



Consorci
Administració Oberta
de Catalunya

**PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA LICITACIÓ DE L'ACORD
MARC PER A L'APROVISIONAMENT DELS SERVEIS, RECURSOS I
INFRAESTRUCTURA DE CLOUD PÚBLIC D'AWS
(EXPEDIENT AOC-2024-01)**

Índex de clàusules i annexos

1.	Introducció	2
2.	Objecte	2
3.	Procés d'homologació	4
4.	Abast	5
5.	Lloc de prestació dels serveis en territori espanyol	8

1. Introducció

El Consorci Administració Oberta de Catalunya (en endavant Consorci AOC), com a organisme públic enfocat a oferir serveis per a la modernització i digitalització de les Administracions Públiques catalanes, disposa des de l'any 2018 d'un catàleg de serveis d'administració electrònica hostatjats al cloud públic. Des d'aleshores ençà, el cloud públic ha esdevingut un element cabdal per al bon funcionament dels serveis de l'AOC per la seva gran capacitat d'escalabilitat i elasticitat, per l'alta fiabilitat i elevat nivell de servei que aporta, per la facilitat per al desenvolupament que ofereix, així com pel control i optimització de costos que proporciona.

El catàleg de serveis del Consorci AOC hostatjats al cloud públic s'anirà incrementant de forma molt significativa en els propers mesos gràcies al procés de transformació digital que el Consorci AOC va encetar l'any 2018 i que ha rebut un fort impuls l'any 2022 amb l'establiment del pla de transformació estratègic 2023-2025, que inclou entre d'altres, la migració al cloud públic l'any 2023 de 6 nous serveis que es desplegaran a AWS. La transformació d'aquests serveis s'està fent d'acord als principis i bones pràctiques del patró de disseny *Re-architect* per convertir-los en serveis de cloud nadius.

El procés de transformació estratègic 2023-2025 està basat en un nou model de gestió global de les plataformes i tecnologies TIC del Consorci AOC, seguint una estratègia manifesta d'evolució i migració dels serveis cap al cloud públic amb un clar full de ruta per millorar l'eficiència i l'eficàcia dels seus serveis gràcies, entre d'altres, a la simplificació i a l'augment de l'eficiència operacional, a l'aplicació d'economies d'escala, a l'obtenció de sinèrgies entre els diferents serveis i a l'optimització dels recursos. L'objectiu principal d'aquest procés de transformació és alinear el nou model TIC amb les necessitats de l'organització i aprofitar les millores tecnològiques presents i futures que ofereix el cloud públic per aconseguir solucions més eficients, flexibles, àgils, robustes i sostenibles.

És important destacar que els contractes que el Consorci AOC té vigents actualment per l'aprovisionament dels serveis de cloud públic d'AWS finalitzen el 31 de desembre de 2023 i que no poden ser prorrogats. Per tal de poder donar continuïtat als serveis que ja estan desplegats a AWS, als 6 nous serveis que ho estaran al llarg del 2023, així com també als nous serveis que s'aniran migrant a AWS fruit del procés de transformació estratègic 2023-2025, el Consorci AOC requereix la licitació d'aquest Acord marc.

Així doncs un dels principals objectius de l'Acord marc és permetre la gestió de l'incessant increment de consum dels serveis d'AWS que el Consorci AOC requerirà al llarg de la durada de l'Acord marc.

2. Objecte

L'objecte de l'Acord marc inclou tota la col·lecció de serveis, recursos i infraestructura d'AWS que són necessaris per a l'execució dels serveis del Consorci Administració Oberta de Catalunya (en endavant Consorci AOC) que estaran allotjats en AWS al llarg de la durada del present Acord marc. És important destacar que els serveis, recursos i infraestructura de cloud públic que es subscriuen a aquest Acord marc són exclusivament els corresponents a AWS. La resta de serveis de cloud públic que el Consorci AOC pugui requerir d'altres hyperscalers (Microsoft Azure, Google Cloud Platform, IBM Cloud, etc.) es vehicularan a través del contracte *SERVEIS D'APROVISIONAMENT I GESTIÓ D'INFRAESTRUCTURA DE CPD DE LA GENERALITAT DE CATALUNYA* EXPEDIENT Núm. CTTI-2023-8 al qual el Consorci AOC està adherit en l'agrupació tecnològica Lot CPD-3.

