Aigües de Barcelona

PLEC DE PRESCRIPCIONS TÈCNIQUES
QUE HA DE REGIR EL CONTRACTE RELATIU AL
"SERVEI DE SUPORT D'ENGINYERIA DEL SOFTWARE EN PROJECTES DE SISTEMES DE CONTROL INDUSTRIAL"

(EXPEDIENT NÚM. AB/2025/048)

CONTINGUT

1. INTRODUCCIÓ

El present Plec de Prescripcions Tècniques (d'ara endavant, PPT) estableix les prescripcions tècniques que regeixen el procediment de contractació per al "**SERVEI DE SUPORT D'ENGINYERIA DEL SOFTWARE EN PROJECTES DE SISTEMES DE CONTROL INDUSTRIAL**" promogut per Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A. (d'ara endavant, AB), així com l'execució d'aquest.

2. OBJECTE DEL CONTRACTE

Els serveis **d'Enginyeria del Software en Projectes de Sistemes de Control Industrial** prestats per l'empresa adjudicatària han d'assegurar l'execució, seguiment i control de tots els processos i procediments associats als serveis de suport especialitzat tècnic i funcional d'enginyeria del software dintre de l'àmbit dels Projectes de Sistemes de Control Industrial (en endavant SCI) d'Aigües de Barcelona.

3. ABAST

Les actuacions que formen part de l'abast del present PPT són les requerides per disposar a Aigües de Barcelona d'un Suport per la Gestió de Projectes referits a les aplicacions que donen suport als Sistemes de Control Industrial per tal d'assegurar la correcta execució dels projectes i el seguiment dels processos i procediments associats al seu desenvolupament i al dels diferents sistemes relacionats.

Per part d'Aigües de Barcelona es requereix un servei amb capacitat per:

- Garantir la disponibilitat i continuïtat operativa del programari SOFTWARE dels Sistemes de Control Industrial .
- Proporcionar suport tècnic especialitzat per a la resolució d'incidències i problemes.
- Mantenir la documentació tècnica actualitzada i accessible.
- Protegir la integritat, confidencialitat i seguretat dels sistemes i dades industrials.
- Desenvolupar programari d'alta qualitat que compleixi amb els requisits establerts.
- Garantir la fiabilitat, mantenibilidad i escalabilitat del programari.
- Facilitar la col·laboració i comunicació entre els membres de l'equip de desenvolupament.
- Promoure l'ús de bones pràctiques i metodologies per a millorar l'eficiència i reduir errors.
- Assegurar la documentació adequada per a facilitar futures modificacions i manteniment.
- Proporcionar formació i transferència de coneixement al personal de Manteniment.
- Realitzar informes periòdics sobre l'estat del servei i les accions realitzades.
- Assessorar en l'optimització i evolució del SOFTWARE per a millorar l'eficiència i la seguretat.

4. DESCRIPCIÓ DE L'ENTORN TECNOLÒGIC ACTUAL

En aquest capítol es descriu la plataforma tecnològica sobre la qual s'haurà de dur a terme els serveis descrits en el present plec. Es pot definir la plataforma tecnològica o entorn tecnològic, com el conjunt d'eines, sistemes, plataformes, infraestructures i processos tecnològics que utilitzaran els recursos dedicats al servei per a gestionar, processar, emmagatzemar i comunicar informació dintre dels SCI.

A continuació es detalla tot el conjunt que forma l'entorn tecnològic d'AB:

L'entorn de desenvolupament:

- Visual Studio 2017 per aquelles aplicacions més antigues.
- Visual Studio 2022 per les noves aplicacions que es van creant.

Les bases de dades:

- SQL Server, Postgre SQL.
- Cassandra i altres BBDD no relacionals.

