

PLEC DE PRESCRIPCIONS TÈCNIQUES

QUE HA DE REGIR EL CONTRACTE RELATIU A LA

"220DIV490902 RENOVACIÓ DELS ENTORNS MIDDLEWARE: SUBSTITUCIÓ DE FUSE"

EXPEDIENT: AB/2026/088

PROCEDIMENT OBERT

CONTINGUT

1. INTRODUCCIÓ	4
2. CONTEXT	4
3. ABAST	5
3.1. Objectius i abast inclosos	5
3.2. Aspectes fora de l'abast	9
4. AS-IS	11
4.1. Arquitectura tecnològica actual	11
4.2. Inventari d'integracions i serveis	11
4.3. Protocols i tecnologies utilitzades	13
4.4. Inventari d'integracions	13
4.4.1. FIRMADIGITAL-AB-CONNECT	14
4.4.2. SICAB-ACUA-CONNECT	15
4.4.3. SWIFT-CONNECT	15
4.4.4. AFECTACIÓ-SIEBEL-CM-CONNECT	16
4.4.5. CM-MAIL-CONNECT	17
4.4.6. EDP-CONNECT	18
4.4.7. GUILBERT-AB-CONNECT	18
4.4.8. INDICADORES-CALIDAD-SIEBEL-MDM-CONNECT	19
4.4.9. LIMS-SAP-CONNECT (RFC)	20
4.4.10. META4SAPPR5 (IDOC)	20
4.4.11. OFEXPAGOTARJETA-CONNECT	21
4.4.12. SAP-NEPTUNO-CONNECT	21
4.4.13. CM-DOWNLOAD-CONNECT	22
4.4.14. FACTURA RECTIFICA	23
4.4.15. MONITORING-AB	23
4.4.16. CM-SICAB-CONNECT	24
4.4.17. DIGI-CONNECT	25
4.4.18. LIMS-SENTINEL-CONNECT	25
4.4.19. OFEX-SIEBEL-MDM-CONNECT	26
4.4.20. AB-SICAB-CONNECT	26
4.4.21. AGM-SICCO-CONNECT	27
4.4.22. AQMOSSIGEDA-CONNECT	27
4.4.23. AQMOSSIGEDA2-CONNECT	28
4.4.24. PENDINGS-INTERFACE → CARTAS IMPAGO	28
4.4.25. PENDINGS-INTERFACE → CARTAS IMPAGO NEXEA	29
4.4.26. PENDINGS-INTERFACE → CARTAS IMPAGO BFS	29
4.4.27. SAP-META4-CONNECT	30
4.4.28. SAP-XRT-AB-CONNECT	30
4.4.29. TOPKAPI-CONNECT (EXPORT)	31
4.4.30. TOPKAPI-CONNECT (DADES PUNTUALS)	31
4.4.31. TOPKAPI-CONNECT (DADES MITJANES)	32
4.4.32. LIMS-SFTP-CONNECT	32

4.4.33. SAP-DOP-CONNECT	33
4.4.34. SAP-SEQUERA-CONNECT	33
4.4.35. AKWAMETRICS-CONNECT (EXPORT)	34
4.4.36. AKWAMETRICS -CONNECT (DADES PUNTUALS)	34
4.4.37. AKWAMETRICS -CONNECT (DADES MITJANES)	35
4.4.38. WATER_QUALITY	35
4.4.39. SIGAB_CONNECT	36
4.4.40. XML-MAIL-CONNECT	36
5. ARQUITECTURA TO-BE	37
5.1. Arquitectura Objectiu	37
5.2. Arquitectura de referència per capes	38
Capa d'orquestració	38
Capa d'exposició i interoperabilitat (API Layer)	39
Capa d'integració funcional i processament	39
Capa de missatgeria i streaming	41
Capa de persistència i staging	41
Capa d'integració SAP	42
Capa d'observabilitat i monitorització	43
Capa de Govern i DevOps	43
Capa de seguretat	44
6. CONSIDERACIONS ESPECÍFIQUES DEL DISSENY	46
7. FASES DEL PROJECTE	47
Fase 0 – Kickoff i Govern del Projecte	47
Fase 1 – Discovery/Anàlisi	47
Fase 2 – Pla de Migració	48
Fase 3 – Arquitectura TO-BE	49
Fase 4 – Migració	49
Fase 5 – Validació i cutover	49
Fase 6 – Desconnexió de Red Hat Fuse	50
8. METODOLOGIA DEL PROJECTE	50
9. REQUISITS DEL LICITADOR	51
9.1. Experiència i capacitat tècnica	51
9.2. Equip de projecte	51
10. GARANTIA	53
11. SUPORT AUDITORIA DE SEGURETAT	53
12. ALTRES REQUERIMENTS	54
12.1. Ubicació i modalitat de treball	54
12.2. Recursos materials requerits	54
12.3. Eines de seguiment i gestió del projecte	54
12.4. Acords de Nivell de Servei (ANS) durante el Projecte	55
12.5. Penalitzacions derivades del incompliment en ANS Projecte	58
12.6. Accés	59
13. SEGURETAT CORPORATIVA	60
14. ANNEX NÚM. 1 - CLASSIFICACIÓ DE LES INCIDÈNCIES	61
15. ANNEX NÚM. 2 - NORMES DE SEGURETAT IT D'AIGÜES DE BARCELONA	64

1. INTRODUCCIÓ

Aigües de Barcelona opera actualment una plataforma corporativa d'integració basada en Red Hat Fuse, sustentada sobre el framework Apache Camel, que ha actuat durant els darrers anys com a component central per al desenvolupament, desplegament i operació de serveis d'interoperabilitat entre múltiples sistemes corporatius i processos crítics de negoci. Aquesta plataforma ha constituït fins ara el nucli del model d'integració corporativa de l'organització, donant suport a fluxos essencials per a la continuïtat operativa de diferents àmbits funcionals.

En aquest context, Aigües de Barcelona impulsa un procés de modernització tecnològica orientat a la substitució progressiva de la plataforma actual per un nou model d'integració més modern, robust, escalable i alineat amb els estàndards arquitectònics i tecnològics corporatius vigents. Aquesta iniciativa respon tant a la necessitat de mitigar els riscos derivats de l'obsolescència de la solució actual com a l'oportunitat d'evolucionar cap a un model d'integració desacoblat, governat i preparat per donar resposta a les necessitats presents i futures de l'organització.

El present Plec de Prescripcions Tècniques té per objecte definir els requisits funcionals, tècnics, arquitectònics, operatius i organitzatius que regiran la contractació dels serveis necessaris per dur a terme la transformació de la plataforma corporativa d'integració. Així mateix, estableix el marc de referència que haurà de respectar la solució proposada, incloent-hi els principis arquitectònics, estàndards tecnològics, requisits de seguretat, model operatiu i criteris d'integració alineats amb l'estratègia tecnològica corporativa d'Aigües de Barcelona.

En aquest context, el present plec defineix una orientació tecnològica preferent basada en el stack corporatiu existent i en els principis d'arquitectura establerts per l'organització, amb l'objectiu de garantir coherència tecnològica, sostenibilitat operativa, governança tècnica i una integració efectiva dins l'ecosistema tecnològic actual i futur d'Aigües de Barcelona.

La solució proposada per l'adjudicatari haurà d'alinejar-se amb el marc arquitectònic, tecnològic i operatiu definit per Aigües de Barcelona en el present plec. Excepcionalment, es podran considerar propostes alternatives o millores específiques, sempre que aquestes estiguin degudament motivades, acreditin un benefici tècnic objectiu, no suposin una desviació respecte dels principis rectors establerts ni comprometin la coherència, sostenibilitat o governança de la solució, i siguin expressament aprovades per Aigües de Barcelona.

2. CONTEXT

Aigües de Barcelona disposa actualment d'una plataforma corporativa d'integració que dona suport a la interoperabilitat entre múltiples sistemes corporatius i processos de negoci crítics, constituint una peça rellevant dins l'ecosistema tecnològic de l'organització.

L'evolució del context tecnològic, els nous requeriments d'integració i la necessitat d'alinejar el model actual amb els estàndards arquitectònics corporatius fan necessari abordar un procés de modernització de la plataforma actual, evolucionant cap a un model més modern, flexible, escalable i sostenible.

En aquest sentit, el model actual presenta limitacions inherents pròpies d'arquitectures centralitzades de middleware tradicional, especialment pel que fa a desacoblament entre sistemes, escalabilitat independent dels components, observabilitat transversal, mantenibilitat operativa i capacitat d'adaptació davant noves necessitats d'integració o evolució dels sistemes corporatius.

Adicionalment, Aigües de Barcelona es troba immersa en un procés continu d'evolució tecnològica i transformació del seu ecosistema aplicatiu, incloent iniciatives de modernització i migració de diferents plataformes i sistemes corporatius cap a nous models tecnològics, fet que requereix disposar d'una arquitectura d'integració preparada per adaptar-se de forma progressiva, controlada i coherent amb aquesta evolució.

En aquest context, la present contractació té per objectiu executar la transformació progressiva del model actual cap a una nova arquitectura d'integració alineada amb l'estratègia tecnològica corporativa d'Aigües de Barcelona, basada en principis d'arquitectura distribuïda, desacoblament funcional, automatització operativa, seguretat per disseny, observabilitat integral i ús preferent de l'ecosistema tecnològic corporatiu definit per l'organització.

Aquest procés no respon exclusivament a una necessitat de renovació tecnològica, sinó també a una decisió estratègica orientada a simplificar l'operació, reduir dependències arquitectòniques, millorar la governança tècnica i establir un model d'integració sostenible a llarg termini, alineat amb les necessitats actuals i futures de l'organització.

3. ABAST

El projecte de modernització de la plataforma d'integració té per objecte la desconexió ordenada de Red Hat Fuse i la seva substitució progressiva per una arquitectura distribuïda, resilient i cloud-native.

A continuació, es detallen els objectius i l'abast que s'hauran de contemplar dins del projecte, així com els elements i les actuacions que queden expressament fora del perímetre d'aquest projecte:

3.1. Objectius i abast inclosos

- **Desconnexió de Red Hat Fuse**

La retirada de Red Hat Fuse s'ha de fer de manera ordenada, identificant totes les dependències tècniques i funcionals que hi ha entre les integracions existents. Aquest objectiu implica no només migrar les integracions, sinó també eliminar completament els acoblaments que s'hagin pogut generar entre sistemes, permetent que cada integració sigui independent i tolerant a fallades, sense afectar la resta de processos. Cal incloure documentació exhaustiva de totes les decisions preses durant la migració, de manera que s'estableixi un precedent per a migracions futures de plataformes.

- **Migració íntegra de totes les integracions**

En el moment de redacció del present plec, s'han identificat un total de 40 integracions actives incloses dins l'abast del projecte, les quals hauran de ser objecte d'anàlisi, transformació i migració cap a l'arquitectura objectiu definida per Aigües de Barcelona.

Per a cadascuna d'aquestes integracions, l'adjudicatari haurà de dur a terme les activitats necessàries de descoberta, anàlisi funcional i tècnica, disseny, desenvolupament, proves, validació i posada en producció, d'acord amb els principis arquitectònics, criteris tècnics i model operatiu establerts en el present plec.

L'adjudicatari haurà de definir, com a part del Pla de Migració, l'estratègia específica aplicable a cada integració o conjunt d'integracions, incloent-ne la classificació segons criticitat, complexitat, dependències, patró tècnic de migració, estratègia de coexistència, mecanismes de validació i criteris de transició cap a producció.

El llistat d'integracions inclòs en aquest plec representa l'escenari conegut en el moment de la seva elaboració i podrà estar subjecte a ajustos derivats de l'evolució de l'ecosistema tecnològic o de les conclusions obtingudes durant les fases inicials d'anàlisi i discovery, dins del marc contractual establert.

- **Validació funcional**

L'adjudicatari haurà de garantir la migració completa d'aquestes integracions mantenint en tots els casos equivalència funcional exacta respecte al comportament actual a la plataforma Red Hat Fuse, respectant en la mesura que sigui possible els contractes existents entre sistemes. Això implica que cada integració haurà de reproduir els mateixos resultats funcionals, amb nivells de servei equivalents o superiors en termes de rendiment, temps de resposta, estabilitat i confiança.

La validació de cada integració constitueix una fita obligatòria prèvia a la posada en producció i s'ha de fer conjuntament amb els responsables funcionals i tècnics dels sistemes implicats. No es podrà executar el cutover ni procedir a la 'desconnexió' de la integració equivalent a Red Hat Fuse fins que aquesta validació hagi estat completada i acceptada formalment per l'equip d'Aigües de Barcelona.

- **Garantia de continuïtat operacional**

L'execució del projecte haurà de garantir, en tot moment, la continuïtat operativa dels serveis d'integració i minimitzar qualsevol impacte sobre els processos de negoci suportats.

A aquest efecte, l'adjudicatari haurà de definir i executar una estratègia de migració progressiva i coexistència controlada entre la plataforma actual i l'arquitectura objectiu, de manera que es permeti una transició ordenada, segura i amb risc operatiu controlat.

El procés de migració no podrà plantejar-se mitjançant un model de substitució massiva o Big Bang, sinó a través d'un enfocament incremental, amb migracions planificades per integració, conjunt d'integracions o onades de migració, segons la criticitat, dependències i impacte operatiu associat.

Cada transició a producció (cutover) haurà d'estar degudament planificada, coordinada i consensuada amb Aigües de Barcelona, incloent finestres de canvi adequades, validacions prèvies, mecanismes de verificació posteriors a la posada en servei i plans de contingència i rollback que permetin revertir els canvis de forma controlada en cas d'incidència o comportament no esperat.

L'adjudicatari serà responsable de definir les mesures tècniques, organitzatives i operatives necessàries per garantir una migració sense afectació no planificada sobre els serveis existents, assegurant la integritat dels fluxos, la consistència operativa i la continuïtat dels processos durant tot el període de transició.

- **Evolució controlada i optimització tècnica de les integracions**

La migració objecte del present projecte no s'haurà d'abordar com una mera conversió tècnica entre plataformes, sinó com un procés d'evolució controlada de les integracions actuals cap a un model més robust, mantenible, desacoblat i alineat amb els principis de l'arquitectura objectiu definida per Aigües de Barcelona.

L'objectiu del projecte no és únicament reproduir els fluxos existents sobre una nova plataforma, sinó aprofitar el procés de transformació per incorporar aquelles millores tècniques que aportin valor objectiu en termes de desacoblament funcional, idempotència, resiliència, observabilitat, traçabilitat, mantenibilitat i sostenibilitat operativa, sempre sota criteris de proporcionalitat, baix impacte funcional i alt valor tècnic.

Caldrà considerar expressament aquelles integracions que, per decisió d'Aigües de Barcelona i segons el model arquitectònic definit en el present plec, hagin d'evolucionar cap a un model d'aplicacions independents o components desacoblats, desplegats sobre les tecnologies corporatives establertes, quan la seva naturalesa funcional, complexitat tècnica, criticitat operativa o necessitat d'evolució futura així ho justifiquin.

De la mateixa manera, l'adjudicatari podrà proposar, durant les fases d'anàlisi i definició de la migració, l'evolució d'altres integracions cap a patrons arquitectònics diferents dels inicialment previstos, sempre que aquesta transformació aportí un benefici tècnic clar, estigui degudament justificada, no impliqui desviacions funcionals no autoritzades, no alteri de forma significativa l'abast contractual ni el calendari compromès, i sigui expressament validada per Aigües de Barcelona.

Aquest enfocament haurà de permetre compatibilitzar la preservació funcional dels processos existents amb una modernització pragmàtica del model d'integració, evitant tant una reproducció crítica de limitacions heretades com una reenginyeria funcional innecessària.

- **Configuració de monitorització i observabilitat**

L'adjudicatari haurà d'implantar un model de monitorització i observabilitat end-to-end que cobreixi de forma homogènia la totalitat dels fluxos d'integració. La solució haurà de centralitzar logs, mètriques i traces a Azure Monitor i Log Analytics, establint un model comú d'observabilitat que permeti correlacionar esdeveniments extrem a extrem mitjançant identificadors únics de traçabilitat, garantint visibilitat completa del cicle d'execució de cada integració.

Aquest model haurà de contemplar la definició i normalització d'un esquema estàndard de logging i traçabilitat per a tota la plataforma, incloent-hi correlation IDs, timestamps, nivells de severitat, context tècnic i context de negoci, de manera que permeti un diagnòstic unificat i consistent amb independència del component executor. Així mateix, cal capturar mètriques tècniques i funcionals de rendiment, disponibilitat, latència, errors i compliment de SLA, així com traces distribuïdes que permetin reconstruir el flux complet d'una transacció a través de tots els seus components i dependències.

- **Quadre de comandament**

La solució haurà d'incorporar un quadre de comandament unificat a Grafana com a punt central de supervisió operativa, alimentat per les dades consolidades a Azure Log Analytics, que permeti visualitzar l'estat global de les integracions, el detall per integració i la salut de cada component

tècnic. Aquest panell haurà d'incloure indicadors agregats i/o segmentats per aplicació, flux, tecnologia, criticitat i protocol, facilitant la detecció primerenca d'incidències, degradacions i patrons anòmals de comportament incloent la parametrització de llindars, regles d'activació i criteris de classificació visual mitjançant semàfor d'estats. Aquest model haurà d'establir de forma consensuada amb Aigües de Barcelona les condicions objectives sota les quals una integració, component o flux haurà de considerar-se en estat verd, groc o vermell, així com els mecanismes d'escalat i notificació associats a cada nivell de severitat.

- **Documentació tècnica i operacional**

L'adjudicatari haurà d'elaborar i mantenir actualitzada la documentació tècnica i operativa associada a la solució, incloent-hi com a mínim l'arquitectura de referència, les especificacions funcionals i tècniques de cada integració, les configuracions parametritzades, els procediments de desplegament, els runbooks operatius, les guies de troubleshooting i la matriu de responsabilitats.

Així mateix, cal generar un catàleg unificat d'integracions que actuï com a repositori de referència de la plataforma, incorporant per a cada flux la seva descripció funcional, sistemes implicats, dependències tècniques i operatives, paràmetres d'execució, SLAs associats si n'hi hagués i un diagrama end-to-end que representi de forma clara el procés complet i les seves interaccions. Aquest catàleg servirà com a referència per a futures integracions i assegurarà consistència a tota la plataforma.