En el cas d'AWS, el Consorci AOC requereix una licitació pròpia per què actualment té implementada una solució a mida de *Landing Zone* que estableix el marc de treball comú per a tots els serveis que el Consorci AOC té desplegats a AWS. Aquesta *Landing Zone* cobreix diferents àmbits com l'automatització de processos, la governança, les comunicacions segures i confiables amb els 2 CPDs on-premise de l'AOC, la seguretat, el compliment normatiu, el pla de continuïtat del servei, i l'observabilitat. Gràcies a la *Landing Zone* el Consorci AOC pot administrar de forma escalable, eficient, a l'hora que garantint en tot moment el control, les desenes de comptes d'AWS que requereix per al funcionament dels seus serveis.

Tots els serveis del Consorci AOC que estan hostatjats a AWS, i també el 6 nous serveis que ho estaran al llarg del 2023, requereixen per al seu bon funcionament la solució de *Landing Zone* anteriorment esmentada. Actualment, febrer de 2023, AWS no disposa d'una funcionalitat per gestionar sub-organitzacions i/o per implementar múltiples solucions de *Landing Zone* dins una mateixa organització. L'adaptació dels serveis del Consorci AOC desplegats a AWS per funcionar amb la nova *Landing Zone* del CTTI és una tasca complexa que requerirà d'un important esforç. Mentre no es pugui dur a terme aquesta adaptació, el Consorci AOC requereix poder mantenir la seva organització actual amb la configuració de *Landing Zone* que ja té implementada.

Per a la resta de serveis que el Consorci AOC té desplegats en altres proveïdors de cloud públic (com l'Hèstia, el Decidim o la Bústia Ètica que estan allotjats a Microsoft Azure) o per nous serveis que es puguin migrar a altres solucions de cloud públic (el propi Microsoft Azure, Google Cloud Platform, o IBM Cloud), el Consorci AOC no té implementada cap *Landing Zone* pròpia i podrà adaptar-se a la solució de *Landing Zone* corporativa del CTTI.

Tots els serveis de cloud públic que són objecte d'aquest Acord marc es regiran per les clàusules incloses en aquest plec de prescripcions tècniques. Entre aquestes clàusules destaquem que tots els serveis i infraestructura de computació d'AWS que es facin servir hauran d'estar certificats de conformitat amb el nivell alt de l'Esquema Nacional de Seguretat (ENS), hauran d'estar ubicats en territori espanyol i s'hauran d'oferir des de diverses zones de disponibilitat.

L'Acord marc tindrà una durada d'1 any, des del dia 1 de gener de 2024 al 31 de desembre del 2024 ambdós inclosos, i serà prorrogable 1 any més. La prorroga de l'Acord marc es podrà realitzar per mesos i serà d'obligat compliment pel proveïdor homologat sempre que el seu avís es produeixi al menys amb 2 mesos d'antelació a la finalització de la durada de l'Acord marc.

El present document recull els requeriments per homologar, mitjançant procediment obert, el proveïdor per a la prestació dels serveis que són objecte de la licitació.

És important destacar que el present acord marc tindrà un únic adjudicatari que serà l'únic proveïdor homologat per oferir els serveis de cloud públic d'AWS al Consorci AOC. Aquesta condició ve justificada pel fet que en l'actualitat AWS només permet implementar la *Landing Zone* en una única organització, i una organització d'AWS només permet tenir un únic compte de pagament associat a una organització. Per aquest motiu no hi ha cap manera de poder segregar els costos d'infraestructura d'AWS en diversos comptes de pagament i per tant només es pot tenir un únic adjudicatari al qual es pugui vincular el compte de pagament de tota l'organització d'AWS del Consorci AOC.

