

PLEC DE PRESCRIPCIONS TÈCNIQUES
QUE HA DE REGIR EL CONTRACTE RELATIU AL
"SERVEI DE SUPORT PER LA GESTIÓ DE PROJECTES DE L'ÀREA DE DADES "

Núm. EXP.: AB/2026/150

Contingut

1 INTRODUCCIÓ	3
2 ABAST	3
3 SITUACIÓ ACTUAL	3
3.1 Àmbit	3
4 CONDICIONS OPERATIVES PER EL DESENVOLUPAMENT DEL SERVEI	4
4.1 Suport per la Gestió de Projectes	4
5 CONDICIONS OPERATIVES PER L'EXECUCIÓ DEL SERVEI	7
5.1 Model de Gestió del Servei	7
6 ALTRES REQUERIMENTS	9
6.1 Ubicació	9
6.2 Recursos Materials requerits	9
6.3 Recepció, control, resolució i canalització d' Incidències	10
6.4 Acords de Nivell de servei (ANS) i penalitzacions derivades del seu incompliment durant l'execució del Servei	10
7 GARANTIA	1
8 SEGURETAT CORPORATIVA	1
1. Objecte i introducció del document	1
2. Intercanvi d'informació i software	1
3. Configuració i administració segura	1
3.1 Configuració segura	1
3.2 Administració segura	1
4. Identificació i autenticació d'usuaris	1
5. Identificació d'usuari	1
6. Gestió de contrasenyes i credencials de clients	1
7. Comunicació dels incidents de seguretat	1

1 INTRODUCCIÓ

Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A. (en endavant, Aigües de Barcelona) està desenvolupant diversos projectes de transformació fet pel qual es requereix disposar d'un **"Servei de suport per a la Gestió de Projectes de l'àrea de dades"**.

El present document estableix la definició, per les àrees tècniques que ho requereixen, de les necessitats que haurà de cobrir aquesta figura.

2 ABAST

Les actuacions que formen part de l'abast del present procediment de contractació són les requerides per disposar a Aigües de Barcelona d'un Servei per la Gestió de Projectes referits a les aplicacions de Dades i s'asseguri de la correcta execució dels projectes i el seguiment dels processos i procediments associats al seu desenvolupament i al dels diferents sistemes relacionats.

3 SITUACIÓ ACTUAL

3.1 Àmbit

L'entorn de dades i analítica es compon d'un conjunt de tecnologies i entorns que podem resumir en:

1. Entorn Azure: les principals tecnologies utilitzades són Blob Storage, Snowflake, CosmosDb, Datafactory, Databricks, Dbt, Airflow. Les plataformes de reporting són MicroStrategy i Power BI.
2. Entorn On premise: en aquest entorn més tradicional els desenvolupaments es duen a terme modelant sobre bases de dades Oracle i amb Microstrategy com a plataforma de reporting.

El servei de suport sol·licitat ha de ser capaç de gestionar els projectes en un entorn tecnològic complex i amb un nombre elevat d'actors tècnics involucrats.

Atès que aquests projectes han de conviure dins del mateix entorn amb altres iniciatives de dada i amb el servei de manteniment, serà imprescindible una coordinació prèvia i una relació fluida amb l'equip del servei del dada abans d'abordar qualsevol canvi. En conseqüència, les modificacions necessàries a la plataforma per donar resposta a noves entitats o a evolutius hauran de ser acordades específicament amb aquest equip.

Així mateix, cal tenir en compte que l'equip del servei del dada treballa d'acord amb un model de gestió basat en Kanban. Per aquest motiu, es requereix que el perfil professional disposi d'experiència pràctica en entorns gestionats amb aquesta metodologia, especialment en la

coordinació amb equips de dada, la gestió de flux, les operacions, el delivery i la millora contínua dels processos.

