Administració Oberta de Catalunya

PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS PER A LA REALITZACIÓ DE LES TASQUES DE DESENVOLUPAMENT EVOLUTIU, MANTENIMENT CORRECTIU I SUPORT DE TERCER NIVELL DELS APLICATIUS PSIS i SIGNADOR

Número d'expedient: AOC-2025-07

Generalitat de Catalunya

Localret

Índex

1. Introducció

El Consorci AOC ofereix a les administracions públiques catalanes el servei de validació i segellat de temps. PSIS és la plataforma tecnològica des d'on es presten aquests serveis. El servei de validació comprèn principalment la validació de certificats i la validació i completat o preservació de signatures electròniques i documents signats. PSIS també permet la creació i validació de segells de temps, i la creació de signatures digitals de forma segura i desatesa.

El servei de validació (PSIS) és consumit per tots els ens que formen part de l'administració pública catalana que disposen d'aplicacions informàtiques on es fa ús de certificats digitals i signatura digital, per tal de dotar de seguretat els processos d'identificació i tractament de documents signats.

PSIS és un servei transversal que es consumeix pràcticament per tots els altres serveis del Consorci AOC, així com per la resta dels ens de l'administració pública catalana. Degut a aquesta transversalitat, és el servei amb el consum més alt: l'any 2023 PSIS va processar 340 milions d'operacions.

El Signador és una eina de generació de signatures electròniques basades en certificats digitals. Les administracions públiques catalanes l'integren en les seves pàgines web com a eina de signatura digital, a fer ús tant per part dels empleats públics, com càrrecs electes, i ciutadans, quan aquests han de signar un document administratiu o tràmit.

El Signador permet signar amb certificats en local en possessió del signatari (certificat en dispositiu criptogràfic o en programari). Però també ofereix la funcionalitat de signatura remota mitjançant la integració amb el servei del Signador Centralitzat del Consorci AOC.

L'any 2023 es van generar més de 54 milions de signatures electròniques amb el Signador.

2. Objecte de la licitació

L'objecte d'aquesta contractació és la prestació dels serveis de desenvolupament evolutiu, manteniment correctiu i suport de tercer nivell dels aplicatius PSIS i Signador, basats ambdós en tecnologia Java.

S'inclou dins l'abast de la licitació totes les tasques necessàries relatives al cicle de vida complet de les aplicacions, com són l'anàlisi, el disseny tècnic, el desenvolupament, i el control de qualitat (incloent tests unitaris, tests d'integració, així com proves de rendiment). Totes aquestes tasques s'hauran de dur a terme d'acord a la metodologia de treball que es descriu a l'apartat 4.

Els principals objectius del projecte són, tant per a PSIS com pel Signador:

- Realització de tasques de desenvolupament evolutiu sobre l'arquitectura actual de cadascun dels aplicatius, en tecnologia JAVA i desplegats en AWS. Aquestes tasques

estaran enfocades tant en la implementació de noves funcionalitats com en la millora del rendiment.

- Realització del manteniment correctiu.
- Oferir suport tècnic especialitzat pel que fa a la detecció, diagnòstic i resolució d'incidències tècniques.

La durada del contracte serà des de la data de formalització del contracte (no abans de l'1 de gener de 2025) fins el 31 de desembre de 2025.

2.1. Desenvolupament evolutiu

Desenvolupament de noves funcionalitats o millores segons el següent procediment (micro-projecte):

- El Consorci AOC proporcionarà la informació funcional i tècnica necessària per tal que l'adjudicatari pugui fer l'anàlisi de la solució a implementar. Aquesta valoració es realitzarà en un temps inferior a 10 dies laborables. La proposta haurà de detallar:
    - Temps previst d'execució
    - Esforç per perfil
- L'adjudicatari realitzarà l'anàlisi detallat i el disseny tècnic de la solució i el Consorci AOC els haurà de validar.
- Un cop aprovada la proposta per part del Consorci AOC i fixat el calendari d'execució, l'empresa adjudicatària assumirà el desenvolupament complet de la solució i la codificació del mateix d'acord a la metodologia que es descriu a l'apartat 4. Les desviacions sobre el mateix, no imputables a canvis en la definició, podran ser imputades a l'empresa adjudicatària, a criteri del Consorci AOC, en funció de la gravetat i l'impacte.
- Gestió i control del codi font. Aquesta gestió es durà a terme amb el sistema centralitzat de codi font de que disposa el Consorci AOC (basat en el sistema de control de versions Git).
- L'adjudicatari serà el responsable de la definició del pla de proves, d'integració i de rendiment, si s'escau, i de la seva execució a l'entorn de desenvolupament. En relació a les proves de rendiment, el responsable de l'execució d'aquestes a l'entorn de preproducció serà el Consorci AOC, amb la participació de l'adjudicatari. L'adjudicatari serà el responsable del control de qualitat i de validar el bon funcionament dels evolutius, tant a nivell funcional com tècnic.
- L'adjudicatari haurà de preparar els paquets de desplegament pels entorns de preproducció i producció, d'acord al procediment de desplegament definit pel Consorci AOC.
- L'adjudicatari haurà d'elaborar la documentació tècnica i els manuals d'usuaris corresponents, així com mantenir actualitzada la documentació existent.

- L'adjudicatari haurà de prestar la formació als usuaris que determini el Consorci AOC quan aquest ho consideri necessari.

Els evolutius a implementar podran respondre a diferents necessitats:

- Evolutius funcionals: Modificació de funcionalitats existents o incorporació de noves.
- Evolutius de caràcter legal i/o normatiu: Relacionats amb el compliment de la normativa vigent (p. ex. Reglament General de Protecció de Dades, Esquema Nacional de Seguretat, etc.).
- Evolutius de caire tècnic: Relacionats amb necessitats de caràcter tecnològic (millores en l'arquitectura base, actualització del programari base i/o de llibreries de tercers, millores de rendiment en determinades funcionalitats, etc.).
- Evolutius de seguretat: El seu propòsit és millorar el nivell de seguretat del servei en aspectes com poden ser les polítiques de control d'accés i els mètodes d'autenticació, les polítiques de xifrat de dades en repòs i en trànsit, el pla de continuïtat i la recuperació de dades, el procediment de gestió de pegats de seguretat i actualitzacions, el procediment de gestió d'incidents de seguretat, etc.

És molt important destacar que l'adjudicatari haurà de tenir un paper especialment proactiu amb els evolutius tant amb els de caràcter tècnic com de caràcter legal o normatiu, proposant al Consorci AOC totes aquelles millores que ajudin al compliment de la normativa vigent, a millorar el rendiment del servei o a enfortir la seguretat. L'adjudicatari per tant haurà de presentar recurrentment, i de forma proactiva, al Consorci AOC, totes aquelles propostes de millora que consideri adients amb el corresponent anàlisis i estimació de costos, i serà decisió unilateral del Consorci AOC decidir quines d'aquestes propostes finalment s'acaben acceptant i executant (d'acord al mateix format de micro-projecte com qualsevol altre evolutiu que hagués proposat el propi Consorci AOC).

Per a cadascun d'aquests micro-projectes l'adjudicatari haurà de proporcionar els següents lliurables:

- Disseny funcional
- Disseny tècnic
- Plans de proves unitàries i d'integració
- Manual d'explotació
- Documentació per al CAU

2.1.1. Evolutius previstos

A continuació s'exposen evolutius previstos a realitzar durant el 2025. No seran exclusius, i en funció de les necessitats del servei es duran a terme aquests i/o caldrà desenvolupar-ne de nous.

PSIS

1. Implementació dels **nous estàndards de signatura electrònica del reglament europeu eIDAS (*electronic IDentification, Authentication and trust Services*)**:
    a. *XAdES (XML Advanced Electronic Signatures) Baseline Profile*
    ETSI EN 319 132 XML Advanced Electronic Signatures (XAdES)
        - Part 1*: Building blocks and XAdES baseline signatures*
        - Part 2*: Extended XAdES signatures*

    b. *CAdES (CMS Advanced Electronic Signature) Baseline Profile*
    - ***ETSI EN 319 122 CMS Advanced Electronic Signatures (CAdES)***
        - Part 1*: Building blocks and CAdES baseline signatures*
        - Part 2*: Extended CAdES signatures*

    c. *PAdES (PDF Advanced Electronic Signature) Baseline Profile*
    ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)
        - Part 1*: Building blocks and PAdES baseline signatures*
        - Part 2*: Additional PAdES signatures profil·les*

2. Implementació de **l'estàndard de signatura electrònica JAdES (*JSON for Advanced Electronic Signatures*)**
    a. *JSON Web Signature (JWS)*
        - RFC7515

    b. *JAdES (JSON for Advanced Electronic Singatures) Baseline Profile*
    ETSI TS 119 182-1 JAdES digital signatures
        - Part 1: *Building blocks and JAdES baseline signatures*

3. Integració de PSIS amb una **autoritat de segellat de temps reconeguda**. Està previst substituir la TSA de PSIS per una TSA qualificada, és a dir, que acompleixi amb els requeriments del reglament eIDAS. Caldrà integrar PSIS amb la TSA qualificada per dur a terme les funcions de completat de signatures.

Signador

1. Integració del Signador amb la nova solució del Consorci AOC per **signatura remota**. Actualment el Signador està integrat amb el Signador Centralitzat del Consorci AOC. Però aquesta solució de signatura remota serà substituïda per una de nova i caldrà substituir la integració actual per la integració amb la nova solució.
2. Integració del Signador amb una **autoritat de segellat de temps reconeguda**. Caldrà integrar el Signador amb la TSA qualificada per afegir segells de temps a les signatures generades.

2.2. Manteniment correctiu

- S'entén per manteniment correctiu la resolució d'incidències de caràcter funcional i/o tècnic que impedeixin el normal funcionament del servei. S'inclouen tant incidències a nivell funcional, com de rendiment.
- Les tasques de manteniment correctiu que el Consorci AOC determini que cal implementar amb caràcter urgent, es prioritzaran per davant de les feines de manteniment evolutiu que s'estiguin realitzant en el moment de la incidència. Aquestes tasques es sotmetran al control de l'Acord Nivell de Servei derivat de la categoria de la incidència que ha originat el correctiu, i les penalitzacions associades es tractaran seguint aquests criteris.
- Els informes de seguiment setmanal hauran de reflectir aquests correctius realitzats, i els Nivells de Servei aconseguits per a cadascun d'ells. Es contemplarà finalitzat el correctiu quan les proves a l'entorn de preproducció determinin la validesa del mateix. L'equip responsable de realitzar el correctiu, haurà de realitzar la documentació necessària per a la pujada a l'entorn de preproducció i la seva corresponent validació.

2.3. Gestió del canvi de configuració

El servei de gestió de canvi de configuracions consisteix en realitzar totes aquelles tasques necessàries per tal que l'aplicació PSIS incorpori els canvis de configuracions sol·licitats pel Consorci AOC.