Posteriorment el Consorci AOC durà a terme la licitació dels contractes basats, dins el marc d'homologació, d'acord a les seves necessitats de provisió de serveis d'AWS per tal de poder assumir la variabilitat dels costos i el pagament per ús implícits al cloud públic. L'adjudicatari dels contractes basats haurà de prestar els serveis d'acord a les condicions i a les clàusules fixades en aquest Acord marc.

L'adjudicatari dels contractes basats haurà de proporcionar al Consorci AOC amb periodicitat mensual els informes de controls de costos que permetin obtenir una visibilitat clara del desglossament de la despesa. Aquests informes hauran d'oferir els detalls dels diferents serveis i

recursos d'AWS consumits i el costos associats. L'objectiu d'aquests informes és permetre al Consorci AOC realitzar el seguiment de l'avanç i el control exhaustiu dels costos, revisant que aquests costos estiguin alineats amb els models previstos i que s'adeqüen a l'estratègia cloud establerta, establint patrons de despesa que permetin inferir i planificar els costos a futur, així com anticipar futures desviacions.

Els informes de control de costos hauran de cobrir diversos aspectes com els costos per servei i plataforma, costos granulars per tipus de recurs, detecció de costos superflus per sobredimensionament, recursos infrautilitzats i propostes d'estalvi, etc.

El Consorci AOC no adquireix però, en cap cas un compromís explícit de despesa mínima dins l'homologació d'aquest Acord marc.

L'Acord marc determinarà un percentatge de descompte mínim que el proveïdor homologat haurà d'aplicar sobre el preu públic fixat pel proveïdor original de cloud públic d'AWS durant tota la durada de l'Acord marc. Aquest descompte serà d'aplicació a la totalitat de serveis, recursos i infraestructura d'AWS consumits pel Consorci AOC, i és un descompte independent i addicional al descompte que ofereixi AWS en funció dels volums de serveis i recursos consumits, en base a les reserves anticipades o compromisos de despesa que es puguin realitzar, o en base al descompte puntual de la modalitat *Spot*.

3. Procés d'homologació

La licitació de l'Acord marc té per objecte l'homologació del proveïdor que haurà de proporcionar al Consorci AOC els serveis de cloud públic d'AWS. Els licitadors podran ser el propi AWS que ofereixi directament els seus serveis de cloud públic o qualsevol distribuïdor autoritzat a oferir aquests serveis.

Els licitadors per la seva banda, si ho estimen oportú, podran nomenar a la seva vegada els distribuïdors que considerin adients com a subcontractistes.

La justificació per homologar un únic proveïdor per proporcionar els serveis de cada cloud públic original és degut als següents motius:

- La concentració dels costos en un únic compte de pagament, ofert a través del proveïdor homologat, permet maximitzar els descomptes que ofereix AWS en funció de les volumetries en els serveis i recursos consumits d'AWS.
- Tots els serveis d'administració electrònica del Consorci AOC desplegats a AWS requereixen d'una infraestructura comú i compartida com pot ser: els elements d'interconnexió amb els 2 data centers del Consorci AOC, els serveis de seguretat perimetral, els serveis d'observabilitat i monitoratge, les eines compartides de governança, etc. El fet de poder oferir aquests serveis de forma centralitzada a través d'un únic proveïdor homologat evita haver de redundar aquests elements amb la corresponent despesa econòmica que això implicaria.
- La gestió de tots els recursos d'AWS des d'una única estructura de comptes comú proporcionada pel proveïdor homologat únic, simplifica enormement l'explotació i el manteniment de tasques com els serveis de backup, el control general de la seguretat, el control efectiu dels costos o l'establiment de les polítiques de governança globals.

El proveïdor homologat haurà de garantir la continuïtat de la prestació dels serveis oferts, o bé hauran de proporcionar d'altres de característiques iguals o superiors, al llarg de la durada de l'Acord marc.

Durant l'etapa de prestació de cada contracte basat, l'adjudicatari serà el responsable de dur a terme les tasques i activitats necessàries per garantir la disponibilitat dels serveis i recursos de cloud públic, així com d'assegurar el compliment dels ANS acordats a nivell de disponibilitat i rendiment d'aquests amb un nivell de suport 24 x 7.

La presentació de les ofertes implica l'acceptació per part dels licitadors de les clàusules d'aquest plec.

