PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HA DE REGIR EL CONTRACTE RELATIU AL

"SERVEI DE SUPORT PER A LA GESTIÓ D'AGILE COACH DE L'ÀREA DE SISTEMES DE LA INFORMACIÓ D'AIGÜES DE BARCELONA"

NÚM. EXP.: AB/2025/223

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 CONTRACTE DE SERVEI DE AGILE COACH promogut per Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A. (d'ara endavant, AIGÜES DE BARCELONA), així com l'execució del mateix.

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 d'Agile Coach per optimitzar fluxos de treball i definir un model de col·laboració per aconseguir una gestió més eficient entre les persones participants en diferents projectes, processos i/o procediments.

3 ÀMBIT D'ACTUACIÓ

El servei de suport sol·licitat ha de ser capaç de coordinar-se amb diferents agents implicats, tant d'IT com de negoci, com d'agents externs, en funció de la necessitat que sorgeixi.

4 CONDICIONS OPERATIVES PER EL DESENVOLUPAMENT DEL SERVEI

4.1 Principals tasques a desenvolupar

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

Facilitació de cerimònies:

- Reunions de sincronització
- Sessions de refinament
- *Sprint planning*
- *Sprint review*
- Retrospectives
- Cerimònies del marc de treball SAFe

Principals línies de treball:

- Assegurar la participació en les cerimònies claus i dedicació als artefactes al llarg de l'actuació
- Acompanyar i promoure la implementació de les metodologies Agile i gestió del canvi cultural
- Fomentar una cultura de col·laboració i transparència,
- Elaborar unes polítiques i acords de treball clars entre els implicats
- Promoure i acompanyar en la millora continua
- Gestionar el flux de treball en JIRA

- Ajudar a establir mètriques i objectius clars per a mesurar el progrés
- Documentació de polítiques de treball en *Confluence*
- Formació en metodologies àgils
- Servir com a mentor per a *Coach Agile* i altres rols àgils
- Col·laborar amb la PMO, en cas que sigui necessari, per assegurar que el flux d'informació generat arriba en format i forma als destinataris adequats.
- Definir i evolucionar els estàndards àgils per posteriorment aplicar-los en equips.
- Crear comunitats de pràctica i col·laborar amb la gestió del canvi.

Seguiment i col·laboració

L'Agile Coach estarà coordinat amb tots els stakeholders implicats en l'actuació a ejecutar. Els principals equips amb qui ha de colaborar son:

- Equip de Negoci
- Equip de IT
- PMO: en el cas de necessitar la seva col·laboració en projectes

4.2 Responsabilitat complementàries

Es requereixen d'unes responsabilitat complementaries que son requerides en el servei per tal de garantir l'èxit del mateix:

Metodologia i forma de treballar

Promoure l'optimització del procés i el flux de treball, i fomentar la millora contínua de l'equip i de la cadena de valor en què està situat.

Assegurar l'orientació dels equips a producte, estabilitzant el grup i evitant la segregació d'aquest.

Vetllar per l'equilibri entre funcionalitat, deute i qualitat. Alinear les diferents demandes si no arriben a compromisos i alertar si aquests poden ser perjudicials a llarg termini.

Fomentar el pensament crític, promoure cicles de retroalimentació freqüents i minimitzar les disfuncions de l'equip.

Mantenir motivades les persones de l'equip, així com elaborar unes polítiques i acords de treball clars.

Acompanyar i evolucionar els rols clau de l'equip durant el seu cicle de vida del producte o servei.

Guiar els equips durant el seu cicle de treball per assegurar que apliquen correctament els principis àgils i els entenen, gestionar riscos.

Lliurament freqüent i continu de valor

Mantenir un pensament sistèmic i iteratiu incremental.

Promoure la preparació àgil de noves funcionalitats de producte o necessitats del servei, posant el focus en la satisfacció del client i el lliurament de valor.

Assistir en la descomposició de funcionalitats en ítems prou petits, a través de diferents estratègies, per afavorir el desenvolupament iteratiu i incremental, així com el lliurament continu de producte útil i de valor.