Plataformes principalment utilitzades:

- .Net Framework 3.5, 4 y superior
  - WPF
  - Arquitectures Client/Servidor
  - Aplicacions monolitiques
  - Arquitectures N Capes
  - Web Services
- .Net 6+
  - Arquitectures Microserveis
  - Unit testing
  - SOLID
- Angular
  - Unit testing Jasmin o similar
  - Components com Kendo, materials, primerNg, etc…

Processos tecnològics:

- Coneixements de tot el cicle de vida de les aplicacions
  - Compilació dels diferents tipus d'aplicacions.
  - Deploy sobre màquines virtuals
  - Deploy sobre Docker/Kubernetes
  - Deploy sobre IIS
  - Anàlisis i resolució d'incidències
  - Capacitat per identificar noves funcionalitats.
  - Gitlab Code Review
  - Sonarqube i d'altres tecnologies aplicades a les bones pràctiques de programació.

5. EVOLUCIÓ DE L'ENTORN TECNOLÒGIC

Durant el desenvolupament del servei les tecnologies en ús per Aigües de Barcelona evolucionaran per a adaptar-se a noves necessitats i a l'estat de l'art. Per això, és imprescindible que el Prestador del servei s'adapti a aquesta evolució i estigui preparat perquè els equips de servei actualitzin les seves capacitats i coneixements.

Així, el licitador que resulti l'adjudicatari haurà de disposar d'un Pla d'incorporació de noves tecnologies per a garantir que, en el termini pactat des que Aigües de Barcelona decideixi la seva adopció, els equips de servei estiguin correctament capacitats per a prestar els serveis del contracte baix dites noves tecnologies.

Aquest Pla d'incorporació ha de contemplar, almenys:

- Accions formatives necessàries per a capacitar als membres de l'equip que es requereixi en les noves tecnologies.
- Adaptació de perfils en el cas que les noves tecnologies han substituït les tecnologies en ús anteriorment.
- Mecanismes d'assegurament i comprovació de l'adequació dels membres de l'equip per al nou entorn tecnològic.

Per tot això, l'adjudicatari al llarg dels anys de prestació del servei s'haurà d'adaptar als nous entorns tecnològics i noves aplicacions que puguin entrar dins de l'abast d'aquest.

Un clar exemple d'aquesta adaptació és l'evolució actual i les noves corrents tecnològiques que ens porten a la dockerització de les aplicacions. Els sistemes actuals en AB, es limiten a serveis de windows i aplicacions d'escriptori i alguna aplicació web publicada en IIS. Una de les noves vies que s'obren amb l'ús de les tecnologies actuals és la construcció de noves aplicacions basades en microserveis i publicades en Kubernetes aprofitant també les corrents actuals de l'Industrial IOT (Industrial 4.0)

6. ABAST DEL SERVEI

A continuació, es presenten els diferents serveis, característiques i requisits que conformen l'objecte del Contracte.

El Prestador del Servei haurà d'aportar els coneixements i metodologies, així com recolzar-se en les eines necessàries per a assegurar el resultat òptim en la prestació del servei.

Les diferents tipus d'activitats i tasques que formen part de l'abast del Servei d'Enginyeria del Software en Projectes de Sistemes de Control Industrial són:

- Disposar d'un canal de resposta prioritari a peticions crítiques i no crítiques realitzades per SCI.
- Anàlisi i seguiment de l'evolució de projectes relacionats amb Aplicacions Web o d'Escriptori (àmbit OT o IT-OT), comunicacions i sistemes d'informació tècnics per l'ajuda a l'explotació.
- Lideratge tecnològic en l'evolució de solucions tecnològiques Web o d'escriptori de l'entorn Industrial.
- Recerca i proposta de tendències tecnològiques en l'àmbit de solucions industrials (plataformes, eines, productes).
- Anàlisi i disseny de solucions tecnològiques Web o d'escriptori en l'entorn Industrial.
- Anàlisi i suport en la confecció d'arquitectures de software, garantit sempre la ciberseguretat aplicable a entorns OT i convergència IT/OT.
- Anàlisi i propostes de millora per a les bones pràctiques de programació i estàndards.
- Participació en la redacció de requeriments funcionals, no funcionals i tècnics, així com manuals o procediments tècnics de solucions de sistemes OT i softwares's industrials.
- Elaboració / Suport en l'elaboració de PoC (Proves de Concepte) i/o MVPs (Producte Mínim Viable).
- Revisió de codi o programari elaborat per tercers i/o ja existent.
- Control de versions de codi o programari i gestió de *merge requests*.
- Realització i documentació de proves FAT, SAT i proves de software (unitàries, funcionals, d'integració, de sistema, d'acceptació, extrem a extrem, etc).

