cada evolutivo escogiendo las tecnologías, plataformas y los patrones de diseño a utilizar.
- Evaluar nuevas tecnologías y determinar si son adecuadas para su inclusión en el proyecto.
- Liderar la fase de construcción de los cambios a realizar: entre otros, diseñar las clases, interfaces y el código necesario para el desarrollo de la aplicación atendiendo a los criterios fijados para cada desarrollo.
- Revisión del código del resto de desarrolladores del equipo para garantizar la calidad y la coherencia del código.
- En los casos de incidencias complejas deberá participar activamente en su diagnosis y resolución.
- Codificación, depuración y mantenimiento del código fuente de los evolutivos y correctivos.
- Implementación de las pruebas unitarias, de integración y de rendimiento para garantizar que los evolutivos y correctivos funcionan correctamente.
- Creación de la documentación técnica de los evolutivos/correctivos.
- Preparación de los paquetes de despliegue para los diferentes entornos de desarrollo, preproducción y producción.

Requisitos:

- Titulación: Ingeniería técnica o titulación superior.

- Experiencia mínima de 5 años como responsable tecnológico de aplicaciones Java/J2EE y bases de datos relacionales SQL.
- Experiencia mínima de 5 años en las siguientes tecnologías:
  - Integración de servicios web (Webservices, SOAP, WSDL, REST, etc.)
  - Hibernate, Spring IoC
  - PostgreSQL
  - MongoDB
  - XSD, XML
  - Docker
  - Contenedores (Kubernetes)
- Experiencia mínima de 3 años en aplicaciones java desplegadas en la nube AWS e integración con servicios AWS.
- Experiencia mínima de 3 años en las siguientes herramientas de gestión y construcción de proyectos:
  - Git, Eclipse, Maven, Gradle
  - Jenkins
- Experiencia mínima de 3 años en las siguientes herramientas de testeo:
  - SoapUI, JMeter

3 Desarrolladores Java/J2EE (mínimo dos de ellos con dedicación completa 100%)

Funciones:

- Codificación, depuración y mantenimiento del código fuente de los evolutivos y correctivos.
- Ejecución exhaustiva del plan de pruebas definido para los evolutivos/correctivos.
- Colaborar en la elaboración de documentación técnica relativa a los evolutivos/correctivos.

Requisitos:

- Titulación: Formación profesional, ingeniería técnica o titulación superior.
- Experiencia mínima de 3 años en:
  - Java en J2EE
  - Servicios Web

- Hibernate, Spring IoC
  - PostgreSQL
  - MongoDB
  - XSD, XML
- Experiencia mínima de 3 años en:
  - Eclipse, Git, Maven, Gradle
  - SoapUI, JMeter
- Experiencia en aplicaciones java desplegadas en la nube AWS e integración con servicios AWS (AWS Lambda, SQS, Aurora, DocumentDB, S3, ...).

Ingeniero Kubernetes y DevOps (dedicación puntual)

Funciones:

- Creación, ejecución y distribución de contenedores docker.
- Optimización de las imágenes docker minimizando el tamaño y optimizando las capas.
- Compilación y ejecución de imágenes docker en registros.
- Garantizar la calidad y la confiabilidad de las actualizaciones de software.
- Colaborar en la elaboración de documentación técnica relativa a las tareas encomendadas.
- Colaborar en la automatización de los procesos de desarrollo en el cloud.

Requisitos:

- Titulación: Ingeniería técnica o titulación superior.
- Experiencia mínima de 3 años en Kubernetes.
- Experiencia mínima de 3 años como ingeniero DevOps.
- Experiencia en CI/CD, IaC, CM, SAST, DAST, OWASP.
- Experiencia en Jenkins.

La dedicación del ingeniero de software y de 2 de los desarrolladores debe ser del 100%. Las horas necesarias para llevar a cabo el servicio se estiman en 7.210 horas, que deberán ejecutarse en su totalidad en el periodo de duración del contrato. La empresa adjudicataria, en función de la duración del contrato, y del volumen de horas previsto para realizar los proyectos, deberá dimensionar adecuadamente el equipo de trabajo para dar respuesta a los requerimientos valorados, en tiempo y forma. Es decir, la disponibilidad de las horas ejecutadas puede, puntualmente, no ser proporcional a la duración del contrato, sino que deberá adaptarse a las necesidades y requerimientos del servicio, pudiendo fluctuar en función de la carga de las tareas encomendadas, debiendo meses en los que se pueda requerir un mayor o menor dimensionado del equipo de trabajo.

El Consorcio AOC se reserva el derecho de 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 Consorcio 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 Consorcio AOC con el fin de minimizar el impacto en los desarrollos en curso.

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

4. Metodología

Las tareas a realizar contempladas se engloban dentro del mantenimiento evolutivo y correctivo de las aplicaciones PSIS y Signador del Consorcio AOC durante la fase continua de su ciclo de vida. Ambos aplicativos tienen un alto grado de madurez y se encierra dentro del conjunto de servicios que ofrece el Consorcio AOC. PSIS está en producción desde el año 2007 y el Signador desde el 2017.

Hay que tener en cuenta que estos servicios presentan una cierta complejidad en su gestión debido a los siguientes motivos:

- La dirección estratégica de cada servicio está liderada por un Jefe de Servicio con unos objetivos y plazos concretos, que ocasionalmente pueden presentar interdependencia con otros servicios.
- Alta dependencia con terceros (p. ej. organismos externos a la AOC que pueden impactar tanto en el alcance funcional como con los plazos de ejecución previstos inicialmente).

Cada una de las versiones a desarrollar se considerará como un proyecto propio que deberá desarrollarse siguiendo el cumplimiento de esta guía metodológica.

A continuación, se detallan las fases por las que debe pasar cada una de las nuevas versiones de un determinado servicio, desde su definición hasta su puesta en marcha.

Introducción de las tareas en JIRA

El Jefe de Servicio traduce los objetivos estratégicos que marca el comité estratégico en las peticiones de mejora y evolutivos que deben permitir alcanzar estos objetivos. A continuación, los introduce como tarea de Servicios a la herramienta JIRA. En el momento de entrar cada tarea (en forma de ticket) indica su prioridad.

Fase de definición

La fase de definición de la versión consiste en seleccionar cuáles son los requerimientos funcionales que deben entrar a formar parte de la próxima versión a desarrollar.

El Jefe de Proyectos (Subdirección de Operaciones) estudia todos aquellos requerimientos que se pueden incluir dentro de una ventana tipo que el Consorcio aplica a sus servicios (por servicios grandes, versiones cada 3 meses aproximadamente entre la puesta en marcha de cada versión, aunque dependiendo de las necesidades, la ventana se puede reducir o ampliar).

El Jefe de Proyectos consensua con el Jefe de Servicio el alcance de la versión y se confecciona la lista definitiva de tareas trasladando esta lista de peticiones en tareas de Proyectos JIRA que representa la versión a desarrollar.

En caso de que sea necesario, es el Jefe de Servicio quién define el plan de comunicación que deberá llevarse a cabo antes de que la versión llegue a los usuarios finales, y dentro de este plan seleccionará a los usuarios y organismos que deberán participar en la prueba piloto, si se estima oportuno.

El Jefe de Proyectos introduce toda esta información en los tickets JIRA que conforman la versión. Una vez cerrado el alcance de la versión, no se aceptará ninguna modificación en la lista de funcionalidades a desarrollar hasta la próxima fase de definición de la nueva versión.

Análisis

El adjudicatario partirá de la recopilación de funcionalidades a satisfacer que se han seleccionado en el JIRA para la nueva versión y deberá realizar las reuniones de toma de requerimientos para poder hacer la recaudación detallada de todos los requisitos tanto funcionales como tecnológicos solicitados. Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afecten al alcance de una determinada versión.

El adjudicatario elaborará un análisis previo de la solución que propone incluyendo una estimación del impacto que supone el evolutivo. En caso de que haya diferentes alternativas, el adjudicatario deberá explicarlas indicando las ventajas e inconvenientes de cada una.

Planificación

El Jefe de Proyectos añadirá al JIRA las tareas técnicas que considera necesarias para poder desarrollar la versión (documentación técnica, plan de pruebas, etc.) y prepara conjuntamente con el adjudicatario la planificación detallada de la versión asignando las tareas entre los diferentes técnicos de desarrollo.

Desarrollo de tareas planificadas

Las tareas que comportará esta fase son:

- Generación del código.
- Ejecución de pruebas unitarias.

- Ejecución de pruebas de integración.
- Ejecución de pruebas de rendimiento, en su caso.
- Elaboración de la documentación funcional y técnica.