- **Pla de desconnexió**

El Pla de Migració haurà d'incloure una estratègia ordenada d'apagat de la plataforma actual una vegada totes les integracions s'hagin migrat. Això inclou la identificació d'integracions crítiques, la planificació de la desactivació per fases, la validació d'equivalència funcional i la certificació de cutover.

- **Traspàs**

L'equip de l'adjudicatari haurà de garantir la transferència efectiva de coneixement a l'equip d'Aigües de Barcelona mitjançant sessions estructurades de mentoring, shadowing, pair programming i formació pràctica, orientades a consolidar el coneixement funcional, tècnic i operatiu necessari per a la futura gestió de l'entorn conforme es traspassen les integracions a la nova plataforma objectiu. Així mateix, l'adjudicatari haurà de coordinar sessions de traspàs amb el servei actual, amb l'objectiu de capturar coneixement implícit, dependències no documentades i consideracions operatives rellevants de la plataforma existent. L'objectiu final serà garantir que, en acabar el projecte, l'equip d'Aigües de Barcelona disposi de l'autonomia necessària per operar, mantenir i evolucionar la nova solució amb plenes garanties.

3.2. Aspectes fora de l'abast

- **Restriccions sobre plataformes i eines d'integració**

Aigües de Barcelona no contempla, dins l'abast del present projecte, la implantació de noves plataformes d'integració de tercers ni l'adopció de solucions iPaaS propietàries alienes a l'ecosistema tecnològic definit per l'organització, com ara Dell Boomi, MuleSoft o altres de naturalesa equivalent.

En conseqüència, no s'acceptaran propostes que basen la solució en la incorporació d'aquest tipus de plataformes com a nucli del model d'integració objectiu, ni aquelles que introdueixin dependències tecnològiques addicionals no alineades amb el patró arquitectònic establert al present plec. Qualsevol proposta que s'aparti d'aquest marc serà considerada fora d'abast, llevat del requeriment exprés o de la justificació excepcional prèviament validada per Aigües de Barcelona.

- **Migració d'aplicacions**

L'abast del present projecte es limita exclusivament a la modernització, transformació i migració de la capa d'integració corporativa, d'acord amb el model arquitectònic objectiu i els principis tècnics definits en el present plec.

En conseqüència, no formen part de l'abast del projecte la migració, substitució, transformació o reenginyeria funcional dels sistemes origen i/o destí que actualment participen en els fluxos d'integració, els quals continuaran essent responsabilitat dels seus respectius equips o àmbits funcionals.

L'adjudicatari haurà d'adaptar les integracions existents al nou model tecnològic i arquitectònic establert per Aigües de Barcelona, incloent la transformació dels mecanismes d'interoperabilitat, desacoblament, orquestració, exposició de serveis o execució funcional que resultin necessaris dins de la pròpia capa d'integració.

Excepcionalment, podran contemplar-se adaptacions tècniques puntuals i acotades sobre sistemes origen o destí, únicament quan aquestes siguin estrictament necessàries per garantir la correcta continuïtat operativa de les integracions, la compatibilitat amb la nova arquitectura o l'execució tècnica de la migració, i sempre que aquestes actuacions siguin expressament validades i consensuades amb Aigües de Barcelona dins del marc del projecte.

- **Reenginyeria**

La migració tindrà caràcter principalment tècnic i no funcional, per tant, el projecte no contempla una reenginyeria dels processos ni la transformació dels patrons d'integració existents. Com a principi general, les integracions hauran de mantenir la seva lògica de negoci, comportament funcional i contractes actuals entre sistemes, llevat dels casos en què Aigües de Barcelona hagi sol·licitat expressament la seva evolució.

Es valorarà positivament que l'adjudicatari proposi certs ajustos tècnics o millores puntuals sobre els mecanismes d'integració, així com adaptacions acotades en origen i/o destí, sempre que no alterin la funcionalitat del procés, aportin una millora objectiva i puguin executar-se dins de l'abast i termini del projecte, sense impacte en la seva planificació i ampliació de cost. Qualsevol ajustament d'aquest tipus haurà de ser consensuat prèviament amb Aigües de Barcelona i incorporat de forma controlada al Pla de Migració.

- **Infraestructura de xarxa**

Es considera com a premissa de partida que la infraestructura base de xarxa, seguretat i connectivitat necessària per suportar la solució objectiu serà existent o proveïda per Aigües de Barcelona, a través dels seus equips d'arquitectura, infraestructura i seguretat.

No obstant això, serà responsabilitat de l'adjudicatari identificar, definir i documentar els requisits tècnics de connectivitat necessaris per a cada integració, component o flux objecte del projecte, així com col·laborar activament amb els equips responsables d'Aigües de Barcelona en la seva validació, coordinació i verificació, amb l'objectiu de garantir que les comunicacions entre sistemes, serveis i components quedin correctament habilitades per a l'execució de la solució proposada.

Aquesta col·laboració inclourà, quan sigui necessari, la definició de requisits de comunicació, protocols, ports, resolució de noms, patrons d'accés, dependències de xarxa i qualsevol altre condicionant tècnic necessari per assegurar la correcta connectivitat entre els diferents elements de l'arquitectura.

- **Aprovisionament i desplegament de recursos a Azure**

L'aprovisionament i el desplegament dels recursos necessaris a Azure no forma part de l'abast directe de l'adjudicatari. Aquestes activitats seran responsabilitat dels equips d'arquitectura, infraestructura i DevOps d'Aigües de Barcelona, que seran els encarregats de proveir i habilitar els serveis, els recursos i els components necessaris per donar suport a la solució dins el marc tecnològic corporatiu definit.

L'adjudicatari haurà d'identificar, definir i documentar de forma anticipada tots els requisits tècnics, dependències i necessitats d'infraestructura associades a cada migració, amb el nivell de detall suficient per permetre la correcta provisió per part d'Aigües de Barcelona, així com mantenir-se alineat per col·laborar amb els diferents equips en la resolució de dubtes, validació de configuracions i suport tècnic durant les tasques de provisió.

Aquesta informació haurà d'incorporar-se al Pla de Migració, incloent per a cada integració els prerequisits tècnics, recursos requerits, configuracions necessàries, dependències de connectivitat, consideracions de desplegament i qualsevol altre condicionant necessari per a la seva correcta execució.

- **Llicències**

Com a principi general, la solució haurà de prioritzar l'ús de serveis nadius d'Azure i tecnologies open source àmpliament consolidades i contrastades al mercat, minimitzant la necessitat d'incorporar components subjectes a llicenciament addicional.

No obstant, en aquells casos en què, per motius tècnics degudament justificats, resulti necessària l'adquisició de llicències per garantir el funcionament correcte de la solució en producció, aquesta necessitat haurà de ser identificada i argumentada prèviament per l'adjudicatari, i consensuada de forma expressa amb Aigües de Barcelona amb caràcter previ a la seva adopció. En aquest cas, l'adquisició de les llicències esmentades correspondrà a Aigües de Barcelona.

En cap cas no es considera inclòs en aquest supòsit el llicenciament associat a eines, entorns o components que l'adjudicatari requereixi per als seus propis processos de desenvolupament, construcció, proves o execució del servei.

4. AS-IS

4.1. Arquitectura tecnològica actual

La plataforma actual Red Hat Fuse es fonamenta en el framework Apache Camel com a motor principal per a la definició de rutes d'integració, orquestració de processos i execució de la lògica funcional associada a la interoperabilitat entre sistemes. Sobre aquesta base, s'utilitzen diversos components de l'ecosistema Red Hat Fuse per proporcionar capacitats de missatgeria, exposició de serveis, transformació de missatges, gestió de protocols i connectivitat amb aplicacions corporatives i sistemes externs.

Entre els principals components utilitzats destaquen:

- **Apache Camel** : motor d'integració basat en patrons d'integració empresarial per a la implementació de fluxos i transformacions.
- **Apache CXF** : framework per a l'exposició i el consum de serveis web (SOAP/REST).
- **Apache ActiveMQ** : sistema de missatgeria utilitzat per a la comunicació asíncrona entre aplicacions.

La versió actualment desplegada de la plataforma és:

- **Versió de Fuse:** 2.9.2
- **Model de desplegament:** On-premise - 3 servidors en configuració de clúster d'alta disponibilitat
- **Balancejador de càrrega:** Encarregat de distribuir les peticions entre els nodes.
- **Entorns** : Dev-Pre-Pro
- **Sistema operatiu:** Red Hat Enterprise Linux 7.7
- **Segmentació i seguretat de xarxa corporativa:**
 - Mecanismes de control d'accés i aïllament entre entorns, sistemes i xarxes.
 - Trànsit controlat entre segments lògics diferenciats, xarxes internes i zones d'exposició.

4.2. Inventari d'integracions i serveis

La plataforma actual d'integració basada en Red Hat Fuse dona suport, en el moment de redacció del present plec, a un total de 40 integracions actives que connecten 21 aplicacions corporatives diferents, amb casuístiques funcionals i tècniques heterogènies quant a protocols, criticitat, dependències i complexitat d'implementació.

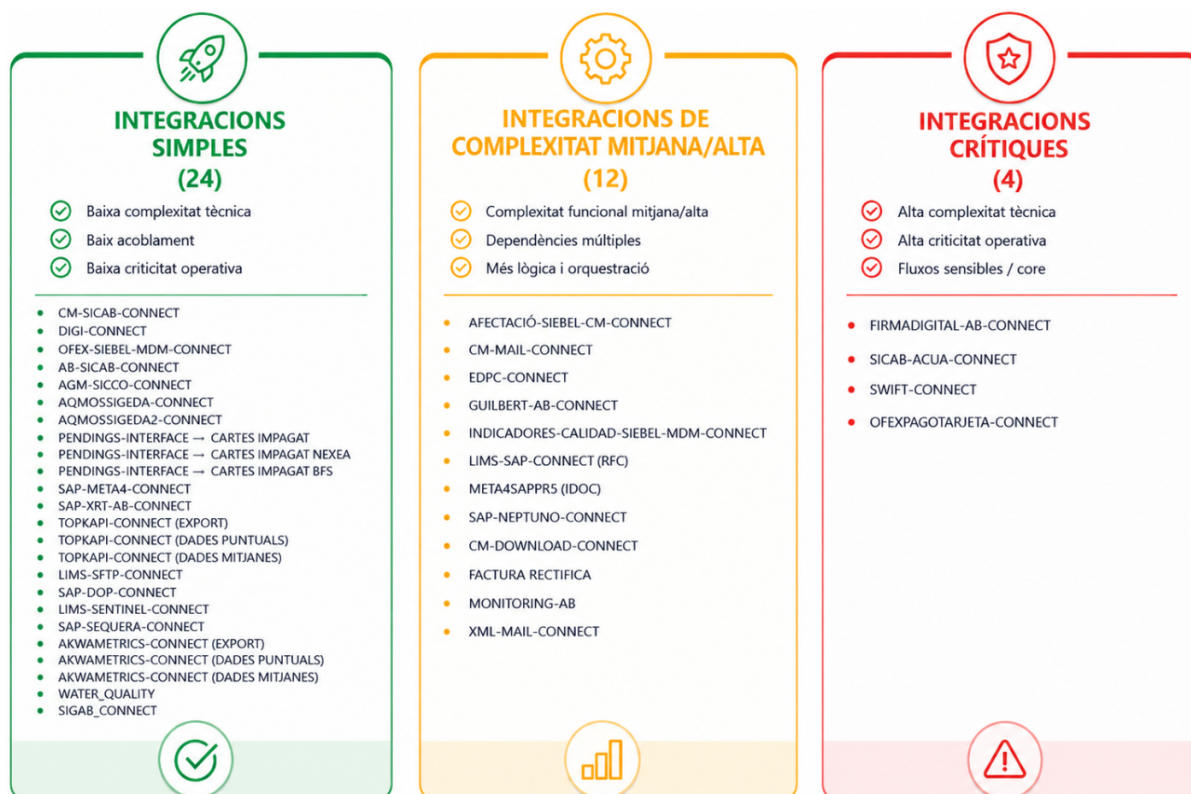
Amb l'objectiu de facilitar la comprensió del context i permetre als licitadors dimensionar adequadament l'abast i l'esforç associat a la proposta, Aigües de Barcelona ha dut a terme una anàlisi preliminar interna de l'ecosistema actual, basada en la revisió tècnica del codi font, configuracions existents, artefactes de la plataforma i coneixement funcional disponible.

Com a resultat d'aquesta anàlisi preliminar, les integracions han estat classificades internament, amb caràcter orientatiu, en les següents categories:

- **Integracions simples**, corresponents a fluxos amb menor complexitat tècnica, baix nivell d'acoblament funcional i menor criticitat operativa. **Total: 24**
- **Integracions de complexitat mitjana/alta**, que presenten major càrrega de lògica funcional, múltiples dependències entre sistemes, major necessitat d'orquestració o requeriments tècnics específics. **Total: 12**
- **Integracions crítiques**, associades a fluxos amb elevada criticitat operativa, alta complexitat tècnica o impacte directe sobre processos sensibles del negoci. **Total: 4**

Aquesta classificació té caràcter exclusivament orientatiu i respon a l'estat del coneixement actual d'Aigües de Barcelona en el moment de preparació de la present licitació. Correspondrà a l'adjudicatari, durant les fases inicials de discovery, anàlisi funcional i revisió tècnica detallada, revalidar aquesta classificació, confirmar-ne la complexitat real, dependències, criticitat i patró de migració més adequat per a cadascuna de les integracions incloses dins l'abast del projecte.

No obstant això, aquesta categorització s'ha de considerar suficient, als efectes de la present licitació, perquè els licitadors puguin comprendre el nivell de complexitat general de l'ecosistema actual i dimensionar adequadament la seva proposta tècnica, metodològica i econòmica.



El detall de cadascuna d'aquestes integracions es troba al punt 4.5

4.3. Protocols i tecnologies utilitzades

La figura següent mostra una visió agregada dels principals protocols, tecnologies i mecanismes d'integració identificats en l'ecosistema actual. Aquesta anàlisi té caràcter orientatiu i té com a objectiu facilitar als licitadors la comprensió del perfil tecnològic de les integracions incloses dins l'abast del projecte. Atès que una mateixa integració pot combinar múltiples protocols o mecanismes de comunicació, els percentatges representats no són excloents ni necessàriament acumulen el 100% del total.

 Protocol		 Ús	 Percentatge
 Fitxers/FS	Intercanvi de fitxers en sistemes d'emmagatzematge	28	70.0%
 FTP/SFTP	Transferència segura de fitxers	21	52.5%
 SOAP	Servèis web amb protocol SOAP	10	25.0%
 REST/HTTP	Servèis web basats en arquitectura REST	3	7.5%
 Email/SMTP	Enviament i recepció de correus electrònics	5	12.5%
 Bases de dades	Lectura i escriptura directa en bases de dades	3	7.5%
 SAP natiu (IDoc/RFC)	Integració mitjançant protocols nadius de SAP	4	10.0%
 Missatgeria / Event Streaming	Missatgeria i streaming d'esdeveniments (Kafka / JMS)	3	7.5%

4.4. Inventari d'integracions

A continuació, es presenta una llista amb una breu descripció funcional i tècnica a alt nivell dels principals processos i serveis d'integració identificats a l'abast actual de la plataforma. Aquest inventari té com a objectiu proporcionar a l'adjudicatari una visió global de l'ecosistema d'integracions existent, permetent comprendre la naturalesa dels fluxos, tecnologies implicades, patrons d'integració utilitzats i nivell aproximat de complexitat associat a cada procés.

La informació inclosa en aquest apartat haurà de servir com a base de referència per a l'elaboració de la proposta per part de l'adjudicatari. Això no obstant, atès el caràcter resumit i orientatiu d'aquest inventari, s'assumeix que determinats detalls tècnics, dependències, configuracions específiques o particularitats funcionals podran requerir una anàlisi addicional durant les fases inicials del projecte.

Serà durant la fase de discovery, on l'adjudicatari tindrà accés a la documentació tècnica completa disponible, així com als entorns i sistemes necessaris per aprofundir en el funcionament de les integracions, validar supòsits tècnics i completar el disseny del Pla de Migració de cadascuna de les integracions i processos que conformen aquesta plataforma.

4.4.1. **FIRMADIGITAL-AB-CONNECT**

Servei d'integració per a la gestió de signatura digital. Rep sol·licituds de signatura des de Salesforce mitjançant SOAP, emmagatzema la informació a la base de dades i gestiona l'enviament al proveïdor

Logalty. Inclou processos associats per a consulta d'estat, cancel·lació de signatures, descàrrega de documents signats i generació de fitxers de marques per a Siebel.

Origen de dades:

- Salesforce (SOAP/XML)
- Content Manager (Base de dades via SOAP/JDBC)
- Logalty (SOAP/Base64)

Destinació de dades:

- Content Manager (SOAP/XML)
- Logalty (SDK/XML)
- Salesforce (SOAP/XML)
- Sistema de fitxers (.mrc)

Freqüència:

- Sota demanda: recepció de sol·licituds i generació de marques
- Programat (Cron):
 - o Enviament a proveïdor: cada 1 minut
 - o Consulta estat: cada 2 hores
 - o Descarrega documents signats: cada 5 minuts

Components tècnics:

- Rutes Camel

Seguretat:

- Validació SOAP/XML
- Seguretat mitjançant API Keys i SSL/TLS
- Autenticació per credencials en serveis
- Inserció controlada a Base de dades
- Logs al Content Manager

Transformacions:

- Conversió SOAP → SOAP (Content Server)
- Base64 → PDF
- Base64 → fitxer .mrc

Volumetria:

- Aproximadament 4.000 peticions/dia

4.4.2. SICAB-ACUA-CONNECT

Procés d'integració entre SICAB i el proveïdor Aqualogy per al tractament de fitxers d'operacions i inventari. Els fitxers generats per l'amfitrió es carreguen en una base de dades PostgreSQL, s'envien al proveïdor mitjançant Kafka i es reben les respostes de forma asíncrona. Un cop processades totes les respostes, es genera un fitxer de sortida per al host.