4 CONDICIONS OPERATIVES PER EL DESENVOLUPAMENT DEL SERVEI

4.1 Suport per la Gestió de Projectes

4.1.1 Tasques a desenvolupar

Les diferents tipus d'activitats i tasques que formen part de l'abast del servei que és licita són:

- Col·laboració amb el client intern d'Aigües de Barcelona en la definició i concreció dels objectius dels projectes a desenvolupar.
- Elaboració dels plecs de licitació quan s'escaigui, i suport durant la fase de licitació i adjudicació.
- Col·laboració en l'elaboració de la documentació formal de la inversió davant les administracions
- Planificació dels projectes en tots els seus aspectes, identificant les activitats a realitzar, els recursos necessaris, terminis i la dedicació d'aquests.
- Planificació i seguiment de la correcta execució dels projectes, així com dirigir la coordinació dels diferents equips executors amb Aigües de Barcelona i, en el seu cas, la requerida quan és donin o és requereixin interferències entre els projectes.
- Assegurar la qualitat i compliment dels objectius del projectes, terminis establerts i ANS.
- Manteniment permanent de les relacions externes del projecte: clients, proveïdors, tercers, IT d'Aigües de Barcelona, etc. De forma específica, pel que fa als equips executors dels projectes, mantenir la requerida interlocució amb els Cap/Gestors de Projecte.
- Participar en els reunions d'inici, de seguiment i tancament dels projectes amb els proveïdors, així com en els que es requereixin en el seguiment post-productiu (període de garantia dels projectes).
- Presa de decisions necessàries per a conèixer en tot moment la situació en relació amb els objectius establerts dels projectes, terminis establerts i lliuraments associats al projecte.
- Adopció de les mesures correctores pertinents per a posar remei a les possibles desviacions que s'haguessin detectat.
- Respondre davant d'Aigües de Barcelona de la consecució dels objectius dels projectes.
- Anticipar possibles riscos per a la consecució dels objectius dels projectes i iniciar les mesures necessàries per al seu control i mitigació.

- Proposar, en el seu cas, modificacions als límits o objectius bàsics del projecte quan concorrin circumstàncies que així ho aconsellin.
- Donar suport funcional i tècnic a l'equip de desenvolupament dels projectes, aportant idees i solucions a les necessitats dels projectes.
- Gestionar l'entrada de les peticions de Remedy corresponents a les sol·licituds de tasques adreçades al servei i derivades de l'activitat del projecte, assumint-ne la tramitació i el seguiment integral fins a la seva resolució satisfactòria. En cas d'incidències, bloquejos o desviacions que puguin comprometre l'execució de les tasques o el compliment dels terminis establerts, aquestes hauran de ser escalades oportunament al Data Manager d'Aigües de Barcelona.
- Assegurar que tot projecte i lliurable compleixi amb els tots el requeriments de seguretat i de protecció de dades necessaris, validant-ho conjuntament amb DPO i el departament de seguretat d'Aigües de Barcelona.
- Valorar diferents productes o opcions de desenvolupament, per escollir la que més s'ajusti a les necessitats d'Aigües de Barcelona, tant a nivell d'estratègia com a nivell de pressupost econòmic del projecte.
- Validació de definicions visuals dels sistemes (maquetis i/o mockUps) per tal d'assegurar que compleixen amb les necessitats de l'usuari final, obtenint la validació d'aquests en cas de ser necessari.

Tot això, des d'un prisma de gestió del desenvolupament de projectes tant amb metodologies tradicionals com amb metodologies de treball dinàmiques i innovadores tipus Agile, o fins i tot amb un model mixt.

4.1.2 Metodologia de Treball

La metodologia de projectes emprada i detallada a continuació serà la que caldrà seguir pel servei sol·licitat en aquest procediment:

- Definició de requeriments:

A partir d'uns requeriments d'alt nivell i en base al pressupost aprovat en el Pla d'Inversions Anual cal elaborar un document detallat d'aquests requeriments amb una valoració aproximada dels mateixos.

El nivell de detall ha de ser suficient com per poder demanar ofertes sobre els mateixos a diversos proveïdors.

- Preparació de la documentació per l'Administració:

A partir dels requeriments detallats i amb la llista d'aplicacions existents afectades o per construir cal emplenar juntament amb Gestió de la Demanda la documentació que cal presentar a l'Administració prèviament a l'inici de la inversió.

- Preparació dels plecs i licitació:

En funció de l'import i tipus de la inversió, les tasques contractades a proveïdors s'hauran de licitar sota diferents procediments de contractació. Caldrà elaborar els plecs de licitació juntament amb Contractació per el procediment que li correspongui.