El adjudicatario deberá hacer un uso frecuente de la herramienta de control de versiones de código (Github) del servicio para sincronizar los diferentes desarrollos. La frecuencia ideal de sincronización (tanto para subir al repositorio los cambios realizados como para descargar todos los cambios que han introducido el resto de desarrolladores) sería hacerlo una vez al día (p. ej. a primera hora de la mañana) de forma que se detecte cuanto antes los conflictos entre los diferentes desarrollos.

Antes de subir nada al repositorio cada desarrollador deberá garantizar en el tamaño que sea posible que el código subido es íntegro. Si no es posible subir los cambios de forma diaria, sí se debe garantizar que cada equipo de desarrollo subirá los cambios como mínimo con una frecuencia semanal.

Los despliegues en el entorno de desarrollo se harán consensuadamente con el Jefe de Proyectos. Aunque los diferentes técnicos tendrán acceso al entorno de desarrollo, no podrán desplegar sin el visto bueno del Jefe de Proyectos. Las pruebas se realizarán preferentemente en los entornos locales de los desarrolladores. Sólo cuando la versión se considere suficientemente estable podrá desplegarse en el entorno de desarrollo.

Implantación y aceptación

En base a las entregas de la fase anterior se procederá a realizar la implantación del evolutivo sobre los diferentes entornos. En primer término, en el entorno de desarrollo. El adjudicatario procederá a realizar la ejecución del plan de pruebas. En caso de que se supere satisfactoriamente, el Jefe de Proyectos procederá a promocionar el cambio en el entorno de preproducción y posteriormente al de producción.

En caso de que en este proceso los resultados obtenidos no sean los esperados (es decir, los que se obtuvieron en el entorno de desarrollo) el adjudicatario deberá dar el apoyo necesario, si es necesario presencial, para solucionarlo.

Una vez se haya realizado la ejecución del plan de pruebas con el 100% de las pruebas funcionando en torno a preproducción y producción, se dará el proyecto por cerrado. A partir de ese instante entrará en vigor el periodo de garantía del evolutivo.

A partir de este momento ya debe entrar en vigor la etapa de apoyo. Es responsabilidad del adjudicatario realizar las tareas necesarias de traspaso, formación y documentación del proyecto, de operación, y de procedimiento, para que los nuevos desarrollos ya puedan ser objeto del servicio de apoyo.

Una vez acabada la etapa de codificación y superadas las pruebas de integración en el entorno de preproducción, el Jefe de Proyectos, con el apoyo del equipo de desarrollo, deberá preparar el plan de implantación con la colaboración del equipo de Apoyo de la AOC (también dependiente de la Subdirección de Operaciones). El plan de implantación incorpora todas las acciones dirigidas a que la versión llegue a los usuarios finales.

Hay que tener en cuenta que ninguno de los técnicos de desarrollo sin embargo, tiene -por defecto- acceso a los entornos de preproducción y producción.

Para llevar a cabo el plan de implantación el Jefe de Proyectos prepara el paquete de despliegue y realiza una petición al proyecto Despliegues del JIRA. En la petición de despliegue se indicará la versión del JIRA a la que corresponde el despliegue.

Los despliegues en el entorno de preproducción se realizan típicamente los jueves por la tarde y la petición de despliegue debe haber llegado como muy tarde el día de antes, para que se pueda preparar junto con el resto de despliegues de otros servicios del Consorcio AOC. Adicionalmente y con el objetivo de agilizar y garantizar la correctas de los despliegues, se está implantando un sistema de integración continua y despliegue automático.

Una vez desplegado en preproducción, es el Jefe de Proyectos con el apoyo del adjudicatario, quien deberá ejecutar el plan de pruebas para realizar la validación final. El Jefe de Proyectos del Consorcio AOC decidirá si la versión supera satisfactoriamente el plan de pruebas. En caso afirmativo, el Jefe de Proyectos preparará y solicitará a través del JIRA la petición de despliegue a producción. En caso contrario, el equipo de desarrollo realizará las correcciones necesarias dando todo el apoyo necesario para corregir las incidencias detectadas en la mayor brevedad posible. Los despliegues en torno a producción se realizan típicamente los miércoles por la tarde.

Una vez la versión se haya desplegado en producción entrará en vigor el periodo de garantía del evolutivo.

Evaluación

Una vez definidos los requerimientos que formarán parte de la versión, el Jefe de Proyectos define las métricas y los indicadores que permitirán evaluar el cumplimiento de los objetivos marcados para la versión.

Tras un cierto tiempo de la puesta en marcha de la versión, el Jefe de Servicio realizará el seguimiento de los indicadores a través de encuestas, auditorías y cualquier otra herramienta de gestión de la calidad que considere adecuada, estableciendo el cuadro de mando del servicio.

Este cuadro de mando se pondrá a disposición del comité estratégico con el objetivo de mantenerlo informado de la marcha del servicio.

Finalmente, el comité de seguimiento realizará una sesión de retrospectiva analizando conjuntamente qué cosas han ido bien durante la versión y qué cosas han ido mal (desde el punto de vista de todos los actores) para poder aprender y mejorar de cara a futuras versiones.

JIRA

La herramienta corporativa JIRA se convierte en la piedra angular de la versión en tanto que permite reflejar en detalle el estado actual y el grado de consecución de la misma, así como la evolución estratégica que seguirá el servicio en un futuro medio. Es por tanto una herramienta fundamental para mantener coordinados a todos los actores.

La información del JIRA se hace visible a todos los actores que participan en el servicio, pero dado que cada uno de los actores priorizará un tipo de información diferente, se requiere de un esfuerzo por parte del Jefe de Servicio y del Jefe de Proyectos para reflejar en el JIRA los diferentes puntos de vista. Esta diferente visión se plasma en el JIRA a partir de los siguientes proyectos:

- Servicio: Evolución estratégica de un servicio a medio/largo plazo. En este proyecto del JIRA los requerimientos se agrupan y se ordenan en ideas conceptuales próximas a las líneas de actuación que marca el comité estratégico. Este proyecto permite obtener una idea global de lo que se pretende conseguir con el servicio a medio o largo plazo.

Para los requerimientos más prioritarios, que inicialmente son los candidatos a ser seleccionados para la próxima versión, el responsable del servicio realizará el análisis funcional detallado.

El Jefe de Servicio es el principal responsable del mantenimiento en el JIRA de este proyecto y debe reflejar todos los cambios y documentos con la máxima periodicidad posible.

- Proyecto: Vista detallada del futuro inmediato del servicio. En este proyecto del JIRA se descomponen las peticiones de evolutivos en los diferentes requerimientos funcionales y técnicos que debe cumplir la nueva versión. Los asuntos que componen este proyecto se encuentran bien definidos y detallados, disponen de una estimación de su coste, los recursos que están asignados, así como su grado de adelanto. Este proyecto permite obtener una idea detallada del estado actual del servicio y su objetivo es mantener informado con el mayor nivel de detalle posible a los diferentes actores que participan en el desarrollo diario del servicio.

El Jefe de Proyectos es el principal responsable del mantenimiento en el JIRA de este proyecto y debe reflejar todos los cambios con la máxima periodicidad posible. En este proyecto se incluirán todos los documentos técnicos (diseño técnico, documentos de integración, etc.).

Los desarrolladores deberán actualizar los tickets que tengan asignados con los detalles técnicos necesarios para comprender no sólo los avances en las tareas encomendadas, sino también para que quede registrada toda la información relativa a la resolución de las mismas.

Por cada ticket Jira que requiera de cambio de código, el desarrollador deberá crear una nueva rama en el repositorio Git correspondiente, identificando en el nombre de la misma el ticket del Jira al que se corresponde.

En su caso, cualquiera de estos 2 proyectos principales se pueden complementar con otros proyectos que permitan agrupar líneas de actuación que se llevarán a cabo a largo plazo o bien que se llevarán a cabo en paralelo, pero en fechas diferentes. El objetivo de estos proyectos complementarios debe ser simplemente el de facilitar a los diferentes actores la lectura del estado presente y futuro del servicio.

Requerimientos técnicos y personales

El licitador deberá disponer en el momento de iniciar el contrato, de los recursos que se han indicado en la descripción del contrato.

El proveedor debe garantizar que para la resolución de incidencias y para dar respuesta a las peticiones básicas de operación siempre habrá un mínimo de dos personas formadas en cada uno de los entornos y que, como mínimo, siempre hay una disponible.

En caso de baja definitiva de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirlo en menos de 15 días laborables de acuerdo con los responsables del Consorcio AOC. Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario deberá ser validado por el Consorcio AOC. Habrá que acordar el calendario de cambio con el Consorcio AOC con el fin de minimizar el impacto en los desarrollos en curso. Quedan fuera de este compromiso los periodos de vacaciones y permisos de todos los miembros del equipo.