Els tipus de canvis de configuracions poden ser diversos, però com a mínim, el servei haurà de cobrir les següents sol·licituds:

- Càrrega de noves entitats de certificació (CA's).
- Càrrega / Renovació de certificats d'entitats de resposta OCSP.
- Càrrega de nous perfils de certificats (que hauran estat emesos per una entitat de certificació carregada a PSIS).
- Canvis en el parseig dels perfils de certificats per obtenir els diferents atributs dels certificats en funció del seu perfil (política de certificat).
- Càrrega de polítiques de signatura.
- Configuració per carregar noves claus dintre de l'aplicació PSIS per poder signar de manera centralitzada (funcionalitat ASC).
- Configuració de permisos d'autoritzacions d'ús d'una clau (privada) carregada a PSIS per part d'una altra clau (pública).

2.4. Suport de tercer nivell

El servei de suport avançat consisteix en realitzar totes aquelles tasques necessàries per tal de donar resposta a totes aquelles consultes que plantegi el Consorci AOC . Els tipus de consultes poden ser diverses:

- Consultes relacionades amb qualsevol funcionalitat del servei.
- Consultes relacionades amb el disseny de qualsevol del mòduls de l'aplicació.
- Consultes relacionades amb la manera com es fa servir de qualsevol de les funcionalitats de l'aplicació.
- Consultes relacionades amb respostes que el Consorci AOC consideri inesperades del servei.
- Consultes relacionades amb els missatges d'error obtinguts del servei.
- Consultes relacionades amb la configuració vigent del servei.
- Consultes relacionades amb els estàndards i normatives en els que es basa el servei.

2.5. Control de qualitat

L'adjudicatari serà el responsable del control de qualitat del servei en tots aquells desenvolupaments de nous evolutius i correctius que realitzi. En particular hauran de dur a terme les següents tasques:

- Definició dels indicadors i mètriques de qualitat que han de complir els evolutius/correctius i identificar les mesures que s'utilitzaran per avaluar la qualitat.
- Creació d'un model de gestió de la qualitat que asseguri i garanteixi els acords de nivell de servei (ANS) definits.
- Control de qualitat dels evolutius. Validació del funcionament correcte d'aquests tant a nivell funcional com tècnic. Execució de proves unitàries i d'integració. Execució de proves funcionals i de regressió. Execució de proves de rendiment, si s'escau.
- Suport als equips de desenvolupament mitjançant la definició dels estàndards i directrius que han de complir tots els evolutius per a ser certificats.
- Revisió i auditoria del compliment d'aquests estàndards/directrius per assegurar que se segueixen els procediments establerts.
- Revisió i seguiment de la qualitat de la documentació generada pels equips de desenvolupament
- Comunicació i formació als usuaris que determini el Consorci AOC.

Totes aquestes activitats estaran dirigides pel Consorci AOC i hauran d'estar coordinades pel Responsable del Servei assignat per l'adjudicatari. Serà responsabilitat de l'adjudicatari vetllar

i preocupar-se de recaptar tots i cadascun dels requeriments que afectin a la sol·licitud dels evolutius i correctius.

2.6. Estàndards de signatura electrònica

Es valorarà també positivament l'acreditació de coneixement i/o experiència en l'àmbit de la signatura electrònica, així com en els estàndards de signatura electrònica i de les llibreries java que els implementen.

Estàndards de signatura electrònica:

- Protocol DSS d'OASIS
- Estàndards de signatura XAdES, CAdES, i PAdES
- Estàndards eIDAS de signatura
- Protocol RFC3161
- Electronic Signature Policies
- Public Key Infrastructure
- Etc.

Llibreries java:

- BouncyCastle
- Apache XML Security

3. Equip de treball

Per garantir la màxima eficiència, control i coordinació del servei objecte d'aquest contracte, l'empresa adjudicatària haurà de disposar en el moment d'iniciar el contracte d'un equip amb un ampli coneixement tecnològic dels serveis a gestionar i amb una forta experiència en tasques similars a les descrites en aquest plec.

L'empresa adjudicatària haurà de conformar l'equip de treball necessari en el moment d'iniciar el contracte. El proveïdor podrà proposar uns perfils i rols de personal superiors als descrits a continuació per garantir l'execució satisfactòria de l'abast d'aquest contracte, però en cap cas podrà presentar uns perfils inferiors als mínims exigits als criteris d'adscripció de mitjans materials i/o personals a l'execució del contracte indicats a l'apartat ***G4.*** del Quadre de Característiques. El Consorci AOC considera necessària la participació mínima dels següents perfils i rols:

Cap de projectes

Funcions:

- Seguiment detallat del pla derivat del contracte, i interlocució amb el Consorci AOC per temes derivats de l'execució del contracte.
- Direcció del servei i coordinació dels recursos assignats al servei, tant materials com personals.

Requeriments:

- Titulació: Enginyeria tècnica o titulació superior.
- Experiència mínima de 5 anys en funcions de gestió d'equips responsables del desenvolupament, testeig, manteniment correctiu i evolutiu d'aplicacions Java, i en especial d'aplicacions crítiques en entorns productius.
- Experiència mínima de 5 anys liderant equips de com a mínim 4 integrants.
- Experiència mínima de 3 anys en gestió de projectes d'aplicacions java al núvol AWS i integració amb serveis AWS.
- Experiència mínima de 3 anys en gestió de projectes amb contenidors.

Enginyer de Software (dedicació 100%)

Funcions:

- Fer el recull dels requeriments dels nous evolutius i correctius a desenvolupar, i assegurar-se que són complets, correctes i consistents des del punt de vista funcional.
- Establir les planificacions dels diferents evolutius i correctius encomanats a l'adjudicatari, vetllant per a que cadascuna d'aquestes tasques es realitzin de forma diligent i dins la planificació acordada. Informar al Consorci AOC de les desviacions tan bon punt es detectin.
- Generar la documentació associada al servei (anàlisis funcional, manuals d'usuari, informes de seguiment, etc.).
- Supervisió de la feina de la resta de persones de l'equip amb l'objectiu de maximitzar la qualitat dels lliurables.
- Proporcionar formació i suport a la resta de membres de l'equip i també al personal del Consorci AOC que aquest determini. Proporcionar mentoria i orientació a la resta de desenvolupadors de l'equip en qüestions d'arquitectura i disseny.
- Confecció del disseny tècnic i de la documentació de l'arquitectura lligada a cada evolutiu i correctiu.

- Prendre les decisions de disseny/arquitectura relatives a cada evolutiu escollint les tecnologies, plataformes i els patrons de disseny a utilitzar.
- Avaluar noves tecnologies i determinar si són adients per a la seva inclusió al projecte.
- Liderar la fase de construcció dels canvis a realitzar: entre altres, dissenyar les classes, interfícies i el codi necessari per al desenvolupament de l'aplicació atenent als criteris fixats per cada desenvolupament.
- Revisió del codi de la resta de desenvolupadors de l'equip per garantir la qualitat i la coherència del codi.
- En els casos d'incidències complexes haurà participar activament en la seva diagnosis i resolució.
- Codificació, depuració i manteniment del codi font dels evolutius i correctius.
- Implementació de les proves unitàries, d'integració i de rendiment per garantir que els evolutius i correctius funcionen correctament.
- Creació de la documentació tècnica dels evolutius/correctius.
- Preparació dels paquets de desplegament per als diferents entorns de desenvolupament, preproducció i producció.

Requeriments:

- Titulació: Enginyeria tècnica o titulació superior.
- Experiència mínima de 5 anys com a responsable tecnològic d'aplicacions Java/J2EE i bases de dades relacionals SQL.
- Experiència mínima de 5 anys en les següents tecnologies:
  - Integració de serveis web (Webservices, SOAP, WSDL, REST, etc.)
  - Hibernate, Spring IoC
  - PostgreSQL
  - MongoDB
  - XSD, XML
  - Docker
  - Contenidors (Kubernetes)
- Experiència mínima de 3 anys en aplicacions java desplegades al núvol AWS i integració amb serveis AWS.
- Experiència mínima de 3 anys en les següents eines de gestió i construcció de projectes:

- Git, Eclipse, Maven, Gradle
  - Jenkins
- Experiència mínima de 3 anys en les següents eines de testeig:
  - SoapUI, JMeter

3 Desenvolupadors Java/J2EE (mínim dos d'ells amb dedicació completa 100%)

Funcions:

- Codificació, depuració i manteniment del codi font dels evolutius i correctius.
- Execució exhaustiva del pla de proves definit per als evolutius/correctius.
- Col·laborar en l'elaboració de documentació tècnica relativa als evolutius/correctius.

Requeriments:

- Titulació: Formació professional, enginyeria tècnica o titulació superior.
- Experiència mínima de 3 anys en:
  - Tecnologia Java i J2EE
  - Web Services
  - Hibernate, Spring IoC
  - PostgreSQL
  - MongoDB
  - XSD, XML
- Experiència mínima de 3 anys en:
  - Eclipse, Git, Maven, Gradle
  - SoapUI, JMeter
- Experiència en aplicacions java desplegades al núvol AWS i integració amb serveis AWS (AWS Lambda, SQS, Aurora, DocumentDB, S3, ...).

Enginyer Kubernetes i DevOps (dedicació puntual)

Funcions:

- Creació, execució i distribució de contenidors docker.
- Optimització de les imatges docker minimitzant el tamany i optimitzant les capes.
- Compilació i execució d'imatges docker en registres.
- Garantir la qualitat i la confiabilitat de les actualitzacions de programari.

- Col·laborar en l'elaboració de documentació tècnica relativa a les tasques encomanades.
- Col·laborar en l'automatització dels processos de desplegament al cloud.

Requeriments:

- Titulació: Enginyeria tècnica o titulació superior.
- Experiència mínima de 3 anys en Kubernetes.
- Experiència mínima de 3 anys com a enginyer DevOps.
- Experiència en CI/CD, IaC, CM, SAST, DAST, OWASP.
- Experiència en Jenkins.

La dedicació de l'enginyer de software i de 2 dels desenvolupadors ha de ser del 100%. Les hores necessàries per dur a terme el servei s'estimen en 7.210 hores, que s'hauran d'executar en la seva totalitat en el període de durada del contracte. L'empresa adjudicatària, en funció de la durada del contracte, i del volum d'hores previst per realitzar els projectes, haurà de dimensionar adequadament l'equip de treball per donar resposta als requeriments valorats, en temps i forma. És a dir, la disponibilitat de les hores executades pot, puntualment, no ser proporcional a la durada del contracte, sinó que s'haurà d'adaptar a les necessitats i requeriments del servei, podent fluctuar en funció de la càrrega de les tasques encomanades, havent mesos en què es pugui requerir un major o menor dimensionament de l'equip de treball.

El Consorci AOC es reserva el dret de demanar el canvi de qualsevol dels membres de l'equip sense haver de justificar-ho, amb una antelació de 20 dies naturals a la data de la substitució.