Origen de dades:

- SICAB (fitxers TXT)
- Aqualogy (SOAP/XML)
- Kafka (topics)
- Base de dades PostgreSQL

Destinació de dades:

- Base de dades PostgreSQL
- Aqualogy (SOAP/XML)
- SICAB (fitxers TXT)

Freqüència:

- Processos de càrrega i recepció: temps real
- Processos d'enviament i generació de fitxers: asíncrons en segon pla

Components tècnics:

- Rutes Camel
- Kafka Consumer (topics)
- Base de dades PostgreSQL

Seguretat:

- Validació de format TXT
- Validació de missatges Kafka
- Validació SOAP/XML
- Reintents configurats: 2

Transformacions:

- TXT → Base de dades
- Base de dades → SOAP/XML
- Kafka → Base de dades
- Base de dades → TXT

Volumetria:

- Aproximadament 13.000 peticions/dia

4.4.3. SWIFT-CONNECT

Procés d'integració per a l'intercanvi automatitzat de fitxers bancaris entre els sistemes interns (SICAB i SAP) i la xarxa SWIFT. Gestiona l'enviament de fitxers generats pels sistemes interns cap a SWIFT i la recepció de respostes per distribuir-los al sistema corresponent.

Origen de dades:

- SICAB (Sistema de fitxers, TXT)
- SAP (FTP/SFTP, TXT/CSV)
- SWIFT (FTP/SFTP)
- Directoris interns de Red Hat Fuse

Destinació de dades:

- SWIFT (FTP/SFTP)
- SICAB (Sistema de fitxers)
- SAP (FTP/SFTP)
- Directoris interns de Red Hat Fuse

Freqüència:

- Lectura SICAB: cada minut (dies feiners)
- Intercanvi amb SWIFT: cada 15 minuts
- Processos interns: temps real o per esdeveniment

Components tècnics:

- Rutes Apache Camel
- Servidors FTP/SFTP

- Sistema de fitxers Red Hat Fuse
- Directoris de treball i processament dinàmic

Seguretat:

- Validació per nom i format de fitxer
- Gestió de carpetes d'error
- Reintents configurats
- Logs d'execució i traçabilitat
- Monitorització mitjançant cues JMS

Transformacions:

- Principalment gestió de rutes i reanomenat de fitxers
- No es modifica el contingut dels fitxers

Errors i monitorització:

- Logging mitjançant Apache Camel
- Gestió d'excepcions amb doTry/doCatch
- Redirecció a cues d'error (DLQ)
- Carpeta d'errors per a fitxers fallits

Volumetria:

- No disponible

4.4.4. AFECTACIÓ-SIEBEL-CM-CONNECT

Procés que processa un fitxer CSV generat des de host amb números de pòlissa i NIF. Consulta els documents associats al Content Manager, descarrega els PDFs corresponents, genera un fitxer de resultat i envia un correu electrònic amb els documents obtinguts.

Origen de dades:

- Host (Sistema de fitxers, CSV)

Destinació de dades:

- Content Manager (SOAP/XML)
- Sistema de fitxers (PDF descarregats)
- Servidor de correu (SMTP)

Freqüència:

- Event-driven
- Execució asíncrona en temps real quan es detecta el fitxer

Components tècnics:

- Apache Camel / Red Hat Fuse
- Rutes Camel

Seguretat:

- Validació de format CSV/TXT
- Control d'errades en lectura de fitxer

Transformacions:

- CSV → XML
- Mapeig de NIF i pòlissa
- Descàrrega de PDFs des de WS
- Generació de correu amb adjunts

Volumetria:

- Aproximadament 1 petició/dia

4.4.5. CM-MAIL-CONNECT

Servei SOAP que permet consultar informació de pòlisses i factures des de SICAB. Consulta els documents associats al Content Manager, descarrega els adjunts i els envia per correu electrònic als destinataris indicats a la petició.

Origen de dades:

- SICAB (SOAP/XML)

Destinació de dades:

- Content Manager (SOAP/XML)
- Servidor de correu (SMTP)

Freqüència:

- Temps real
- Activat per petició síncrona des de SICAB

Components tècnics:

- Apache Camel / Red Hat Fuse
- Rutes Camel
- JAXB per a transformació de dades
- Configuració d'accés al Content Manager

Seguretat:

- Validació d'estructura de petició
- Validació de credencials
- Validació de format de correu i adjunts

Transformacions:

- Marshalling / Unmarshalling JAXB
- Generació de correus
- Adjuntar documents PDF obtinguts de Content Manager

Volumetria:

- Aproximadament 70 peticions/dia

4.4.6. EDPC-CONNECT

Procés que recupera documents PDF des d'un sistema de fitxers i localitza l'XML associat amb el mateix nom. A partir de la informació continguda a l'XML es generen correus electrònics amb els PDFs adjunts que s'envien als destinataris definits.

Origen de dades:

- Sistema de fitxers

Destinació de dades:

- Servidor de correu (SMTP, emails HTML amb adjunts PDF)

Freqüència:

- Cron programat:
 - o Ruta 1: cada 5 minuts
 - o Ruta 2: cada 30 segons
 - o Horari: 00:00–01:00 i 03:00–23:00

Components tècnics:

- Apache Camel / Red Hat Fuse
- Rutes Camel
- Configuració mitjançant fitxers .properties

Seguretat:

- Validació de noms de fitxer
- Validació de format PDF/XML

Transformacions:

- XML → HTML (plantilles de correu)
- Injecció dinàmica de dades al cos de l'email

Volumetria:

- Aproximadament 650 peticions/dia

4.4.7. GUILBERT-AB-CONNECT

Procés d'integració entre SAP i el proveïdor extern Lyreco. Rep missatges IDOC des de SAP, invoca un web service extern i torna la resposta al sistema SAP.

Origen de dades:

- SAP (RFC / IDOC – XML)
- SAP (Sistema de fitxers – TXT)
- Web Service Lyreco (SOAP/XML)

Destinació de dades:

- Web Service Lyreco (SOAP/XML)
- SAP (RFC/IDOC)

Freqüència:

- Temps real
- Processament síncron

Components tècnics:

- Apache Camel / FUSE
- Rutes Camel

Seguretat:

- Validació de missatges SOAP
- Control de concurrència i processament paral·lel

Transformacions:

- IDOC → XML (SOAP)
- TXT → XML (SOAP)
- XML (SOAP) → IDOC

Volumetria:

- Aproximadament 1 petició/dia

4.4.8. INDICADORES-CALIDAD-SIEBEL-MDM-CONNECT

Servei que rep peticions SOAP des de sistemes de Telectura o Siebel i fa trucades a un servei REST del sistema Telectura per registrar o consultar indicadors de qualitat. Els resultats i esdeveniments es publiquen també al sistema de missatgeria.

Origen de dades:

- Telectura i Siebel (SOAP)

Destinació de dades:

- Sistema MDM (REST)
- ActiveMQ

Freqüència:

- Temps real
- Event-driven amb resposta immediata

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel
- Beans Java personalitzats
- Motor de mapeig Dozer

Seguretat:

- Validació de format de missatges
- Validació de camps obligatoris

Transformacions:

- Mapeig i normalització de dades
- Aplicació de regles de negoci mitjançant Dozer

Volumetria:

- Aproximadament 1.000 peticions/dia

4.4.9. LIMS-SAP-CONNECT (RFC)

Rep fitxers CSV generats per LIMS, processa cada línia individualment i realitza una trucada RFC a SAP. Amb la resposta obtinguda es genera un fitxer de resultat per línia i, en acabar el fitxer complet, s'envia un correu amb el resum del resultat.

Origen de dades:

- LIMS
- Sistema de fitxers (CSV)

Destinació de dades:

- SAP (RFC)
- Generació de fitxers de resposta en sistema de fitxers
- Enviament de notificació per correu electrònic

Freqüència:

- Cron programat cada 5 minuts

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel: lims-sap-connect

Seguretat:

- Validació de format CSV
- Control d'errors per línia processada
- Eliminació del fitxer original després de processament

Transformacions:

- CSV → XML
- Mapeig de dades al model d'entrada de la RFC
- Enriquiment i validació de dades
- Generació de fitxer de resposta

Volumetria:

- Aproximadament 1 petició cada 1–2 dies

4.4.10. META4SAPPR5 (IDOC)

Integra META4 amb SAP mitjançant enviament automàtic de seients comptables. Els fitxers .pr5 generats per META4 es recullen, es converteixen a IDOC i s'envien a SAP mitjançant RFC gestionat per Red Hat Fuse.

Origen de dades:

- META4
- Sistema de fitxers (.pr5)

Destinació de dades:

- SAP
- Protocol RFC / IDOC

Freqüència:

- Cada 5 minuts
- Intervals: 00:00–01:55 i 03:00–23:55

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel
- Connector SAP JCo

Seguretat:

- Validació d'existència de fitxer
- Control de duplicats
- Reintents davant de fallada de connexió
- Redirecció de fitxers erronis a carpeta d'errors

Transformacions:

- Conversió de fitxer .pr5 a IDOC SAP

Volumetria:

- Aproximadament 1 petició/dia

4.4.11. OFEXPAGOTARJETA-CONNECT

Gestiona la notificació de pagaments de rebuts mitjançant targeta des de Redsys. Rep trucada SOAP amb informació de la transacció, processa les dades i les envia al sistema Host SAP mitjançant FTP/SFTP.

Origen de dades:

- Redsys (SOAP/XML HTTPS)

Destinació de dades:

- Sistema Host i SAP (FTP/SFTP)
- Format XML

Freqüència:

- Cron programat cada 5 minuts

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel: BBVA
- WSDL: BBVA
- Directoris temporals de processament

Seguretat:

- Validació estructura XML
- Validació de camps obligatoris
- Comprovació de disponibilitat del servidor FTP
- Registre de transaccions i traçabilitat

Transformacions:

- XML SOAP → XML destinació SAP
- Mapeig de camps
- Enriquiment de dades
- Inclusió d'identificadors o timestamps

Volumetria:

- Aproximadament 250 peticions/dia

4.4.12. SAP-NEPTUNO-CONNECT

Automatitza la transferència de fitxers des de SAP cap al sistema Neptuno. SAP genera fitxers CSV de control amb instruccions per copiar fitxers TXT/PDF des de rutes d'origen cap a rutes de destinació.

Origen de dades:

- SAP (CSV, TXT/PDF)
- FTP/SFTP

Destinació de dades:

- Servidor de fitxers Neptuno
- File System

Freqüència:

- Cada 15 minuts
- Interval: 08:00–20:00

Components tècnics:

- Apache Camel / Red Hat Fuse
- Rutes Camel per a descàrrega i còpia de fitxers
- Configuració FTP externa
- Directoris temporals de processament

Seguretat:

- Validació del fitxer CSV de control
- Verificació d'existència de fitxers origen
- Registre d'operacions de còpia
- Maneig de línies invàlides a CSV

Transformacions:

- No hi ha transformació de contingut
- Extracció de dades del CSV
- Reanomenat de fitxers durant la còpia

Volumetria:

- Menys de 1 petició/dia

4.4.13. CM-DOWNLOAD-CONNECT

Permet la descàrrega massiva de documents des del Content Manager. A partir d'un fitxer CSV amb identificadors de documents (ITEMID), Red Hat Fuse processa cada línia, baixa el document i genera un fitxer de sortida amb el resultat de l'operació.

Origen de dades:

- Sistema de fitxers local
- CSV generat des de base de dades

Destinació de dades:

- Content Manager (SOAP)
- Sistema de fitxers local (documents descarregats i fitxer de resultat)

Freqüència:

- Cron programat cada 15 minuts

Components tècnics:

- Apache Camel / Red Hat Fuse
- Servei SOAP viewDocumentAttach
- Rutes d'entrada i de sortida configurades

Seguretat:

- Processament únicament de registres amb camp ESBORRAT = N
- Validació de presència d'ITEMID
- Maneig d'excepcions SOAP

Transformacions:

- Descàrrega de documents des de CM
- Reanomenat de documents amb el vostre ITEMID
- Generació de CSV de sortida amb estat de l'operació

Volumetria:

- No disponible

4.4.14. FACTURA RECTIFICA

A partir d'un fitxer CSV amb identificadors de factures generat per SICAB, consulta els documents associats al Content Manager, genera un fitxer JSON amb els resultats, descarrega els PDFs relacionats i empaqueta tota la informació en un fitxer ZIP per a Aigües de Barcelona.

Origen de dades:

- SICAB
- File System (CSV)

Destinació de dades:

- Content Manager (SOAP)
- Sistema de fitxers (JSON + PDF comprimits a ZIP)

Freqüència:

- Cron programat:
 - o Procés 1: cada 5 minuts
 - o Procés 2: cada 2 minuts

Components tècnics:

- Apache Camel / Red Hat Fuse
- Servei SOAP de Content Manager
- Rutes d'entrada/sortida configurades a properties

Seguretat:

- Validació de format CSV
- Verificació d'existència de documents a CM
- Validació de resposta del servei CM
- Gestió d'errors per document no trobat

Transformacions:

- CSV → JSON
- Recuperació de metadades de documents a CM
- Compensió de resultats a ZIP

Volumetria:

- Aproximadament 1 petició/dia

4.4.15. MONITORING-AB

Procés de monitorització centralitzat que rep missatges d'esdeveniments i errors des de diferents serveis Red Hat Fuse mitjançant ActiveMQ. Els missatges es processen i s'envien com a notificacions per correu segons la configuració.

Origen de dades:

- Serveis Red Hat Fuse i sistemes d'Aigües de Barcelona
- ActiveMQ (JMS – cua Q.Ab.Monitoring)
- Format JSON

Destinació de dades:

- Servidor de correu SMTP
- Emails de notificació

Freqüència:

- Temps real
- Escolta contínua a la cua JMS

Components tècnics:

- Apache Camel / Red Hat Fuse
- ActiveMQ
- Servidor SMTP
- Base de dades PostgreSQL per a persistència d'esdeveniments

Seguretat:

- Validació estructura del missatge JSON
- Verificació de destinataris configurats
- Gestió de fallades de connexió amb ActiveMQ o SMTP

Transformacions:

- Conversió de missatge JSON → email
- Enriquiment amb informació contextual del procés origen

Volumetria:

- Aproximadament 1 esdeveniment/dia (estimat)

4.4.16. CM-SICAB-CONNECT

Detecta fitxers generats al Content Manager i els envia al host de SICAB. Recupera el contingut mitjançant servei SOAP de CM i envia per FTP/SFTP al host SICAB.

Origen de dades:

- Content Manager
- File System compartit + servei SOAP (TXT)

Destinació de dades:

- Host SICAB (FTP/SFTP, TXT)

Freqüència:

- Cron programat cada 10 minuts
- Interval: 05:00 – 14:00

Components tècnics:

- Apache Camel / Red Hat Fuse
- Servei SOAP de Content Manager
- Connexió FTP/SFTP al host SICAB
- Configuració de comandes especials del host

Seguretat:

- Verificació de mida de fitxer > 0
- Validació de credencials i connexió FTP
- Validació de resposta del host després d'enviament

Transformacions:

- Conversió de missatges SOAP a format TXT/JSON mitjançant JAXB
- Enriquiment amb metadades del document

Volumetria:

- Aproximadament 1 petició/dia

4.4.17. DIGI-CONNECT

Recopila diàriament els fitxers de marques (.mrc) generats per Siebel, els concatena en un únic fitxer i els envia al host SICAB mitjançant FTP/SFTP. Els fitxers originals s'eliminen després de confirmació d'enviament.

Origen de dades:

- Siebel
- File System (.mrc)

Destinació de dades:

- SICAB (FTP/SFTP, TXT unificat)

Freqüència:

- Cron programat diàriament a les 21:00

Components tècnics:

- Apache Camel / Red Hat Fuse
- Lectura de directori compartit
- Processament i concatenació de fitxers
- Connexió FTP/SFTP al host SICAB

Seguretat:

- Validació d'extensió .mrc
- Verificació de correcta concatenació del fitxer final
- Validació de resposta del host després d'enviament

Transformacions:

- Conversió de múltiples .mrc → únic .txt
- Concatenació seqüencial de fitxers
- Inclusió d'estructura requerida per SICAB

Volumetria:

- Aproximadament 1 execució/dia

4.4.18. LIMS-SENTINEL-CONNECT

Envia fitxers generats per LIMS des d'un recurs compartit cap a un servidor SFTP corporatiu. Els CSV detectats es transmeten sense transformació.

Origen de dades:

- LIMS
- File System (CSV)

Destinació de dades:

- Servidor SFTP corporatiu (CSV)

Freqüència:

- Cron programat a les 08:10

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel
- Connector SFTP

Seguretat:

- Control de disponibilitat del fitxer
- Reintents en cas d'error de transferència

Transformacions:

- No hi ha transformació de format
- CSV → CSV (passthrough)

Volumetria:

- Aproximadament 5 peticions/dia

4.4.19. OFEX-SIEBEL-MDM-CONNECT

Actua com a intermediari entre sistemes SOAP (SICAB) i serveis REST externs. Rep peticions SOAP, les transforma a trucades REST i converteix la resposta REST novament a SOAP.

Origen de dades:

- SICAB (SOAP/XML, HTTPS 443)

Destinació de dades:

- Serveis REST de Telelectura
- Serveis REST de Tokenització (JSON, HTTPS)

Freqüència:

- Sota demanda
- Processament asíncron

Components tècnics:

- Apache Camel / Red Hat Fuse
- Ruta Camel
- Serveis REST externs

Seguretat:

- Control de timeouts en trucades REST
- Gestió d'excepcions en la transformació de missatges
- Monitorització d'estat de la ruta Camel

Transformacions:

- SOAP/XML → REST/JSON (petició)
- REST/JSON → SOAP/XML (resposta)

Volumetria:

- Aproximadament 80.000 peticions/dia

4.4.20. AB-SICAB-CONNECT

Rep fitxers de cobraments de clients des d'un SFTP, els mou de "Entrada" a "Processos" i els copia a rutes destinació per a SICAB i POWER.