A més serà necessari fer una valoració tècnica de les ofertes rebudes.

- Seguiment i coordinació del projecte:

Cal assegurar que l'empresa adjudicatària disposa de totes les eines i accessos necessaris per desenvolupar les seves tasques, fer el seguiment de que aquestes tasques es van fent segons la planificació, convocar i coordinar les reunions de direcció del projecte i fer, en general, de corretja de transmissió entre l'adjudicatari i la resta de components del projecte o altres departaments d'Aigües de Barcelona.

Es requereix un seguiment actiu dels riscos en els quals pugui incórrer el projecte, ja siguin econòmics, tècnics, de retard, o de qualsevol tipus. El licitador haurà de detallar en la seva oferta el procediment estructurat per a aquesta gestió proactiva de riscos

En cas de projectes complexos amb diverses empreses adjudicatàries, o amb interrelació amb altres projectes, cal assegurar la coordinació necessària entre totes les parts.

Més enllà de la gestió individual de cada projecte, es valorarà la descripció de la metodologia que s'aplicarà per a l'avaluació i evolució del propi servei de gestió. Així mateix, es valorarà la proposta de mecanismes analítics estructurats per auditar els propis procediments interns durant la vigència del contracte, amb l'objectiu d'identificar ineficiències i optimitzar l'esforç dedicat a la gestió.

Tancament del projecte:

Cal un informe de tancament amb el resum del que s'ha aconseguit i la justificació de les possibles desviacions temporals, econòmiques o d'abast.

A més cal una acta de tancament signada amb el proveïdor i l'àrea d'Aigües de Barcelona afectada per el projecte i l'elaboració d'una enquesta de satisfacció.

La metodologia de seguiment de projectes dins d'Aigües de Barcelona pot anar canviant a mida que més projectes es desenvolupin amb mètodes Agile.

4.1.3 Lliurables

La documentació que haurà d'elaborar el cap de projecte segons la fase en la que es trobi és:

- Actes de les reunions de presa de requeriments
- Document de "descripció ampliada del projecte" (requeriments detallats)

- Plecs de Licitació amb els Criteris de Valoració definits
- Valoració tècnica dels plecs presentats
- Informes de seguiment per el Comitè de Direcció
- Pla de proves a executar i executades.
- Acta de tancament a signar amb cada proveïdor
- Informe de tancament del projecte
- Enquestes de Satisfacció

De forma habitual la documentació dels projectes, pels plecs de licitació o per l'administració, es fa en català. Per la qual cosa és molt desitjable un domini escrit d'aquest idioma juntament amb el castellà.

5 CONDICIONS OPERATIVES PER L'EXECUCIÓ DEL SERVEI

5.1 Model de Gestió del Servei

5.1.1 Cobertura del servei

El servei s'haurà de dur a terme en horari compatible amb el d'Aigües de Barcelona y la prestació del servei es realitzarà en un temps estimat de 4-5 hores diàries, que poden augmentar o disminuir de forma puntual depenent de les necessitats del treball, les reunions de seguiment etc.

No hi ha un mínim d'hores diàries facturables, és a dir, en cap cas no es facturarà a Aigües de Barcelona un mínim d'hores diàries sense que aquestes s'hagin efectuat durant el desenvolupament del servei.

S'estima un volum anual de 1000 hores.

5.1.2 Equip de treball i actors per la prestació del servei

Equip de treball

L'equip mínim que s'haurà d'adscriure a l'execució del contracte per part del Prestador del Servei haurà d'incloure:

- **UN (1) Responsable del Servei**

L'adjudicatari nomenarà un Responsable global del Servei. Aquest Responsable del Servei haurà de tenir la capacitat, coneixements i experiència suficients als efectes de supervisar, coordinar i velar per la correcta prestació del Servei, i exercir labors d'interlocució amb

Aigües de Barcelona per al seguiment de l'execució del Contracte. Haurà de vetllar perquè l'estratègia seguida en la prestació del servei estigui en tot moment alineada amb la necessitats establertes en el present plec, controlant i garantint que totes les decisions i accions que es preguin, estiguin focalitzades en la correcta execució de les activitats del servei. Pot ser el mateix perfil que el gestor del projecte.