En cas de baixa de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC. En aquests casos, es fixarà un temps de 2 setmanes de formació/adaptació del nou membre que anirà a càrrec de l'adjudicatari.

Caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs.

L'adjudicatari pot presentar perfils superiors als mínims exigits, però mai inferiors.

4. Metodologia

Les tasques a realitzar contemplades s'engloben dins el manteniment evolutiu i correctiu de les aplicacions PSIS i Signador del Consorci AOC durant la fase continua del seu cicle de vida. Ambdós aplicatius tenen un alt grau de maduresa i s'encabeixen dins el conjunt de serveis que ofereix el Consorci AOC. PSIS està en producció des de l'any 2007 i el Signador des del 2017.

Cal tenir en compte que aquests serveis presenten una certa complexitat en la seva gestió degut als següents motius:

- La direcció estratègica de cada servei està liderada per un Cap de Servei amb uns objectius i terminis concrets, que ocasionalment poden presentar interdependència amb altres serveis.
- Alta dependència amb tercers (p. ex. organismes externs a l'AOC que poden impactar tant en l'abast funcional com amb els terminis d'execució previstos inicialment).

Cadascuna de les versions a desenvolupar es considerarà com un projecte propi que s'haurà de desenvolupar seguint el compliment d'aquesta guia metodològica.

A continuació es detallen les fases per les que ha de passar cadascuna de les noves versions d'un determinat servei, des de la seva definició fins a la seva posada en marxa.

Introducció de les tasques a JIRA

El Cap de Servei tradueix els objectius estratègics que marca el comitè estratègic en les peticions de millora i evolutius que han de permetre assolir aquests objectius. A continuació els introdueix com a tasca de Serveis a l'eina JIRA. En el moment d'entrar cada tasca (en forma de tiquet) indica la seva prioritat.

Fase de definició

La fase de definició de la versió consisteix en seleccionar quins són els requeriments funcionals que han d'entrar a formar part de la propera versió a desenvolupar.

El Cap de Projectes (Subdirecció d'Operacions) estudia tots aquells requeriments que es poden incloure dins una finestra tipus que el Consorci aplica als seus serveis (per serveis grans, versions cada 3 mesos aproximadament entre la posada en marxa de cada versió, tot i que depenent de les necessitats, la finestra es pot reduir o ampliar).

El Cap de Projectes consensua amb el Cap de Servei l'abast de la versió i es confecciona la llista definitiva de tasques traslladant aquesta llista de peticions en tasques de Projectes JIRA que representa la versió a desenvolupar.

En cas que s'escaigui, és el Cap de Servei qui defineix el pla de comunicació que s'haurà de dur a terme abans de que la versió arribi als usuaris finals, i dins aquest pla seleccionarà els usuaris i organismes que hauran de participar a la prova pilot, si s'estima oportú.

El Cap de Projectes introdueix tota aquesta informació en els tiquets JIRA que conformen la versió. Un cop tancat l'abast de la versió, no s'acceptarà cap modificació en la llista de funcionalitats a desenvolupar fins a la propera fase de definició de la nova versió.

Anàlisi

L'adjudicatari partirà del recull de funcionalitats a satisfer que s'han seleccionat al JIRA per a la nova versió i haurà de realitzar les reunions de presa de requeriments per poder fer la recaptació detallada de tots els requisits tant funcionals com tecnològics demanats. Serà responsabilitat de l'adjudicatari vetllar i preocupar-se de recaptar tots i cadascun dels requeriments que afectin a l'abast d'una determinada versió.

L'adjudicatari elaborarà un anàlisi previ de la solució que proposa incloent una estimació de l'impacte que suposa l'evolutiu. En cas que hi hagi diferents alternatives, l'adjudicatari haurà d'explicar-les indicant els avantatges i inconvenients de cadascuna.

Planificació

El Cap de Projectes afegirà al JIRA les tasques tècniques que considera necessàries per poder desenvolupar la versió (documentació tècnica, pla de proves, etc.) i prepara conjuntament amb l'adjudicatari la planificació detallada de la versió assignant les tasques entre els diferents tècnics de desenvolupament.

Desenvolupament de tasques planificades

Les tasques que comportarà aquesta fase són:

- Generació del codi.
- Execució de proves unitàries.
- Execució de proves d'integració.
- Execució de proves de rendiment, si s'escau.
- Elaboració de la documentació funcional i tècnica.

L'adjudicatari haurà de fer un ús freqüent de l'eina de control de versions de codi (Github) del servei per sincronitzar els diferents desenvolupaments. La freqüència ideal de sincronització (tant per pujar al repositori els canvis realitzats com per descarregar tots els canvis que han introduït la resta de desenvolupadors) seria fer-ho un cop al dia (p. ex. a primera hora del matí) de forma que es detecti quan abans millor els conflictes entre els diferents desenvolupaments.

Abans de pujar res al repositori cada desenvolupador haurà de garantir en la mida que sigui possible que el codi pujat és íntegre. Si no és possible pujar els canvis de forma diària, sí que s'ha de garantir que cada equip de desenvolupament pujarà els canvis com a mínim amb una freqüència setmanal.

Els desplegaments en l'entorn de desenvolupament es faran consensuadament amb el Cap de Projectes. Malgrat que els diferents tècnics tindran accés a l'entorn de desenvolupament, no podran desplegar sense el vistiplau del Cap de Projectes. Les proves es realitzaran preferentment als entorns locals dels desenvolupadors. Només quan la versió es consideri suficientment estable podrà desplegar-se en l'entorn de desenvolupament.

Implantació i acceptació

En base als lliuraments de la fase anterior es procedirà a realitzar la implantació de l'evolutiu sobre els diferents entorns. En primer terme, en l'entorn de desenvolupament. L'adjudicatari procedirà a realitzar l'execució del pla de proves. En cas que es superi satisfactòriament, el Cap de Projectes procedirà a promocionar el canvi a l'entorn de preproducció i posteriorment al de producció.

Cas que en aquest procés els resultats obtinguts no siguin els esperats (és a dir, els que es van obtenir en l'entorn de desenvolupament) l'adjudicatari haurà de donar el suport necessari, si cal presencial, per solucionar-ho.

Una vegada s'hagi realitzat l'execució del pla de proves amb el 100% de les proves funcionant als l'entorn de preproducció i producció, es donarà el projecte per tancat. A partir d'aquest instant entrarà en vigor el període de garantia de l'evolutiu.

A partir d'aquest moment ja ha d'entrar en vigor l'etapa de suport. És responsabilitat de l'adjudicatari realitzar les tasques necessàries de traspàs, formació i documentació del projecte, d'operació, i de procediment, per tal que els nous desenvolupaments ja puguin ser objecte del servei de suport.

Una vegada acabada l'etapa de codificació i superades les proves d'integració a l'entorn de preproducció, el Cap de Projectes, amb el suport de l'equip de desenvolupament, haurà de preparar el pla d'implantació amb la col·laboració de l'equip de Suport de l'AOC (també depenent de la Subdirecció d'Operacions). El pla d'implantació incorpora totes les accions adreçades a que la versió arribi als usuaris finals.

Cal tenir en compte que cap dels tècnics de desenvolupament però, té -per defecte- accés als entorns de preproducció i producció.

Per dur a terme el pla d'implantació el Cap de Projectes prepara el paquet de desplegament i realitza una petició al projecte Desplegaments del JIRA. En la petició de desplegament s'indicarà la versió del JIRA a la que correspon el desplegament.

Els desplegaments a l'entorn de preproducció es realitzen típicament els dijous a la tarda i la petició de desplegament ha d'haver arribat com a molt tard el dia d'abans, per tal que es pugui preparar juntament amb la resta de desplegaments d'altres serveis del Consorci AOC. Addicionalment i amb l'objectiu d'agilitzar i garantit la correctesa dels desplegaments, s'està implantant un sistema d'integració continua i desplegament automàtic.

Una vegada desplegat a preproducció, és el Cap de Projectes amb el suport de l'adjudicatari, qui haurà d'executar el pla de proves per realitzar la validació final. El Cap de Projectes del Consorci AOC decidirà si la versió supera satisfactòriament el pla de proves. En cas afirmatiu, el Cap de Projectes prepararà i sol·licitarà a través del JIRA la petició de desplegament a producció. En cas contrari, l'equip de desenvolupament realitzarà les correccions necessàries donant tot el suport necessari per corregir les incidències detectades en la major brevetat possible. Els desplegaments a l'entorn de producció es realitzen típicament els dimecres a la tarda.

Una vegada la versió s'hagi desplegat a producció entrarà en vigor el període de garantia de l'evolutiu.

Avaluació

Una vegada definits els requeriments que formaran part de la versió, el Cap de Projectes defineix les mètriques i els indicadors que permetran avaluar el compliment dels objectius marcats per a la versió.

Després d'un cert temps de la posada en marxa de la versió, el Cap de Servei realitzarà el seguiment dels indicadors a través d'enquestes, auditories i qualsevol altra eina de gestió de la qualitat que consideri adient, establint el quadre de comandament del servei.

Aquest quadre de comandament es posarà a disposició del comitè estratègic amb l'objectiu de mantenir-ho informat de la marxa del servei.

Finalment, el comitè de seguiment realitzarà una sessió de retrospectiva analitzant conjuntament quines coses han anat bé durant la versió i quines coses han anat malament (des del punt de vista de tots els actors) per tal de poder aprendre i millorar de cara a futures versions.

JIRA

L'eina corporativa JIRA esdevé la pedra angular de la versió en tant que permet reflectir en detall l'estat actual i el grau d'assoliment d'aquesta, així com l'evolució estratègica que seguirà el servei en un futur mitjà. És per tant una eina fonamental per mantenir coordinats tots els actors.

La informació del JIRA es fa visible a tots els actors que participen en el servei, però donat que cadascun dels actors prioritzarà un tipus d'informació diferent, es requereix d'un esforç per part del Cap de Servei i del Cap de Projectes per reflectir al JIRA els diferents punts de vista. Aquesta diferent visió es plasma al JIRA a partir dels següents projectes:

- Servei: Evolució estratègica d'un servei a mig/llarg termini. En aquest projecte del JIRA els requeriments s'agrupen i s'ordenen en idees conceptuals properes a les línies d'actuació que marca el comitè estratègic. Aquest projecte permet obtenir una idea global del que es pretén aconseguir amb el servei a mig o llarg termini.

Pels requeriments més prioritaris, que inicialment són els candidats a ser seleccionats per a la propera versió, el responsable del servei realitzarà l'anàlisi funcional detallat.

El Cap de Servei és el principal responsable del manteniment al JIRA d'aquest projecte i ha de reflectir tots els canvis i documents amb la màxima periodicitat possible.