Cuando se cambie un miembro del equipo de trabajo a instancias del adjudicatario, se fijará un tiempo de 2 semanas de formación/adaptación del nuevo miembro que serán a cargo del adjudicatario.

El Consorcio AOC se reserva el derecho a solicitar el cambio de cualquiera de los miembros del equipo sin necesidad de justificación con una antelación de 20 días naturales a la fecha de sustitución.

Además de los perfiles descritos, habrá que aportar un gestor del servicio de alto nivel sin cargo y que se encargará de las siguientes tareas:

- Interlocución a alto nivel.
- Diseño y seguimiento del plan derivado del contrato.
- Velar para que cada fase del proyecto se realice de forma diligente y dentro de las fechas acordadas.
- Informar de las desviaciones de las fechas de finalización de cada fase tan pronto como se detecten.
- Gestionar los recursos asignados, tanto materiales como personales.

5. Acuerdos de Nivel de Servicio

En este apartado se describe el marco contextual de aplicación de los Acuerdos de Nivel de Servicio. Se establecerá el siguiente procedimiento de trabajo y el Acuerdo de Nivel de Servicio (ANS) que se detalla a continuación para todos los entregables que se desarrollen en el entorno de producción.

Las posibles penalizaciones que se deriven del incumplimiento de los ANS, se aplicarán sobre descuento en la siguiente factura emitida tras la penalidad. La aplicación de penalidades será acumulativa.

Los Acuerdos de Nivel de Servicio se podrán revisar y modificar siempre y cuando haya acuerdo mutuo entre el adjudicatario y el Consorcio AOC.

Requerimientos de nivel de servicio

Resolución de incidencias sin errores:

- Porcentaje de la resolución de incidencias sin errores en el plazo.
    - Cálculo: (A/B)*100

      A: Número total de incidencias resueltas sin error en el plazo

      B: Total de incidencias resueltas en el plazo
- Nocturnidad: Diaria
- El porcentaje de incidencias sin error en el plazo establecido deberá ser como mínimo del 90%.
- El nivel ofrecido por quien resulte adjudicatario constituirá un Acuerdo de Nivel de Servicio (ANS), cuyo cumplimiento se medirá durante toda la duración de la prestación del servicio.

ANS para la gestión de las incidencias

Este ANS aplica a la totalidad del servicio contratado.

Definiciones:

Nivel	Descripción
Bloqueando	Una incidencia se catalogará con criticidad bloqueando si impide la utilización total del servicio a todos los usuarios del mismo.
Alta	Una incidencia se catalogará con criticidad alta si impide la utilización de una parte concreta del servicio, a todos o algunos usuarios, y la afectación por el negocio es elevada.
Media	Una incidencia se catalogará con criticidad media si impide la utilización de una funcionalidad concreta de alguno de los servicios a todos o algunos usuarios y la afectación por el negocio es relativamente baja.
Baja	Una incidencia se catalogará con criticidad baja si no impide la utilización ni parcial ni total de alguno de los servicios a alguno de los usuarios.

El tiempo de respuesta y de resolución se establecen según el tipo de incidencia:

- Tiempo de respuesta

  Se define como tiempo de respuesta el tiempo que transcurre desde que la incidencia es comunicada, y el usuario recibe el ticket de su incidencia. El tiempo de respuesta se cuenta sobre el horario de apoyo de recepción de incidencias.
- Tiempo de resolución

Se define el tiempo de resolución de una incidencia como el número de horas que transcurren desde que el usuario recibe el ticket de la incidencia hasta el momento en que la incidencia está solucionada. En el cálculo del tiempo de resolución de una incidencia no se tienen en cuenta los posibles incrementos de tiempo provocados por la intervención inevitable de terceros en el proceso de resolución (por ejemplo, intervención de otros organismos).

El tiempo máximo permitido por la respuesta y resolución de una incidencia dependerá del nivel de criticidad de la incidencia. En la siguiente tabla se muestran los tiempos máximos permitidos por la resolución de una incidencia en función del nivel de criticidad:

Criticidad Incidencia	**Tiempo de respuesta (horas)**	**Tiempo de resolución (horas)**	**% de resolución dentro del tiempo comprometido**
0 Bloqueando	0,5	2	95 %
1 Alta	1	16	95 %
2 Media	1	40	95 %
3 Baja	1	64	95 %

Para el cálculo del tiempo de resolución de una incidencia se excluirán los posibles incrementos de tiempo provocados por la intervención inevitable en el proceso de resolución por parte de terceros.

En el caso de que el adjudicatario no cumpla el acuerdo de nivel de servicio definido anteriormente al menos en el 95% de las de incidencias con criticidad 0 y 1 que hayan ocurrido dentro del mes se le aplicará las siguientes penalizaciones:

Porcentaje de incidencias con criticidad 0 y 1 dentro del mes que cumplen la ANS	Penalización sobre la cuota mensual de la factura
Superior al 95%	0%
Entre 95% y 80%	5%
Entre 80% y 70%	10%
Inferior al 70%	15%

En caso de que el adjudicatario no cumpla el acuerdo de nivel de servicio definido anteriormente para al menos el 90% de las de incidencias con criticidad 2 y 3 que hayan ocurrido al mes, se le aplicará las siguientes penalizaciones:

Porcentaje de incidencias con criticidad 2 y 3 dentro del mes que cumplen la ANS	Penalización sobre la cuota mensual de la factura
Superior al 90%	0%
Entre 90% y 51%	5%
Inferior al 51%	10%

Requerimientos de nivel de servicio en la protección de datos

Se considerará incumplimiento del contrato la no aplicación de las medidas de seguridad impuestas al contratista. Aparte de las posibles responsabilidades que se puedan derivar de dicho incumplimiento, y que en función de la gravedad del mismo pueda comportar la resolución del contrato, se prevé la imposición de penalidades.

Las penalidades a imponer serán por cada incumplimiento que se produzca y con el tope máximo establecido en el artículo 192 de la Ley 9/2017, de Contratos del Sector Público:

- Medidas de seguridad de nivel bajo: 0,5% del precio de adjudicación del lote.
- Medidas de seguridad de nivel medio: 0,75% del precio de adjudicación del lote.
- Medidas de seguridad de nivel alto: 1% del precio de adjudicación del lote.

Incidentes de seguridad

Es importante destacar que cualquier incidente de Seguridad o de protección de datos personales que puedan afectar a los sistemas del Consorcio AOC, deberá informarse en un tiempo inferior a las 24h.

En la fase inicial del proyecto se deberá definir un procedimiento de coordinación ante incidentes que puedan afectar a los sistemas del Consorcio AOC. Este procedimiento deberá contemplar los flujos de información y las interacciones entre Consorcio AOC y el adjudicatario durante la gestión del incidente.

A su vez el adjudicatario deberá informar periódicamente de los incidentes que hayan afectado a los sistemas o plataformas del Consorcio AOC.

6. Condiciones de ejecución

El adjudicatario deberá cumplir las siguientes obligaciones básicas:

- Gestionar cualquier alteración del servicio en las condiciones expresadas en este pliego.
- Realizar reuniones periódicas con el Consorcio AOC con el fin de exponer el cumplimiento del servicio y tratar los posibles problemas o mejoras del servicio.
- Establecer un marco metodológico de trabajo basado en la metodología Agile.
- Realizar la formación de los técnicos designados, en todos aquellos aspectos que el Consorcio AOC crea oportunos y que sean de directa aplicación a los servicios requeridos.
- Elaboración de los manuales y otra documentación destinada a la formación de los usuarios.

- Elaboración de la documentación técnica.
- Mantener en todo momento la actualización del código fuente y de la documentación en el sistema de control de versiones del Consorcio AOC (GitHub) para que pueda estar disponible en todo momento para el personal asignado y también para disponer de la opción de control de versiones.
- Toda la documentación generada por el equipo será preferentemente en catalán y en el formato corporativo propuesto por Consorcio AOC.
- Presentación de informes mensuales con el detalle del estado del servicio de acuerdo con los indicadores que el Consorcio AOC considere apropiados. Algunos ejemplos de estos informes serían:
    - Informe resumen de las actuaciones realizadas.
    - Informe de situación de las actuaciones en curso.
    - Informe resumen de las actuaciones pendientes.
    - Planificación de las actuaciones a realizar.
- Informe de finalización del contrato con el resumen de las tareas realizadas.

El Consorcio AOC se reserva el derecho a validar, y en su caso definir, las herramientas que se tengan que utilizar para la gestión y control del servicio.