Ajudar l'equip a millorar en la tasca d'estimació de funcionalitats o de temps d'execució de servei.

Facilitació i desbloqueig d'impediments

Conscienciar l'equip en la seva autogestió, en la recerca de l'excel·lència, així com a assolir el seu màxim nivell de productivitat i temps de procés.

Facilitar els diferents esdeveniments del marc de treball utilitzat i vetllar perquè es compleixi el seu objectiu.

Potenciar l'orientació de l'equip cap a la resolució de problemes i que siguin capaços de posar en dubte el perquè del que se'ls demana.

Transparència i mètriques de seguiment

Construir, mantenir i publicar mètriques de seguiment que ajudin l'equip a millorar de forma contínua, i que serveixin per transparentar el seu estat de salut.

Assegurar que s'utilitzen les mètriques adequades per posar en valor o ajudar l'equip a evolucionar (eficàcia, eficiència, qualitat, satisfacció...).

Conèixer la maduresa de l'equip i portar-los a un equip d'alt rendiment.

Estratègia

Contribuir a què els equips segueixin les bones pràctiques i normes de l'organització (codi, metodologia, usabilitat, seguretat...).

Col·laborar activament per definir les millors pràctiques i compartir avenços i millors pràctiques del seu equip.

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 i la prestació del servei es realitzarà en un temps estimat de 2 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'haguin efectuat durant el desenvolupament del servei. Mensualment i amb detall diari hauran de ser reportades les hores de dedicació a l'actuació que serviran com a base per a la facturació del mes.

S'estima un volum anual màxim de 900 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 ha de nomenar un Responsable global del Servei. Aquest Responsable del Servei haurà de tenir la capacitat, els coneixements i l'experiència suficients als efectes de supervisar, coordinar i vetllar per la prestació correcta del Servei, i exercir tasques 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 les necessitats establertes al present plec, controlant i garantint que totes les decisions i accions que es prenguin estiguin focalitzades en la correcta execució de les activitats del servei.

  En concret, haurà de disposar com a mínim de:
  - Estudis d'educació universitària de caràcter científic o tecnològic com graus i/o màsters en enginyeria (industrial, telecomunicacions, informàtica o similar) o ciències;
  - Experiència mínima de TRES (3) anys com a Responsable de Projectes de Transformació en empreses multinacionals (com a intern o consultor extern).

- **UN (1) Agile Coach**

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

  - Titulació universitària de caràcter científic o tecnològic com graus i/o màsters en enginyeria (industrial, telecomunicacions, informàtica o similar) o ciències.

- Experiència mínima de TRES (3) anys com a Agile Coach en la en la creació i gestió d'oficines de gestió de projectes (PMO) i establiment d'estàndards de qualitat i de millors pràctiques, en la gestió de projectes complexos, així com en la coordinació d'equips multidisciplinars i multiproveïdor, amb els següents aspectes tecnològics:
  - Domini avançat de metodologies àgils com SAFE, Kanban, Scrum i Lean.
  - Domini avançat de Jira i Confluence
  - Certificació en SAFe tipus "SAFe PRACTICE CONSULTANT (SPC)"
- Experiència contrastable en posició similar a altres empreses.
- Habilitats de comunicació i presentació
- Capacitat de resolució de conflictes
- Pensament analític i estratègic
- Adaptabilitat i flexibilitat

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

Habilitats Interpersonals:

- Capacitat per construir i mantenir relacions de confiança amb stakeholders interns i externs.
- Habilitats en comunicació i negociació per assegurar l'alineament d'expectatives entre clients, equips i proveïdors.
- Enfocament col·laboratiu per coordinar equips multifuncionals i proveïdors externs.

Competències Clau:

- Enfocament estratègic amb capacitat per aterrar iniciatives a nivell operatiu.
- Forta orientació a resultats amb habilitats analítiques per resoldre problemes complexos.
- Adaptabilitat al canvi i compromís amb la millora continua.
- Capacitat per mentoritzar en metodologies Agile i desenvolupar equips tècnics, promovent un entorn d'aprenentatge i creixement continu.