Origen de dades:

- SFTP (TXT)

Destinació de dades:

- Servidor SICAB
- POWER

Freqüència:

- Cada hora entre 05:00 i 10:00

Components tècnics:

- Apache Camel / Red Hat Fuse
- Rutes Camel

Seguretat:

- 2 intents amb delay de 5 s
- Validació i routing cap a SICAB o POWER
- Enriquiment de headers

Transformacions:

- Normalització de fitxers
- Enriquiment de headers
- Routing segons destinació

Volumetria:

- 200 peticions/mes

4.4.21. AGM-SICCO-CONNECT

Recull fitxers des de l'SFTP d'AGM i els envia a l'SFTP de SICCO, notificant per correu a l'adreça de servei.

Origen de dades:

- AGM (SFTP/FTP, TXT)

Destinació de dades:

- SICCO (SFTP/FTP)
- SFTP Aigües Barcelona

Freqüència:

- Cron cada 5 minuts

Components tècnics:

- Rutes Camel

Seguretat:

- Validació d'existència i contingut del fitxer
- Reintents: 3 amb delai de 60 s

Transformacions:

- Reanomenat del fitxer
- Formateig i normalització del contingut
- Garantia de traçabilitat

Volumetria:

- 80 peticions/mes

4.4.22. AQMOSSIGEDA-CONNECT

Recull fitxers des d'un recurs compartit i els envia a l'SFTP de destinació, gestionant rutes locals per èxit o error.

Origen de dades:

- Sistema de fitxers local (TXT/CSV)

Destinació de dades:

- SFTP

Freqüència:

- Cron cada 5 minuts

Components tècnics:

- Rutes Camel

Seguretat:

- Validació de format CSV/TXT
- Reintents: 3, delai 5 minuts

Transformacions:

- Enriquiment de dades
- Normalització de capçaleres, tipus/dates i delimitadors

Volumetria:

- 4.500 peticions/mes

4.4.23. AQMOSSIGEDA2-CONNECT

Recull fitxers des d'un recurs compartit i els envia a l'SFTP de SIGEDA, mantenint còpia local en cas d'èxit o error.

Origen de dades:

- Sistema de fitxers muntat (TXT)

Destinació de dades:

- SIGEDA (SFTP)
- Host local

Freqüència:

- Cron cada 5 minuts

Components tècnics:

- Rutes Camel: ingesta FS → Validació/Enriquiment

Seguretat:

- Validació de fitxers TXT
- Reintents: 3 amb delai de 5 minuts

Transformacions:

- Passthrough TXT amb possible enriquiment de headers

Volumetria:

- 8.500 peticions/mes

4.4.24. PENDINGS-INTERFACE → CARTAS IMPAGO

Rep documents PDF d'un SFTP extern i els copia a una carpeta del Content Manager per al processament.

Origen de dades:

- Impressor via SFTP (PDF)

Destinació de dades:

- Content Manager (File System, PDF)

Freqüència:

- Cron diari a les 04:00

Components tècnics:

- Apache Camel / Red Hat Fuse

Seguretat:

- Validació de format PDF
- Reintents: 3 amb delai de 10 s

Transformacions:

- Cap

Volumetria:

- 1 execució/dia

4.4.25. PENDINGS-INTERFACE → CARTAS IMPAGO NEXEA

Rep documents PDF d'un SFTP de Nexea i els copia al Content Manager.

Origen de dades:

- SFTP: Impressor Nexea (PDF)

Destinació de dades:

- Content Manager (File System, PDF)

Freqüència:

- Cron diari a les 14:00

Components tècnics:

- Ruta Camel: SFTP Nexea → File (CM)

Seguretat:

- No especificades

Transformacions:

- Cap

Volumetria:

- 1 execució/dia

4.4.26. PENDINGS-INTERFACE → CARTAS IMPAGO BFS

Rep documents PDF d'un SFTP de BFS i els copia al Content Manager a la carpeta d'input Cartes.

Origen de dades:

- SFTP: Impressor BFS (PDF)

Destinació de dades:

- Content Manager / Input Cartes (File System, PDF)

Freqüència:

- Cron diari a les 15:00

Components tècnics:

- Ruta Camel: SFTP BFS → File (Cartes input)

Seguretat:

- Filtre per nom "Cartes"

Transformacions:

- Cap

Volumetria:

- 1 execució/dia

4.4.27. SAP-META4-CONNECT

Consulta FTP com a origen extret de SAP cada 30 minuts per a fitxers CSV, els descarrega a carpeta temporal i els diposita a la carpeta compartida de Meta4.

Origen de dades:

- SAP (FTP, CSV)

Destinació de dades:

- Meta4 (File System)

Freqüència:

- Cron cada 30 minuts

Components tècnics:

- Xarxa Hat Fuse / Middleware AB
- Processament en carpeta temporal, còpia a destinació
- Configuració: 3 reintents, delay 50 s, threads 3

Seguretat:

- Comprovació d'extensió .csv
- Validació d'existència a FTP
- Confirmació de còpia a destinació

Transformacions:

- No s'aplica (CSV original)

Volumetria:

- 50 peticions/dia

4.4.28. SAP-XRT-AB-CONNECT

Recull fitxers generats a SAP per transaccions Z000F_PREVISION_XRT, Z001F_EXTR_DOCS i Z001F_EXTR_PDFS cada 5 minuts i els diposita a PRVXRT.

Origen de dades:

- SAP (SFTP, TXT/PDF)

Destinació de dades:

- PRVXRT (File System)

Freqüència:

- Cron cada 5 minuts

Components tècnics:

- Xarxa Hat Fuse / Middleware AB
- Descàrrega a carpeta local i dipòsit final
- Configuració: 2 reintents, delay 20 s

Seguretat:

- Verificació d'extensió (.txt/.pdf)
- Comprovació d'existència a SFTP
- Confirmació de còpia a la destinació

Transformacions:

- No s'aplica (fitxers originals)

Volumetria:

- 1-2 peticions/mes

4.4.29. TOPKAPI-CONNECT (EXPORT)

Transfereix fitxers entre LIMS i TOPKAPI usant Red Hat Fuse. S'executa diàriament a les 22.00. Gestió d'errors i monitorització mitjançant ActiveMQ.

Origen de dades:

- LIMS (File System, TXT)

Destinació de dades:

- TOPKAPI (FTP/SFTP, TXT)

Freqüència:

- Diari a les 22:00

Components tècnics:

- Entrada: Lectura des de File System
- Processament: Còpia a carpeta temporal i enviament a FTP TOPKAPI

- Configuració: 2 reintents, delai 5 s, FTP passiu

Seguretat:

- Comprovació existència fitxers
- Validació de format TXT
- Confirmació de còpia a FTP

Transformacions:

- Cap (TXT pla)

Volumetria:

- 60 peticions/mes

4.4.30. TOPKAPI-CONNECT (DADES PUNTUALS)

Transfereix fitxers puntuals, coneguts com a dades puntuals per definició funcional, entre LIMS i TOPKAPI.

Origen de dades:

- LIMS (File System, TXT)

Destinació de dades:

- TOPKAPI (FTP/SFTP)

Freqüència:

- Diari a les 04:00

Components tècnics:

- Entrada: LIMS
- Processament: Còpia a temporal → FTP
- Configuració: 2 reintents, delai 5 s, FTP passiu

Seguretat:

- Existència de fitxers
- Format TXT
- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 60 peticions/mes

4.4.31. TOPKAPI-CONNECT (DADES MITJANES)

Transfereix fitxers de dades mitjanes, coneguts com a dades mitjanes per definició funcional, entre LIMS i TOPKAPI.

Origen de dades:

- LIMS (File System, TXT)
- Carpeta: /mnt/LIMS/Interfases/Topkapi/import/Dades_mitjanes/

Destinació de dades:

- TOPKAPI (FTP/SFTP)

Freqüència:

- Diari a les 02:00 i 10:00

Components tècnics:

- Entrada: LIMS
- Processament: Còpia a temporal → FTP
- Configuració: 2 reintents, delai 5 s

Seguretat:

- Existència de fitxers
- Format TXT
- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 60 peticions/mes

4.4.32. LIMS-SFTP-CONNECT

Envia fitxers CSV des de LIMS a AB (SFTP), validant i enriquint els headers abans de l'enviament.

Origen de dades:

- LIMS (File System, CSV)

Destinació de dades:

- AB (SFTP)

Freqüència:

- 05:50, 11:50, 17:50, 23:50

Components tècnics:

- Entrada: LIMS
- Processament: Validació, enriquiment de headers, còpia a temporal, enviament SFTP
- Configuració: 3 reintents, delai 5 min

Seguretat:

- Existència de fitxers
- Format CSV
- Confirmació de còpia

Transformacions:

- Cap (CSV pla)

Volumetria:

- 30 peticions/mes

4.4.33. SAP-DOP-CONNECT

Integra fitxers SAP → AB Operacions Territorials.

Origen de dades:

- SAP (FTP/SFTP, CSV)

Destinació de dades:

- AB Operacions Territorials (File System / SFTP)

Freqüència:

- Diari 06:00 i 20:00; escomeses 05:00

Components tècnics:

- Entrada: SAP
- Processament: Validació, còpia a temporal → File System

- Configuració: 2 reintents, delai 5 s

Seguretat:

- Existència de fitxers
- Format CSV
- Confirmació de còpia

Transformacions:

- Cap (CSV pla)

Volumetria:

- No disponible

4.4.34. SAP-SEQUERA-CONNECT

Integra fitxers SAP amb carpeta compartida (/SEQUERA).

Origen de dades:

- SAP (FTP/SFTP, TXT)

Destinació de dades:

- SEQUERA (recurs compartit intern, File System)

Freqüència:

- Cada hora

Components tècnics:

- Entrada: SAP
- Processament: Validació, filtratge TXT, còpia a temporal → destinació
- Configuració: 2 reintents, delai 5 s

Seguretat:

- Existència de fitxers
- Format TXT
- Confirmació de còpia

Transformacions:

- Cap (TXT pla)

Volumetria:

- No disponible

4.4.35. AKWAMETRICS-CONNECT (EXPORT)

Transfereix fitxers entre LIMS i AKWAMETRICS usant Red Hat Fuse. S'executa diàriament a les 22.00. Gestió d'errors i monitorització mitjançant ActiveMQ.

Origen de dades:

- LIMS (File System, TXT)

Destinació de dades:

- AKWAMETRICS (FTP/SFTP, TXT)

Freqüència:

- Diari a les 22:00

Components tècnics:

- Entrada: Lectura des de File System
- Processament: Còpia a carpeta temporal i enviament a FTP AKWAMETRICS
- Configuració: 2 reintents, delai 5 s, FTP passiu

Seguretat:

- Comprovació existència fitxers
- Validació de format TXT
- Confirmació de còpia a FTP

Transformacions:

- Cap (TXT pla)

Volumetria:

- 60 peticions/mes

4.4.36. AKWAMETRICS -CONNECT (DADES PUNTUALS)

Transfereix fitxers puntuals, conegut com a dades puntuals per definició funcional, LIMS ↔ AKWAMETRICS.

Origen de dades:

- LIMS (File System, TXT)

Destinació de dades:

- AKWAMETRICS (FTP/SFTP)

Freqüència:

- Diari a les 04:00

Components tècnics:

- Entrada: LIMS
- Processament: Còpia a temporal → FTP
- Configuració: 2 reintents, delai 5 s, FTP passiu

Seguretat:

- Existència de fitxers
- Format TXT
- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 60 peticions/mes

4.4.37. AKWAMETRICS -CONNECT (DADES MITJANES)

Transfereix fitxers de dades mitjanes, conegut com a dades mitjanes per definició funcional, entre LIMS i AKWAMETRICS.

Origen de dades:

- LIMS (File System, TXT)
- File System AKWAMETRICS

Destinació de dades:

- AKWAMETRICS (FTP/SFTP)

Freqüència:

- Diari a les 02:00 i 10:00

Components tècnics:

- Entrada: LIMS
- Processament: Còpia a temporal → FTP

- Configuració: 2 reintents, delai 5 s

Seguretat:

- Existència de fitxers
- Format TXT
- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 60 peticions/mes

4.4.38. WATER_QUALITY

Transfereix fitxers de dades mitjançant LIMS a DataHUB.

Origen de dades:

- LIMS (File System, TXT)
- File System Water_Quality

Destinació de dades:

- Aigües de Barcelona (FTP/SFTP)

Freqüència:

- Diari a les 02:00

Components tècnics:

- Entrada: LIMS
- Processament: Còpia a temporal → SFTP
- Configuració: 2 reintents, delai 5 s

Seguretat:

- Existència de fitxers
- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 30 peticions/mes

4.4.39. SIGAB_CONNECT

Transfereix fitxers CSV de SAP entre rutes internes Aigües de Barcelona.

Origen de dades:

- SAP (File System)

Destinació de dades:

- Aigües de Barcelona (File System)

Freqüència:

- Semestral (10 gener i 10 Juliol)

Components tècnics:

- File System - Aigües de Barcelona
- Configuració: 2 reintents, delai 5s

Seguretat:

- Existència de fitxers

- Confirmació de còpia

Transformacions:

- Cap

Volumetria:

- 1 petició/semestre

4.4.40. XML-MAIL-CONNECT

Realitzar enviaments de correus a partir de fitxers que recupera de recurs compartit. Recull destinataris i construeix el cos del correu a partir dels fitxers d'entrada.

Origen de dades:

- Aigües Barcelona (File System)

Destinació de dades:

- Aigües de Barcelona (File System BACKUP)
- Correu a destinataris

Freqüència:

- Cada minut

Components tècnics:

- File System red Aigües de Barcelona
- SMTP

Seguretat:

- Existència de fitxers
- Protocols SMTP

L'inventari de processos Red Hat Fuse inclòs en aquest document reflecteix la situació identificada al moment de la realització del plec. Atès que l'entorn pot evolucionar amb el temps, podrien existir nous processos desenvolupats amb posterioritat a l'elaboració del present document. En aquest cas, aquests processos també s'han de considerar dins de l'abast de la migració i s'han d'avaluar durant les fases corresponents del projecte.

Així mateix, durant l'execució del projecte, Aigües de Barcelona estarà duent a terme iniciatives paral·leles de migració i modernització de sistemes corporatius cap a entorns cloud, per la qual cosa l'adjudicatari haurà de coordinar-se i alinear-se amb aquests projectes per adaptar, evolucionar o redissenyar, quan calgui les integracions i/o processos afectats per la transformació dels sistemes origen.

5. ARQUITECTURA TO-BE**5.1. Arquitectura Objectiu**

L'arquitectura de referència de la solució objectiu definida per Aigües de Barcelona es basa en un model d'integració distribuït, desacoblat i cloud-native, construït principalment sobre capacitats natives d'Azure i components open source àmpliament consolidats al mercat. L'objectiu d'aquesta arquitectura no és replicar el comportament d'un ESB monolític tradicional sobre una nova tecnologia, sinó evolucionar progressivament cap a un model basat en responsabilitats clarament separades,

components reutilitzables i serveis independents, mantenint sempre el control operatiu i la sostenibilitat tècnica de la plataforma.

L'arquitectura proposada estableix com a principi fonamental la separació entre orquestració, integració, lògica funcional, transport i observabilitat i evita concentrar tota la responsabilitat del flux en una única eina. Cada component de l'ecosistema haurà de tenir una responsabilitat clarament definida i fitada, permetent evolucionar, mantenir i escalar les integracions de manera independent.

La plataforma objectiu haurà de mantenir un model de segregació d'entorns equivalent al model actual d'Aigües de Barcelona, contemplant com a mínim els entorns de desenvolupament, preproducció i producció, amb independència lògica, tècnica i operativa entre ells, d'acord amb els criteris de seguretat i govern definits al present plec.

L'adjudicatari haurà de considerar dins de l'abast del projecte la correcta implantació, configuració, validació i desplegament dels components necessaris en cadascun dels entorns requerits, així com la seva parametrització i automatització per facilitar un model de desplegament repetible, governat i sostenible.

Com a criteri general, les integracions hauran de mantenir correspondència entre entorns origen i destí (desenvolupament, preproducció i producció). No obstant això, en aquells casos en què algun dels sistemes origen o destí no disposi d'un entorn equivalent o alineat amb aquest model, l'estratègia d'integració, proves, validació o desplegament haurà de ser analitzada i consensuada conjuntament amb Aigües de Barcelona durant les fases inicials del projecte.

5.2. Arquitectura de referència per capes

L'arquitectura es basa en les capes i components principals següents:

Capa d'orquestració

Objectiu:

Centralitzar la coordinació global dels processos d'integració, actuant com a element vertebrador del flux operacional de la plataforma i com a font de veritat de l'estat d'execució de les integracions.

Components principals: Azure Data Factory (ADF)

Responsabilitats:

- Orquestració global d'integracions batch i fluxos de dades.
- Planificador d'execucions.
- Coordinació de dependències entre processos i integracions.
- Control operacional i consolidació de l'estat global d'execució.
- Parametrització i gestió de configuracions de processos.
- Coordinació de components externs.
- Execució d'activitats de còpia i moviments de dades mitjançant Self-Hosted Integration Runtime desplegats a cada entorn.
- Ingestió batch i processament orientat a flux de dades.
- Rotatge d'informació i control d'estats.
- Transformacions lleugeres i validacions simples.
- Gestió tècnica bàsica d'errors i reintents.
- Coordinació del flux extrem a extrem entre components d'integració.

- Integracions orientades a la ingesta de dades des de sistemes SAP, especialment en escenaris d'extracció, còpia o consum d'informació estructurada. Consultar, capa d'Integració SAP.

Consideracions:

- Azure Data Factory s'estableix com a component central d'orquestració de la plataforma i ha d'actuar com a font de veritat operacional dels processos d'integració.
- ADF s'haurà d'utilitzar prioritàriament per a activitats de coordinació, automatització, còpia de dades i control d'execució, evitant concentrar lògica funcional complexa dins els pipelines.
- ADF no s'haurà d'utilitzar com a substitut directe de les capacitats avançades d'integració anteriorment implementades mitjançant Apache Camel sobre Red Hat Fuse.
- Tota lògica de negoci complexa, processament transaccional, validacions avançades, transformacions complexes, enriquiment de dades, gestió funcional d'errors o integració amb protocols propietaris haurà d'externalitzar cap a components aplicatius desacoblats desplegats sobre AKS.
- Els pipelines ADF hauran de mantenir un disseny modular, reutilitzable i fàcilment traçable, prioritzant simplicitat operacional i mantenibilitat.
- L'orquestració haurà de desacoblar-se de la lògica funcional i permet evolucionar independentment cada component d'integració.
- L'adjudicatari haurà de definir patrons, plantilles reutilitzables o pipelines parametrizables per homogeneïtzar l'orquestració i el comportament de les integracions, així com facilitar futurs desenvolupaments de noves integracions i/o evolucions de la plataforma.