4. Abast

L'abast de l'Acord marc inclou tota la col·lecció de serveis, infraestructura, llicències i recursos de cloud públic necessaris per a l'execució dels serveis del Consorci AOC allotjats en AWS al llarg de la durada de l'Acord marc.

El proveïdor homologat haurà de proporcionar els serveis, infraestructura i recursos d'AWS necessaris per als entorns d'integració, reproducció i producció. Aquests 3 entorns s'hauran de segmentar i aïllar per poder funcionar de forma totalment autònoma i independent.

És important destacar que tant les subscripcions com els comptes i identitats del cloud públic necessaris per a la gestió dels entorns d'integració, reproducció i producció del Consorci AOC, hauran de ser de titularitat del Consorci AOC.

El proveïdor homologat haurà de garantir la disponibilitat dels serveis, recursos, llicències i infraestructura d'AWS que s'hauran de proporcionar al Consorci AOC dins l'abast d'aquest Acord marc i que poden ser de la combinació de qualsevol de les següents tipologies:

- Serveis en modalitat IaaS per poder consumir infraestructura bàsica de computació (servidors virtuals amb Amazon EC2), emmagatzemament (volums d'emmagatzematge a nivell de bloc amb Amazon EBS) i serveis virtuals de xarxa (Amazon VPC i tots els serveis i recursos que inclou Amazon VPC com Internet Gateway, NAT Gateway, AWS Transit Gateway, Elastic IP addresses, etc.). El control sobre aquests serveis recau en el Consorci AOC. Els serveis IaaS s'hauran de poder oferir en diferents classes i opcions per optimitzar els seus costos d'acord a les necessitats del Consorci AOC: sota demanda (sense compromís mínim per part del Consorci AOC), amb reserva d'un o 3 anys, o *Spot* (accés puntual sense garanties de disponibilitat).
- Serveis en modalitat PaaS totalment autogestionats i oferts en alta disponibilitat des d'un mínim de 2 zones de disponibilitat. El control sobre aquests serveis, el manteniment, les actualitzacions de seguretat periòdiques, etc. recauen en aquest cas en el proveïdor de cloud públic. Alguns exemples del catàleg de serveis PaaS que requereix el Consorci AOC són:
 - Bases de dades relacionals Amazon RDS: PostgreSQL, Aurora, MySQL, Oracle, SQL Server.
 - Bases de dades NoSQL: Amazon DynamoDB, Amazon DocumentDB, Amazon QLDB
 - Serveis d'anàlisi de dades: Amazon Athena, Amazon Redshift, AWS Lake Formation, Amazon Kinesis Data Analytics
 - Serveis de migració de dades: AWS DMS, AWS SCT, AWS DataSync, AWS Snowball