- Realització i documentació de desplegaments en integració i preproducció, així com suport en desplegaments en producció.
- Desenvolupament de petits evolutius o correctius en les aplicacions i/o serveis ja existents, incloent resolució de bugs si es necessari.
- Instal·lació i configuració de connectors, tecnologies, API's i/o serveis per garantir les comunicacions entre les diferents aplicacions, SCADA's o serveis/microserveis.
- Execució de proves de rendiment en entorns de preproducció i producció per assegurar el correcte funcionament de les aplicacions, drivers i/o SCADA's rere les noves implementacions.
- Anàlisi de problemes i proposta de solucions a curt i mig termini.
- Interlocució amb l'usuari final sobre solucions tecnològiques existents i futures.
- Interlocució i Col·laboració amb partners/proveïdors i/o altres departaments o àrees d'Aigües de Barcelona (Manteniment Sistemes, Automatització, Ciberseguretat, TI, Operacions).
- Validació de les solucions a implementar (incloent requeriments i especificacions funcionals) o implementades (proves FAT i SAT) col·laborativament amb usuaris finals / Operacions.

6.1 ORGANITZACIÓ DE L'EQUIP

El Licitador podrà proposar l'organització que consideri més oportuna sempre que el servei cobreixi els requeriments d'horari esmentats que permetin complir amb els ANS del servei.

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos humans propis de l'adjudicatari amb la qualificació necessària per a la prestació del servei en el seu estat actual i en la seva evolució futura.

A continuació es descriuen els rols i les responsabilitats de les mínimes persones que es consideren més rellevants en la prestació dels serveis a contractar.

6.1.1. COORDINADOR DEL SERVEI

Al capdavant del servei d'Explotació el Licitador disposarà d'un perfil de Coordinador del Servei que actuarà de punt de coordinació davant el Responsable de l'àrea de Projectes del Departament de Sistemes de Control Industrial d'Aigües de Barcelona.

Els requisits mínims que deurà complir el Coordinador del Servei són:

- Estudis d'educació Universitària de caràcter científic o tecnològic com a graus i/o màsters en enginyeria (industrial, telecomunicacions, informàtica o similar) o ciències.
- Experiència, en els últims cinc (5) anys, d'almenys tres (3) anys com a Coordinador de serveis/projectes d'infraestructures OT a l'àmbit dels Sistemes industrials i/o SCADA.

Serà la persona assignada per l'Adjudicatari que tindrà la visió complerta del servei i serà el principal interlocutor amb Aigües de Barcelona dintre de l'àmbit de la gestió del contracte.

Entre les seves funcions destaquem:

- Assegurar el compliment general dels compromisos adquirits.
- Assegurar la correcta assignació dels recursos pel compliment dels objectius en cada projecte.
- Generar un informe de seguiment global anual del Servei.
- 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 realitzi conforme als acords i resoldre qualsevol problema sobre preus i pagaments.
- Participar en el Comité de Crisi en cas de necessitats del servei. Aquestes reunions, son excepcionals, i es poden derivar d'un problema greu en el programari de software d'AB. A efectes de la valoració del contracte s'han comptabilitzat 8 reunions anuals de 4h hores de durada.

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

6.1.2. TÈCNICS ESPECIALISTES DE SOFTWARE

Existirà un conjunt de tècnics, d'un perfil de SOFTWARE que seran qui executaran les tasques pròpies de la operativa del contracte.