- Projecte: Vista detallada del futur immediat del servei. En aquest projecte del JIRA es descomponen les peticions d'evolutius en els diferents requeriments funcionals i tècnics que ha de complir la nova versió. Els assumptes que composen aquest projecte es troben ben definits i detallats, disposen d'una estimació del seu cost, els recursos que estan assignats, així com el seu grau d'avançament. Aquest projecte permet obtenir una idea detallada de l'estat actual del servei i el seu objectiu és mantenir informat amb el major nivell de detall possible els diferents actors que participen en el desenvolupament diari del servei.

El Cap de Projectes és el principal responsable del manteniment al JIRA d'aquest projecte i ha de reflectir tots els canvis amb la màxima periodicitat possible. En aquest projecte s'inclouran tots els documents tècnics (disseny tècnic, documents d'integració, etc.).

Els desenvolupadors hauran d'actualitzar els tiquets que tinguin assignats amb els detalls tècnics necessaris per comprendre no només els avenços en les tasques encomanades, sinó també per a que quedi enregistrada tota la informació relativa a la resolució d'aquestes.

Per cada tiquet Jira que requereixi de canvi de codi, el desenvolupador haurà de crear una nova branca al repositori Git corresponent, identificant en el nom de la mateixa el tiquet del Jira al que es correspon.

Si s'escau, qualsevol d'aquests 2 projectes principals es poden complementar amb altres projectes que permetin agrupar línies d'actuació que es duran a terme a llarg termini o bé que es duran a terme en paral·lel, però en dates diferents. L'objectiu d'aquests projectes complementaris ha de ser simplement el de facilitar als diferents actors la lectura de l'estat present i futur del servei.

Requeriments tècnics i personals

El licitador haurà de disposar en el moment d'iniciar el contracte, dels recursos que s'han indicat a la descripció del contracte.

El proveïdor ha de garantir que per a la resolució d'incidències i per donar resposta a les peticions bàsiques d'operació sempre hi haurà un mínim de dues persones formades en cadascun dels entorns i que, com mínim, sempre hi ha una disponible.

En cas de baixa definitiva de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC. Qualsevol canvi en un dels membres de l'equip a instàncies de l'adjudicatari haurà de ser validat pel Consorci AOC. Caldrà acordar el calendari de canvi amb el Consorci AOC per tal de minimitzar l'impacte en els desenvolupaments en curs. Resten fora d'aquest compromís els períodes de vacances i permisos de tots els membres de l'equip.

Quan es canviï un membre de l'equip de treball a instàncies de l'adjudicatari, es fixarà un temps de 2 setmanes de formació/adaptació del nou membre que seran a càrrec de l'adjudicatari.

El Consorci AOC es reserva el dret a demanar el canvi de qualsevol dels membres de l'equip sense necessitat de justificació amb una antelació de 20 dies naturals a la data de substitució.

A més dels perfils descrits, caldrà aportar un gestor del servei d'alt nivell sense càrrec i que s'encarregarà de les següents tasques:

- Interlocució a alt nivell.
- Disseny i seguiment del pla derivat del contracte.
- Vetllar per a que cada fase del projecte es realitzi de forma diligent i dins de les dates acordades.
- Informar de les desviacions de les dates de finalització de cada fase tan bon punt es detectin.
- Gestionar els recursos assignats, tant materials com personals.

5. Acords de Nivell de Servei

En aquest apartat es descriu el marc contextual d'aplicació dels Acords de Nivell de Servei. S'establirà el següent procediment de treball i l'Acord de Nivell de Servei (ANS) que es detalla a continuació per a tots els lliurables que es despleguin a l'entorn de producció.

Les possibles penalitzacions que es derivin de l'incompliment dels ANS, s'aplicaran sobre descompte en la següent factura emesa després de la penalitat. L'aplicació de penalitats serà acumulativa.

Els Acords de Nivell de Servei es podran revisar i modificar sempre i quan hi hagi acord mutu entre l'adjudicatari i el Consorci AOC.

Requeriments de nivell de servei

Resolució d'incidències sense errors:

- Percentatge de la resolució d'incidències sense errors en el termini.
    - Càlcul: (A/B)*100

      A: Número total d'incidències resoltes sense error en el termini

      B: Total d'incidències resoltes en el termini
- Periodicitat: Diària
- El percentatge d'incidències sense error en el termini establert haurà de ser com a mínim del 90%.
- El nivell ofert per qui resulti adjudicatari constituirà un Acord de Nivell de Servei (ANS), el compliment del qual es mesurarà durant tota la durada de la prestació del servei.

ANS per a la gestió de les incidències

Aquest ANS aplica a la totalitat del servei contractat.

Definicions:

Nivell	Descripció
Bloquejant	Una incidència es catalogarà amb criticitat bloquejant si impedeix la utilització total del servei a tots els usuaris d'aquest.
Alta	Una incidència es catalogarà amb criticitat alta si impedeix la utilització d'una part concreta del servei, a tots o alguns usuaris, i l'afectació pel negoci és elevada.
Mitja	Una incidència es catalogarà amb criticitat mitja si impedeix la utilització d'una funcionalitat concreta d'algun dels serveis a tots o alguns usuaris i l'afectació pel negoci és relativament baixa.
Baixa	Una incidència es catalogarà amb criticitat baixa si no impedeix la utilització ni parcial ni total d'algun dels serveis a algun dels usuaris.

El temps de resposta i de resolució s'estableixen segons el tipus d'incidència:

- Temps de resposta

  Es defineix com a temps de resposta el temps que transcorre des de que la incidència es comunicada, i l'usuari rep el tiquet de la seva incidència. El temps de resposta es compta sobre l'horari de suport de recepció d'incidències.

- Temps de resolució

  Es defineix el temps de resolució d'una incidència com el nombre d'hores que transcorren des de que l'usuari rep el tiquet de la incidència fins el moment en que la incidència està solucionada. En el càlcul del temps de resolució d'una incidència no es tenen en compte els possibles increments de temps provocats per la intervenció inevitable de tercers en el procés de resolució (per exemple, intervenció d'altres organismes).

El temps màxim permès per la resposta i resolució d'una incidència dependrà del nivell de criticitat de la incidència. En la següent taula es mostren els temps màxims permesos per la resolució d'una incidència en funció del nivell de criticitat:

Criticitat Incidència	Temps de resposta (hores)	Temps de resolució (hores)	% de resolució dins del temps compromès
0 Bloquejant	0,5	2	95 %
1 Alta	1	16	95 %
2 Mitja	1	40	95 %
3 Baixa	1	64	95 %

Pel càlcul del temps de resolució d'una incidència s'exclouran els possibles increments de temps provocats per la intervenció inevitable en el procés de resolució per part de tercers.

En el cas que l'adjudicatari no compleixi l'acord de nivell de servei definit anteriorment almenys en el 95% de les d'incidències amb criticitat 0 i 1 que hagin ocorregut dins el mes se li aplicarà les següents penalitzacions:

Percentatge d'incidències amb criticitat 0 i 1 dins el mes que compleixen l'ANS	Penalització sobre la quota mensual de la factura
Superior al 95%	0%
Entre 95% i 80%	5%
Entre 80% i 70%	10%
Inferior al 70%	15%

Cas que l'adjudicatari no compleixi l'acord de nivell de servei definit anteriorment per al menys el 90% de les d'incidències amb criticitat 2 i 3 que hagin ocorregut al mes, se li aplicarà les següents penalitzacions:

Percentatge d'incidències amb criticitat 2 i 3 dins el mes que compleixen l'ANS	Penalització sobre la quota mensual de la factura
Superior al 90%	0%
Entre 90% i 51%	5%
Inferior al 51%	10%

Requeriments de nivell de servei en la protecció de dades

Es considerarà incompliment del contracte la no aplicació de les mesures de seguretat imposades al contractista. A banda de les possibles responsabilitats que es puguin derivar de dit incompliment, i que en funció de la gravetat del mateix pugui comportar la resolució del contracte, es preveu la imposició de penalitats.

Les penalitats a imposar seran per cada incompliment que es produeixi i amb el topall màxim establert a l'article 192 de la Llei 9/2017, de Contractes del Sector Públic:

- Mesures de seguretat de nivell baix: 0,5% del preu d'adjudicació del lot.
- Mesures de seguretat de nivell mig: 0,75% del preu d'adjudicació del lot.
- Mesures de seguretat de nivell alt: 1% del preu d'adjudicació del lot.

Incidents de seguretat

És important destacar que qualsevol incident de Seguretat o de protecció de dades personals que puguin afectar els sistemes del Consorci AOC, s'haurà d'informar en un temps inferior a les 24h.

En la fase inicial del projecte s'haurà de definir un procediment de coordinació davant incidents que puguin afectar els sistemes del Consorci AOC. Aquest procediment haurà de contemplar els fluxos d'informació i les interaccions entre Consorci AOC i l'adjudicatari durant la gestió de l'incident.

Al seu torn l'adjudicatari haurà d'informar periòdicament dels incidents que hagin afectat els sistemes o plataformes del Consorci AOC.

6. Condicions d'execució

L'adjudicatari haurà de complir les següents obligacions bàsiques:

- Gestionar qualsevol alteració del servei en les condicions expressades en aquest plec.
- Realitzar reunions periòdiques amb el Consorci AOC per tal d'exposar el compliment del servei i tractar els possibles problemes o millores del servei.
- Establir un marc metodològic de treball basat en la metodologia Agile.

- Realitzar la formació dels tècnics designats, en tots aquells aspectes que el Consorci AOC cregui oportuns i que siguin de directa aplicació als serveis requerits.
- Elaboració dels manuals i altra documentació destinada a la formació dels usuaris.
- Elaboració de la documentació tècnica.
- Mantenir en tot moment l'actualització del codi font i de la documentació en el sistema de control de versions del Consorci AOC (GitHub) per tal que pugui estar disponible en tot moment pel personal assignat i també per disposar de l'opció de control de versions.
- Tota la documentació generada per l'equip serà preferentment en català i en el format corporatiu proposat per Consorci AOC.
- Presentació d'informes mensuals amb el detall de l'estat del servei d'acord amb els indicadors que el Consorci AOC consideri apropiats. Alguns exemples d'aquests informes serien:
    - Informe resum de les actuacions realitzades.
    - Informe de situació de les actuacions en curs.
    - Informe resum de les actuacions pendents.
    - Planificació de les actuacions a realitzar.
- Informe de finalització del contracte amb el resum de les tasques realitzades.

El Consorci AOC es reserva el dret a validar, i si s'escau definir, les eines que s'hagin de fer servir per a la gestió i control del servei.

7. Model de relació

L'adjudicatari haurà d'incloure en la seva proposta quin és el model de relació que proposa per garantir l'èxit del projecte: l'estructura organitzativa del servei, els canals i eines de comunicació a tots els nivells entre el proveïdor i el Consorci AOC, els procediments d'escalat davant d'incidències susceptibles d'afectar o amb afectació als serveis sota responsabilitat del proveïdor, i quines eines de control (addicionals a les eines corporatives JIRA i Microsoft Teams del Consorci AOC), proposa per dur a terme el seguiment i control global del servei. Cal destacar que el Consorci AOC es reservarà el dret a validar, i si s'escau definir, aquestes eines de control.