Capa d'exposició i interoperabilitat (API Layer)**Objectiu:**

Actuar com a punt centralitzat d'exposició, securització, mediació i govern de serveis i integracions.

Components principals: Azure API Management (APIM)

Responsabilitats:

- Exposició centralitzada d'API corporatives.
- Securització de trucades mitjançant autenticació i autorització corporativa.
- Mediació i transformació de protocols SOAP ↔ REST.
- Publicació i versió d'APIs.
- Aplicació de polítiques de throttling, rate limiting i control de trànsit.
- Registre i traçabilitat de peticions.
- Punt únic d'entrada per a integracions síncrones.
- Invocació controlada de pipelines ADF o microserveis.

Consideracions:

- Tota integració REST o SOAP haurà de passar per APIM.
- APIM haurà d'actuar com a capa transversal de govern.
- No heu de contenir lògica funcional de negoci.
- La transformació de protocols s'haurà de limitar a una mediació lleugera.
- L'adjudicatari haurà de facilitar el paquet tècnic de publicació d'API complet i coordinar-se amb l'equip de DevOps d'Aigües de Barcelona, que tindrà la responsabilitat del desplegament, configuració i publicació de les API mitjançant Terraform.
-

Capa d'integració funcional i processament

Objectiu:

Implementar la lògica funcional d'integració, transformacions complexes, processament transaccional i connectivitat especialitzada que no ha de residir a l'Azure Data Factory. Aquesta capa permetrà desacoblar la lògica de negoci de l'orquestració global, facilitant el manteniment, l'escalat i l'evolució independent de cada integració.

Components principals:

- Azure Kubernetes Service (AKS).
- Microserveis desplegats en contenidors.
- Spring Boot, .NET o Python/Fast API, segons el cas d'ús.
- GitLab com a repositori corporatiu de codi.
- Jenkins com a eina corporativa de construcció i desplegament.
- Azure Container Registry (ACR) com a registre corporatiu d'imatges.
- Helm Charts per a parametrització i desplegament a AKS.
- Azure Key Vault per a gestió de secrets.
- External Secrets per a injecció segura de configuració sensible.

Responsabilitats:

- Implementació de lògica funcional complexa.
- Transformacions avançades de dades i formats.
- Validacions funcionals i tècniques complexes.
- Processament transaccional i gestió dels estats funcionals.
- Integracions amb protocols específics o llibreries de fabricant.
- Desenvolupament de microserveis desacoblats i reutilitzables.
- Exposició d'endpoints interns o externs quan s'apliqui.
- Generació de logs estructurats, mètriques i traces distribuïdes.
- Gestió d'errors funcionals, reintents i respostes normalitzades.
- Col·laboració amb l'equip DevOps per a la construcció, empaquetat i desplegament a AKS.
- Definició de requisits de CPU, memòria, escalat, límits i quotes per servei.
- Generació IDocs SAP.
- Execució de RFC SAP.

Consideracions:

- Els microserveis s'hauran de desplegar sobre AKS seguint les guies i les bones pràctiques corporatives proporcionades per l'equip DevOps d'Aigües de Barcelona.
- L'adjudicatari haurà de repositoritzar el codi font a GitLab, respectant l'estructura, el model de branques, la nomenclatura, els estàndards de versionat i les polítiques de revisió definides per l'organització.
- El procés de build de la imatge Docker, publicació a ACR i desplegament a AKS s'haurà d'integrar amb els pipelines corporatius basats a Jenkins, que serà responsabilitat de l'equip de DevOps d'Aigües de Barcelona.
- L'adjudicatari haurà de proporcionar o col·laborar en la definició dels Helm Charts necessaris per desplegar cada microservei, incloent-hi valors parametritzables per entorn, configuració de rèpliques, proves, recursos, variables d'entorn, secrets, ingress i polítiques de desplegament si s'aplica.
- La configuració sensible, credencials, claus i paràmetres protegits s'hauran de gestionar mitjançant Azure Key Vault, consumits pels pods a través d'External Secrets o mecanisme equivalent definit per Aigües de Barcelona. No es permet incloure secrets en codi font, imatges Docker, fitxers de configuració versionats ni variables no securitzades.

- Per a cada microservei, l'adjudicatari haurà de definir els requisits de recursos i límits operatius, incloent-hi requests i límits de CPU i memòria, quotes de namespace, nombre mínim i màxim de rèpliques, criteris d'escalat i comportament esperat davant de pics de càrrega.
- Els microserveis hauran d'implementar health checks i readiness/liveness probes, permetent al clúster gestionar correctament disponibilitat, reinicis i retirada controlada de trànsit.
- El disseny haurà de contemplar resiliència, idempotència, control d'errors, timeouts, reintents controlats i gestió de respostes normalitzades cap a ADF o cap al consumidor que correspongui.
- Els logs s'han d'emetre en format estructurat i han de ser compatibles amb el model corporatiu d'observabilitat, incorporant correlation ID, nom d'integració, identificador d'execució, severitat, timestamps, resultat funcional i errors tècnics o de negoci.
- Quan un microservei sigui invocat des d'ADF, haureu de tornar una resposta clara i normalitzada que permeti a ADF determinar el resultat de l'execució i actualitzar l'estat global del flux.
- Els microserveis han de ser independents i desacoblats.
- Els serveis han de ser stateless sempre que sigui possible.

Capa de missatgeria i streaming

Objectiu:

Actuar com a punt centralitzat d'exposició, securització, mediació i govern de serveis i integracions.

Components principals:

- Apache Kafka
- Kafka Connect
- Strimzi sobre AKS

Responsabilitats:

- Publicació i consum d'esdeveniments.
- Distribució desacoblada de dades.
- Replay d'esdeveniments.
- Processament near real-time.
- Integració productor-consumidor desacoblada.
- Disponibilització de dades cap a múltiples destinacions.
- Persistència temporal d'esdeveniments.

Consideracions:

- Kafka s'haurà d'utilitzar només quan aporti valor clar i consensuat dins del Pla de Migració.
- No totes les integracions requeriran streaming.
- Especialment orientat a:
 - Alt volum
 - Near real-time
 - Replay
 - Múltiples consumidors
 - Alta resiliència
- En cas que l'adjudicatari hagi de desenvolupar, adaptar o aplantillar un nou connector o plugin per a Kafka Connect, aquest s'haurà d'empaquetar de manera desacoblada respecte a la imatge base corporativa de Kafka Connect. La imatge base s'ha de mantenir tan neta,

estable i reutilitzable com sigui possible, evitant incorporar lògica específica de projecte o dependències particulars d'una integració concreta.

- Els connectors, llibreries addicionals i fitxers jar específics s'han de gestionar mitjançant una imatge derivada, artefacte independent o mecanisme de distribució validat per Aigües de Barcelona, garantint traçabilitat, versionat, reproductibilitat i control del cicle de vida del component. L'adjudicatari haurà de documentar les dependències incorporades, compatibilitats, procediment de build, desplegament i actualització del connector, així com les implicacions operatives sobre el clúster Kafka Connect gestionat mitjançant Strimzi a AKS.

Capa de persistència i staging

Objectiu:

Desacoblar processos i garantir persistència temporal i reprocés.

Components principals:

- Azure Data Lake Storage (ADLS)
- Azure Blob Storage

Responsabilitats:

- Landing de dades.
- Persistència temporal d'integracions.
- Reprocessament.
- Històrics tècnics.
- Intercanvi desacoblat entre sistemes.
- Emmagatzematge de fitxers.
- Versionat d'informació.

Consideracions:

- ADLS/Blob actuaran com a capa intermèdia de desacoblament.
- Permetrà recuperació davant d'errors i replay funcional.
- Especialment important per a integracions batch i fitxers.
- L'adjudicatari haurà de notificar a l'equip d'Infraestructura d'Aigües de Barcelona, si cal aplicar regles o polítiques de gestió del cicle de vida dels blobs.

Capa d'integració SAP

Objectiu:

Gestionar integracions SAP natives mitjançant components especialitzats compatibles amb protocols SAP.

Components principals:

- SAP Java Connector
- SAP .Net Connector
- Microserveis AKS especialitzats SAP.

Responsabilitats:

- Comunicació RFC.
- Processament i generació de IDocs.
- Reintents i control errors SAP.
- Conversió de formats cap a estructures SAP.
- Compatibilitat amb protocols propietaris SAP.

Consideracions:

- Les integracions SAP complexes no s'han d'implementar directament a l'ADF.

- Cal utilitzar llibreries oficials suportades per SAP.
- Els components s'han de desplegar desacoblats sobre AKS.
- Es prioritzarà la mantenibilitat i el suport fabricant.
- Azure Data Factory disposa de connectors nadius i capacitats preestablertes que es podran fer servir en aquelles integracions orientades a la ingesta de dades des de sistemes SAP, especialment en escenaris d'extracció, còpia o consum d'informació estructurada. L'adjudicatari haurà d'analitzar i validar, per a cada integració, si les capacitats proporcionades pels connectors esmentats, juntament amb l'ús del Self-hosted Integration Runtime corporatiu, resulten suficients per cobrir els requisits funcionals, tècnics, operatius i de rendiment definits per al procés.
- En aquells casos on les limitacions del connector nadiu, del model d'execució d'ADF o de la connectivitat mitjançant Self-hosted Integration Runtime no permetin satisfer adequadament les necessitats d'integració, especialment en escenaris basats en RFC, BAPI, IDoc, processament transaccional, validacions complexes o lògica funcional presents, els adjudicataris hauran d'externalitzar aquesta implementant components especialitzats desacoblats sobre AKS i utilitzant les llibreries oficials suportades per SAP quan correspongui.

Capa d'observabilitat i monitorització

Objectiu:

Garantir visibilitat end-to-end de tota la plataforma.

Components principals:

- Azure Monitor
- Log Analytics
- Grafana

Responsabilitats:

- Centralització de logs.
- Mètriques tècniques i funcionals.
- Traçabilitat distribuïda.
- Correlation IDs.
- Alertes proactives.
- Dashboards operacionals.
- Monitorització SLA.
- Diagnòstic end-to-end.

Consideracions:

- Tota integració haurà de ser monitoritzada.
- Tots els components han de seguir un esquema comú de logging.
- Els dashboards haurien d'unificar visió tècnica i funcional.
- El model haurà de suportar troubleshooting distribuït.

Capa de Govern i DevOps

Objectiu:

Garantir consistència, traçabilitat, governança tècnica i homogeneïtat operativa sobre tots els components d'integració, desplegament i cicle de vida programari de la plataforma.

Components principals:

- Azure DevOps
- GitLab
- Jenkins

- Catàleg d'integracions
- Plantilles reutilitzables de desplegament i orquestració

Responsabilitats:

- Gestió i versió de codi font.
- Gestió de pipelines CI/CD.
- Construcció i publicació d'imatges Docker.
- Gestió de releases i promoció entre entorns.
- Estandardització de desplegaments i configuracions.
- Gestió de nomenclatures i convencions corporatives.
- Generació de plantilles reutilitzables.
- Gestió documental i catàleg tècnic d'integracions.
- Traçabilitat completa del cicle de vida de cada integració.
- Automatització de desplegaments sobre AKS i ADF.
- Control de configuració i parametrització per entorn.

Consideracions:

- Tota integració desenvolupada dins del projecte haurà de seguir els estàndards, nomenclatures, estructures de repositori i procediments definits per Aigües de Barcelona.
- Per a components desplegats sobre AKS, GitLab s'estableix com a repositori corporatiu de codi font i Jenkins com a eina corporativa de construcció i desplegament.
- L'adjudicatari haurà de repositoritzar tot el codi desenvolupat a GitLab i col·laborar amb l'equip DevOps d'Aigües de Barcelona en la definició i adaptació de pipelines de CI/CD, construcció d'imatges Docker, publicació a ACR i desplegament automatitzat sobre AKS.
- A causa de la incompatibilitat actual d'Azure Data Factory amb GitLab com a repositori Git corporatiu, tota la gestió de codi font, versionat i desplegament associada a ADF s'haurà de realitzar mitjançant Azure DevOps, utilitzant l'organització corporativa ja existent i actualment operativa a Aigües de Barcelona.
- L'adjudicatari haurà d'adaptar-se al model CI/CD definit per Aigües de Barcelona per a ADF, aplicant les estratègies de versionat, branching, publicació i promoció entre entorns existents a la plataforma, contemplant com a mínim els entorns de desenvolupament, preproducció i producció.
- Els desplegaments s'han de fer mitjançant mecanismes automatitzats i controlats, evitant configuracions manuals o canvis directes sobre els entorns.
- Els desplegaments entre entorns hauran de poder executar-se mitjançant mecanismes automatitzats i governats, basats en configuració parametritzable, facilitant la promoció controlada dels components entre desenvolupament, preproducció i producció, reduint dependències manuals i millorant la sostenibilitat operativa futura.
- Els components desplegats sobre AKS han d'utilitzar Helm Charts parametritzables i reutilitzables, alineats amb els estàndards corporatius definits per Aigües de Barcelona.
- A causa de la naturalesa distribuïda i desacoblada de l'arquitectura objectiu, es considera crític establir mecanismes homogenis de govern i automatització que permetin mantenir consistència operativa entre pipelines ADF, microserveis AKS, connectors Kafka, APIs i components auxiliars.
- L'adjudicatari haurà de col·laborar activament amb l'equip DevOps per garantir que tots els components compleixin les guies corporatives de desplegament, observabilitat, seguretat, naming, gestió de secrets i operació.
- S'hauran de generar patrons reutilitzables tant per a pipelines ADF com per a microserveis, Helm Charts, connectors Kafka i components d'integració, amb l'objectiu de reduir complexitat operativa i facilitar evolucions futures.

- El catàleg d'integracions serà obligatori i s'haurà de mantenir actualitzat durant tot el projecte, incorporant-hi informació funcional, tècnica, dependències, diagrames de flux, endpoints, components utilitzats, versionat i estratègia de desplegament.
- El model definit haurà de facilitar l'autonomia futura d'Aigües de Barcelona, permetent que els equips interns puguin evolucionar, desplegar, operar i mantenir la plataforma sense dependència estructural de l'adjudicatari.

Capa de seguretat

Objectiu:

Garantir l'aplicació transversal de controls de seguretat sobre tots els components, les integracions, les comunicacions i els processos de la plataforma, assegurant el compliment dels estàndards corporatius d'Aigües de Barcelona en matèria d'identitat, accés, connectivitat, protecció de secrets i securització d'entorns cloud-native.

Components principals:

- Azure Key Vault.
- Azure API Management (APIM).
- Seguretat d'AKS.
- Private Endpoints.
- Pipelins d'anàlisi de vulnerabilitats.

Responsabilitats:

- Gestió segura de secrets, certificats i credencials.
- Control d'accés i segregació de permisos.
- Autenticació i autorització de serveis i APIs.
- Protecció i securització de comunicacions.
- Gestió de certificats i xifratge.
- Segmentació i aïllament entre entorns.
- Validació de vulnerabilitats i hardening de components.
- Aplicació de controls de seguretat sobre imatges Docker i desplegaments.
- Garantir el compliment de les polítiques corporatives de connectivitat i exposició de serveis.

Consideracions:

- Cap secret, credencial, certificat o informació sensible no es pot emmagatzemar en codi font, imatges Docker, pipelines, repositoris Git ni configuracions no securitzades. Tota informació sensible s'haurà de gestionar mitjançant Azure Key Vault.
- La seguretat haurà d'aplicar-se de forma transversal sobre totes les capes de l'arquitectura, incloent-hi pipelins ADF, microserveis AKS, APIs, connectors Kafka, emmagatzematge i processos d'integració.
- Tots els entorns s'han de mantenir completament segregats entre si evitant la cruïlla de comunicacions, recursos, configuracions o desplegaments entre entorns de desenvolupament, preproducció i producció.
- Qualsevol recurs Azure que requereixi connectivitat dins de la solució haurà de desplegar-se utilitzant Private Endpoints evitant exposició pública innecessària i garantint comunicacions internes securitzades.
- Com a principi general, totes les comunicacions s'han de fer mitjançant connectivitat privada i interna dins la xarxa corporativa d'Aigües de Barcelona. Únicament es poden exposar externament aquelles integracions o processos que requereixin comunicació amb sistemes aliens a l'organització passant pels mecanismes corporatius de securització i govern definits per Aigües de Barcelona.

- Els microserveis desplegats sobre AKS han de complir les polítiques corporatives de hardening, segmentació, control d'accés, gestió d'identitats i limitació de privilegis si s'apliqués així.
- Abans de la promoció de qualsevol imatge Docker cap a entorns productius, aquesta haurà de passar obligatòriament pels pipelines corporatius d'anàlisi de vulnerabilitats i de validació de seguretat definits per Aigües de Barcelona.
- L'adjudicatari serà responsable d'analitzar, corregir i resoldre les vulnerabilitats detectades durant aquests processos de validació, i no es podran promoure a producció imatges que incompleixin els llindars de seguretat definits per l'organització.
- Totes les APIs i serveis exposats han d'implementar autenticació, autorització i xifratge de comunicacions d'acord amb els estàndards vigents.
- L'adjudicatari haurà de col·laborar amb els equips de Seguretat, Arquitectura i DevOps d'Aigües de Barcelona per garantir el compliment de totes les polítiques corporatives de seguretat cloud i operació segura sobre Azure i AKS.

6. CONSIDERACIONS ESPECÍFIQUES DEL DISSENY

El present projecte no planteja, amb caràcter general, una reenginyeria integral dels processos existents ni una transformació indiscriminada dels patrons d'integració actuals, sinó una migració controlada i alineada amb l'arquitectura objectiu definida per Aigües de Barcelona.

No obstant això, Aigües de Barcelona considera que determinades integracions, ja sigui per la seva complexitat funcional, criticitat operativa, nivell d'acoblament tècnic, dependències associades o rellevància dins l'ecosistema corporatiu, no resulten adequades per ser implementades exclusivament mitjançant patrons d'orquestració o fluxos d'integració simples sobre Azure Data Factory.

