PLEC DE PRESCRIPCIONS TÈCNIQUES
QUE HA DE REGIR EL CONTRACTE RELATIU AL
"20-0-DIV-4_6_2_01_03 SERVEI DE SUPORT PER A LA GESTIÓ DE PROJECTES DE L'ÀREA GIS"

Núm. EXP.: AB/2026/064

1 INTRODUCCIÓ

Aigües de Barcelona desenvolupa diversos projectes de transformació per fer els quals es requereix la figura d'un Analista GIS que pugui fer la coordinació entre els diferents projectes i serveis.

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

2 OBJECTE

L'objecte del present Plec de Prescripcions Tècniques (d'ara endavant, PPT) és definir l'abast i les especificacions tècniques que regeixen el procediment de contractació del **Servei de Suport per a la gestió de Projectes de l'Àrea GIS**, promogut per **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A**. (en endavant, "Aigües de Barcelona"), així com l'execució d'aquest.

3 ABAST

L'abast del procediment és el que s'indica a continuació:

Servei de suport a la gestió de projectes i servei GIS

Les actuacions del procediment són les requerides per disposar a Aigües de Barcelona d'un Suport per a la gestió de Projectes i servei referits a les aplicacions de l'àrea GIS i s'asseguri de la correcta execució dels projectes i el seguiment dels processos i procediments associats al seu desenvolupament i dels diferents sistemes relacionats.

S'està buscant un perfil de cap de projecte amb capacitat per:

- Recollir la informació de les necessitats dels usuaris, valorar-la i traduir-la en plecs de licitació per als quals diverses empreses puguin proposar solucions.
- Coordinar les tasques de les diverses parts participant al projecte (Proveïdors, àrees d'Aigües de Barcelona, àrees d'IT) de manera que es puguin controlar els terminis d'execució i els costos dels projectes.
- Analitzar les solucions proposades pels proveïdors i/o proposar solucions per donar compliment a les necessitats dels usuaris.
- Realitzar i/o supervisar tasques de validació de la qualitat dels lliurables (documentació, requeriments d'accessibilitat web, requeriments de rendiment, etc.)

4 CONDICIONS OPERATIVES PEL DESENVOLUPAMENT DEL PROJECTE

4.1 Tasques a desenvolupar

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

- Col·laboració amb el client intern d'Aigües de Barcelona en la definició i la concreció dels objectius dels projectes a desenvolupar.

- Elaboració dels plecs de licitació quan passi, i suport durant la fase de licitació i adjudicació.

- Col·laboració en l'elaboració de la documentació formal de la inversió davant de les administracions

- Planificació dels projectes en tots els aspectes, identificant les activitats a realitzar, els recursos necessaris, els 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, si escau, la requerida quan es donin o es requereixin interferències entre els projectes.

- Assegurar la qualitat i el 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 Caps/Gestors de Projecte.

- Participar en les reunions d'inici, seguiment i tancament dels projectes amb els proveïdors, així com en les que es requereixin en el seguiment post-productiu (període de garantia dels projectes).

- Presa de decisions necessàries per 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 posar remei a les possibles desviacions detectades.

- Respondre davant 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, si escau, 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.

- Tramitació i gestió del tiquet intern per coordinar la realització de les diferents tasques dels equips interns, seguint els procediments establerts, i les eines corporatives.

- Assegurar que tot projecte i entregable compleixi tots els requeriments de seguretat i de protecció de dades necessaris, validant-lo conjuntament amb DPO i el departament de seguretat d'Aigües de Barcelona.

- Valorar diferents productes o opcions de desenvolupament, per escollir la que s'ajusti més a les necessitats d'Aigües de Barcelona, tant a nivell d'estratègia com de pressupost econòmic del projecte.

- Validació de definicions visuals dels sistemes (maquetes i/o mockUps) per tal d'assegurar que compleixen les necessitats de l'usuari final, obtenint-ne 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 de tipus Agile, o fins i tot amb un model mixt.

4.1.1 Metodologia de Treball

Els projectes dins Aigües de Barcelona passen per diverses fases en les quals cal donar suport des del servei gestionat per aquest acord marc.

Definició de requeriments

A partir d'uns requeriments d'alt nivell i sobre la base del pressupost aprovat al 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 per poder demanar ofertes sobre aquests a diversos proveïdors.

Preparació de la documentació per a l'Administració

A partir dels requeriments detallats i amb la llista d'aplicacions existents afectades o per construir cal omplir juntament amb la 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 el 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 pel procediment que li correspongui.

A més, caldrà 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 els accessos necessaris per desenvolupar les seves tasques, fer el seguiment 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 què pugui incórrer el projecte, ja siguin econòmics, tècnics, de retard, o de qualsevol tipus.