Com a mínim, caldrà que s'estableixin els següents nivells d'interlocució:

Reunions de direcció amb les següents característiques:

- Interlocutors: Gerent de comptes i/o cap de projectes per part de l'adjudicatari. Gestor del servei i/o Cap de Projectes per part del Consorci AOC.
- Periodicitat mínima: 1 mes
- Objectiu: Fer el seguiment del contracte, analitzant diversos aspectes: productivitat, control d'hores, temes de facturació, seguiment de fites (a alt nivell), etc.
- Escandall d'hores totals realitzades en el mes.
- Lliurables: actes de les reunions, informes executius, informes amb control d'hores (fetes i pendents) etc.

Reunions de seguiment amb les següents característiques:

- Interlocutors: Enginyer de software per part de l'adjudicatari. Cap de Projectes per part del Consorci AOC.
- Periodicitat mínima: 1 setmana
- Objectiu: Seguiment del compliment de l'ANS, rendiment de la plataforma i incidències més destacables.
- Lliurables:
    - Informes de l'estat del servei
    - Informe resum de les actuacions ja resoltes i hores realitzades.
    - Informe de situació de les actuacions en curs i hores realitzades.
    - Informe resum de les actuacions pendents i hores estimades.
    - Planificació de les actuacions a realitzar.
    - Informe de les incidències obertes, resoltes, temps de resolució,...

8. Horari d'execució del servei

El licitador haurà d'incloure a la seva proposta la disponibilitat horària del personal associat al servei, tot i que haurà de garantir la disponibilitat de com a mínim 1 membre de l'equip durant les franges horàries següents:

- De dilluns a divendres, excepte festius de la ciutat de Barcelona, **de 09:00 a 17:00 hores**.

- El 90% dels treballs es realitzaran en l'horari indicat. En el 10% dels casos restants es podrà sol·licitar prèviament la realització de tasques fora de l'horari anteriorment establert sense cost addicional.

En cas de baixa de qualsevol dels membres de l'equip, l'adjudicatari haurà de substituir-lo en menys de 15 dies laborables d'acord amb els responsables del Consorci AOC.

Qualsevol canvi en un dels membres de l'equip a instàncies de l'adjudicatari haurà de ser pactat amb el Consorci AOC. En aquests casos, es fixarà un temps de 2 setmanes de formació/adaptació del nou membre que seran a càrrec de l'adjudicatari.

9. Infraestructura necessària

L'adjudicatari haurà d'aportar la infraestructura tècnica, llicències, i qualsevol altre component o mitjà tècnic necessari per a la realització dels treballs. Els costos d'aquesta infraestructura tecnològica aniran a càrrec dels adjudicataris. És important destacar que aquesta infraestructura tecnològica no podrà contenir en cap moment dades reals. Per als tests i proves dels diferents lliurables, els adjudicataris hauran de disposar d'entorns d'integració a les seves instal·lacions per fer el control de qualitat dels evolutius desenvolupats. A l'Annex 1 s'inclou una descripció de la infraestructura tecnològica de PSIS i a l'Annex 2 del Signador.

L'adjudicatari mantindrà en tot moment l'actualització del codi font en el sistema de control de versions del Consorci AOC (Git).

Les tasques s'hauran de dur a terme a les oficines de cadascuna de les empreses adjudicatàries, tot i que de forma puntual és possible que en alguna ocasió sigui necessari el desplaçament d'algun dels membres del adjudicataris a les instal·lacions del Consorci AOC o de tercers. Per aquest motiu es recomana que tots els membres de l'equip disposin d'ordinadors portàtils.

Tots els treballs desenvolupats, i en particular els lliurables entregats, hauran de seguir les guies d'estil definides pel Consorci AOC. El Consorci AOC facilitarà a tots els adjudicataris aquestes guies d'estil i el seu compliment serà obligatori per a l'acceptació dels treballs.

10.Propietat intel·lectual

L'adjudicatari accepta expressament que la propietat intel·lectual de tots els lliurables, independentment de la seva naturalesa i resultats dels treballs realitzats, i en particular els productes i serveis objectes del contracte, corresponen únicament al Consorci AOC amb exclusivitat i amb caràcter general, sense que l'adjudicatari pugui conservar, ni obtenir còpia dels mateixos o facilitar-lo a tercers.

L'empresa adjudicatària no podrà fer cap ús o divulgació dels estudis i documents utilitzats o elaborats com a resultat de la prestació del servei objecte del contracte, bé sigui en forma total o parcial, directament o extractada, original o reproduïda, sense autorització expressa del Consorci AOC, que la donaria, si escau, prèvia petició formal de l'adjudicatari amb expressió de la fi.

11.Garantia

Totes les tasques que formen part de l'abast del contracte tindran una garantia de 6 mesos. Durant aquest període, l'adjudicatari s'haurà de comprometre a resoldre satisfactòriament totes aquelles incidències o defectes detectats en qualsevol de les activitats dutes a terme pel seu equip de treball que li siguin imputables amb ell per acció o omissió.

12.Requeriments de seguretat

L'adjudicatari haurà de complir amb els següents requeriments de seguretat:

12.1. Mesures de seguretat i per defecte

El Consorci AOC, amb el suport de l'adjudicatari, implementarà durant la fase de desenvolupament, les mesures de protecció de dades des del disseny i per defecte, recollides a la guia del APDCAT: La privacitat des del disseny i la privacitat por defecte. Guia per a desenvolupadors (gencat.cat)

Els adjudicataris hauran de documentar:

- L'anàlisi dut a terme de les mesures necessàries.
- La verificació de que les mesures han estat aplicades.

12.2. Valoració dels serveis

El Consorci AOC ha valorat les dades i el servei de PSIS de la següent 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: Agència Catalana de Ciberseguretat
RGDP: Reglament General de Protecció de Dades
ENS: Esquema Nacional de Seguretat
RTO: Temps màxim de recuperació del servei en cas d'indisponibilitat

12.3. Mesures de seguretat que ha d'incorporar PSIS com a solució

Durant el temps d'execució del contracte, l'adjudicatari haurà d'implementar les mesures de seguretat de nivell ALT de l'Esquema Nacional de Seguretat que afectin directament a PSIS com a solució i plataforma tecnològica. El Consorci liderarà l'adequació del servei als requeriments de seguretat.

12.4. Mesures de seguretat a complir per part de l'adjudicatari

Certificacions de seguretat

Durant el temps d'execució del contracte, l'adjudicatari haurà d'implementar les mesures de seguretat de nivell BAIX de l'Esquema Nacional de Seguretat en tots els seus sistemes d'informació involucrats en la prestació del servei. Concretament són les descrites a:

- *Annex 3 - Requeriments de seguretat (ENS) pels proveïdors de software.*

El Consorci AOC auditarà en un termini no superior a 6 mesos, que l'adjudicatari compleix amb els requeriments de l' *Annex 3 - Requeriment de seguretat (ENS) pels proveïdors de software.*

L'auditoria es farà mitjançant la entrega d'evidències indicades en l'annex al Consorci AOC per a que aquest determini el grau de compliment.

L'adjudicatari estarà exempt de l'auditoria si aporta una declaració de conformitat en el nivell BAIX de l'Esquema Nacional de Seguridad.

En cas d'auditoria externa de la plataforma PSIS, l'adjudicatari haurà de participar en l'auditoria en les tasques que li corresponguin, entregant les evidències que l'auditor reclami i fent les adequacions necessàries que els hi pertoquin.

12.5. Mesures addicionals

Control d'accés al sistema

L'adjudicatari haurà d'adaptar-se en tot moment als mecanismes de control d'accés als sistemes d'informació que imposi el Consorci AOC per accedir als seus sistemes.

Control de personal

L'adjudicatari haurà d'informar en tot moment de les altes i baixes del personal intern o subcontractat que en nom seu accedeixi als sistemes del Consorci AOC.

En cas de baixa d'un usuari, de manera immediata l'adjudicatari haurà d'informar al Consorci AOC per tal de revocar els seus drets d'accés als sistemes.

Protecció de la informació

L'adjudicatari no podrà fer ús de les dades reals dels sistemes de producció en els sistemes de desenvolupament.

L'adjudicatari no podrà descarregar informació del Consorci AOC en els seus sistemes o en suports portàtils com USBs, DVDs, portàtils, tabletes, etc. En el cas d'haver de fer-ho caldrà demanar l'autorització del Consorci AOC i que el suport estigui xifrat.

Els fitxers temporals que s'haguessin creat exclusivament per a la realització de treballs temporals auxiliars hauran de complir amb les mesures establertes que s'apliquin als fitxers considerats definitius.

Tot fitxer temporal així creat serà esborrat una vegada hagi deixat de ser necessari per la finalitat que va motivar la seva creació.

13.Pla de devolució del servei

L'adjudicatari haurà d'assumir dins el contracte la planificació i execució del pla de devolució del servei al final de la prestació. El pla de devolució haurà de complir amb els següents requeriments mínims:

- Una durada d'1 mes amb una dedicació mínima de 160h i tant la durada (1 mes) com la dedicació (160h) seran addicionals a la prestació principal del servei de 24 mesos i hauran d'anar a càrrec de l'adjudicatari.
- L'adjudicatari haurà de retornar el codi font, scripts, documentació, etc. de totes les actualitzacions realitzades.

L'adjudicatari haurà de destruir i/o retornar al Consorci AOC (o en aquell tercer que aquest designi) la informació propietat del Consorci AOC. Aquest retorn s'haurà de realitzar d'acord amb allò que s'estableixi legalment i segons les indicacions del Consorci AOC. El retorn contemplarà tots els productes i programaris que siguin de propietat del Consorci AOC juntament amb els suports o documents en que consti alguna dada d'aquest. El retorn de les dades al Consorci AOC, o en un tercer designat, es durà a terme en el format i els suports que s'acordaran en el moment de planificar i detallar el pla de finalització del contracte. L'adjudicatari haurà de disposar d'un procediment d'esborrat segur de suports reutilitzats o que arribin al final de la seva vida útil. El proveïdor haurà d'informar com fa l'eliminació segura de la informació i haurà de proporcionar els certificats corresponents conforme ha realitzat aquesta eliminació segura.

Barcelona, 21 d’octubre de 2024

Áurea Alcaide Izquierdo

Cap de Projectes de la Subdirecció d’Operacions del Consorci AOC

Annex 1 – PSIS

Descripció funcional

Les principals funcionalitats de l'aplicació PSIS són les següents:

1. **Validació de certificats digitals**: permet consultar l'estat d'un certificat. L'aplicació respon si és vàlid o no és vàlid (per exemple, perquè està revocat). En la mateixa resposta també pot retornar informació addicional, com per exemple, dades útils del certificat digital (pe. el nom i cognoms, el DNI, etc.) i el nivell de seguretat associat al certificat digital (pe. nivell 3 en cas del certificat idCAT, nivell 4 en cas d'un certificat de signatura de treballador públic, etc.).