Els requisits mínims que deurà complir els tècnics del Servei són:

- Estudis de CFGS (Aplicacions Informàtiques, Desenvolupament d'Aplicacions Web, Desenvolupament d'Aplicacions Multiplataforma o similars) o Estudis d'educació Universitària de caràcter científic o tecnològic com a graus i/o màster en enginyeria (industrial, telecomunicacions, informàtica o similar) o ciències, o equivalent.
- Experiència entre 3 i 5 anys en la realització i suport de projectes d'enginyeria del software en entorns industrials i/o relacionats amb grans centres de control o infraestructures complexes.

Coneixements tècnics i experiència en els següents aspectes:

- Arquitectures monolítiques i arquitectures orientades a microserveis.
- Eines / Tecnologies per al control de versions: GitLab o GitHub.
- Llenguatges de programació: .NET (Visual Studio: C++, C#, Visual Basic), Java, JavaScript, Angular, C, HTML, CSS.
- Comunicació / Intercanvi de dades: API's (JSON o XML), OPC-DA, OPC-UA.
- Base de dades: SQL Server, Postgre SQL, Cassandra.
- Entorns Virtuals (VMware, Stratus, Hyper-V...) amb Sistemes Operatius Windows i Linux, a nivell d'usuari i/o gestió de sol·licituds de creació de noves màquines virtuals.
- Altres coneixements altament desitjables:
    - Llibreries de log (Serilog, Log4Net, etc..)
    - Llibreries Job Planners (Quartz .Net)
    - Altres llenguatges de programació (Python, React, React Native, Jquery, TypeScript)
    - Altres protocols de comunicació (Apache Kafka, RabbitMQ, MQTT).

- Experiència en eines pipeline CI/CD: Jenkins, CodeShip, etc.
- Experiència en arquitectures de software basades en contenidors i dockers, així com plataformes de gestió de dockers (Tanzu, OpenShift, Kubernetes, etc).
- Coneixements mínims en ciberseguretat, aplicable a arquitectures de software.
- Experiència valorable en plataformes tecnològiques, altres llenguatges i/o components, bases de dades i eines de desenvolupament com: WPF NET, AngularJS, VueJS, NodeJS, Laravel, Oracle, MySQL, jQuery, LinQ, Entity Framework, etc.
- Molt valorable coneixements tècnics en Sistemes Scada: System Platform (Application Server - Wonderware), Ignition o similar.
- Valorable coneixements tècnics en AVEVA PI System i els seus mòduls i components.
- Experiència valorable en BI (Business Intelligence) i Big Data: Power BI, Datamart, Datawarehouse, etc.
- Valorable coneixements tècnics en altres Sistemes i Protocols de comunicació com: OPC-HDA, Protobuf, GPRS, UMTS, Ràdio, Tetra, LTC, etc.
- Valorable el domini de processos de tractament d'aigua potable i de depuració d'aigües residuals.
- Valorable l'experiència en l'àmbit de projectes/manteniment de solucions de software, SCADA's. PLC's, EDGE Computing i Plataformes IIoT.

Un punt important sobre l'organització del Servei és la transferència de coneixement sobre l'equip prestador del servei, de tal forma que AB només farà un traspàs de coneixement als tècnics del servei a l'inici del contracte. Posteriorment, en cas de noves incorporacions serà l'adjudicatari el responsable de fer aquesta transferència de coneixement.

6.2 REPORTING

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

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

6.3 REUNIONS DE SEGUIMENT

Es podran establir reunions periòdiques de seguiment del servei amb la freqüència que s'estableixi per ambdues parts, en tot cas no més d'1 mensual (de forma ordinaria), o de forma puntual i excepcional 3 dies laborables després d'una petició per qualsevol de les parts.

7. ALTRES REQUERIMENTS

7.1 COBERTURA DEL SERVEI

El servei es prestarà de dilluns a divendres, excloent els dies festius nacionals i locals, coincidint amb el calendari de personal tècnic d'Aigües de Barcelona (Cornellà) a fi de donar cobertura amb la finalitat del contracte. La quantitat d'hores de servei atenen al calendari del personal tècnic d'Aigües de Barcelona (Cornellà) és de 1672 hores.

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 Aigües de Barcelona.