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

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 al projecte i l'elaboració d'una enquesta de satisfacció.

La metodologia de seguiment de projectes dins Aigües de Barcelona pot anar canviant a mesura que més projectes es desenvolupin amb mètodes Agile

4.1.2 Lliurables

La documentació que haurà d'elaborar el cap de projecte segons la fase en què 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 al 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 manera habitual la documentació dels projectes, pels plecs de licitació o per a l'administració es fa en català. Per això 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 es prestarà de dilluns a divendres, excloent-ne els festius nacionals i locals, coincidint amb l'horari

d'Aigües de Barcelona per tal de donar cobertura a fi del contracte.

L'adjudicatari haurà de garantir la cobertura horària davant de possibles imprevistos o tasques pròpies del servei, tenint en compte que aquestes situacions succeeixen amb caràcter puntual o excepcional, com pugui ser la posada en marxa d'un projecte, la resolució d'incidències greus provocades per un nou projecte, etc. Tot això, sense cap cost per a Aguas de Barcelona.

5.1.2 Equip de treball i actors per a la prestació del servei.

Àmbit GIS

Per desenvolupar les tasques que formen part d'aquesta licitació, l'adjudicatari aportarà el següent perfil el qual haurà de complir amb els requisits mínims que s'indiquen a continuació:

1.**UN (1) Analista GIS al 100% de dedicació.** El qual ha de complir aquests requisits mínims

• Estudis d'educació Universitària: Grau en Geografia, Enginyeria Geomàtica, Ciències Ambientals, Topografia o àmbits relacionats.

• Experiència mínima de cinc (5) anys en l'àmbit GIS, desitjable al sector utilities.

• Gestió de projectes de manera telemàtica mitjançant eines col·laboratives.

En cas de necessitat de substitució del perfil anteriorment descrit, s'haurà d'assignar una altra persona que disposi de la qualificació requerida, i si per assegurar la permanència del coneixement adquirit i la transferència fos necessària la concurrència entre els recursos entrants i sortints, durant el període esmentat només es tindran en compte com a hores productives les d'un dels recursos, per a qualsevol comptabilitat de l'esforç.

CONEIXEMENTS ESPECÍFICS

Els coneixements específics que es valorarà que disposi el perfil que realitzarà el servei seran:

- **Coneixements tècnics:**
    - Domini avançat de la suite de programari ESRI, incloent ArcGIS Desktop, ArcGIS Pro, i ArcGIS Online.
    - Experiència en l'ús de PostgreSQL amb extensió PostGIS per a l'emmagatzematge i l'anàlisi de dades espacials.
    - Experiència en projectes amb ArcGIS Utility Network per a serveis públics.
    - Coneixement pràctic de llenguatges de programació com Python i SQL per a automatització de processos i consultes espacials.
    - Familiaritat amb eines de visualització de dades geoespacials i creació de mapes interactius.
    - Experiència en l'ús de diversos formats de dades geoespacials (shapefile, GeoJSON, KML, etc.).

- Coneixement de sistemes de coordenades, projeccions cartogràfiques, anàlisis espacials modelat i transformació de dades.

• Experiència en Projectes GIS:

- Participació en projectes d'anàlisi espacial per a sectors com aigua, medi ambient, energia i gestió de recursos naturals.
- Projectes de desenvolupament d'aplicacions web GIS utilitzant ArcGIS Web AppBuilder i API for JavaScript d'ESRI.
- Implementació i manteniment de bases de dades espacials a PostgreSQL/PostGIS.
- Col·laboració en la creació de models de geoprocessament per automatitzar fluxos de treball.
- Experiència en la integració de dades de diferents fonts i formats a sistemes GIS.

• Habilitats:

- Capacitat per treballar en equip i col·laborar amb professionals de diferents disciplines ○Habilitats de comunicació per explicar conceptes tècnics a audiències no especialitzades ○Capacitat per atendre els usuaris, anàlisi i definició de nous requisits tècnics i funcionals.
- Aptitud per a l'aprenentatge continu i adaptació a noves tecnologies GIS.
- Experiència en la documentació de processos i metodologies GIS.
- Coneixement bàsic d'estàndards i normatives relacionades amb informació geoespacial.

5.1.3 Eines de gestió i control

Per a la gestió dels projectes i de les incidències associades a aquests, Aigües de Barcelona podrà determinar l'ús per al prestador del Servei d'eines de gestió específiques, com ara el Jira.

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

Rols i responsabilitats

Els prestadors del servei hauran de trucar als rols següents, aportant recursos l'experiència i el nivell de decisió dels quals s'adapti al seu nivell de responsabilitat.