2. **Validació i completat de signatures digitals**: el servei permet realitzar la comprovació de la validesa d'una signatura digital. El servei inspecciona la signatura i verifica per una part que, criptogràficament, la signatura estigui ben formada. Per una altra banda comprova l'estat del certificat en el moment que s'ha produït la signatura. En funció dels resultats anteriors respon si la signatura és vàlida o no és vàlida.

El servei permet la validació de signatures digitals *simples* (CMS i l'XMLDsig) i signatures *avançades* (CAdES i XAdES i PAdES). Aquestes últimes, a més de permetre identificar el signatari i detectar qualsevol canvi posterior de les dades signades (al igual que les signatures *simples*), permeten que la signatura digital sigui perdurable en el temps més enllà de la vida del propi certificat del signatari. Això ho permet fer l'ampliació per mitjà del completat de la signatura: afegint a la pròpia signatura un *segell de temps* que permeti ubicar-la en el temps de manera fiable, i afegint també informació sobre l'estat de revocació del certificat del signatari i de la cadena de certificats.

3. **Creació de signatures digitals**: L'aplicació permet generar signatures de forma desatesa fent ús de claus privades ubicades en un mòdul hardware de seguretat (HSM *Hardware Security Module*) propi de PSIS. Addicionalment, la pròpia PSIS fa ús del mòdul de creació de signatures quan es sol·licita el retorn de la resposta signada.

4. **Emissió de segells de temps**: L'aplicació ofereix la possibilitat *d'estampar* un segell de temps a un document, proporcionant d'aquesta manera evidències (tècniques i jurídiques) de que l'acte en qüestió s'ha produït en un determinat moment del temps. El servei, per tal de proveir la data i hora, està sincronitzat amb el *Real Instituto y Observatorio de la Armada* (ROA), que és la font de temps oficinal a Espanya.

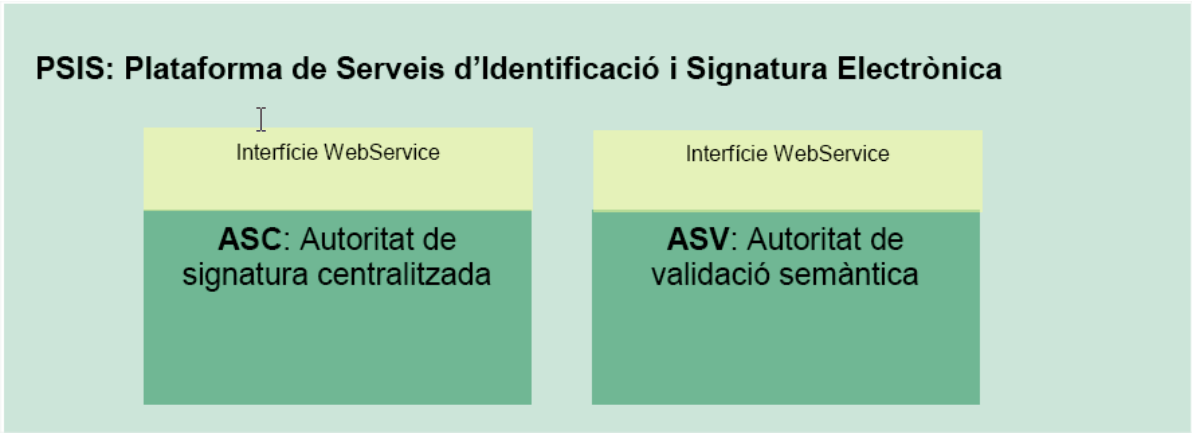
Descripció arquitectura

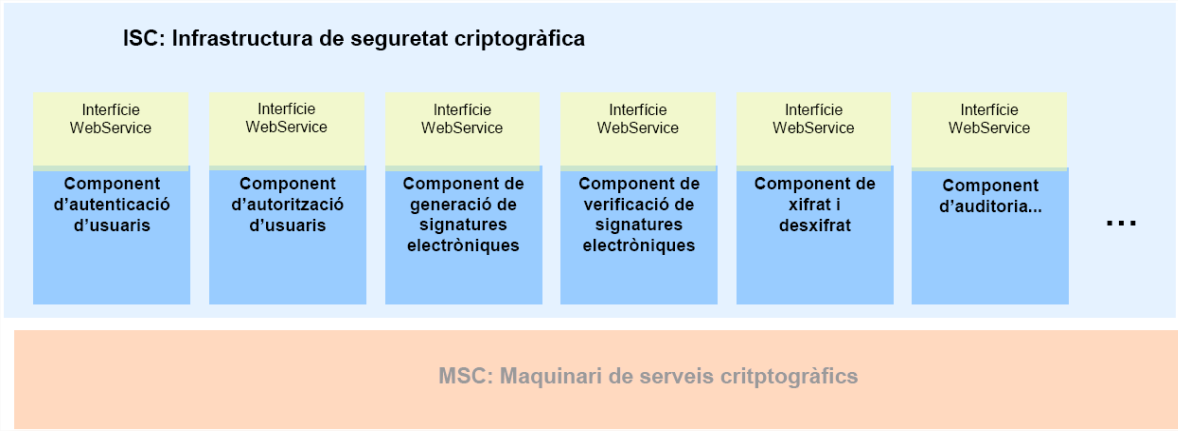
L'aplicació PSIS està composada principalment per dos mòduls. A continuació s'enumeren i més endavant es fa una explicació detallada:

• Autoritat de validació semàntica (AVS)
• Autoritat de signatura centralitzada (ASC)

Aquests mòduls formen part d'un **entorn de serveis web comú** que ofereix les funcionalitats recollides a la fig. 1.
Aquest entorn de serveis web comú està construït sobre una **infraestructura de seguretat criptogràfica (ISC)** formada, entre d'altres, pels següents **components (agrupacions funcionals)**:

- Component d'autenticació d'usuaris
- Component d'autorització d'usuaris
- Component de gestió de claus i certificats
- Component de generació de signatures electròniques
- Component de verificació de signatures electròniques
- Component d'auditoria, registre d'operacions (*log*) i registre de consum
- Consola única de configuració d'aplicacions i components.





Autoritat de Validació Semàntica

L'Autoritat de Validació Semàntica (AVS) permet validar elements de confiança, incloent-hi signatures electròniques en diversos formats i certificats digitals X.509. Aquests elements de confiança són emesos per diferents proveïdors de serveis de confiança que han de ser classificats i gestionats a la plataforma de serveis de l'autoritat de validació semàntica.
Addicionalment, l'AVS executa treballs semàntics, localitzant i extraient informació continguda als elements de confiança que gestiona.
El mòdul AVS registra els perfils d'elements de confiança que emet cada proveïdor de serveis de confiança.
La classificació de cada perfil, a més d'assignar-li un nivell de classificació vinculat a la seguretat del certificat, permet establir el mètode de validació preferit, de tots els controls establerts pel proveïdor a l'element de confiança, indicant-ne l'ordre prioritari per ser validat (CRL, OCSP, mètodes propietaris, @firma).

Autoritat de Signatura Centralitzada

L'Autoritat de Signatura Centralitzada (ASC) permet la generació de signatura electrònica assistida des de servidor. La interacció entre l'usuari i el maquinari de serveis criptogràfics es fa a través de l'aplicació de creació de signatura, mitjançant un canal segur, d'acord amb les especificacions tècniques CEN CWA 14169 i CEN CWA 141701.

Descripció tecnològica

A continuació es fa una descripció de les tecnologies i estàndards més rellevants de les que fa ús l'aplicació PSIS. L'adjudicatari haurà de detallar en la seva proposta el coneixement i experiència que té d'aquestes tecnologies en concret, i altres de similars si ho estima oportú.

Llenguatge de programació

L'aplicació PSIS està desenvolupada, principalment, en **J2EE** (*Java 2 Platform Enterprise Edition*), en una arquitectura distribuïda en nivells i basada en components de programari.

L'aplicació està dissenyada per operar en diverses capes lògiques. Aquestes són:

- Capa web: Entorn amb funcions de frontal web i interfície d'usuari.
- Capa d'aplicació: Entorn amb funcions de servidor d'aplicacions on s'executa tota la lògica de negoci. Es fa ús del framework ***Spring***.
- Capa base de dades: les pròpies bases de dades de l'aplicació. L'accés a la base de dades des de l'aplicació es fa per mitjà d' ***Hibernate***.

Aquests diferents entorns o nivells tenen la capacitat de poder estar executant-se en la mateixa màquina o en maquinari diferent i fins i tot clusteritzat. Aquest punt depèn de l'arquitectura que en cada moment pugui proveir l'Àrea de Sistemes del Consorci AOC.

Addicionalment, es fan servir una sèrie de llibreries d'altres fabricants. Les més rellevants són:

- Bouncy Castle
- Apache XML Security
- iText
- Rhino

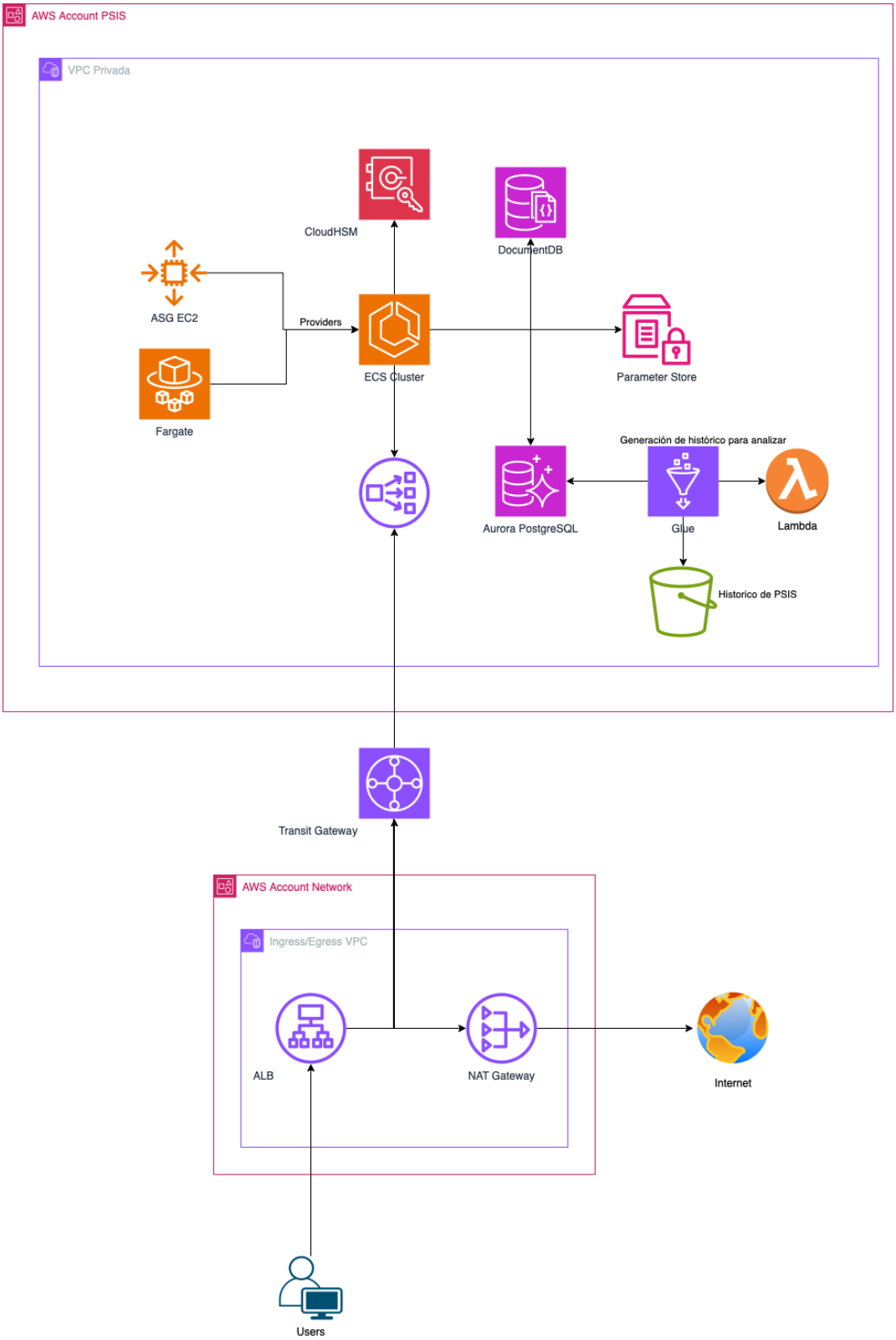
Infraestructura de programari

PSIS està desplegat al núvol de Amazon Web Services (AWS). El codi de PSIS és independent de la plataforma de desplegament. És a dir, que es pot desplegar en qualsevol entorn kubernetes.

Serveis AWS que s'utilitzen a PSIS, entre d'altres:

- Desplegament en ECS sobre EC2.
- Base de dades Aurora PostgreSQL Serverless.
- Base de dades DocumentDB.
- Cloud HSM.

Adjuntem un gràfic 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

Descripció de la missatgeria: Digital Signature Services

En aquest apartat es fa una descripció de la missatgeria que utilitza l'aplicació PSIS per les comunicacions entre servidor i client.

Nota: el contingut que es mostra a continuació és un extracte de la documentació (pública) que es facilita als clients del Consorci AOC per fer la integració amb PSIS. El document es diu "Guia d'integradors de PSIS" i està disponible a la web del Consorci AOC.

Per a poder fer ús de PSIS es requereix del desenvolupament d'uns clients que construiran missatges de petició i extrauran les respostes dels missatges provinents del servidor abstraient al client del procés d'invocació remota que es porta a terme.

Un dels protocols amb què treballa la plataforma és el DSS (*Digital Signature Services*), del consorci d'estandardització OASIS (*Organization for the Advancement of Structured Information Standards*) un protocol per a la prestació de serveis de signatura digital obert i extensible (mitjançant l'ús de perfils).

El protocol DSS Core conté una aproximació generalista als problemes derivats de la provisió de serveis de signatura electrònica. Els perfils de DSS són extensions del DSS Core que aporten més detalls i funcionalitats per a solucionar problemes més concrets.

De perfils es poden trobar diversos, però PSIS dóna suport principalment el perfil *XSS* (desenvolupat pel Consorci AOC i que amplia DSS permetent, entre d'altres, la validació de certificats X509) , el perfil *XAdES* (que permet l'actualització de signatures), el *Timestamping Profile,* que aporta més control i detalls en l'àmbit dels segells de temps sobre DSS, i el *DSS_PDF* per la validació i completat de signatures electròniques en documents PDF.

Profiles	
DSS Protocol bàsic de creació i validació de signatures .	urn:oasis:names:tc:dss:1.0:core:schema
XADES Ampliació de DSS que permet treballar amb signatures avançades XAdES i CAdES.	urn:oasis:names:tc:dss:1.0:profiles:XAdES
XSS Ampliació de DSS que permet, entre d'altres validar certificats X509 de clau púbica, extreure informació dels mateixos i fer servir polítiques de signatura .	urn:oasis:names:tc:dss:1.0:profiles:XSS
TIMESTAMP Defineix restriccions extres sobre la creació i validació de segells de temps via DSS.	urn:oasis:names:tc:dss:1.0:profiles:timestamping
DSS_PDF Permet validar i completar signatures en documents PDF.	urn:oasis:names:tc:dss:1.0:profiles:DSS_PDF

La documentació detallada del protocol i els seus perfils està disponible en el paquet distribuït pel Consorci AOC.

***NOTA:** Totes les descripcions d'estructures / elements que formen part de la missatgeria DSS contenen el nom del document on es pot trobar el detall de la descripció, juntament amb possibles comentaris particulars de la plataforma PSIS.*

La missatgeria que intervé a la plataforma PSIS ve definida per l'estàndard DSS i funciona sota el protocol SOAP (*Simple Object Access Protocol*).

SOAP és un protocol estàndard sobre el qual es fonamenta la tecnologia de serveis web (*Web Services*). A diferència d'altres protocols de tipus binari com poden ser COM, COM+ o DCOM, els quals són propis de Microsoft, SOAP es basa en documents de text pla codificats en format XML. L'avantatge principal de codificar en XML és que els missatges són llegibles per éssers humans; però, per contra, aquests documents resultants són, en general, de gran tamany.

SOAP està dissenyat per a funcionar sobre qualsevol protocol d'internet, tot i que l'ús més habitual és sobre HTTP. El fet d'utilitzar HTTP minimitza l'impacte de dispositius com Firewalls i similars, i fa accessible SOAP a pràcticament qualsevol tipologia de comunicació client-servidor.

Els missatges SOAP estan composats per dos grans blocs funcionals: "Capçalera" (*envelope*) destinat a subministrar dades d'enrutament i "Cos" (*body*), el qual conté les dades del missatge d'usuari. Una explicació més detallada de SOAP no forma part de l'abast d'aquest document.

En aquest apartat es tracten els aspectes més importants involucrats en l'ús del protocol DSS. Tot i això, s'adjunta la referència on es pot consultar el document de l'estàndard corresponent per si fos necessària més informació sobre l'apartat concret.

A més, es defineixen una sèrie de prefixos per als diferents espais de noms involucrats. El seu mapeig contra les uri's dels espais de noms és el següent:

• 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: urn:OASIS:names:tc:dss:1.0:profiles:DSS_PDF

Aquí mostrem els dos tipus bàsics d'estructures que s'utilitzen a l'estàndard DSS, juntament amb els elements bàsics que es faran servir per a composar els missatges. Els dos tipus principals de missatges que defineix DSS són *VerifyRequest* (per a peticions de validació) i *SignRequest* (per a peticions de signatura o estampació de segell de temps).

Documentació

L'adjudicatari d'aquest concurs disposarà de tota la documentació relacionada amb l'aplicació que sigui necessària per la prestació del servei objecte d'aquest contracte.

A continuació s'enumera els principals documents:

- Guia d'integradors de PSIS
- Plec de requeriments inicial de PSIS
- Document anàlisi funcional
- Document d'arquitectura
- Diagrames seqüencials de signatura
- Perfils internacionals i del Consorci AOC (DSS, XSS, XAdES, DSS_PDF, TimeStamping)
- Documentació sobre gestió dels perfils dels proveïdors i fitxers de configuració
- Documentació d'usuari
    - Guia d'integradors
    - Guia de Signatura
- Documentació de gestió i configuració de PSIS

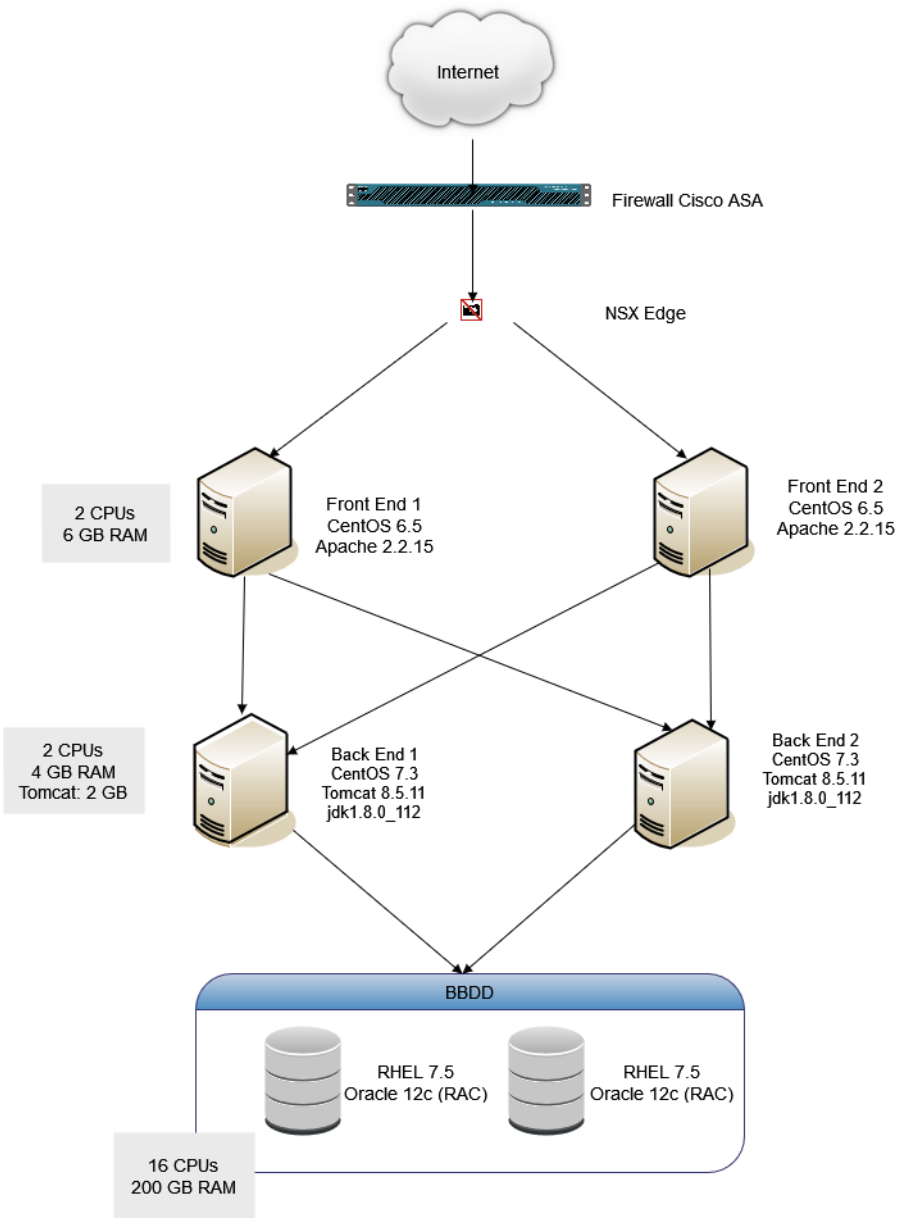
Annex 2 – Signador

Eina de signatura centralitzada basada en Java WebStart que disposa d'una aplicació nativa que permet l'execució d'una eina de signatura electrònica basada en certificats digitals d'usuari final dins les aplicacions que funcionen amb un navegador web.