7.2 UBICACIÓ DELS SERVEIS

El serveis es realitzaran de forma ordinaria en les dependències de l'Adjudicatari. De forma puntual i per necessitats del servei, es podria solicitar la presència de part de l'equip de l'adjudicatari per reunions de seguiment de servei. A efectes de la valoració del contracte s'han comptabilitzat **12 desplaçaments**, incloent les dietes, sota petició explícita d'Aigües de Barcelona, sempre dins de l'àrea metropolitana de Barcelona i sense que aquest fet (12 desplaçaments + dietes) pugui donar lloc a un increment en el cost del servei.

7.3 RECURSOS MATERIALS REQUERITS

Els Prestadors del Servei seran responsables de disposar de l'equip de treball i de l'equipament Maquinari i Programari necessari per a l'execució de les prestacions contractades. En cap cas no es 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 això, Aigües 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 o Smartsheet).

7.4 ACCÉS A LES INSTAL·LACIONS

L'accés del Prestador del Servei als sistemes d'informació d'Aigües de Barcelona es 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.

7.5 MANTENIMENT DE LA INFRAESTRUCTURA

Aquest contracte no contempla cap cost de manteniment d'infraestructura hardware.

7.6 MANTENIMENT DE LLICÈNCIES SOFTWARE

Aquest contracte no contempla cap cost de manteniment de llicències software.

8. ACORDS DE NIVELL DE SERVEI I PENALITZACIONS

El present apartat té per objecte fixar els nivells d'acord 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 servei, per a la provisió dels mateixos.

8.1 ACORDS DE NIVELL DE SERVEI (ANS)

Els acords de nivell de servei (ANS) s'han definit en funció de les característiques dels serveis objecte del contracte i de l'impacte que tenen sobre l'Explotació o sobre el Departament de SCI. Tanmateix depenen de la tipologia de l'ANS s'han determinat els períodes de temps i el càlcul per obtenir el seu resultat i poder mantenir la seva traçabilitat durant el període del contracte.

8.1.1. REQUERIMENTS DE NIVELL DE SERVEI PER L'ASSISTÈNCIA EN MATÈRIA D'ENGINYERIA DEL SOFTWARE

Es defineixen dos indicadors ANS dintre del servei per l'assistència tècnica als sistemes SOFTWARE d'AB: petició crítica i petició no critica.

En funció a la caracterització de les peticions (**crítica i no crítica**) es defineixen els següents temps de resolució depenen del tipus de petició:

Taula de referència de peticions		
Descripció	**Trep -> Temps màxim de resposta** [2]	**Tmax -> Temps màxim de proposta de solució** [2]
Crítica	<2h	<8h
No crítica	<16h [1]	*n.a*

[1] *és el temps màxim de resposta sobre una petició de valoració.*

[2] *temps dintre de l'horari laboral establert*

En funció del tipus petició i dels temps definits com a màxims es detallen els següents ANS mínims:

Codi	**Descripció**	**Mètrica**	**Període**	**Objectiu**
PET01	Resposta a peticions crítiques	Número de peticions crítiques sense resposta, en un temps superior al de la taula de referència	Mensual	<2
PET02	Resposta a peticions no crítiques	Número de peticions no crítiques sense resposta, en un temps superior al de la taula de referència	Mensual	<4
PET03	Resolució de peticions crítiques	Número de peticions crítiques no gestionades en un temps superior al de la taula de referència	Mensual	<3

8.2 PENALITZACIONS DERIVADES DE L'INCOMPLIMENT AMB ELS ANS

Els Prestadors del Servei, es comprometen a complir amb els ANS establerts al 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 servei.

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[1] de l'ANS PET01, s'afegeix un 3% de penalització a l'acumulat.
P2	Per cada incompliment[1] de l'ANS PET02, s'afegeix un 1% de penalització a l'acumulat.
P3	Per cada incompliment[1] de l'ANS PET03, s'afegeix un 3% de penalització a l'acumulat.