En aquest sentit, les integracions identificades preliminarment per Aigües de Barcelona com a crítiques, així com aquelles altres que, com a resultat de les fases de discovery, anàlisi funcional i validació tècnica, es determini justificadament que requereixen un model arquitectònic diferenciat, hauran d'evolucionar cap a components aplicatius independents dins l'abast del present projecte.

L'adjudicatari haurà de dissenyar, desacoblar, desenvolupar i desplegar aquests components seguint les directrius arquitectòniques definides en el present plec per a entorns basats en AKS, adoptant un model cloud-native basat en microserveis, amb criteris de resiliència, escalabilitat, observabilitat, seguretat, mantenibilitat i autonomia operativa.

Aquests components deixaran de concebre's com a simples fluxos d'integració dependents d'una plataforma middleware centralitzada, passant a tractar-se com a aplicacions independents amb cicle de vida propi, responsabilitats clarament delimitades i capacitat d'evolució futura dins del model operatiu corporatiu.

La lògica funcional, el processament transaccional, les validacions específiques i qualsevol capacitat d'integració avançada associada a aquests casos hauran de residir dins d'aquests components aplicatius, evitant reproduir patrons d'acoblament o dependència estructural similars als del model actual.

Un cop implementats, aquests nous aplicatius passaran a integrar-se dins el model operatiu habitual d'Aigües de Barcelona i seran mantinguts pels equips responsables de les diferents àrees tecnològiques que actualment gestionen altres sistemes crítics corporatius.

Adicionalment, Aigües de Barcelona sol·licita a l'adjudicatari la implementació d'una capa lleugera de serveis orientada al desacoblament progressiu de l'actual sistema Content Manager.

Aquesta capa haurà d'actuar com a façade o gateway d'interoperabilitat, exposant mitjançant APIs REST un conjunt d'operacions actualment suportades mitjançant serveis SOAP relacionats principalment amb la pujada, la descàrrega i la consulta de documents, factures i fitxers associats.

L'objectiu d'aquesta capa no és únicament modernitzar l'exposició tècnica dels serveis esmentats, sinó reduir l'acoblament directe existent entre les integracions i l'actual Content Manager, facilitant evolucions o migracions futures d'aquesta plataforma sense necessitat de modificar novament els consumidors integrats. Així mateix, aquesta aproximació respon a les limitacions inherents al model SOAP dins d'Azure API Management, ja que, si bé APIM permet exposar i transformar serveis SOAP cap a REST, aquestes capacitats presenten restriccions funcionals i de flexibilitat que no sempre són adequades per a determinats escenaris d'integració complexa o manipulació documental.

Per aquest motiu, Aigües de Barcelona considera més adequat evolucionar progressivament aquests serveis cap a una capa d'API REST desacoblades i controlades mitjançant microserveis específics, securitzats i governats a través d'APIM i desplegats sobre l'arquitectura definida al model TO-BE.

7. FASES DEL PROJECTE

El procés de modernització i migració de la plataforma d'integració corporativa s'haurà d'executar mitjançant un enfocament progressiu, controlat i estructurat en diferents fases funcionals i tècniques, permetent minimitzar el risc operacional i garantir la continuïtat dels serveis durant tota la transició des de la plataforma actual basada en Red Hat Fuse cap a l'arquitectura objectiu definida per Aigües de Barcelona.

L'adjudicatari haurà de plantejar una estratègia de coexistència temporal entre els entorns AS-IS i TO-BE que permeti garantir l'estabilitat operativa en tot moment.

Les fases i els lliurables descrits a continuació estableixen el marc mínim d'execució esperat per Aigües de Barcelona. Això no obstant, l'adjudicatari podrà proposar ajustos metodològics o refinaments sobre les fases aquí plantejades:

Fase 0 – Kickoff i Govern del Projecte

Objectiu general

Constitució i posada en marxa formal del projecte, definint el model organitzatiu, de govern i de seguiment que regirà tota l'execució de la migració.

Objectius específics	• Constitució formal del projecte • Definició d'equips, rols i responsables. • Definició del model de govern i seguiment. • Validació de la metodologia de treball. • Definició de canals de comunicació i escalat.
Lliurables	• Organització i estructura del projecte. • Matriu RACI. • Planificació inicial i roadmap. • Model de reporting i seguiment.

Fase 1 – Discovery/Anàlisi

Objectiu general	Realitzar una anàlisi funcional i tècnica detallada de les integracions actuals, validant l'inventari existent i completant tota la informació necessària per dissenyar l'estratègia de migració.
Objectius específics	• Anàlisi detallada de totes les integracions. • Revisió de fluxos Red Hat Fuse. • Identificació de dependències tècniques i funcionals. • Anàlisi de protocols utilitzats. • Classificació d'integracions per complexitat i criticitat. • Identificació de patrons reutilitzables. • Anàlisi de volumetria i finestres operatives. • Revisió de monitorització i traçabilitat actual. • Identificació de riscos i restriccions tècniques. • Anàlisi de necessitats SAP RFC/BAPI/IDoc. • Validació d'integracions candidates a microserveis. • Identificació d'integracions simples candidates a ADF.
Lliurables	• Document AS-IS validat. • Catàleg tècnic d'integracions. • Classificació d'integracions per patró, criticitat i complexitat. • Matriu de dependències. • Riscos inicials. • Recomanació tècnica per integració.

Fase 2 – Pla de Migració

Objectiu general	Definir l'estratègia detallada de migració i consensuar amb Aigües de Barcelona l'arquitectura final aplicable a cada integració.
-------------------------	---

**Objectius
específics**

- Definició d'arquitectura TO-BE definitiva.
- Assignació de patró tècnic per integració.
- Disseny de coexistència AS-IS/TO-BE.
- Definició de l'estratègia de rollback.
- Definició de l'observabilitat end-to-end.
- Definició de pipelines CI/CD.
- Definició del pla de proves.
- Priorització i seqüenciació de migracions.

Lliurables

- Pla de Migració detallat amb arquitectura TO-BE validada que inclogui:
 - Llistat de necessitats per abordar la migració.
 - Roadmap d'execució.
 - Pla de coexistència.
 - Estratègia de rollback.
 - Pla de proves.
 - Estratègia DevOps.
 - Estratègia d'observabilitat.
 - Diagrama d'arquitectura TO-BE.

Fase 3 – Arquitectura TO-BE**Objectiu
general**

Plataforma preparada per iniciar migracions, components base desplegats, patrons reutilitzables definits, mecanismes de desplegament i observabilitat operatius i model de col·laboració entre equips activat.

Fase 4 – Migració**Objectiu
general**

Migrar progressivament les integracions des de Red Hat Fuse cap a la nova arquitectura minimitzant-ne l'impacte operatiu.

Estratègia

- La migració haurà de realitzar-se de forma incremental i controlada, agrupant integracions per:
 - Complexitat
 - Criticitat
 - Dependències
 - Patró tècnic
 - Risc operacional

Consideracions

- No es permetrà migració Big Bang.
- Tota integració s'haurà de validar individualment.
- Cal mantenir rollback controlat.
- Tota integració haurà de disposar de traçabilitat end-to-end.

- Tota migració haurà d'estar documentada.

Fase 5 – Validació i cutover

Objectiu general	Validar funcionalment i tècnicament les integracions migrades, garantint una transició controlada entre la plataforma AS-IS i TO-BE mitjançant mecanismes de coexistència, rollback i continuïtat operativa.
Objectius específics	• Validació funcional i tècnica de cada integració. • Validació de rendiment, seguretat i observabilitat. • Execució controlada del cut-over. • Gestió de coexistència AS-IS/TO-BE. • Definició i validació de mecanismes de rollback i contingència.
Lliurables	• Evidències de proves funcionals i tècniques. • Pla de cut-over i rollback. • Procediments operatius de transició i suport.

Fase 6 – Desconnexió de Red Hat Fuse

Objectiu general	Retirada controlada i definitiva de la plataforma AS-IS
Objectius específics	• Certificació de negoci abans de desconnectar Fuse. • Validació de migració completa. • Eliminació de dependències. • Apagat controlat. • Retirada de configuracions. • Actualització documental. • Transferència operativa final.
Lliurables	• Document o fitxa de tancament del projecte. • Catàleg actualitzat. • Documentació operativa final i actualitzada. • Traspàs i capacitat feta a l'equip d'Aigües de Barcelona. • Informe de deute tècnic o estratègia de millora futura.

8. METODOLOGIA DEL PROJECTE

L'adjudicatari haurà de plantejar una metodologia d'execució alineada amb un model híbrid de gestió del projecte, combinant planificació estructurada, control de fites i govern global del programa amb una execució iterativa i incremental de les integracions.

Atesa la criticitat de la plataforma actual i la necessitat de garantir continuïtat operativa durant tota la migració, Aigües de Barcelona no considera viable una estratègia de substitució tipus Big Bang ni un enfocament purament waterfall per a l'execució de les integracions. La migració s'haurà de fer mitjançant onades progressives, permetent desenvolupar, validar i desplegar integracions de forma independent i controlada.

La proposta haurà d'incloure com a mínim:

- Organització de fases.
- Estratègia d'execució per 'waves' incloent coexistència i rollback.
- Model de seguiment.
- Gestió de riscos i dependències.
- Estratègia i model de validació.
- Gestió del canvi.
- Model de comunicació.
- Mecanismes de control de qualitat i govern tècnic.

9. REQUISITS DEL LICITADOR

9.1. Experiència i capacitat tècnica

L'abast del present projecte requereix capacitats que van més enllà del desenvolupament tècnic d'integracions individuals, exigint una comprensió integral d'arquitectures middleware, fluxos d'informació empresarials, patrons d'integració i estratègies de modernització tecnològica. En aquest sentit, el licitador haurà de demostrar experiència acreditada en projectes de modernització, transformació o substitució de plataformes middleware corporatives, així com iniciatives orientades al desacoblament d'integracions, eliminació de dependències rígides entre sistemes i evolució cap a arquitectures distribuïdes més resilents, escalables i mantenibles.

Es valorarà especialment l'experiència del licitador en projectes d'anàlisi, transformació i modernització d'ecosistemes complexos d'integració empresarial, incloent-hi la capacitat de comprendre fluxos de dades end-to-end, identificar dependències entre sistemes, avaluar patrons d'integració existents i definir estratègies d'evolució tecnològica alineades amb principis moderns d'arquitectura empresarial.

Resultarà particularment rellevant acreditar experiència en projectes on hagi estat necessari redistribuir responsabilitats entre components tecnològics, desacoblar sistemes fortament integrats, definir patrons reutilitzables d'integració, establir models d'observabilitat extrem a extrem i executar migracions progressives amb coexistència temporal entre arquitectures legacy i noves plataformes utilitzant tecnologies semblants a les descrites.

Així mateix, el licitador haurà d'acreditar experiència sòlida i contrastable de mínim cinc (5) anys, en tecnologies de l'ecosistema Microsoft Azure, incloent-hi arquitectures híbrides, arquitectures basades en microserveis i patrons moderns d'integració empresarial, exposició de serveis, capacitats de disseny, desenvolupament, desplegament i operació sobre entorns empresarials productius.

El licitador haurà d'aportar referències de projectes executats de naturalesa equivalent, incloent-hi una descripció de l'abast, la complexitat, les tecnologies involucrades, la durada aproximada del projecte, la tipologia del client i el rol exercit per la seva organització. Aigües de Barcelona podrà valorar especialment aquelles referències que demostrin experiència real en projectes de migració amb característiques similars a les contemplades al present plec.

9.2. Equip de projecte

L'adjudicatari haurà d'assignar al projecte un equip multidisciplinari amb experiència acreditada en integració empresarial, arquitectures distribuïdes, desenvolupament cloud-native i execució de projectes de modernització tecnològica.

La composició indicada a continuació constitueix una proposta orientativa de perfils tècnics de referència que Aigües de Barcelona considera coherent amb la naturalesa, complexitat i abast del projecte. Aquesta composició NO implica necessàriament dedicacions permanents, exclusives ni simultànies durant tota l'execució contractual, però sí la disponibilitat efectiva dels perfils i capacitats requerides en funció de les necessitats específiques de cada fase, integració, nivell de complexitat tècnica o activitat prevista dins del projecte.

Es considera necessari disposar, com a mínim, dels perfils equivalents següents:

- **Arquitecte d'Integració**

Perfil amb una experiència mínima acreditada de **SIS (6) anys** en integració empresarial, arquitectura middleware, arquitectures distribuïdes i modernització d'ecosistemes complexos d'integració. Aquest perfil actuarà com a principal responsable tècnic del projecte, liderant l'anàlisi de les integracions existents, la definició dels patrons arquitectònics aplicables, la validació de decisions tècniques i el correcte alineament amb el model TO-BE definit per Aigües de Barcelona.

Haurà d'acreditar coneixement pràctic en tecnologies i patrons d'integració empresarial, exposició i consum d'APIs, arquitectures desacoblades, microserveis i entorns cloud-native. Es considerarà necessari que disposi d'un ampli coneixement en l'ecosistema Azure objecte del projecte, especialment en components descrits a l'arquitectura objectiu: Azure Data Factory, AKS, APIM, Azure Log Analytics, etc i models de desplegament moderns. Es valorarà positivament que aquest perfil disposi també de capacitats pràctiques de desenvolupament backend i experiència directa en implementació tècnica.

- **Desenvolupador Backend Senior / Integració**

Perfil amb una experiència mínima acreditada de **CINC (5) anys** en desenvolupament de components backend, integracions empresarials i serveis distribuïts.

Haurà d'acreditar experiència pràctica en algun dels stacks tecnològics previstos al projecte (Java/Spring Boot, .NET o Python), així com en desenvolupament de microserveis, consum i exposició d'APIs, Kafka, Docker, Kubernetes, Helm i desplegament sobre entorns AKS.

Es considera igualment necessari que aquest perfil disposi de coneixement tècnic suficient en l'ecosistema Azure requerit per al projecte, especialment en aquells components amb els quals interactuarà directament.

- **Project Manager**

Perfil amb una experiència mínima acreditada de **CINC (5) anys** en gestió de projectes tecnològics d'integració, modernització aplicativa o transformació cloud.

Serà responsable del seguiment global de l'execució, planificació, coordinació d'activitats, gestió de riscos, interlocució amb stakeholders, preparació de comitès de seguiment i control de dependències.

Haurà d'acreditar experiència en eines de gestió i seguiment com Jira i/o Azure DevOps, incloent gestió de backlog, incidències, planificació, roadmaps, dependències i reporting executiu.

- **Capacitats especialitzades complementàries**

Atesa la naturalesa del projecte, l'adjudicatari haurà de garantir la disponibilitat efectiva de capacitats tècniques especialitzades complementàries quan resultin necessàries.

En particular, amb la presència d'integracions amb sistemes SAP mitjançant protocols específics (RFC, IDoc, BAPI o mecanismes equivalents), l'adjudicatari haurà de disposar d'experiència acreditable en integració amb entorns SAP, ja sigui mitjançant perfils propis integrats dins l'equip proposat o com a capacitat tècnica especialitzada directament disponible durant el projecte.

L'adjudicatari haurà de disposar, en tot moment durant la vigència del contracte, de l'equip humà necessari per garantir la correcta execució dels serveis objecte del present plec, amb independència de la denominació concreta dels perfils professionals proposats. Les dedicacions associades hauran de ser coherents amb el volum, la complexitat i la planificació de les activitats plantejades, garantint en tot moment una capacitat real, suficient i efectiva de participació. No s'acceptaran propostes basades en assignacions merament nominals o en perfils sense disponibilitat efectiva per atendre les necessitats reals del projecte.

Aigües de Barcelona complementarà l'equip del projecte amb perfils interns especialitzats en data i arquitectura cloud d'Azure, perfils DevOps, infraestructura i gestió del projecte, que actuaran com a interlocutors i responsables d'aquelles activitats sota competència interna. Això no obstant, això no eximeix l'adjudicatari d'aportar l'equip tècnic necessari per garantir la correcta execució de l'abast contractat.

Es valorarà positivament que el licitador pugui proposar una composició alternativa de l'equip de treball, sempre que estigui degudament justificada i aporti valor real al projecte.

10. GARANTIA

El període de garantia aplicable als desenvolupaments, les integracions i els serveis lliurats en el marc del present projecte s'ha d'aplicar de forma individual i independent a cadascuna de les versions, onades o lliuraments parcials que siguin posats en producció, incloent-hi expressament l'últim lliurament corresponent a la finalització del projecte.

A aquests efectes, cada integració, procés o component que sigui desplegat en producció i acceptat d'acord amb el procediment de validació definit, disposarà d'un període mínim de garantia de **SIS (6) mesos**, comptats des de la posada en producció efectiva, activació operativa i acceptació per part d'Aigües de Barcelona.

En el cas de la darrera release o darrera posada en producció del projecte, aquest període de garantia començarà a computar-se des de la formalització del tancament del projecte mitjançant la corresponent Fitxa de Tancament de Projecte o document equivalent d'acceptació final.

Durant el període de garantia, l'adjudicatari haurà de corregir, sense cost addicional per a Aigües de Barcelona, qualsevol defecte, error, mal funcionament, desviació funcional o incidència imputable als desenvolupaments, configuracions, integracions o components lliurats, garantint-ne la correcta operació d'acord amb els requisits establerts en aquest plec.

11. SUPORT AUDITORIA DE SEGURETAT

Els desenvolupaments implementats i desplegats als entorns d'Aigües de Barcelona hauran de complir els requisits de seguretat establerts per l'organització i no podran presentar vulnerabilitats que comprometin la confidencialitat, integritat i/o disponibilitat dels sistemes i serveis corporatius.

Amb aquesta finalitat, Aigües de Barcelona requerirà la realització d'una auditoria de seguretat independent, executada per un proveïdor especialitzat extern, sobre els components desenvolupats en el marc del projecte. Aquesta auditoria podrà incloure anàlisi de vulnerabilitats, revisió de configuracions, validacions de seguretat sobre els desenvolupaments implementats i qualsevol altra prova que es consideri necessària per garantir el compliment dels requisits de seguretat corporatius.