- Serveis d'extracció, transformació i càrrega de dades (ETL): AWS Glue, Amazon Kinesis Data Firehose
 - Plataforma de processament de Big Data: Amazon EMR
 - Memòria cau de dades d'alt rendiment: Amazon ElastiCache
 - Serveis de cues i agents de missatgeria: AWS SQS, AWS SNS, Amazon MQ, etc.
 - Serveis de transmissió de dades en temps real: Amazon Kinesis Data Streams i Amazon Managed Streaming for Apache Kafka (MSK)
 - Motors de cerca: Amazon Opensearch Service
 - Serveis d'identitat: AWS Cognito
 - Serveis de fitxers NFS: AWS EFS
 - Serveis de balanceig de càrrega: AWS ELB
 - Serveis d'escalat d'aplicacions: AWS Auto Scaling (ASG)
 - Serveis de DNS: Amazon Route 53
 - Serveis d'entrega de continguts (CDN): Amazon CloudFront
 - Serveis d'integració i distribució continua (CI/CD): AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline, AWS CodeStar, AWS CodeArtifact
 - Serveis per a la creació i publicació d'APIs: Amazon API Gateway
 - Serveis per a la custòdia segura de secrets: AWS Secrets Manager, AWS Systems Manager Parameter Store
 - Serveis per a la gestió de claus criptogràfiques: AWS Key Management Service (AWS KMS) i AWS CloudHSM
- Serveis estandarditzats necessaris per a l'execució de contenidors Linux a través d'una plataforma d'orquestració de contenidors que ofereixi l'automatització de l'aprovisionament, el desplegament, l'escalat, l'administració, la restauració, i l'execució consistent i fiable dels contenidors: Amazon ECS i Amazon EKS. Aquestes plataformes de contenidors hauran d'estar equipades amb totes les capacitats de computació, comunicacions, emmagatzematge i seguretat totalment integrades per oferir una arquitectura de desenvolupament basada en microserveis.
 - Serveis d'emmagatzematge segur d'objectes, Amazon S3 i Amazon S3 Glacier, amb alta escalabilitat, disponibilitat de dades, durabilitat, seguretat i rendiment. Aquests serveis d'emmagatzematge d'objectes s'hauran de poder oferir en diferents modalitats, varietats de classes i nivells d'accés per optimitzar els costos en funció dels patrons d'accés o dels diferents casos d'ús a implementar.
 - Serveis de computació sense servidor basats en events per a l'execució de codi amb un nivell d'escalabilitat molt alt sense necessitat d'aprovisionament o administració de servidors: AWS Lambda.
 - Serveis d'interconnectivitat i comunicacions que permetin establir una arquitectura de cloud híbrida segura i fiable entre el CPD on-premise d'AOC, el cloud privat d'AOC i AWS: AWS Direct Connect i AWS Site-to-Site VPN.
 - Eines de tipus SIEM i SOAR per a l'administració d'events d'informació de seguretat i resposta automatitzada de seguretat. Aquestes eines hauran de monitoritzar de forma continua l'activitat de la xarxa, els patrons d'accés a les dades i el comportament del cloud públic amb l'objectiu de permetre la detecció integral i la prioritització de tot tipus d'activitat maliciosa (accessos indeguts, canvis en les polítiques de seguretat, accessos inusuals de dades, etc.), però també hauran de realitzar una cerca proactiva per donar resposta a altres tipus de possibles amenaces i hauran de proporcionar les alertes i informes d'incidents de seguretat.

Les eines de tipus SIEM i SOAR seleccionades hauran d'ingerir dades de diferents orígens i hauran d'analitzar la correlació entre aquests orígens de dades per oferir una resposta intel·ligent que permeti una detecció d'amenaques proactiva.

- Eines de seguretat avançades que permetin establir un perímetre de seguretat amb diverses línies de defensa que protegeixin tots els recursos i serveis desplegats dins el cloud públic:
 - Protecció perimetral davant d'atacs per provocar indisponibilitat del servei tipus DDoS: AWS Shield Advanced)
 - Protecció amb una solució de tipus IDS/IPS davant intents d'intrusió a serveis frontals: AWS Network Firewall
 - Protecció amb una solució de tipus Web Application Firewall que eviti l'explotació de vulnerabilitats de tipus injecció d'SQL, Cross-site scripting, etc. recollides en el conjunt de normes CRS 3 de l'OWASP: AWS WAF
- Solució d'antivirus i antimalware integrada amb el servei d'emmagatzematge d'objectes que ofereixi protecció davant virus, troians i altres tipus de programari maliciós amb resposta automatitzada per esborrar, etiquetar o posar en quarantena els documents infectats: bucketAV for Amazon S3. Aquesta solució d'antivirus haurà d'estar permanentment actualitzada i haurà d'integrar-se amb les eines SIEM i SOAR per generar les alertes corresponents.
- Sistema d'observabilitat que reculli els logs dels diferents sistemes, dispositius, serveis i aplicacions. Aquest sistema d'observabilitat ha de permetre el filtratge i ordenació dels registres de log per diferents criteris o categories i ha d'oferir funcionalitats d'anàlisi avançades.
El sistema d'auditoria ha de garantir la integritat, immutabilitat i la possibilitat de verificació mitjançant criptografia de tots els logs enregistrats.
- AWS Backup: sistema de backup integral i automatitzable per cobrir tots els tipus de dades, infraestructura, o qualsevol element específic, inclosos en les diferents solucions de cloud públic que són objecte d'aquest Acord marc. Tots els components de la solució de backup hauran d'estar xifrats i hauran de complir els requeriments que defineix l'ENS en l'àmbit dels backups. La solució de backup ha de poder oferir diferents polítiques de retenció d'acord a les pautes determinades pel Consorci AOC (p. ex. backup diari incremental i backup complet setmanal amb 2 setmanes de retenció). Un altre requeriment que haurà de complir la solució de backup és disposar de funcionalitats de backup offline amb la possibilitat fins i tot d'hostatjar aquest backup offline en un altre cloud públic o en el propi CPD del Consorci AOC (backup off-site).
- AWS Business Support com a pla de suport de nivell empresarial que ha de permetre al Consorci AOC rebre assistència per part d'AWS en cas d'incident amb algun dels seus serveis.