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 transferència fos necessària la concurrència entre els recursos entrants i sortints, durant el esmentat període només es 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 a aquest, Aigües de Barcelona podrà determinar l'ús per al prestador del Servei d'eines de gestió específiques, com Jira.

Aigües de Barcelona proveirà els usuaris i els 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-ne còpia 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 l'haurà d'aprovar el personal d'Aigües de Barcelona.

6 ALTRES REQUERIMENTS

6.1 Ubicació

El servei es prestarà des de les oficines d'Aigües de Barcelona: Collblanc o Badalona, no obstant això, es poden donar situacions on es pot treballar de forma remota. Per altra banda, l'assistència a reunions d'especial importància i altres situacions d'especial rellevància per al bon èxit del projecte es realitzaran de forma presencial sense excepció.

Per tant, el servei inclou el suport presencial. 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

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, el subministrament o la instal·lació d'equips i recanvis que siguin necessaris per realitzar els serveis objecte d'aquest contracte.

Tot i això, Aigües De Barcelona proporcionarà als Prestadors de 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 de cada lot haurà d'utilitzar les eines d'Aigües de Barcelona per al reporting i seguiment de les incidències detectades:

- En fase de definició, proves d'acceptació i engegada, hauran de fer ús de l'eina JIRA i de Confluence.
- En fase d'implantació (parcial o total), a més, hauran de fer ús de l'eina de tiquet 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 te 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 servei contractat, 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 (**ANS-01**).
Compliment:	Si **ANS-01 ≤ 0** Sense efecte. Si **ANS-01 > 0** Incompliment.
Periodicitat de càlcul:	Finalitzat cada període de seguiment definit (15 dies naturals per exemple).
Fórmula aplicada:	**ANS-01 = (Nde – 5)** *(expressat en dies)* *On,* **Nde:** *Un cop finalitzat un període de seguiment (15 dies naturals), anomeni de dies hàbils transcorreguts fins al lliurament de l'Informe de seguiment corresponent.*
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.

- **ANS-02** (**NPS - Net Promoter Score**): Recomanació principals stakeholders dels serveis d'acompanyament del Agile Coach a tercers.

Indicador:	NPS (**ANS-02**).
Compliment:	Si **ANS-02 ≤ 7** Incompliment (es necessita un mínim del 60% de respostes de l'enquesta per validar un incompliment). Si **ANS-02 > 7** Sense efecte.

Periodicitat de càlcul:	Cada dos mesos. En cas de sortir incompliment es pot repetir mesura al cap de 15 dies.
Fórmula aplicada:	**ANS-02 = nota enquesta** *(del 1 al 10)* *On,* **nota enquesta:** Enquesta simple on es pregunta si recomanarien els serveis a un altre equip. La pregunta pot estar inclosa entre altres preguntes relacionades.
Càlcul de la Penalització acumulada P1:	Per cada incompliment s' afegeix un **2% a** l' acumulat.

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**.
P2	Per cada incompliment de l **' ANS-02**, s' afegeix un **2%** de penalització a l' acumulat. Per tant: $P2 = (\sum_{i=1}^{n} 2)\%$, on n és el nom d'incompliments de **l'ANS-02**.

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 + P2

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 a partir 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.

9 ESTIMACIÓ DE COSTOS

Els costos estimats per aquesta actuació on està estimada en 900 hores es de 81.000 € anual màxim.

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 TIP 10 d'Owasp Security Mobile i/o OWASP Top 10 Security Web (https://www.owasp.org). A més a més haurà de complir-la hi normativa de gestió d'usuaris i contrasenyes establerta en el present Annex.

Aquesta normativa pot complir-s'utilitzant l'Activi Directory d'Aigües de Barcelona com 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

3.1. 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.

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 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, haurà de reportar-ho igualment.