[1] *incompliment atribuible a l'Adjudicatari*

On la penalització total PT = (P1+P2+P3) a aplicar a la finalització del servei, serà el valor que resulti inferior d'entre els dos següents:

- Valor obtingut d'aplicar la fórmula següent: PT = P1+P2+P3.
- En cas que el valor anterior (PT) sigui superior al 25%, s'aplicarà com a penalització aquest 25%.

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

En cas que l'Adjudicatari 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.

ANNEX 1. 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 d'ús intern, restringit o confidencial que realitzi Aigües de Barcelona 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 de l'esmentat 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 l'etiquetatge de la informació que es faci durant l'esmentat intercanvi.

Els intercanvis d'informació classificada com restringida, així com de dades de caràcter personal de nivell alt, s'han de realitzar utilitzant 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 obligacions legals quan es duguin a terme, especialment les relacions amb les dades de caràcter personal.

En aquests acords s'ha 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 cada acord amb la responsabilitat de controlar i fer un seguiment del seu desenvolupament.

En l'àmbit legal, els acords han d'establir els responsabilitats i obligacions legals relatives a l'intercanvi, especialment aquelles derivades de l'intercanvi de dades de caràcter personal amb altres entitats, cessionaris o cedents, d'acord amb la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD) i amb el Reglament de Desenvolupament de la LOPD. No es podran realitzar intercanvis d'aquella informació classificada com a confidencial.

És responsabilitat de la Direcció de Seguretat identificar els mecanismes especials requerits per protegir actius crítics, amb els de xifratge indicats anteriorment o l'ús de solucions de no repudi, amb la finalitat d'assegurar la recepció de la informació per part del destinatari.

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 els 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 ha de regir-se pel 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 requereixi per a l'exercici de les 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: "és prohibeix tot allò que no és trobi explícitament permès", o el que és el mateix, s'han de desactivar tots els serveis en xarxa que s'activen per

defecte durant la instal·lació i en què el seu ús no és 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 inactives.
- Limitacions en el nombre 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'utilitzar-se mecanismes d'autenticació mútua basats en claus precompartides, certificats digitals i altres mecanismes que proporcionin més seguretat.

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

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 per al fet que els credencials d'aquest usuari administrador viatgen xifrades per la xarxa de comunicacions utilitzant 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 facilita 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 serveis centrals i sistemes d'informació d'Aigües de Barcelona, que corregeix possibles errors que apareguin durant el procés d'esborrament de fitxers temporals. El tractament d'aquests fitxers temporals s'han d'ajustar en el que s'ha disposat en les normatives legals vigents en matèria de protecció de dades de caràcter personal (LOPD).

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 tal manera que es restringeixen els recursos a què ha d'accedir cada usuari.

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

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

- Programari de control d'accés inherent al mateix 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 en l'apartat de "Gestió de contrasenyes i credencials".

Tots els mecanismes d'autenticació hauran de ser supervisats per la Direcció de Seguretat TU, 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 compliment de les seves funcions, no disposant de permisos d'accés als eines pròpies del sistema, excepte que els necessiti pel desenvolupament dels 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 avis pot alertar a l'usuari de l'existència d'accessos no autoritzats. En aquest cas s'haurà de comunicar immediatament al Capdavant de Seguretat de la Informació de l'entitat a la qual pertanyi.

Quan la criticidad del servei o recurs el 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 a 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 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 d'originada pel bloqueig d'un identificador d'usuari, el mateix usuari haurà de sol·licitar formalment, a través del correu electrònic corporatiu, la rehabilitació dels seus privilegis d'usuari. En 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 manual com automàticament tindran que implantar-es controls que permetin identificar i detectar intents d'accés no autoritzats.

Amb l'objectiu d'evitar atacs de denegació de servei als usuaris administradors, els cercausuaris administradors no es bloquejaran. S'hauran d'establir els controls compensatoris adequats per monitorar intents fallits d'inici de sessió per aquests usuaris, així com l'augment de temps per reintents o bloquejos temporals, sempre que sigui tècnicament possible.

5. Identificació d'usuari

L'accés a qualsevol dels sistemes d'informació d'Aigües de Barcelona és realitzarà utilitzant a 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 a l'identificador d'usuari com la persona física.