• Responsable del Servei

És la persona que tindrà la visió complerta del servei i serà el principal interlocutor amb Aguas de Barcelona. Entre les seves funcions destaquem:

- Assegurar el compliment general dels compromisos adquirits
- Assegurar la correcta assignació dels recursos pel compliment dels objectius a cada projecte

- Generar un informe de seguiment global anual
- Actuar com a interlocutor principal per a la gestió de les modificacions a l'abast del servei que puguin sorgir
- Controlar que la facturació es faci conforme als acords i resoldre qualsevol problema sobre preus i pagaments.

El responsable de servei tindrà un interlocutor per part d'Agües de Barcelona amb qui mantindrà la comunicació, interlocució i resolució de problemes

Es poden establir reunions periòdiques de seguiment del servei amb la freqüència que s'estableixi o de manera puntual 3 dies laborables després d'una petició per qualsevol de les parts.

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 la pugui conservar, ni obtenir-ne còpia o facilitar-ne a tercers. Així, l'adjudicatari haurà de subministrar a Aigües de Barcelona la documentació derivada de la pròpia gestió.

6 ALTRES REQUERIMENTS

6.1 Ubicació

El servei es prestarà des de les mateixes oficines de l'adjudicatari, no obstant això, n'hi haurà **situacions habituals** que es requereixi de la presència a les mateixes oficines d'Aigües de Barcelona per motiu d'assistència a reunions, per a formació, les tasques realitzades al servei, seguiment del servei, resolució de problemes, etc.

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

6.2 Recursos Materials requerits

Els prestadors del servei seran responsables de disposar de l'equip de treball i de l'equipament maquinari i programari que sigui necessari per a l'execució de les prestacions contractades. En cap cas no es podrà facturar la compra, el subministrament o la instal·lació d'equips i recanvis que siguin necessaris per realitzar els serveis objecte d'aquest contracte.

Això no obstant, Aguas de Barcelona proporcionarà als Prestadors del Servei 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 engegada, hauran de fer ús de l'eina JIRA.
- Mentrestant, en fase de taula implantació (parcial o total) hauran de fer ús de l'eina de ticketing utilitzada per Aguas 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)

Aquest 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 als prestadors del servei durant l'execució del projecte, per proveir-los.

1. **ANS-01** (**Puntualitat en el lliurament dels informes de seguiment de projectes**): Desviació en el nombre de dies, pel que fa al termini de lliurament de l'informe quinzenal establert al 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 al projecte (15 dies naturals per exemple).

Fórmula aplicada:

Càlcul de la Penalització acumulada P1:

ANS-01 = (Nde – 5) (expressat en dies)

On,

Nde: Un cop finalitzat un període de seguiment (15 dies naturals), nombre de dies hàbils transcorreguts fins al lliurament de l'informe de seguiment corresponent.

Per cada incompliment s'hi afegeix un **2,00%** a l'acumulat.

L'informe final de projecte es considera un informe de seguiment adicional.

6.4.2 Penalitzacions derivades de l'incompliment amb els ANS

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

L'incompliment dels ANS podrà reduir l'import a facturar entre un 10,00% i un 25,00% 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 **2,00%** de penalització a l'acumulat.	
	Per tant: $P1 = (\sum_{i=1}^{n} 2{,}00)\%$, on n es el nombre de incompliments del **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 25,00%, s'aplicarà com a penalització aquest 25,00%.

Mentrestant **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**) abast o superi el 10,00%.

En cas que el Prestador del Servei acumuli un **PT** superior al 25,00%, Aigües de Barcelona estarà facultada per:

- resoldre el contracte, 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 es farà mitjançant connexió VPN Lan-to-Lan o amb usuaris VPN nominals.

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

7 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 a 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 facilitar-ne el seguiment i els 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.

ANNEX Núm. 1 - "NORMES DE SEGURETAT IT D'AIGÜES DE BARCELONA"

Els sistemes d'informació proporcionats no han de ser vulnerables, i segons apliqui, als TOP 10 d'Owasp Security Mobile i/o OWASP Top 10 Security Web (https://www.owasp.org). A més, haurà de complir la normativa de gestió d'usuaris i contrasenyes establerta en aquest annex.

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

"NORMES DE SEGURETAT IT D'AIGÜES DE BARCELONA"

ÍNDEX

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 dels contrasenyes d'accés als mateixos.

2. Intercanvi d'informació i programari SI-N-07-02/01

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

Quan, per raons d'urgència i eficiència del servei, sigui impossible la formalització prèvia del dit acord, l'intercanvi d'informació estarà subjecta a les condicions generals que preveu aquesta norma i el remitent és el responsable del seu compliment.

L'intercanvi s'ha de fer respectant la classificació i l'etiquetat de la informació que es faci servir durant aquest intercanvi.