La documentació d'integració del Signador està disponible a:

http://consorciaoc.github.io/signador/

Diagrama d'infraestructura de hardware:



Annex 3 – Requeriments de seguretat (ENS) pels proveïdors de software

Objecte de l'annex

El present annex defineix els controls que hauria de fer front una empresa adjudicatària de desenvolupament de programari en cas d'auditoria de l'ENS.

Requeriments

ID 1. Política de Seguretat

Es disposa d'una Política de Seguretat que inclou:

- Objectius de l'organització.
- Marc legal i regulador.
- Rols relacionats amb la seguretat, així com les seves responsabilitats i procediment de designació.
- Estructura del comitè de gestió i coordinació de seguretat.
- Criteri per a la classificació de la documentació.
- Referència a la legislació aplicable en matèria de tractaments de dades de caràcter personal.
- La Política de Seguretat ha de ser un document en paper o suport electrònic.
- La Política de Seguretat inclou l'especificació del termini i condicions de la seva revisió i que ha d'estar aprovada per un òrgan superior.
- La Política de Seguretat inclou un apartat específic de gestió dels usuaris i els seus privilegis, així com la persona responsable.
- La Política de Seguretat inclou un apartat específic indicant els responsables de la informació gestionada pel sistema.

ID 3. Procediment de revisió de la Política de Seguretat

Document contenint el Procediment de revisió i aprovació de la Política de Seguretat o en el seu defecte, apartat de la Política de Seguretat on s'especifiqui el període de revisió i aprovació.

ID 4. Evidència de la difusió de la Política de Seguretat

Evidència de què la Política de Seguretat és accessible pel personal afectat a la Intranet, pàgina web, portal, repositori o ha estat distribuïda a tots els usuaris dels quals són responsables mitjançant el correu electrònic.

ID 10. Evidència de la difusió de la Normativa de Seguretat

Evidència que la Normativa de Seguretat - ja sigui pròpia o s'empri el Marc Normatiu de l'Agència de Ciberseguretat de Catalunya - està disponible a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats o bé que els ha estat distribuïda a través del correu electrònic.

ID 11. Procediments de Seguretat

Es disposa de Procediments de Seguretat per a la realització de les tasques rutinàries.

Aquests han d'incloure com a mínim:

- Com portar a terme les tasques habituals.
- Qui ha de fer cada tasca.
- Com identificar i reportar comportaments anòmals.

ID 13. Evidència de la difusió dels Procediments de Seguretat o de la possibilitat d'accés per part dels usuaris

Evidència de que els Procediments de Seguretat - siguin propis o s'emprin els del Marc Normatiu de l'Agència de Ciberseguretat de Catalunya - estan disponibles a la Intranet, pàgina web, portal, repositori, llibreria o a qualsevol altre mitjà accessible per a tots els usuaris implicats.

ID 40. Document d'Identificació del Control d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.
- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.
- El període de retenció dels usuaris.

ID 43. Procediment d'Autenticació del Sistema

Es disposa d'un procediment degudament aprovat i actualitzat on es descriuen els mecanismes d'autenticació dels usuaris o s'especifica dins del procediment formalitzat de gestió d'usuaris els següents punts:

- Es detalla els sistemes d'autenticació dels usuaris amb l'obligació de tenir almenys un factor d'autenticació.
- Es detalla i s'obté l'evidència de que l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions.
- S'explica com gestionar les baixes d'usuaris i el lligam amb RRHH que permeti avisar als responsables de gestió d'usuaris del canvi en les relacions amb aquests.

- S'indica que es facin servir almenys dos factors d'autenticació en els sistemes categoritzats com a nivell mig i alt.
- En el cas que es facin servir tokens, que aquests utilitzen un algorisme autoritzat pel CCN, per exemple AES.

ID 46. Document de Requeriments d'Accés al sistema

Es disposa d'un procediment formalitzat de gestió d'usuaris degudament aprovat i actualitzat que indiqui:

- Com es realitza la gestió dels usuaris i dels seus privilegis així com la persona responsable de la gestió dels usuaris.
- Que els identificadors dels usuaris han de ser nominals i no es poden compartir.
- El període de retenció dels usuaris.

ID 50. Eina corporativa específica per a la gestió dels usuaris propis

Es disposa d'una eina corporativa específica per a la gestió dels usuaris.

ID 54. Procediment de Gestió de Drets d'Accés al Sistema

Es disposa d'un procediment on s'inclouen, dins del procediment formalitzat d'usuaris del sistema, els següents punts:

- S'assignarà el rol adequat a cada usuari amb els mínims privilegis possibles i revisant-se els mateixos periòdicament.
- S'inclourà la relació entre els permisos que ha de tenir cada usuari en funció del seu rol.
- S'especificarà quins son els responsables dels recursos dels sistemes (físics i lògics) i qui té la responsabilitat delegada de concedir, alterar o anul·lar l'accés als mateixos.

ID 62 Evidència de què l'usuari confirma la recepció de l'identificador, coneix i accepta les obligacions

Es disposa de l'evidència que demostra que els nous usuaris confirmen la recepció de l'identificador, coneixen i accepten les obligacions. Aquesta evidència pot prendre diverses formes:

- Evidència de que en crear el seu identificador s'informa l'usuari per correu electrònic, i en accedir per primer cop ha d'acceptar els drets i deures d'accés a l'aplicatiu.
- Que el personal d'un proveïdor signi un document d'obligacions el primer dia, així com un acord de confidencialitat i quedi constància del lliurament de l'identificador.
- Que en la part inferior de la pantalla d'accés s'indiquin els termes i condicions, pel que els usuaris estan implícitament acceptant-les per accedir al sistema.

ID 63. Acord de confidencialitat on es fa constar el lliurament de l'identificador

Es disposa del document contenint l'Acord de Confidencialitat signat per l'usuari fent constar la recepció del seu identificador. Ha d'existir un registre de cada usuari confirmant la recepció de l'identificador.

ID 64. Evidència de l'últim usuari propi donat de baixa

Es disposa de l'evidència mostrant la baixa d'un usuari amb la data efectiva de la baixa.

ID 67. Procediment d'Accés en Local

Es disposa d'un Procediment d'Accés en Local què especifiqui que:

- Els sistemes abans d'entrar en explotació o els ja existents han estat configurats de forma que no revelin informació del sistema abans d'un accés autoritzat.
- Els diàlegs d'accés (al lloc de treball, dins les pròpies instal·lacions de l'organització, al servidor, al domini de xarxa, etc.) no revelin informació sobre el sistema al qual s'està accedint.
- Faci constar que s'ha d'informar sempre als usuaris de les seves obligacions un cop han accedit al sistema.
- S'ha d'informar a l'usuari del seu darrer accés al sistema.
- Defineixi uns horaris en què és possible la connexió al sistema i altres en què no ho és.
- No es pot accedir al sistema fora de les hores autoritzades.
- Indiqui punts de renovació d'autenticació durant la sessió d'un usuari.

ID 107. Evidència què es disposa d'antivirus als sistemes d'informació

Es disposa de l'evidència de l'ús de mecanismes de prevenció davant de codi perjudicial (antivirus) per a tots els equips (Servidors i llocs de treball) del sistema i també en les maquetes, així com de la seva configuració.

ID 111. Evidència de què el programa antivirus es troba actualitzat

Es disposa de l'evidència que les opcions de configuració aplicades als antivirus són les recomanades pels fabricants (p.ex. Anàlisi d'execució de programes, anàlisi de correu entrant i sortint, bloqueig automàtic de codi nociu, etc.), així com les referents a la freqüència d'actualització.

ID 172. Evidències de la difusió del contingut del Pla de Conscienciació

Es disposa d'evidència de la difusió del contingut del pla de conscienciació (en la intranet o per algun altre mitjà es llancen missatges de conscienciació (p. ex. correus, comunicats interns,…)).

ID 174. Evidències de la difusió del contingut del Pla de Formació

Es disposa d'evidència amb la difusió del contingut del pla de formació en els darrers 3 anys.

ID 241. Document on s'indica el mecanisme d'autenticació i identificació

Es disposa d'una política o normativa documentada respecte al disseny d'un sistema que contempli els mecanismes d'identificació i autenticació i a més contempla els mecanismes de protecció de la informació tractada.

Així mateix no ha de ser possible accedir a informació del sistema que pugui ser utilitzada per a l'escalada de privilegis, ni executar accions fent-se passar per un altre usuari, etc.

ID 244. Procediment per a l'elaboració i execució del pla de proves de l'aplicació

Es disposa d'un procediment d'Acceptació i Posada en Servei de Protecció de les Aplicacions Informàtiques. Abans de passar a producció s'ha de comprovar el funcionament correcte de l'aplicació. S'ha de comprovar que:

- Es compleixen els criteris d'acceptació en matèria de seguretat.
- No es deteriora la seguretat d'altres components del servei.
- Les proves s'han de fer en un entorn aïllat (preproducció).
- Les proves d'acceptació no s'han de fer amb dades reals, llevat que s'asseguri el nivell de seguretat corresponent.
- Es realitzen anàlisis de vulnerabilitats.
- Es realitzen anàlisis de coherència i codi font.

ID 273. Procediment de configuració segura del correu

Es disposa d'un procediment el qual es detalla com es configura el correu per tal de disposar d'un sistema segur.

ID 276. Evidència de l'eina monitoratge dels elements de seguretat

Es disposa de l'evidència en la qual s'observa que es disposa d'una eina per monitoritzar els elements de seguretat com ara els virus o l'spam degudament configurat i mantingut.

ID 330. Normativa documentada que especifica els deures i obligacions del personal contractat a través d'un tercer

Es disposa de normativa on s'especifiquen els deures i obligacions del personal contractat a través d'un tercer.

ID 460. Protocol d'actuació envers l'incompliment de les obligacions per part del personal tercer

Es disposa d'un procediment que defineix la resolució d'incidents relacionats amb l'incompliment de les obligacions per part del personal del tercer, a més d'identificar a la persona de contacte amb el tercer per a la resolució d'aquest tipus d'incidents.

Barcelona, a 21 d’octubre de 2024

Áurea Alcaide Izquierdo

Cap de Projectes de la Subdirecció d’Operacions del Consorci AOC