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.

La nomenclatura de l'identificador d'usuari es construirà amb independència de la funció exercida per l'usuari, del seu lloc de treball, del departament en la qual pertany i del sistema en el qual està connectat. L'identificador d'usuari romandrà associat al seu propietari d'Aigües de Barcelona amb independència dels canvis de destinació o de categoria que puguis tenir o, fins i tot de baixa; i d'acord a la legislació vigent en matèria de protecció de dades de caràcter personal.

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 només pel període de temps estrictament necessari i hauran de ser novament avaluats periòdicament.

No estarà permesa la creació o utilització d'usuaris genèrics excepte en aquells casos en els quals sigui estrictament necessari per raons operatives, funcionals, etc., que, per la seva naturalesa, aconsellen o obliguin l'ús dels mateixos i prèvia autorització específica del Cap de Seguretat de la Informació de l'entitat corresponent. En aquests casos, s'estrenarà el seguiment de les actividades realitzades amb l'usuari genèric, assegurant que es coneixen, en tot moment, el grup d'usuari que l'utilitzen. Quan la necessitat d'utilitzar l'usuari genèric per a 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 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 cas que els privilegis assignats a cada un 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 a qüestions de seguretat.

6. Gestió de contrasenyes i credencials de clients

Per evitar el possible esbrinament dels contrasenyes per part de tercers, aquestes hauran de complir una sèrie de requisits a l'hora de la generació de les mateixes.

Com a pauta general, les contrasenyes dels usuaris no hauran de tenir una longitud inferior a 6 (sis) caràcters alfanumèrics, incloent almenys dos caràcters numèrics i dos d'alfabètics.

Per evitar la selecció de contrasenyes fàcilment endevinables, quan sigui tecnològicament possible, els sistemes de control d'accés disposaran d'una col·lecció de regles de sintaxi que impediran, per exemple, que la contrasenya coincideix amb l'identificador d'usuari, o correspongui en una seqüència de longitud vàlida d'un mateix caràcter repetit, coincideixi amb blancs o constitueixi una paraula coneguda. Aquesta verificació s'executarà de manera automàtica durant el procés de canvi de contrasenyes en les aplicacions o eines en els quals s'utilitzi.

Els sistemes han de permetre a l'usuari el canvi de la seva contrasenya de forma autònoma quan aquest l'estimi 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 el 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 disposi de l'opció per canviar-la o desconeixen com realitzar el canvi.

Després de cinc intents fallits consecutius en la introducció de la contrasenya per part de l'usuari, com a màxim, el sistema haurà d'inhabilitar l'identificador associat fins a la seva inicialització o desbloqueig.

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 en tots els usuaris abans que aquests accedeixin a qualsevol dels recursos d'ús intern, restringit o confidencial pels 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 algoritmes estàndards de xifratge.
    - No mostrar-se 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'estabiran 5 minuts com a valor de referència, encara que haurà de ser configurable en funció de la criticidad 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 programes, "scripts" o codis desenvolupats per a connexió automàtica als sistemes d'informació. Exceptuant excepcions prèviament autoritzades per la Direcció de Seguretat TU. La Direcció de Seguretat TÚtindrà que 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 dels noves versions i/o productes alternatius o complementaris.

La Direcció de Seguretat TÚ tindrà que 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 destral.

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 Aigües de Barcelona haurà de ser informada amb la brevetat més gran possible a través de les línies de comunicació que s'establiran prèviament amb aquest propòsit.

La Direcció de Seguretat s'encarregarà d'iniciar un informe amb les figures, escollides entre aquelles que prèviament havien estat identificades, la qual la seva participació sigui necessària en la resolució de l'incident. Aquesta elecció es farà en funció de la criticidad 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 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 al davant d'incidents de seguretat.

El reporting d'informació sobre incidents de seguretat quedarà restringit únicament a aquelles persones absolutament necessàries. Qualsevol divulgació d'aquella 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 reporting 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-lo igualment.