7. Modelo de relación

El adjudicatario deberá incluir en su propuesta cuál es el modelo de relación que propone para garantizar el éxito del proyecto: la estructura organizativa del servicio, los canales y herramientas de comunicación a todos los niveles entre el proveedor y el Consorcio AOC, los procedimientos de escalado ante incidencias susceptibles de afectar o con afectación a los servicios bajo responsabilidad del proveedor, y qué herramientas de control (adicionales a las herramientas corporativas JIRA y Microsoft Teams del Consorcio AOC), propone para llevar a cabo el seguimiento y control global del servicio. Cabe destacar que el Consorcio AOC se reservará el derecho a validar, y en su caso definir, estas herramientas de control.

Como mínimo, será necesario que se establezcan los siguientes niveles de interlocución:

Reuniones de dirección con las siguientes características:

- Interlocutores: Gerente de cuentas y/o jefe de proyectos por parte del adjudicatario. Gestor del servicio y/o Jefe de Proyectos por parte del Consorcio AOC.
- Periodicidad mínima: 1 mes

- Objetivo: Hacer el seguimiento del contrato, analizando diversos aspectos: productividad, control de horas, temas de facturación, seguimiento de metas (a alto nivel), etc.
- Escandallo de horas totales realizadas en el mes.
- Entregables: actas de las reuniones, informes ejecutivos, informes con control de horas (hechas y pendientes) etc.

Reuniones de seguimiento con las siguientes características:

- Interlocutores: Ingeniero de software por parte del adjudicatario. Jefe de Proyectos por parte del Consorcio AOC.
- Periodicidad mínima: 1 semana
- Objetivo: Seguimiento del cumplimiento de la ANS, rendimiento de la plataforma e incidencias más destacables.
- Entregables:
    - Informes del estado del servicio
    - Informe resumen de las actuaciones ya resueltas y horas realizadas.
    - Informe de situación de las actuaciones en curso y horas realizadas.
    - Informe resumen de las actuaciones pendientes y horas estimadas.
    - Planificación de las actuaciones a realizar.
    - Informe de las incidencias abiertas, resueltas, tiempo de resolución,...

8. Horario de ejecución del servicio

El licitador deberá incluir en su propuesta la disponibilidad horaria del personal asociado al servicio, aunque deberá garantizar la disponibilidad de como mínimo 1 miembro del equipo durante las franjas horarias siguientes:

- De lunes a viernes, excepto festivos de la ciudad de Barcelona, **de 09:00 a 17:00 horas**.
- El 90% de los trabajos se realizarán en el horario indicado. En el 10% de los casos restantes se podrá solicitar previamente la realización de tareas fuera del horario anteriormente establecido sin coste adicional.

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 Consorcio AOC.

Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario deberá ser pactado con el Consorcio AOC. En estos casos, se fijará un tiempo de 2 semanas de formación/adaptación del nuevo miembro que serán a cargo del adjudicatario.

9. Infraestructura necesaria

El adjudicatario deberá aportar la infraestructura técnica, licencias, y cualquier otro componente o medio técnico necesario para la realización de los trabajos. Los costes de esta infraestructura tecnológica irán a cargo de los adjudicatarios. Es importante destacar que esta infraestructura tecnológica no podrá contener en ningún momento datos reales. Para los tests y pruebas de los diferentes entregables, los adjudicatarios deberán disponer de entornos de integración en sus instalaciones para realizar el control de calidad de los evolutivos desarrollados. En el Anexo 1 se incluye una descripción de la infraestructura tecnológica de PSIS y en el Anexo 2 del Signador.

El adjudicatario mantendrá en todo momento la actualización del código fuente en el sistema de control de versiones del Consorcio AOC (Git).

Las tareas deberán llevarse a cabo en las oficinas de cada una de las empresas adjudicatarias, aunque de forma puntual es posible que en alguna ocasión sea necesario el desplazamiento de alguno de los miembros de los adjudicatarios a las instalaciones del Consorcio AOC o de terceros. Por este motivo se recomienda que todos los miembros del equipo dispongan de ordenadores portátiles.

Todos los trabajos desarrollados, y en particular los entregables entregados, deberán seguir las guías de estilo definidas por el Consorcio AOC. El Consorcio AOC facilitará a todos los adjudicatarios estas guías de estilo y su cumplimiento será obligatorio para la aceptación de los trabajos.

10.Propiedad intelectual

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

La empresa adjudicataria 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, directa o extractada, original o reproducida, sin

autorización expresa del Consorcio AOC, que la daría, si procede, previa petición formal del adjudicatario con expresión del fin.

11.Garantía

Todas las tareas que forman parte del alcance del contrato tendrán una garantía de 6 meses. Durante este periodo, el adjudicatario deberá comprometerse a resolver satisfactoriamente todas aquellas incidencias o defectos detectados en cualquiera de las actividades llevadas a cabo por su equipo de trabajo que le sean imputables con él por acción u omisión.

12.Requerimientos de seguridad

El adjudicatario deberá cumplir con los siguientes requerimientos de seguridad:

12.1. Medidas de seguridad y por defecto

El Consorcio AOC, con el apoyo del adjudicatario, implementará durante la fase de desarrollo, las medidas de protección de datos desde el diseño y por defecto, recogidas en la guía del APDCAT:La privacidad desde el diseño y la privacidad por defecto. Guía para desarrolladores (gencat.cat)

Los adjudicatarios deberán documentar:

- El análisis llevado a cabo de las medidas necesarias.
- La verificación de que las medidas han sido aplicadas.

12.2. Valoración de los servicios

El Consorcio AOC ha valorado los datos y el servicio de PSIS de la siguiente manera:

	ACC		RGDP	ENS					
SERVEI	Seguretat	Disponibilitat	DP	Confidencialitat	Disponibilitat	Autenticitat	Integritat	Traçabilitat	RTO
Validador - PSIS	Molt Crític	Servei essencial	Mitja	Baixa	Alta	Alta	Mitja	Alta	<4h

ACC: Agencia Catalana de Ciberseguridad
RGDP: Reglamento General de Protección de Datos
ENS: Esquema Nacional de Seguridad
RTO: Tiempo máximo de recuperación del servicio en caso de indisponibilidad

12.3. Medidas de seguridad que debe incorporar PSIS como solución

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad de nivel ALT del Esquema Nacional de Seguridad que afecten directamente a PSIS como solución y plataforma tecnológica. El Consorcio liderará la adecuación del servicio a los requerimientos de seguridad.

12.4. Medidas de seguridad a cumplir por parte del adjudicatario

Certificaciones de seguridad

Durante el tiempo de ejecución del contrato, el adjudicatario deberá implementar las medidas de seguridad de nivel BAJO del Esquema Nacional de Seguridad en todos sus sistemas de información involucrados en la prestación del servicio. Concretamente son las descritas en:

- *Anexo 3 - Requerimientos de seguridad (ENS) para los proveedores de software.*

El Consorcio AOC auditará en un plazo no superior a 6 meses, que el adjudicatario cumple con los requerimientos del *Anexo 3 - Requerimiento de seguridad (ENS) para los proveedores de software.*

La auditoría se hará mediante la entrega de 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 declaración de conformidad en el nivel BAJO del Esquema Nacional de Seguridad.

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

12.5. Medidas adicionales

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 Consorcio AOC para acceder a sus sistemas.

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 Consorcio AOC.

En caso de baja de un usuario, de manera inmediata el adjudicatario deberá informar al Consorcio AOC con el fin de revocar sus derechos de acceso a los sistemas.

Protección de la información

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

El adjudicatario no podrá descargar información del Consorcio AOC en sus sistemas o en soportes portátiles como USBs, DVDs, portátiles, tablets, etc. En el caso de tener que hacerlo habrá que pedir la autorización del Consorcio AOC y que el apoyo esté cifrado.

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

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

13.Plan de devolución del servicio

El adjudicatario deberá asumir dentro del contrato la planificación y ejecución del plan de devolución del servicio al final de la prestación. El plan de devolución deberá cumplir con los siguientes requerimientos mínimos:

- Una duración de 1 mes con una dedicación mínima de 160h y tanto la duración (1 mes) como la dedicación (160h) serán adicionales a la prestación principal del servicio de 24 meses y deberán ir a cargo del adjudicatario.
- El adjudicatario deberá devolver el código fuente, scripts, documentación, etc. de todas las actualizaciones realizadas.