En aquest context, l'adjudicatari haurà de:

- Facilitar la col·laboració necessària amb l'equip auditor, proporcionant suport tècnic, aclariments funcionals i tota la informació requerida sobre l'arquitectura, configuració, desenvolupaments implementats i mecanismes de seguretat adoptats.
- Analitzar, corregir i remediador, sense cost addicional per a Aigües de Barcelona, totes les vulnerabilitats, desviacions o deficiències de seguretat identificades que siguin imputables als desenvolupaments, configuracions o components objecte del projecte.
- Executar les correccions necessàries en un termini màxim de **QUINZE (15) dies** naturals des de la notificació dels resultats de l'auditoria, tant en la revisió inicial com en eventuais processos de retest, no considerant-se acceptable el pas a producció definitiu o el tancament de l'entrega mentre persisteixin vulnerabilitats crítiques o altes pendents de resolució, llevat d'acceptació expressa per part d'Aigües de Barcelona.

12. ALTRES REQUERIMENTS

12.1. Ubicació i modalitat de treball

La prestació dels serveis es realitzarà amb caràcter general en modalitat remota, des de les instal·lacions de l'adjudicatari o des de la ubicació que aquest determini per a la correcta execució dels treballs, sempre que es garanteixi la disponibilitat, coordinació i qualitat del servei compromès.

No obstant això, Aigües de Barcelona podrà requerir, quan la naturalesa del projecte, determinades activitats específiques o necessitats de coordinació així ho aconsellin, la presència puntual de membres de l'equip de l'adjudicatari a les seves oficines o centres de treball, especialment per a sessions d'arrencada, workshops de discovery, reunions de seguiment, sessions tècniques, validacions funcionals, activitats de transferència de coneixement interacció presencial.

Així mateix, en funció de circumstàncies concretes del projecte o de tasques específiques que així ho justifiquin, Aigües de Barcelona podrà sol·licitar la prestació presencial total o parcial de determinats treballs als seus centres de treball, ubicats dins l'àmbit territorial de l'Àrea Metropolitana de Barcelona, sense que això suposi un increment addicional en el cost dels serveis contractats.

12.2. Recursos materials requerits

Els Prestador dels Serveis serà responsable de disposar de l'equip de treball, així com de tot l'equipament maquinari, programari, i altres especificacions fixades en el present Plec, que sigui necessari per a l'execució del servei contractat, sense que en cap cas puguin facturar-se la compra, el subministrament o bé la instal·lació d'equips i recanvis que siguin necessaris per a realitzar el servei objecte d'aquest Contracte.

No obstant això, Aigües de Barcelona proporcionarà al Prestador del Servei:

- Usuaris locals o de domini amb els permisos necessaris.
- Les eines de reporting i seguiment del projecte, segons s'indiquen en el present plec.

12.3. Eines de seguiment i gestió del projecte

Aigües de Barcelona posarà a disposició de l'adjudicatari les eines corporatives de seguiment i gestió del projecte, i es podrà utilitzar Jira o Azure DevOps, en funció del model operatiu finalment definit durant la fase de Kick-Off del projecte.

Aquestes eines constituïran el repositori oficial per a la gestió i el seguiment operatiu del projecte, incloent-hi el registre i la traçabilitat del backlog, la planificació d'activitats, la gestió de tasques, les incidències, els defectes detectats durant les diferents fases de validació, els comentaris tècnics, les dependències, els bloquejos, els riscos i el seguiment general de l'execució.

El model de treball s'haurà de recolzar en un tauler de seguiment tipus Kanban o equivalent, que permeti disposar en tot moment de visibilitat sobre l'estat de les activitats, les integracions en curs, les validacions pendents, les incidències obertes i l'evolució global del projecte.

Serà responsabilitat de l'adjudicatari mantenir actualitzada de forma contínua la informació relativa a l'estat d'execució de les tasques sota la seva responsabilitat, garantint la traçabilitat, transparència i seguiment correcte del projecte per part d'Aigües de Barcelona.

La documentació funcional, tècnica, operativa i de projecte associada al servei s'haurà de registrar als repositoris documentals corporatius que Aigües de Barcelona determini, podent utilitzar eines com Google Drive o equivalents corporatius, en funció de la tipologia de la documentació i del model de treball acordat.

12.4. **Acords de Nivell de Servei (ANS) durante el Projecte**

El present apartat té per objectiu fixar els nivells de servei (ANS), estàndards d'execució i els criteris i processos de mesura o valoració dels resultats exigits als Prestadors del Servei per a la provisió dels mateixos.

- **ANS-01 (Puntualitat en l'entrega dels Informes de Seguiment del projecte):** Desviació en el número de dies, respecte el termini d'entrega de l'informe quinzenal establert en el present plec.

Indicador:	Puntualitat en l'entrega dels Informes de Seguiment del projecte (ANS-01).
Compliment:	Si ANS-01 ≤ 0 ☐ Sense efecte Si ANS-01 > 0 ☐ Incompliment
Periodicitat de càlcul:	Finalitzat cada període quinquenal (15 dies naturals).
Fórmula aplicada:	ANS-01 = (Nde - 5) (expressat en dies) On, Nde: Un cop finalitzat un període quinquenal (15 dies naturals), número de dies hàbils transcorreguts fins l'entrega de l'Informe de seguiment corresponent.
Càlcul de la Penalització acumulada P1:	Per cada incompliment s'afegeix un 2% al acumulat.

Nota: Els 15 dies naturals s'estableixen a tall d'exemple. La periodicitat dels informes dependrà de la metodologia de desenvolupament utilitzada i serà definida en el moment del Kick-Off, adaptant-se els càlculs a aquest període de seguiment definit.

- **ANS-02 (Retard en la data de finalització del projecte):** Desviació en el número de dies, respecte al termini màxim de finalització del projecte acordat.

Indicador:	Retard en la data de finalització del projecte (ANS-02).
Compliment:	Si ANS-02 ≥ 0 ☐ Sense efecte. Si ANS-02 < 0 ☐ Incompliment (excepte quan sigui per causes no imputables al Prestador del Servei).
Periodicitat de càlcul:	A la finalització del projecte (entregats en producció tots els requeriments de l'abast del projecte - entrega de la Fitxa de tancament de Projecte).
Fórmula aplicada:	ANS-02 = (Ndpe - Ndre) (expressat en dies naturals) On, Ndpe: Número de dies previstos per l'execució del projecte. Ndre: Número de dies reals usats per l'execució del projecte.

Indicador:	Retard en la data de finalització del projecte (ANS-02).		
Càlcul de la Penalització P2:	Si $0\% < (\text{ANS-02}/\text{Ndpe}) \leq 8\%$ S'afegeix un 4% de penalització a l'acumulat.	Si $8\% < (\text{ANS-02}/\text{Ndpe}) \leq 15\%$ S'afegeix un 8% de penalització a l'acumulat.	Si $(\text{ANS-02}/\text{Ndpe}) > 15\%$ S'afegeix un 10% de penalització a l'acumulat.

- **ANS-03 (Puntualitat en l'entrega dels Informes d'Incidència Significativa):** Desviació en el número de dies, respecte el termini d'entrega de l'informe establert en el present plec.

Indicador:	Puntualitat en l'entrega dels Informes d'Incidència Significativa (ANS-03).
Compliment:	Si ANS-03 ≤ 3 ☐ Sense efecte. Si ANS-03 > 3 ☐ Incompliment.
Periodicitat de càlcul:	Quan es produeix la incidència greu (tipificades com <i>Crítica</i> o <i>Alta</i>).
Fòrmula aplicada:	ANS-03 = (Fei – Fci) (<i>expressat en dies hàbils</i>) On, Fei: Data d'enviament a Aigües de Barcelona de l'Informe d'Incidència Significativa. Fci: Data de la comunicació de la incidència.
Càlcul de la Penalització acumulada P3:	Per cada incompliment s'afegeix un 2% a l'acumulat.

- **ANS-04 (Qualitat Producte Lliurat I):** Número d'incidències totals generades amb posterioritat a la posada a producció (post implantació) parcials, per cada Release, incloent l'última o de finalització del projecte.

Indicador:	Qualitat Producte Lliurat I (ANS-04).
Compliment:	Si ANS-04 ≤ 35 ☐ Sense efecte Si ANS-04 > 35 ☐ Incompliment
Periodicitat de càlcul:	A la finalització del període de garantia.
Fòrmula aplicada:	ANS-04 = (Nºincidències crítiques*9) + (Nºincidències altes*5) + (Nºincidències mitges*3)

Indicador:	Qualitat Producte Lliurat I (ANS-04).
Càlcul de la Penalització acumulada P3:	Si ANS-04 > 35, s'afegeix un 3% a l'índex de penalització acumulat. Si ANS-04 > 50, s'afegeix un 6% a l'índex de penalització acumulat. Si ANS-04 > 65, s'afegeix un 10% a l'índex de penalització acumulat..

• **ANS-05 (Qualitat Resolució d'incidències en Projecte)**

A continuació es descriuen el ANS-05 a aplicar durant el projecte, de les releases ja a productiu a partir dels indicadors reflectits en la següent taula:

Codi	Indicador	Descripció	Vc	Va	Vi	Unitat	Pes	Bonus	Malus
INC P1	Temps de resolució d'incidència amb categoria assignada "alta"	% d'incidències catalogades com a altes per impedir la feina d'un gran nombre d'usuaris o afectar processos crítics de l'empresa, ateses i resoltes en el termini: Temps de resposta <1 hora; Temps de resolució menor de 6 hores.	100	95	85	%	35	% per sobre del 95	- % entre el 95 i 85 - 10% de 85 cap avall
INC P2	Temps de resolució d'incidència amb categoria assignada "mitjana"	% d'incidències catalogades com a mitjanes, ateses i resoltes en el termini: Temps de resposta <5 hores; Temps de resolució menor de 8 dies hàbils.	100	95	85	%	20	% per sobre del 95	- % entre el 95 i 85 - 10% de 85 cap avall
INC P3	Temps de resolució d'incidència amb categoria assignada "baixa"	% d'incidències catalogades com a baixes, ateses i resoltes en el termini: Temps de resposta <6 hores; Temps de resolució menor de 30 dies hàbils.	100	95	85	%	14	% per sobre del 95	- % entre el 95 i 85 - 10% de 85 cap avall
INC P4	Reapertures d'incidències i Petició Operatives	Percentatges d'incidències o peticions que es van donar per resoltes i han tornat a produir-se	0	5	15	%	10	% fins al 5%	- % entre el 5 i 15 - 10% de 15 cap avall
INC P5	Tiquets oberts amb ANS incomplet	% de tiquets oberts amb ANS incomplet en el moment del tancament del projecte	0	5	15	%	7	% fins al 5%	- % entre el 5 i 15 - 10% de 15 cap avall
POP P1	Temps resolució de Peticions Operatives	% de Peticions Operatives ateses i resoltes en termini. Temps resolució 10 dies hàbils	100	95	85	%	14	% per sobre del 95	- % entre el 95 i 85 - 10% de 85 cap avall

Indicador:	Qualitat resolució incidències (ANS-05).
Compliment:	La fórmula de càlcul de la penalització contempla el criteri Bonus/Malus
Periodicitat de càlcul:	Al inici del servei de manteniment (Lot X) amb la signatura del acta d'acceptació
Fórmula aplicada:	$\mathbf{ANS-05} = \left(\sum (W_i * VW_i) \right)$ Donde: W_i (%) =Peso Indicador VW_i (%) = Valor Penalización Indicador = $B_i + M_i$ Con B_i="Bonus" Indicador; M_i="Malus" Indicador
Càlcul de la Penalització P5:	$P5 = \mathbf{ANS-05} * ,1$

On:

W_i (%) =Peso Indicador

VW_i (%) = Valor Penalización Indicador = $B_i + M_i$

Con B_i ="Bonus" Indicador; M_i ="Malus" Indicador

12.5. Penalitzacions derivades del incompliment en ANS Projecte

Els Prestadors del Servei es comprometen a complir amb els ANS establerts en el present Plec. Per tant, el no compliment d'aquests derivarà en les penalitzacions exposades en aquest apartat.

L'incompliment dels ANS podrà reduir l'import a facturar entre un 10% i un 25% del total adjudicat per a l'execució del projecte.

El percentatge de penalització a aplicar-se s'obté a partir de la suma dels percentatges parcials acumulats com a conseqüència dels incompliments registrats amb els ANS, segons els següents criteris:

Penalització	Criteri
P1	Per cada incompliment del ANS-01 , s'afegeix un 2% de penalització al acumulat. Per tant: $P1 = \left(\sum_{i=1}^n 2 \right) \%$, on n és el número d'incompliments del ANS-01 .
P2	Per incompliment del ANS-02 , s'afegeixen els següents percentatges de penalització, segons cada cas: • P2.1: Si $[0\% < (\mathbf{ANS-02}/\mathbf{Ndpf}) \leq 8\%]$, s'afegeix un 4% de penalització al acumulat. • P2.2: Si $[8\% < (\mathbf{ANS-02}/\mathbf{Ndpf}) \leq 15\%]$, s'afegeix un 8% de penalització al acumulat. • P2.3: Si $[(\mathbf{ANS-02}/\mathbf{Ndpf}) > 15\%]$, s'afegeix un 10% de penalització al acumulat.
P3	• Per cada incompliment del ANS-03, s'afegeix un 2% de penalització al acumulat. Per tant: $P1 = \left(\sum_{i=1}^n 2 \right) \%$, on n és el número d'incompliments del ANS-03 .
P4	Si ANS-04 > 35, s'afegeix un 3% a l'índex de penalització al acumulat. Si ANS-04 > 50, s'afegeix un 6% a l'índex de penalització al acumulat.

	Si ANS-04 > 65, s'afegeix un 10% a l'índex de penalització al acumulat.
P5	$P-05 = ANS - 05 * 0,1$

On la penalització total (PT) a aplicar a la finalització del projecte i/o del període de garantia serà el valor que resulti inferior d'entre els dos següents:

- Valor resultant d'aplicar la següent fórmula: $PT = P1 + P2 + P3 + P4 + P5$
- En cas de que el valor anterior (PT) sigui superior al 25%, s'aplicarà com a penalització el màxim del 25%.

Mentre **PT** sigui inferior al 10%, no s'aplicaran penalitzacions econòmiques derivades del incompliment amb els ANS.

Les penalitzacions econòmiques s'aplicaran a la finalització del "Pas a Productiu" i/o a la finalització del període de garantia, coincidint amb les fites de facturació associades i un cop que la penalització acumulada (**PT**) superi el 10%.

En el cas de que un Prestador del Servei acumuli un **PT** superior al 25%, Aigües de Barcelona estarà facultada per:

- resoldre el Contracte amb aquest Prestador del Servei, o bé
- continuar amb la imposició de penalitzacions en els termes previstos anteriorment.

12.6. Accés

L'accés als sistemes d'informació d'Aigües de Barcelona es realitzarà mitjançant connexió VPN Lan-to-Lan o amb usuaris VPN nominals.

Tot el personal extern que hagi de treballar en el projecte tindrà usuari personalitzat en els sistemes necessaris. A tal efecte s'haurà de proporcionar a l'inici del servei el email, nom, cognoms i DNI/NIE dels mateixos.

13. SEGURETAT CORPORATIVA

Tant el Prestador del Servei com els seus treballadors hauran de respectar les normes i regulacions internes que dicti l'àrea de Seguretat Corporativa, en matèria de Seguretat de la informació i ús de les TIC, com a mínim:

Acceptar les normes establertes en l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions (vegeu **Annex Núm. 2**).

Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte.

Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per a Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions realitzades per l'auditor per a facilitar el seguiment de les mateixes i els seus possibles impactes no desitjats.

A la finalització del contracte, el Prestador del Servei quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

14. ANNEX NÚM. 1 - CLASSIFICACIÓ DE LES INCIDÈNCIES

1. Introducció

En el següent annex es descriuen els criteris a aplicar per a categoritzar i prioritzar les incidències gestionades per l'actual eina de ITSM en Aigües de Barcelona.

A aquests efectes, es considerarà com Incidència: Error o qualsevol anomalia funcional o tècnica que desencadena un resultat no desitjat, no esperat o incomplet detectat en el sistema disponible per al client.

2. Criteris

2.1. Impacte

Determina la importància de l'incident depenent de com aquest afecta als processos i/o del número d'usuaris afectats. És a dir, el grau d'afectació que la incidència té en el servei.

Criteris per establir l'impacte		
Impacte	Descripció	Ponderació
0-Crític (Extens/Generalitzat)	- Parada total d'un Procés Crític - Parada total d'un servei/aplicació crític; - Degradació d'un servei/aplicació crític amb afectació massiva; - Incidència reportada per un usuari SVIP.	9
1-Alt (Significatiu/Ampli)	- Degradació d'un servei/aplicació crític sense afectació massiu; - Parada total o degradació d'un servei/aplicació NO crítica amb afectació massiva; - Incidència reportada per un usuari VIP; - Petició de servei d'un usuari SVIP;	5
2-Mitjà (Moderat/Limitat)	- Parada total o degradació d'un servei/aplicació NO crítica sense afectació massiva; - Petició de servei d'un usuari VIP.	3
3-Baix (Menor/Legalitzat)	La resta d'incidències i peticions de servei.	0

L'impacte que pot tenir un valor predeterminat per el tipus de servei afectat o ser calculat directament per el tècnic. L'impacte predeterminat pot modificar-se de forma automàtica si l'usuari en nom del qual es realitza el registre pertany a un nivell SVIP o VIP.

2.2. Urgència

Depenent del temps màxim d'espera que accepti el client per la resolució de l'incident i/o el nivell de servei acordat en els ANS. En definitiu, és el grau fins al que és possible esperar la solució.