- **UN (1) Gestor de Projectes**

Serà el responsable de la correcta execució de les diferents d'activitats i tasques requerides. Aquest perfil professional haurà de disposar com a mínim de:

- Experiència mínima de dotze (12) anys en l'àmbit TI.
- Experiència mínima de vuit (8) anys com a Cap de Projecte.
- Experiència mínima de cinc (5) anys en organitzacions amb metodologia àgil.
- Experiència mínima de tres anys (3) en sector Utilities.
- Es valorarà experiència pràctica en la gestió d'equips de servei de dades, així com en la gestió de flux, operacions, delivery i millora de processos.

En qualsevol cas, el perfil proposat pel licitador ha de comptar amb les competències i habilitats necessàries per a desenvolupar amb garanties, les activitats definides que permetin oferir la correcta presentació del servei, a saber:

- Destresa comunicativa i interpersonal.
- Capacitat de detectar i resoldre problemes.
- Alta capacitat d'organització i control de la informació.
- Persones actives i amb iniciativa, per a la millora dels serveis.
- Capacidad de mentoría, docencia o experiencia como Agile Coach.
- Se valoraran certificaciones oficiales y actualizadas en metodología Kanban (KMP I, KMP II) y en menor medida en metodología Scrum (PSM I)
- Se valorará experiencia en proyectos de adopción e implantación de metodología Kanban aplicada a un equipo de servicio
- Es valorarà experiència en l'àmbit de dades o business intelligence en organitzacions complexes.
- Orientació al treball en equip.

En cas de necessitat de substitució d'algun membre de l'equip, s'haurà d'assignar una altra persona que disposi de la qualificació requerida, i si per assegurar la permanència del coneixement adquirit i la seva transferència fos necessària la concurrència entre els recursos entrants i sortints, durant

l'esmentat període solament és tindran en compte com a hores productives les d'un dels recursos, per a qualsevol comptabilitat de l'esforç.

5.1.3 Eines de gestió i control

Per a la gestió dels projectes i de les incidències associades als mateixos, Aigües de Barcelona podrà determinar l'ús pel Prestador del Servei d'eines de gestió específiques, com Jira o Remedy.

Aigües de Barcelona proveirà d'usuaris i de rols suficients per a la gestió del servei requerit.

5.1.4 Documentació del servei

La documentació generada durant l'execució del contracte és propietat exclusiva d'Aigües de Barcelona, sense que l'Adjudicatari pugui conservar-la, ni obtenir còpia de la mateixa o facilitar-la a tercers. Així, l'Adjudicatari haurà de subministrar a Aigües de Barcelona la documentació derivada de la pròpia gestió dels projectes. Aquesta documentació serà revisada i haurà de ser aprovada pel personal d'Aigües de Barcelona.

6 ALTRES REQUERIMENTS

6.1 Ubicació

El servei és prestarà dins de les pròpies oficines de l'adjudicatari, no obstant això, és donessin situacions que requereixin de la presència en les pròpies oficines d'Aigües de Barcelona per motiu d'assistència a reunions, per a formació, suport a les tasques realitzades en el servei, seguiment del servei, resolució de problemes, etc.

El servei inclou el suport presencial quan és consideri necessari. És per això, que l'adjudicatari haurà d'assegurar la possibilitat de donar resposta presencial dins de l'àmbit de l'àrea metropolitana de Barcelona sense que aquest fet pugui donar lloc a un increment en el cost del servei.

6.2 Recursos Materials requerits

El Prestador del Servei serà responsable de disposar de l'equip de treball i de l'equipament Hardware i Software necessari per l'execució de les prestacions contractades. En cap cas és podrà facturar la compra, subministrament o instal·lació d'equips i recanvis que siguin necessaris per realitzar els serveis objecte d'aquest contracte.