El adjudicatario deberá destruir y/o devolver al Consorcio AOC (o en aquel tercero que éste designe) la información propiedad del Consorcio AOC. Este retorno deberá realizarse de acuerdo con lo establecido legalmente y según las indicaciones del Consorcio AOC. La devolución contemplará todos los productos y softwares que sean de propiedad del Consorcio AOC junto con los soportes o documentos en que conste algún dato del mismo. La devolución de los datos al Consorcio AOC, o en un tercero designado, se llevará a cabo en el formato y los soportes que se acordarán en el momento de planificar y detallar el plan de finalización del contrato. El adjudicatario deberá disponer de un procedimiento de borrado seguro de soportes reutilizados o que lleguen al final de su vida útil. El proveedor deberá informar cómo hace la eliminación segura de la información y deberá proporcionar los certificados correspondientes conforme ha realizado esta eliminación segura.

Barcelona, 21 de octubre de 2024

Áurea Alcaide Izquierdo

Jefa de Proyectos de la Subdirección de Operaciones del Consorcio AOC

Anexo 1 – PSIS

Descripción funcional

Las principales funcionalidades de la aplicación PSIS son las siguientes:

1. **Facturación de certificados digitales**: permite consultar el estado de un certificado. La aplicación responde si es válido o no es válido (por ejemplo, porque está revocado). En la misma respuesta también puede devolver información adicional, como por ejemplo, datos útiles del certificado digital (pe. el nombre y apellidos, el DNI, etc.) y el nivel de seguridad asociado al certificado digital (pe. nivel 3 en caso del certificado idCAT, nivel 4 en caso de un certificado de firma de trabajador público, etc.).

2. **Facturación y completado de firmas digitales**: el servicio permite realizar la comprobación de la validez de una firma digital. El servicio inspecciona la firma y verifica por una parte que, criptográficamente, la firma esté bien formada. Por otra parte, comprueba el estado del certificado en el momento que se ha producido la firma. En función de los resultados anteriores responde si la firma es válida o no es válida.

El servicio permite la validación de firmas digitales *simples* (CMS y el XMLDsig) y firmas *avanzadas* (CAdES y XAdES y PAdES). Estas últimas, además de permitir identificar el signatario y detectar cualquier cambio posterior de los datos firmados (al igual que las firmas *simples*), permiten que la firma digital sea perdurable en el tiempo más allá de la vida del propio certificado del signatario. Esto lo permite hacer la ampliación por medio del completado de la firma: añadiendo a la propia firma un *sello de tiempo* que permita ubicarla en el tiempo de manera fiable, y añadiendo también información sobre el estado de revocación del certificado del signatario y de la cadena de certificados.

3. **Creación de firmas digitales**: La aplicación permite generar firmas de forma desatendida haciendo uso de claves privadas ubicadas en un módulo hardware de seguridad (HSM *Hardware Security Module*) propio de PSIS. Adicionalmente, la propia PSIS hace uso del módulo de creación de firmas cuando se solicita la devolución de la respuesta firmada.

4. **Emisión de sellos de tiempo**: La aplicación ofrece la posibilidad *de estampar* un sello de tiempo a un documento, proporcionando de esta manera evidencias (técnicas y jurídicas) de que el acto en cuestión se ha producido en un determinado momento del tiempo. El servicio, con el fin de proveer la fecha y hora, está sincronizado con el *Real Instituto y Observatorio de la Armada* (ROA), que es la fuente de tiempo oficinal en España.

Descripción arquitectura

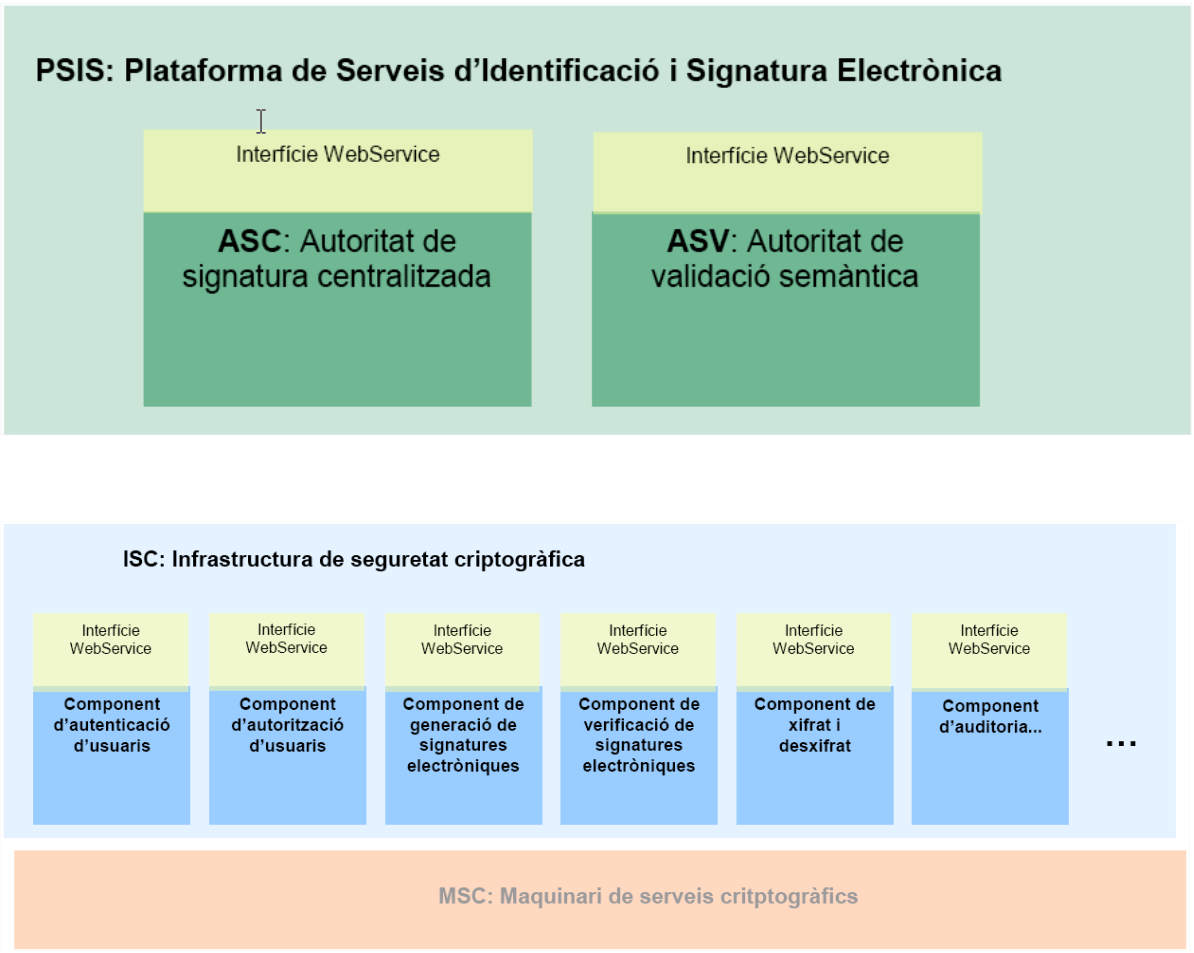
La aplicación PSIS está compuesta principalmente por dos módulos. A continuación se enumeran y más adelante se hace una explicación detallada:

• Autoridad de validación semántica (AVS)
• Autoridad de firma centralizada (ASC)

Estos módulos forman parte de un **entorno de servicios web común** que ofrece las funcionalidades recogidas en la fig. 1.
Este entorno de servicios web común está construido sobre una **infraestructura de seguridad criptográfica (ISC)** formada, entre otros, por los siguientes **componentes (agrupaciones funcionales)**:

- Componente de autenticación de usuarios
- Componente de autorización de usuarios
- Componente de gestión de claves y certificados
- Componente de generación de firmas electrónicas
- Componente de verificación de firmas electrónicas
- Componente de auditoría, registro de operaciones (*log*) y registro de consumo

- Consola única de configuración de aplicaciones y componentes.



Autoridad de Facturación Semántica

La Autoridad de Facturación Semántica (AVS) permite validar elementos de confianza, incluyendo firmas electrónicas en diversos formatos y certificados digitales X.509. Estos elementos de confianza son emitidos por diferentes proveedores de servicios de confianza que deben ser clasificados y gestionados en la plataforma de servicios de la autoridad de validación semántica.
Adicionalmente, la AVS ejecuta trabajos semánticos, localizando y extrayendo información contenida a los elementos de confianza que gestiona.
El módulo AVS registra los perfiles de elementos de confianza que emite cada proveedor de servicios de confianza.
La clasificación de cada perfil, además de asignarle un nivel de clasificación vinculado a la seguridad del certificado, permite establecer el método de validación preferido, de todos los controles establecidos por el proveedor al elemento de confianza, indicando el orden prioritario para ser validado (CRL, OCSP, métodos propietarios, @firma).