Criteris per establir la urgència		
Urgència	Descripció	Ponderació
1-Crítica	- El Procés Crític no es pot executar. - L'usuari o departament no pot realitzar cap de les funcions principals que tenen assignades. L'usuari o departament es troba parat fins la resolució de la incidència.	20
2-Alta	L'usuari o departament no pot realitzar alguna de les funcions principals que tenen assignades. L'usuari o departament pot continuar amb altres activitats fins la resolució de la sol·licitud.	15
3-Mitjana	L'usuari o departament pot realitzar les funcions principals que tenen assignades però presenten dificultats (lentitud, errors puntuals, ...). L'usuari o departament pot continuar amb altres activitats fins la resolució de la sol·licitud.	10
4-Baixa	Es veuen afectades les funcions secundàries de l'usuari o departament que no impedeixen el desenvolupament de les seves principals funcions.	0

2.3. Prioritat i temps de resposta

El càlcul de la prioritat en l'eina de gestió d'incidències es realitza de forma automàtica a partir dels valors d'impacte i d'urgència. La següent taula mostra el càlcul en base d'ambdós paràmetres.

Quantificació de la prioritat = Impacte + Urgència						
Criteri	Valor		Urgència			
		Ponderació	Crítica	Alta	Mitjana	Baixa
			20	15	10	0
Impacte	Extens/ Generalitzat	9	29 Crítica	24 Crítica	19 Alta	9 Baixa
	Significatiu/ Ampli	5	25 Crítica	20 Alta	15 Mitjana	5 Baixa
	Moderat/ Limitat	3	23 Alta	18 Alta	13 Mitjana	3 Baixa
	Menor/ Localitzat	0	20 Alta	15 Mitjana	10 Mitjana	0 Baixa

El temps de resposta per cada una de les tipologies d'incidències haurà de ser el següent:

Prioritat	Valor	Actuació
1-Crítica	[24-29]	El temps de resposta a la incidència haurà de ser immediat. Es posposarà a qualsevol activitat que s'estigui realitzant en aquest moment excepte aquelles que tinguin el mateix nivell de prioritat.
2-Alta	[18-23]	El temps de resposta a la incidència haurà de ser molt ràpid. Es posposarà qualsevol activitat que s'estigui realitzant en aquest moment excepte aquelles que tinguin el mateix nivell de prioritat o superior.
3-Mitjana	[10-15]	El tècnic al que se li assigna la incidència haurà de començar la seva resolució en quan acabi les activitats de major prioritat.
4-Baixa	[0-9]	El tècnic al que se li assigni la incidència haurà de començar la seva resolució quan acabi les activitats de major prioritat.

15. ANNEX NÚM. 2 - NORMES DE SEGURETAT IT D'AIGÜES DE BARCELONA

Els Sistemes d'Informació proporcionats no han de ser vulnerables, i segons apliqui, als TIP 10 de Owasp Security Mobile i/o OWASP Top 10 Security Web (<https://www.owasp.org>). A més a més haurà de complir-se la normativa de gestió d'usuaris i contrasenyes establerta en el present Annex.

Aquesta normativa pot complir-se utilitzant el Active Directory d'Aigües de Barcelona com repositori dels usuaris mitjançant una connexió segura amb el sistema ADFS de Aigües de Barcelona.

"NORMES DE SEGURETAT IT D'AIGÜES DE BARCELONA"

ÍNDEX

- 1. Objecte i introducció del document**
- 2. Intercanvi d'informació i software SI-N-07-02/01**
- 3. Configuració i administració segura**
 - 3.1 Configuració segura**
 - 3.2 Administració segura**
- 4. Identificació i autenticació d'usuaris**
- 5. Identificació d'usuari**
- 6. Gestió de contrasenyes i credencials de clients**
- 7. Comunicació dels incidents de seguretat**

1. Objecte i introducció del document

L'objecte del present document és establir la normativa de seguretat en la gestió dels Sistemes d'Informació d'Aigües de Barcelona i en la identificació, autenticació d'usuaris i gestió de les contrasenyes d'accés als mateixos.

2. Intercanvi d'informació i software

L'intercanvi d'informació o programari qualificats com d'ús No Sensible, Sensible o Crítica que Aigües de Barcelona realitzi amb altres organitzacions, ha d'estar formalitzat en acords, validats per la Direcció Jurídica, que han d'establir les condicions en les quals es realitzaran aquests intercanvis.

Quan, per raons d'urgència i eficiència del servei, sigui impossible la formalització prèvia d'aquest acord, l'intercanvi d'informació estarà subjecte a les condicions generals previstes en aquesta norma i serà el remitent el responsable del seu compliment.

L'intercanvi s'ha de realitzar respectant la classificació i etiquetatge de la informació que es gestioni durant aquest intercanvi.

Els intercanvis d'informació classificada com a Crítica, així com de dades de caràcter personal de nivell alt, s'han de realitzar emprant mecanismes de xifrat que impedeixin la divulgació no autoritzada.

En els acords s'han d'establir els mecanismes oportuns per facilitar la gestió d'aquests intercanvis i plasmar les responsabilitats i obligacions legals quan es duguin a terme, especialment les relacionades amb les dades de caràcter personal.

Aquests acords han d'indicar les responsabilitats de control i notificació de l'enviament, transmissió i recepció de la informació que s'intercanvia. S'ha d'assignar un gestor per a cada acord amb la responsabilitat de controlar i fer un seguiment del seu desenvolupament.

En l'àmbit legal, els acords han d'establir les responsabilitats i obligacions legals relatives a l'intercanvi, especialment aquelles derivades de l'intercanvi de dades de caràcter personal amb altres entitats, cessionàries o cedents, d'acord amb el RGPD i la LOPDGDD.

3. Configuració i administració segura

3.1. Configuració segura

Tots els sistemes hauran d'estar configurats per verificar la identitat dels usuaris que hi accedeixen, de manera que no es comprometin les credencials d'autenticació i es garanteixi la seva identificació unívoca.

Així mateix, en funció del perfil dels usuaris i la informació que el sistema processa, s'haurà de determinar l'assignació de privilegis i els serveis habilitats en cada cas. La configuració i assignació de privilegis s'ha de regir pel principi de menor privilegi, limitant els permisos únicament als estrictament necessaris per a l'operativa diària de treball dels usuaris. En aquest sentit, únicament els administradors i operadors dels sistemes d'informació han de tenir accés a les utilitats de gestió i administració del sistema que requereixen per a l'exercici de les seves funcions, i poden existir diferents nivells de drets d'administració.

S'hauran de limitar els serveis de xarxa oberts en els diferents sistemes d'informació. La configuració dels serveis de xarxa actius s'ha de regir pel següent principi: "Es prohibeix tot allò que no es troba explícitament permès", o el que és el mateix, s'han de desactivar tots els serveis de xarxa que s'activen per defecte durant la instal·lació i l'ús dels quals no es troba motivat per una necessitat de negoci o operativa clara.

Adicionalment, per evitar, en la mesura del possible, l'exposició a atacs de denegació de servei, els dispositius i elements de comunicacions hauran d'estar adequadament configurats mitjançant l'establiment de mesures de protecció com podrien ser:

- Limitacions en el temps màxim de vida de connexions inactives.
- Limitacions en el nombre màxim de connexions obertes.
- Restriccions en els algorismes de propagació d'informació d'encaminament.

Així mateix, en aquells elements de comunicacions que proveeixin accés a la xarxa de comunicacions d'Aigües de Barcelona o que utilitzin algorismes d'encaminament dinàmics, s'hauran d'emprar mecanismes d'autenticació mútua basats en claus precompartides, certificats digitals o altres mecanismes que proporcionin major seguretat.

Finalment, els sistemes d'informació hauran d'estar configurats per registrar tots aquells esdeveniments que siguin necessaris per assegurar la traçabilitat de les accions realitzades en el sistema, amb especial atenció als fitxers classificats com de nivell alt segons el RGPD i la LOPDGDD.

3.2. Administració segura

L'administració remota dels sistemes d'informació ha de ser realitzada per mitjà d'eines i/o protocols d'administració que proveeixin mitjans per identificar unívocament l'usuari administrador i perquè les credencials d'aquest usuari administrador viatgin xifrades per la xarxa de comunicacions emprant tècniques criptogràfiques.

Així mateix, es limitarà el temps màxim de connexió dels usuaris administradors per evitar que les sessions romanguin obertes de manera indefinida, la qual cosa facilitaria la captura de sessions per part d'usuaris no autoritzats.

Inclòs en els processos d'administració de sistemes, s'haurà de dur a terme un procés de revisió periòdica de fitxers temporals en servidors centrals i sistemes d'informació d'Aigües de Barcelona, que corregeixi possibles fallades ocorregudes durant el procés d'esborrat de fitxers temporals. El tractament d'aquests fitxers temporals s'ha d'ajustar al que disposen les normatives legals vigents en matèria de protecció de dades de caràcter personal (RGPD i LOPDGDD).

4. Identificació i autenticació d'usuaris

Tots els sistemes d'informació no públics de les unitats i societats operatives d'Aigües de Barcelona hauran de disposar de mecanismes que verifiquin la identitat dels usuaris que els utilitzen, de manera que es restringeixin els recursos als quals ha d'accedir cada usuari.

Els usuaris disposaran d'un identificador personal per als sistemes d'informació, permetent determinar les operacions que pugui realitzar en els diferents sistemes a través del seu identificador, excepte les excepcions reflectides a l'apartat "Identificació d'usuari".

El mecanisme d'autenticació de cada sistema es podrà implantar mitjançant:

- Programari de control d'accés inherent al propi sistema.
- Eina de programari de control d'accés agregat al sistema.

L'autenticació, normalment, es realitzarà mitjançant l'ús de contrasenyes seguint els criteris de robustesa de contrasenyes indicats a l'apartat de "Gestió de contrasenyes i credencials".

Tots els mecanismes d'autenticació hauran de ser supervisats per la Direcció de Seguretat TI, que verificarà la correcta parametrització de la normativa de seguretat relativa a l'autenticació d'usuaris. L'autenticació en el sistema haurà de garantir que l'usuari només tingui accés als recursos que necessiti per al desenvolupament de les seves funcions, no disposant de permisos d'accés a les eines pròpies del sistema, llevat que les necessiti per al desenvolupament de les seves funcions (per exemple, administradors de sistemes).

En els processos d'autenticació a través de xarxes s'evitarà la transmissió de la clau d'accés de manera llegible. Quan l'usuari accedeixi al sistema se li haurà de mostrar, si és possible, la data i hora del seu últim accés. Aquest avís pot alertar l'usuari de l'existència d'accessos no autoritzats.

Quan la criticitat del servei o recurs ho requereixi, l'Organització de Seguretat de la Informació promourà l'ús de mecanismes d'autenticació basats en infraestructura de clau pública (PKI) i emmagatzematge de claus en dispositius externs (SmartCards, E-Tokens, etc.). Quan es necessiti accés a arxius o transaccions especialment sensibles, l'usuari ha de ser reautenticat, en cas que sigui possible tècnicament.

Amb la finalitat d'evitar l'accés no autoritzat, el procés d'identificació i autenticació d'usuaris haurà d'estar dotat de controls per al bloqueig automàtic de l'identificador d'usuari i la seva inhabilitació temporal per a l'accés al sistema en els següents casos:

- Per nombre d'intents d'accés incorrectes.
- Per inactivitat de l'usuari en el sistema.

En aquestes situacions, i en qualsevol altra originada pel bloqueig d'un identificador d'usuari, el propi usuari haurà de sol·licitar formalment, a través del correu electrònic corporatiu, la rehabilitació dels seus privilegis d'usuari. En el cas que l'identificador d'usuari bloquejat sigui el de correu electrònic, el superior jeràrquic de l'usuari implicat haurà de sol·licitar, pels procediments establerts, la rehabilitació dels privilegis del mateix. Tant si el desbloqueig es realitza manualment com automàticament s'hauran d'implantar controls que permetin identificar i detectar intents d'accés no autoritzats.

5. Identificació d'usuari

L'accés a qualsevol dels sistemes d'informació d'Aigües de Barcelona es realitzarà utilitzant un identificador d'usuari convenientment autoritzat ([UserID]). L'identificador d'usuari haurà d'estar assignat a una persona física i tindrà caràcter personal i intransferible. Conseqüentment, i associat a

cada identificador assignat a una persona física, es conservaran les dades que, com a mínim, permetin relacionar unívocament l'identificador d'usuari amb la persona física.

Les persones que no pertanyen a la plantilla de treballadors d'Aigües de Barcelona han de rebre identificadors que segueixin els mateixos processos d'aprovació que per als nous empleats. Els drets d'accés dels usuaris que no pertanyen a Aigües de Barcelona s'han d'atorgar només pel període de temps estrictament necessari i hauran de ser reavaluats periòdicament.

No estarà permesa la creació o utilització d'usuaris genèrics, excepte en aquells casos en què sigui estrictament necessari per raons operatives, funcionals, etc., que, per la seva naturalesa, aconsellen o obliguen al seu ús i prèvia autorització específica del Cap de Seguretat de la Informació de l'entitat corresponent. En aquests casos, s'extremarà el seguiment de les activitats realitzades amb l'usuari genèric, assegurant que es coneix, en tot moment, el grup d'usuaris que l'empren. Quan la necessitat d'emprar l'usuari genèric per un usuari del grup finalitzi, s'haurà de modificar la contrasenya d'accés compartida per fer efectiva la sortida d'aquest usuari del grup i impedir l'ús de l'usuari genèric més enllà de les seves necessitats.

Així mateix, excepte en situacions justificades per l'acompliment de les funcions, cada persona física tindrà associat un únic identificador d'usuari. Com a excepció, un usuari podrà disposar de més d'un identificador d'usuari, en el cas que els privilegis assignats a cadascun siguin diferents i tècnicament no sigui possible recollir tots els privilegis en un sol identificador d'usuari o no sigui recomanable mantenir tots els privilegis en un únic identificador d'usuari per qüestions de seguretat.

6. Gestió de contrasenyes i credencials de clients

Per evitar la possible descoberta de les contrasenyes per part de tercers, aquestes hauran de complir una sèrie de requisits a l'hora de la seva generació.

Els sistemes han de permetre a l'usuari el canvi de la seva contrasenya de forma autònoma quan aquest ho consideri oportú. Així mateix, quan s'accedeixi per primera vegada a un sistema o quan s'hagi sol·licitat, a través dels procediments establerts a tal efecte, una rehabilitació o desbloqueig de la contrasenya, el sistema de control d'accés obligarà l'usuari al canvi de la mateixa en el seu primer accés. La contrasenya inicial haurà de ser generada de manera aleatòria.

Els usuaris podran sol·licitar, seguint els procediments establerts, el desbloqueig del seu identificador o un canvi de contrasenya quan no la recordin o tinguin sospita que ha perdut el caràcter de secreta i no disposin de l'opció per canviar-la o desconeixin com realitzar el canvi.

Els sistemes d'informació d'Aigües de Barcelona hauran de disposar de mecanismes de control d'accés que permetin:

- Restringir, individualitzar, registrar, controlar i, eventualment, bloquejar l'accés a la informació i a les aplicacions.
- Protegir la informació i les aplicacions d'accessos realitzats per personal no autoritzat.
- Autenticar a tots els usuaris abans que aquests accedeixin a qualsevol dels recursos d'ús intern, restringit o confidencial per als quals estiguin autoritzats.
- Impedir l'existència d'identificadors d'usuari sense contrasenya assignada.
- Protegir les contrasenyes dels usuaris de la següent manera:
 - Emmagatzemant el resum o "hash" generat amb algorismes estàndard de xifrat.
 - No mostrar-se en pantalla en text clar.

- Restringir a tots els usuaris, en la mesura del possible, la possibilitat d'establiment de sessions concurrents.
- Finalitzar sessions per inactivitat durant un temps determinat. S'establirà 5 minuts com a valor de referència, encara que haurà de ser configurable en funció de la criticitat i sensibilitat de les dades que es manegin.
- No permetre la visualització d'informació referent al sistema fins que el procés d'inici de sessió hagi acabat satisfactòriament.
- No permetre l'emmagatzematge de contrasenyes en programes, "scripts" o codis desenvolupats per a connexió automàtica als sistemes d'informació. Excepte excepcions prèviament autoritzades per la Direcció de Seguretat TI. La Direcció de Seguretat TI haurà de definir mecanismes de control d'accés alternatius que efectuïn controls no coberts pels sistemes de control d'accés instal·lats en els entorns, així com avaluar els avantatges i debilitats de les noves versions i/o productes alternatius o complementaris.

La Direcció de Seguretat TI haurà d'avaluar els mecanismes d'autenticació disponibles alternatius a les contrasenyes, per exemple, biomètrics, targetes, tokens, etc., per a aquells sistemes on es requereixi un nivell d'autenticació més segur.

7. Comunicació dels incidents de seguretat

En cas de detecció d'un incident greu de seguretat (mitjançant sistemes de detecció d'intrusions, anàlisi de registres, comunicació d'un tercer, alarmes de seguretat, etc.), la Direcció de Seguretat Aigües de Barcelona haurà de ser informada el més aviat possible a través de línies de comunicació que s'establiran prèviament amb aquest propòsit.

La Direcció de Seguretat s'encarregarà d'iniciar un informe cap a les figures, escollides entre aquelles que prèviament havien estat identificades, la participació de les quals sigui necessària en la resolució de l'incident. Aquesta elecció es farà en funció de la criticitat de l'incident, el grau de coneixement necessari o els sistemes als quals afecti.

Les Àrees d'Assumptes Legals (Direcció Jurídica) i Recursos Humans hauran de ser informades en cas que l'incident necessiti prendre accions disciplinàries o legals i en cas que pugui tenir repercussions legals per a Aigües de Barcelona.

S'hauran de reportar aquells incidents significatius als nivells jeràrquics superiors establerts amb la finalitat d'obtenir autoritzacions o d'informar sobre l'actuació d'Aigües de Barcelona davant d'incidents de seguretat.

El reporting d'informació sobre incidents de seguretat quedarà restringit únicament a aquelles persones absolutament necessàries. Qualsevol divulgació d'aquesta informació haurà de ser autoritzada per la Direcció de Seguretat.

És responsabilitat de la Direcció de Seguretat mantenir un registre amb les dades d'aquelles persones que han estat informades de cada incident amb la finalitat de detectar una possible divulgació no autoritzada.

Tant els empleats de les entitats d'Aigües de Barcelona com els treballadors d'empreses externes coneixeran les línies de report d'incidents de seguretat i tenen el deure d'utilitzar-les en cas de detectar un incident de seguretat. Si la persona que detecta l'incident no està segura de si es tracta d'un incident o no, haurà de reportar-ho igualment.