Els intercanvis d'informació classificada com a Crítica, així com de dades de caràcter personal de nivell alt, s'han de fer emprant mecanismes de xifratge 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 les 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, la transmissió i la recepció de la informació que s'intercanvia. S'ha d'assignar un gestor per a cada acord amb la responsabilitat de controlar i fer-ne un seguiment del desenvolupament.

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

3. Configuració i administració segura

▪ Configuració segura

Tots els sistemes hauran d'estar configurats per verificar la identitat dels usuaris que accedeixen a ells, de manera que no es comprometin els credencials d'autenticació i és 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 ha de regir-es per el principi de menor privilegi, limitant els permisos únicament als estrictament necessaris per l'operativa diària de treball dels usuaris. En aquest sentit, únicament els administradors i operadors dels sistemes d'informació han de tenir accés als utilitats de gestió i administració del sistema que requereixin per a l'exercici dels seves funcions, i puguin existir diferents nivells de drets d'administració.

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

Addicionalment, per evitar, en la mesura que sigui 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 inactivar.
- Limitacions en el número màxim de connexions obertes.
- Restriccions en els algoritmes 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 algoritmes d'encaminament dinàmics, hauran d'usar-es mecanismes d'autenticació mútua basats en claus pre-compartides, certificats digitals i altres mecanismes que proporcionin major seguretat.

Per últim, 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 la RGPD i LOPDGDD.

- ***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 a l'usuari administrador i per al fet que els credencials d'aquest usuari administrador viatgin xifrades per la xarxa de comunicacions utilitzant tècniques criptogràfiques.

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

Inclòs en els processos d'administració de sistemes, s'haurà de portar a terme un procés de revisió periòdica de fitxers temporals en serveis centrals i sistemes d'informació d'AIGÜES DE BARCELONA, que corregeixi possibles errors que apareguin durant el procés d'esborrament de fitxers temporals. El tractament d'aquests fitxers temporals s'han d'ajustar al que s'ha disposat en els 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 dels unitats i societats operatives d'AIGÜES DE BARCELONA hauran de disposar de mecanismes que verifiquin la identitat dels usuaris que els utilitzen, de tal manera que és restringeixen els recursos als que deuen accedir cada usuari.

Els usuaris disposaran d'un identificador personal per tots els sistemes d'informació, permetent determinar les operacions que pugui realitzar en els diferents sistemes a través del seu identificador, excepte les excepcions recollides a l'apartat "Identificador 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, és realitzarà mitjançant l'ús de contrasenyes seguint els criteris de robustesa de contrasenyes indicats en 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 a l'acompliment 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'autentificació 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 avis pot alertar a 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 l'accés a arxius o transaccions especialment sensibles, l'usuari ha de ser re-autentificat, 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 l'accés al sistema en els següents casos:

- Per número 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 del correu electrònic, el superior jeràrquic de l'usuari implicat haurà de sol·licitar, a través dels procediments establerts, la rehabilitació dels privilegis del mateix. Tant si el desbloqueig es realitza manual com automàticament, hauran d'implantar-se 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 és 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 han d'atorgar-se únicament pel període de temps estrictament necessari i hauran de ser re-avaluats periòdicament.

No estarà permesa la creació o utilització d'usuaris genèrics excepte en aquells casos en els que sigui estrictament necessari per raons operatives, funcionals, etc., que, per la seva naturalesa, aconsellen o obliguen l'ús dels mateixos 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'utilitza. 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 de l'esmentat 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'exercici dels 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 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 tal d'evitar el possible esbrinament 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 manera 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 aquest efecte, una rehabilitació o desbloqueig de la contrasenya, el sistema de control d'accés obligarà l'usuari al canvi d'aquesta en el primer accés. La contrasenya inicial s'haurà de generar 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 disposi de l'opció per canviar-la o desconeguin 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 els que 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 algoritmes estàndards 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, tot i que haurà de ser configurable en funció de la criticitat i sensibilitat de les dades que es tracten.
    - 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. Llevat d'excepcions prèviament autoritzades per la Direcció de Seguretat TI. La Direcció de Seguretat el TI haurà de definir mecanismes de control d'accés alternatius que efectuïn controls no coberts per els sistemes de control d'accés instal·lats en els entorns, així com avaluar els avantatges i debilitats dels noves versions i/o productes alternatius o complementaris.

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

7. Comunicació dels incidents de seguretat

En el cas de detecció d'un incident greu de seguretat (mitjançant sistemes de detecció d'intrusos, anàlisi de logs, comunicació d'un tercer, alarmes de seguretat, etc.), la Direcció de Seguretat d'AIGÜES DE BARCELONA haurà de ser informada amb la major brevetat possible a través dels 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 que 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 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 els 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 reporting d'incidents de seguretat i tenen el deure d'emprar-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, ho haurà de reportar igualment.