Autoridad de Firma Centralizada

La Autoridad de Firma Centralizada (ASC) permite la generación de firma electrónica asistida desde servidor. La interacción entre el usuario y el hardware de servicios criptográficos se realiza a través de la aplicación de creación de firma, mediante un canal seguro, de acuerdo con las especificaciones técnicas CEN CWA 14169 y CEN CWA 141701.

Descripción tecnológica

A continuación, se hace una descripción de las tecnologías y estándares más relevantes de las que hace uso la aplicación PSIS. El adjudicatario deberá detallar en su propuesta el conocimiento y experiencia que tiene de estas tecnologías en concreto, y otras similares si lo estima oportuno.

Lenguaje de programación

La aplicación PSIS está desarrollada, principalmente, en **J2EE** (*Java 2 Platform Enterprise Edition*), en una arquitectura distribuida en niveles y basada en componentes de software.

La aplicación está diseñada para operar en varias capas lógicas. Estas son:

- Capa web: Entorno con funciones de frontal web e interfaz de usuario.
- Capa de aplicación: Entorno con funciones de servidor de aplicaciones donde se ejecuta toda la lógica de negocio. Se hace uso del framework ***Spring***.
- Capa base de datos: las propias bases de datos de la aplicación. El acceso a la base de datos desde la aplicación se realiza por medio de ***Hibernate***.

Estos diferentes entornos o niveles tienen la capacidad de poder estar ejecutándose en la misma máquina o en hardware diferente e incluso clusterizado. Este punto depende de la arquitectura que en cada momento pueda proveer el Área de Sistemas del Consorcio AOC.

Adicionalmente, se utilizan una serie de librerías de otros fabricantes. Las más relevantes son:

- Bouncy Castle
- Apache XML Security
- iText
- Rhino

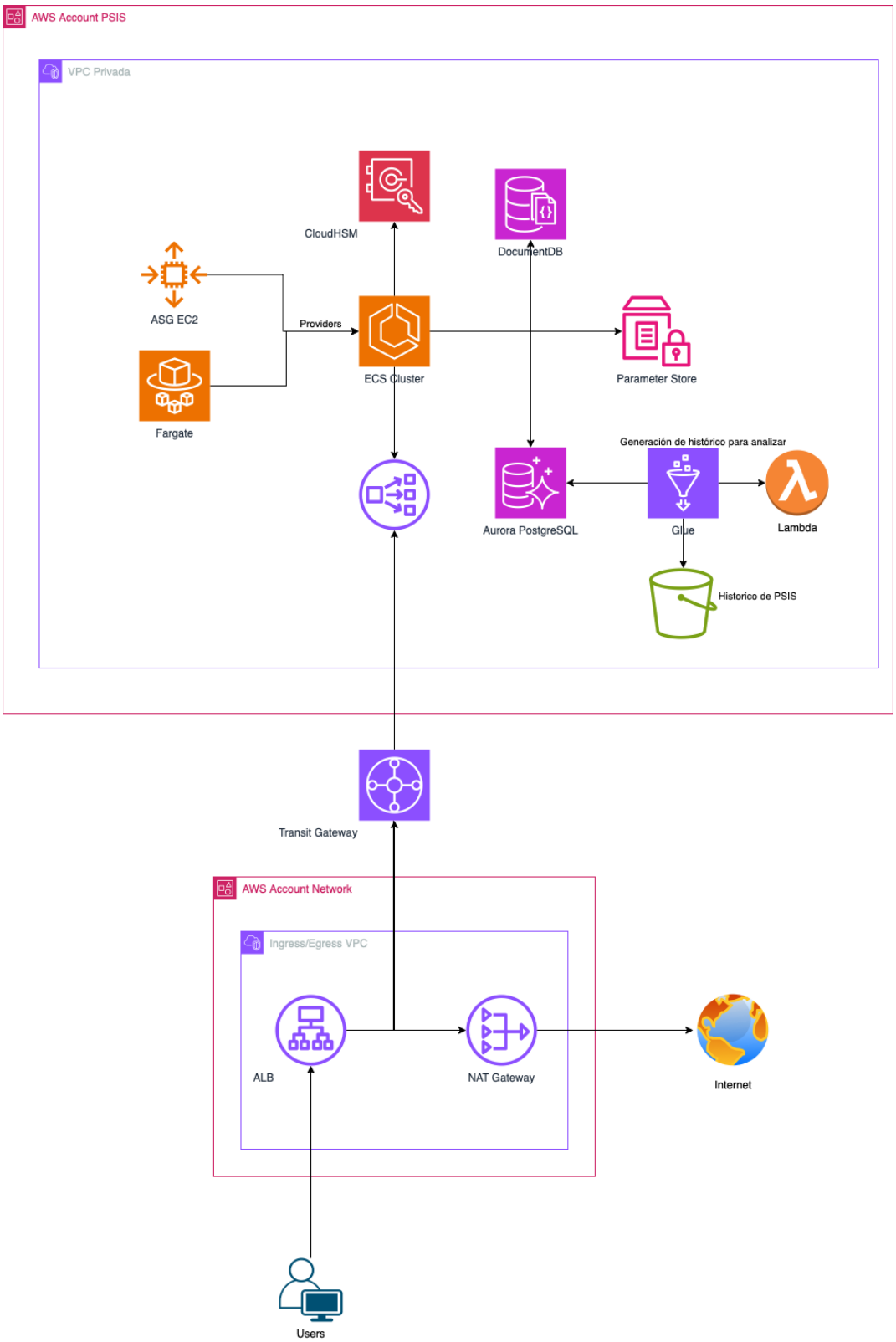
Infraestructura de software

PSIS está desplegado en la nube de Amazon Web Services (AWS). El código de PSIS es independiente de la plataforma de despliegue. Es decir, que se puede desplegar en cualquier entorno kubernetas.

Servicios AWS que se utilizan en PSIS, entre otros:

- Despliegue en ECS sobre EC2.
- Base de datos Aurora PostgreSQL Serverless.
- Base de datos DocumentDB.
- Cloud HSM.

Adjuntamos un gráfico de la infraestructura:


AWS Account PSIS
VPC Privada
CloudHSM
DocumentDB
ASG EC2
Providers
ECS Cluster
Parameter Store
Fargate
Generación de histórico para analizar
Aurora PostgreSQL
Glue
Lambda
Historico de PSIS
Transit Gateway
AWS Account Network
Ingress/Egress VPC
ALB
NAT Gateway
Internet
Users

Descripción de la mensajería: Digital Signature Services

En este apartado se hace una descripción de la mensajería que utiliza la aplicación PSIS para las comunicaciones entre servidor y cliente.

Nota: el contenido que se muestra a continuación es un extracto de la documentación (pública) que se facilita a los clientes del Consorcio AOC para hacer la integración con PSIS. El documento se llama "Guía de integradores de PSIS" y está disponible en la web del Consorcio AOC.

Para poder hacer uso de PSIS se requiere del desarrollo de unos clientes que construirán mensajes de petición y extraerán las respuestas de los mensajes provenientes del servidor abstrayente al cliente del proceso de invocación remota que se lleva a cabo.

Uno de los protocolos con los que trabaja la plataforma es el DSS (*Digital Signature Services*), del consorcio de estandarización OASIS (*Organization for the Advancement of Structured Information Standards*) un protocolo para la prestación de servicios de firma digital abierto y extensible (mediante el uso de perfiles).

El protocolo DSS Core contiene una aproximación generalista a los problemas derivados de la provisión de servicios de firma electrónica. Los perfiles de DSS son extensiones del DSS Core que aportan más detalles y funcionalidades para solucionar problemas más concretos.

De perfiles se pueden encontrar varios, pero PSIS apoya principalmente el perfil *XSS* (desarrollado por el Consorcio AOC y que amplía DSS permitiendo, entre otros, la validación de certificados X509) , el perfil *XAdES* (que permite la actualización de firmas), el *Timestamping Profile,* que aporta más control y detalles en el ámbito de los sellos de tiempo sobre DSS, y el *DSS_PDF* por la validación y completado de firmas electrónicas en documentos PDF.

Perfiles	
DSS Protocolo básico de creación y validación de firmas .	urn:oasis:names:tc:dss:1.0:core:schema
CHADES Ampliación de DSS que permite trabajar con firmas avanzadas XAdES y CAdES.	urn:oasis:names:tc:dss:1.0:profiles:XAdES
XSS Ampliación de DSS que permite, entre otros validar certificados X509 de clave púbica, extraer información de los mismos y utilizar políticas de firma .	urn:oasis:names:tc:dss:1.0:profiles:XSS
TIMESTAMP Define restricciones extras sobre la creación y validación de sellos de tiempo vía DSS.	urn:oasis:names:TC:DSS:1.0:profiles: timestamping
DSS_PDF Permite validar y completar firmas en documentos PDF.	urn:oasis:names:TC:DSS:1.0:profiles:DSS_PDF

La documentación detallada del protocolo y sus perfiles está disponible en el paquete distribuido por el Consorcio AOC.