Un dels objectius fonamentals que persegueix el Consorci AOC amb aquest Acord marc és assolir un alt grau d'agilitat, flexibilitat i adaptabilitat en el consum dels recursos IT, però sense haver de sobredimensionar aquests recursos ni tampoc haver d'aprovisionar-los amb antelació.

Dins l'abast d'aquest contracte s'ha d'incloure tota la infraestructura, serveis i recursos de cloud públic descrits anteriorment, però a mida que es vagi avançant en el procés de transformació digital del nou model TIC serà necessari incrementar aquest catàleg de serveis i recursos. D'aquesta forma és important ressaltar que potencialment el Consorci AOC podrà requerir i consumir qualsevol servei o recurs de cloud públic que AWS ofereixi en els seus catàlegs actuals o futurs.

Els costos dels contractes basats es facturaran amb periodicitat mensual i en tots els casos l'import de la factura s'haurà d'emetre exclusivament en €.

Dins de l'abast de serveis del Consorci AOC coberts per aquest contracte, hi ha serveis que el Consorci ha categoritzat en nivell ALT a nivell de seguretat amb la metodologia de l'Esquema Nacional de Seguretat. El proveïdor haurà de revisar que tots els serveis i recursos dels que es faci ús dins de la infraestructura estaran certificats en l'Esquema Nacional de Seguretat en nivell ALT. El proveïdor haurà d'informar al Consorci AOC en el cas de que algun recurs no ho estigui per a que el Consorci AOC valori el riscs d'afegir-lo a la infraestructura.

5. Lloc de prestació dels serveis en territori espanyol

El Consorci AOC proveeix, per encàrrec de la Generalitat de Catalunya, el servei d'identificació i signatura idCAT Mòbil. L'idCAT Mòbil és un sistema d'identificació i signatura dels previstos a la lletra c dels articles 9 i 10 de Llei 39/2015 del procediment administratiu comú.

Per a la provisió de l'idCAT Mòbil el Consorci AOC, tal i com es preveu el l'AIPD que va elaborar el Departament de Vicepresidència i d'Economia i Hisenda de la Generalitat de Catalunya en data 17 de desembre 2020, recull la dada biomètrica imatge que té la consideració de categoria especial de dades de conformitat amb l'establert a l'article 9 del Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE.

Els articles 9 i 10 de la Llei 39/2015 en el seu apartat tercer disposa, en relació als sistemes d'identificació i signatura previstos a la lletra c dels articles 9 i 10, que com s'ha dit comprèn l'idCAT Mòbil, la *"obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español."*

Per aquest motiu tant el propi servei idCAT Mòbil com el servei DESA'L que és on s'allotjaran aquests vídeos d'identificació, com qualsevol altre servei del Consorci AOC que allotgi o processi aquestes dades (p. ex. el servei DESA'L) hauran d'estar ubicats a la seva vegada en territori espanyol.

Està previst que els vídeos d'identificació de l'idCAT Mòbil es guardin al servei DESA'L i és per aquest motiu que el Consorci AOC limitarà l'ús de tots els serveis d'AWS a la regió d'Espanya.

Barcelona, 03 d'Agost de 2023

Sergio Gutiérrez Palomino
Responsable Unitat d'Arquitectura Consorci AOC