No obstant, Aigües de Barcelona proporcionarà als Prestadors des Serveis les eines següents:

- Usuaris locals o de domini amb els permisos necessaris
- Eines de reporting i seguiment dels projectes i incidències (JIRA, Remedy)

6.3 Recepció, control, resolució i canalització d' Incidències

L'adjudicatari haurà d'utilitzar les eines d'Aigües de Barcelona per al reporting i seguiment de les incidències detectades:

- En fase de proves d'acceptació i posada en marxa, hauran de fer ús de l'eina JIRA
- Mentre que, en fase de post implantació (parcial o total) hauran de fer ús de l'eina de ticketing utilitzada per Aigües de Barcelona (actualment BMC Remedy).

6.4 Acords de Nivell de servei (ANS) i penalitzacions derivades del seu incompliment durant l'execució del Servei

6.4.1 Acords de Nivell de Servei (ANS)

El present apartat té per objecte fixar els nivells de servei (ANS), estàndards d'execució i els criteris i processos de mesurament o valoració dels resultats exigits al Prestador del Servei durant l'execució del projecte, per a la provisió dels mateixos.

1. **ANS-01 (Puntualitat en el lliurament dels Informes de Seguiment de projectes):** desviació en el nom de dies, respecte al termini de lliurament de l'informe quinzenal establert en el present plec.

Indicador:	Puntualitat en el lliurament 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 de seguiment definit en el projecte (15 dies naturals per exemple).
Fórmula aplicada:	ANS-01 = (Nde – 5) (<i>expressat en dies</i>) <i>On,</i> Nde: <i>Un cop finalitzat un període de seguiment (15 dies naturals), anomeni de dies hàbils transcorreguts fins al lliurament de l'Informe de seguiment corresponent.</i>
Càlcul de la Penalització acumulada P1:	Per cada incompliment s'afegeix un 2% a l' acumulat.

Es considera l'informe de final de projecte com un informe de seguiment addicional.

6.4.2 Penalitzacions derivades de l'incompliment amb els ANS

Els Prestadors del Servei, és 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 s'obté a partir de la suma dels percentatges parcials acumulats com a conseqüència dels incompliments registrats amb els ANS, segons els criteris següents:

Penalització	Criteri
P1	Per cada incompliment de l' ANS-01, s'afegeix un 2% de penalització a l'acumulat. Per tant: $P1 = (\sum_{i=1}^n 2)\%$, on n és el nom d'incompliments de l'ANS-01.

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:

1. Valor resultant d'aplicar la fórmula següent: $PT = P1$
2. En cas que el valor anterior (**PT**) sigui superior al 25%, s'aplicarà com a penalització aquest 25%.

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

Les penalitzacions econòmiques s'aplicaran de forma semestral i/o a la finalització del servei i un cop la penalització acumulada (**PT**) assoleixi o superi el 10%.

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

- resoldre el contracte amb l'esmentat Prestador del Servei, o bé
- continuar amb la imposició de penalitzacions en els termes previstos anteriorment.

6.5 Accés

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

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

7 GARANTIA

El període mínim que hauran de tenir com a garantia serà de TRES (3) mesos, a comptar des de la finalització del contracte.

Aquesta garantia fa referència a la garantia post-treballs dels treballs realitzats pels perfils durant l'execució del contracte. Durant el període de garantia és podrà requerir la correcció d'errors detectats en la documentació lliurada pels perfils durant l'execució del contracte.

8 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. 1).
- 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 impactis 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.

ANNEX N°1 - "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 l'Active Directory d'AIGÜES DE BARCELONA com repositori dels usuaris mitjançant una connexió segura amb el sistema ADFS d'AIGÜES DE BARCELONA.

"NORMES DE SEURETAT IT D'AIGÜES DE BARCELONA"

ÍNDEX

- 1. Objecte i introducció del document***
- 2. Intercanvi d'informació i software***
- 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 y 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 revaluats 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:

1. Restringir, individualitzar, registrar, controlar i, eventualment, bloquejar l'accés a la informació i a les aplicacions.
2. Protegir la informació i les aplicacions d'accessos realitzats per personal no autoritzat.
3. Autenticar a tots els usuaris abans que aquests accedeixin a qualsevol dels recursos d'ús intern, restringit o confidencial per als quals estiguin autoritzats.
4. Impedir l'existència d'identificadors d'usuari sense contrasenya assignada.
5. 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'incidentes 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'incidentes 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-lo igualment.