NOTA: *Todas las descripciones de estructuras / elementos que forman parte de la mensajería DSS contienen el nombre del documento donde se puede encontrar el detalle de la descripción, junto con posibles comentarios particulares de la plataforma PSIS.*

La mensajería que interviene en la plataforma PSIS viene definida por el estándar DSS y funciona bajo el protocolo SOAP (*Simple Object Access Protocol*).

SOAP es un protocolo estándar sobre el que se fundamenta la tecnología de servicios web (*Web Services*). A diferencia de otros protocolos de tipo binario como pueden ser COM, COM+ o DCOM, los cuales son propios de Microsoft, SOAP se basa en documentos de texto plano codificados en formato XML. La ventaja principal de codificar en XML es que los mensajes son legibles por seres humanos; pero, por el contrario, estos documentos resultantes son, en general, de gran tamaño.

SOAP está diseñado para funcionar sobre cualquier protocolo de internet, aunque el uso más habitual es sobre HTTP. El hecho de utilizar HTTP minimiza el impacto de dispositivos como Firewalls y similares, y hace accesible SOAP a prácticamente cualquier tipología de comunicación cliente-servidor.

Los mensajes SOAP están compuestos por dos grandes bloques funcionales: "Cabecera" (*envelope*) destinado a suministrar datos de enrutamiento y "Cuerpo" (*body*), el cual contiene los datos del mensaje de usuario. Una explicación más detallada de SOAP no forma parte del alcance de este documento.

En este apartado se tratan los aspectos más importantes involucrados en el uso del protocolo DSS. Sin embargo, se adjunta la referencia donde se puede consultar el documento del estándar correspondiente por si fuera necesaria más información sobre el apartado concreto.

Además, se definen una serie de prefijos para los diferentes espacios de nombres involucrados. Su mapeo contra las uri's de los espacios de nombres es el siguiente:

• XD: http://www.w3.org/2000/09/XMLDsig#

• dss : urn:OASIS:names:tc:dss:1.0:core:schema

• xss : urn:OASIS:names:tc:dss:1.0:profiles:XSS

• pdf: urna:OASIS:nombres:tc:dss:1.0:profiles:DSS_PDF

Aquí mostramos los dos tipos básicos de estructuras que se utilizan en el estándar DSS, junto con los elementos básicos que se utilizarán para componer los mensajes. Los dos tipos principales de mensajes que define DSS son *VerifyRequest* (para peticiones de validación) y *SignRequest* (para peticiones de firma o estampación de sello de tiempo).

Documentación

El adjudicatario de este concurso dispondrá de toda la documentación relacionada con la aplicación que sea necesaria para la prestación del servicio objeto de este contrato.

A continuación se enumera los principales documentos:

- Guía de integradores de PSIS
- Pliego de requerimientos inicial de PSIS
- Documento análisis funcional
- Documento de arquitectura
- Diagramas secuenciales de firma
- Perfiles internacionales y del Consorcio AOC (DSS, XSS, XAdES, DSS_PDF, TimeStamping)
- Documentación sobre gestión de los perfiles de los proveedores y ficheros de configuración

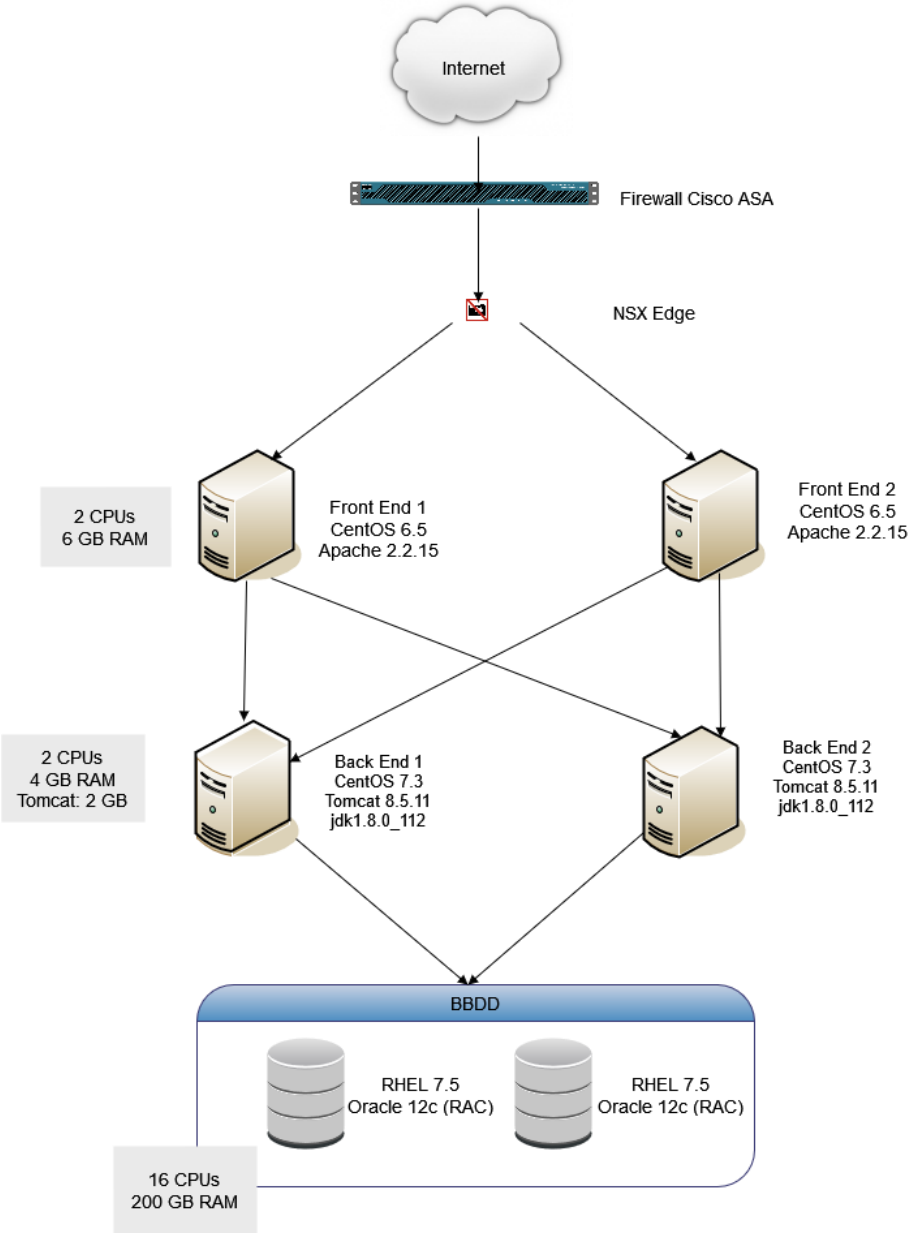
- Documentación de usuario
    - Guía de integradores
    - Guía de Firma
- Documentación de gestión y configuración de PSIS

Anexo 2 – Signador

Herramienta de firma centralizada basada en Java WebStart que dispone de una aplicación nativa que permite la ejecución de una herramienta de firma electrónica basada en certificados digitales de usuario final dentro de las aplicaciones que funcionan con un navegador web.

La documentación de integración del Signador está disponible en:
http://consorciaoc.github.io/signador/

Diagrama de infraestructura de hardware:



Anexo 3 – Requerimientos de seguridad (ENS) para los proveedores de software

Objeción al anexo

El presente anexo define los controles que debería hacer frente una empresa adjudicataria de desarrollo de software en caso de auditoría del ENS.

Requerimientos

ID 1. Política de Seguridad

Se dispone de una Política de Seguridad que incluye:

- Objetivos de la organización.
- Marco legal y regulador.
- Roles relacionados con la seguridad, así como sus responsabilidades y procedimiento de designación.
- Estructura del comité de gestión y coordinación de seguridad.
- Criterio para la clasificación de la documentación.
- Referencia a la legislación aplicable en materia de tratamientos de datos de carácter personal.
- La Política de Seguridad debe ser un documento en papel o soporte electrónico.
- La Política de Seguridad incluye la especificación del plazo y condiciones de su revisión y que debe estar aprobada por un órgano superior.
- La Política de Seguridad incluye un apartado específico de gestión de los usuarios y sus privilegios, así como la persona responsable.
- La Política de Seguridad incluye un apartado específico indicando los responsables de la información gestionada por el sistema.

ID 3. Procedimiento de revisión de la Política de Seguridad

Documento conteniendo el Procedimiento de revisión y aprobación de la Política de Seguridad o en su defecto, apartado de la Política de Seguridad donde se especifique el periodo de revisión y aprobación.

ID 4. Evidencia de la difusión de la Política de Seguridad

Evidencia de que la Política de Seguridad es accesible para el personal afectado en la Ctra, página web, portal, repositorio o ha sido distribuida a todos los usuarios de los que son responsables mediante el correo electrónico.

ID 10. Evidencia de la difusión de la Normativa de Seguridad

Evidencia que la Normativa de Seguridad - ya sea propia o se emplee el Marco Normativo de la Agencia de Ciberseguridad de Cataluña - está disponible en la Ctra, página web, portal, repositorio, librería o en cualquier otro medio accesible para todos los usuarios implicados o bien que les ha sido distribuida a través del correo electrónico.

ID 11. Procedimientos de Seguridad

Se dispone de Procedimientos de Seguridad para la realización de las tareas rutinarias.

Estos deben incluir como mínimo:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.

ID 13. Evidencia de la difusión de los Procedimientos de Seguridad o de la posibilidad de acceso por parte de los usuarios

Evidencia de que los Procedimientos de Seguridad - sean propios o se empleen los del Marco Normativo de la Agencia de Ciberseguridad de Cataluña - están disponibles en la Ctra, página web, portal, repositorio, librería o en cualquier otro medio accesible para todos los usuarios implicados.

ID 40. Documento de Identificación del Control de Acceso al sistema

Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que indique:

- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios.
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir.
- El período de retención de los usuarios.

ID 43. Procedimiento de Autenticación del Sistema

Se dispone de un procedimiento debidamente aprobado y actualizado donde se describen los mecanismos de autenticación de los usuarios o se especifica dentro del procedimiento formalizado de gestión de usuarios los siguientes puntos:

- Se detalla los sistemas de autenticación de los usuarios con la obligación de tener al menos un factor de autenticación.
- Se detalla y se obtiene la evidencia de que el usuario confirma la recepción del identificador, conoce y acepta las obligaciones.
- Se explica cómo gestionar las bajas de usuarios y el vínculo con RRHH que permita avisar a los responsables de gestión de usuarios del cambio en las relaciones con los mismos.

- Se indica que se utilicen al menos dos factores de autenticación en los sistemas categorizados como nivel medio y alto.
- En el caso de que se utilicen tokens, que estos utilizan un algoritmo autorizado por el CCN, por ejemplo AES.

ID 46. Documento de Requerimientos de Acceso al sistema

Se dispone de un procedimiento formalizado de gestión de usuarios debidamente aprobado y actualizado que indique:

- Cómo se realiza la gestión de los usuarios y de sus privilegios así como la persona responsable de la gestión de los usuarios.
- Que los identificadores de los usuarios deben ser nominales y no se pueden compartir.
- El período de retención de los usuarios.

ID 50. Herramienta corporativa específica para la gestión de los usuarios propios

Se dispone de una herramienta corporativa específica para la gestión de los usuarios.

ID 54. Procedimiento de Gestión de Derechos de Acceso al Sistema

Se dispone de un procedimiento donde se incluyen, dentro del procedimiento formalizado de usuarios del sistema, los siguientes puntos:

- Se asignará el rol adecuado a cada usuario con los mínimos privilegios posibles y revisándose los mismos periódicamente.
- Se incluirá la relación entre los permisos que debe tener cada usuario en función de su rol.
- Se especificará cuáles son los responsables de los recursos de los sistemas (físicos y lógicos) y quién tiene la responsabilidad delegada de conceder, alterar o anular el acceso a los mismos.

ID 62 Evidencia de que el usuario confirma la recepción del identificador, conoce y acepta las obligaciones

Se dispone de la evidencia que demuestra que los nuevos usuarios confirman la recepción del identificador, conocen y aceptan las obligaciones. Esta evidencia puede tomar diversas formas:

- Evidencia de que al crear su identificador se informa al usuario por correo electrónico, y al acceder por primera vez debe aceptar los derechos y deberes de acceso al aplicativo.
- Que el personal de un proveedor firme un documento de obligaciones el primer día, así como un acuerdo de confidencialidad y quede constancia de la entrega del identificador.

- Que en la parte inferior de la pantalla de acceso se indiquen los términos y condiciones, por lo que los usuarios están implícitamente aceptándolas para acceder al sistema.

ID 63. Acuerdo de confidencialidad donde se hace constar la entrega del identificador

Se dispone del documento conteniendo el Acuerdo de Confidencialidad firmado por el usuario haciendo constar la recepción de su identificador. Debe existir un registro de cada usuario confirmando la recepción del identificador.

ID 64. Evidencia del último usuario propio dado de baja

Se dispone de la evidencia mostrando la baja de un usuario con la fecha efectiva de la baja.

ID 67. Procedimiento de Acceso en Local

Se dispone de un Procedimiento de Acceso en Local que especifique que:

- Los sistemas antes de entrar en explotación o los ya existentes han sido configurados de forma que no revelen información del sistema antes de un acceso autorizado.
- Los diálogos de acceso (en el lugar de trabajo, dentro de las propias instalaciones de la organización, en el servidor, en el dominio de red, etc.) no revelen información sobre el sistema al que se está accediendo.
- Haga constar que se debe informar siempre a los usuarios de sus obligaciones una vez han accedido al sistema.
- Se debe informar al usuario de su último acceso al sistema.
- Define unos horarios en los que es posible la conexión al sistema y otros en los que no lo es.
- No se puede acceder al sistema fuera de las horas autorizadas.
- Indique puntos de renovación de autenticación durante la sesión de un usuario.

ID 107. Evidencia qué se dispone de antivirus en los sistemas de información

Se dispone de la evidencia del uso de mecanismos de prevención ante código perjudicial (antivirus) para todos los equipos (Servidores y puestos de trabajo) del sistema y también en las maquetas, así como de su configuración.

ID 111. Evidencia de que el programa antivirus se encuentra actualizado

Se dispone de la evidencia de que las opciones de configuración aplicadas a los antivirus son las recomendadas por los fabricantes (p.ej. Análisis de ejecución de programas, análisis de correo entrante y saliente, bloqueo automático de código nocivo, etc.), así como las referentes a la frecuencia de actualización.

ID 172. Evidencias de la difusión del contenido del Plan de Concienciación

Se dispone de evidencia de la difusión del contenido del plan de concienciación (en la intranet o por algún otro medio se lanzan mensajes de concienciación (p. ej. correos, comunicados internos,...)).

ID 174. Evidencias de la difusión del contenido del Plan de Formación

Se dispone de evidencia con la difusión del contenido del plan de formación en los últimos 3 años.

ID 241. Documento donde se indica el mecanismo de autenticación e identificación

Se dispone de una política o normativa documentada respecto al diseño de un sistema que contemple los mecanismos de identificación y autenticación y además contempla los mecanismos de protección de la información tratada.

Asimismo no debe ser posible acceder a información del sistema que pueda ser utilizada para la escalada de privilegios, ni ejecutar acciones haciéndose pasar por otro usuario, etc.

ID 244. Procedimiento para la elaboración y ejecución del plan de pruebas de la aplicación

Se dispone de un procedimiento de Aceptación y Puesta en Servicio de Protección de las Aplicaciones Informáticas. Antes de pasar a producción se debe comprobar el funcionamiento correcto de la aplicación. Se debe comprobar que:

- Se cumplen los criterios de aceptación en materia de seguridad.
- No se deteriora la seguridad de otros componentes del servicio.
- Las pruebas deben realizarse en un entorno aislado (preproducción).
- Las pruebas de aceptación no deben hacerse con datos reales, salvo que se asegure el nivel de seguridad correspondiente.
- Se realizan análisis de vulnerabilidades.
- Se realizan análisis de coherencia y código fuente.

ID 273. Procedimiento de configuración segura del correo

Se dispone de un procedimiento el cual se detalla cómo se configura el correo con el fin de disponer de un sistema seguro.

ID 276. Evidencia de la herramienta monitorización de los elementos de seguridad

Se dispone de la evidencia en la que se observa que se dispone de una herramienta para monitorizar los elementos de seguridad como los virus o el spam debidamente configurado y mantenido.

ID 330. Normativa documentada que especifica los deberes y obligaciones del personal contratado a través de un tercero

Se dispone de normativa donde se especifican los deberes y obligaciones del personal contratado a través de un tercero.

ID 460. Protocolo de actuación hacia el incumplimiento de las obligaciones por parte del personal tercero

Se dispone de un procedimiento que define la resolución de incidentes relacionados con el incumplimiento de las obligaciones por parte del personal del tercero, además de identificar a la persona de contacto con el tercero para la resolución de este tipo de incidentes.