Aigües de Barcelona

La gestió responsable

PLEC DE PRESCRIPCIONS TÈCNIQUES

QUE HAN DE REGIR EL CONTRACTE PER ELS SERVEIS CORRESPONENT A LA RENOVACIÓ COMUNICACIONS NIVELL 3 EDARs"

Novembre 2019 - Versió 5.0

ÍNDEX

1. Objecte

El present Plec de Prescripcions Tècniques (en endavant, PPT) estableix les prescripcions tècniques que regeixen el procediment de contractació per el **Serveis corresponents a la Renovació Comunicacions Nivell 3 EDARs** promogut per **Aigües de Barcelona, Empresa Metropolitana de Gestió del Cicle Integral de l'Aigua, S.A.** (en endavant, AB), així com l'execució del mateix.

2. Abast

Es desitja renovar la electrònica de Xarxa que forma els “Cores OT” de les següents EDARs (Estació de Depuració d’Aigües Residuals) d’Aigües de Barcelona de:

1. Montcada;
2. Prat del Llobregat;
3. Gavà-Viladecans;
4. Begues;
5. Sant Feliu del Llobregat;
6. Vallvidrera;

L’equipament de commutació que forma actualment els Cores OT sobre el que es vol actuar fa funcions de nivell 2 (estan darrera d’un Firewall que fa de nivell 3), fan de funció de ”xarxa d’accés” pels hosts i servidors local i de “xarxa de distribució” pels switches remots.
L’equipament de commutació que forma actualment els Cores OTs està en EoS (End of Support) i no és “gestionable”.

3. Condicions tècniques

Aspectes Generals.

- L'equipament que es proposi ha de ser Cisco;
- Els switches de 24/48 ports de Core, muntat en stack, han de tenir ports Ethernet a 1Gbps, han de suportar SFP+ MM a 1Gbps, doble font d'alimentació, i protocol REP; han de ser telegestionables i permetre un Forwarding bandwidth = 108 Gbps i un Forwarding rate: 64-byte Layer 3 packets = 95.2 Mpps;
- Els switches de 12 ports han de ser de la mateixa gama i han de tenir característiques similar que els de 24/48 ports.
- L'equipament que s'instal·li, ha d'integrar-se operativament a la LAN-WAN de Aigües de Barcelona, i serà gestionat pel proveïdor al que AB té delegada la gestió de la LAN;
- La instal·lació té de seguir unes normes de configuració que vindran marcades pel proveïdor encarregat de la gestió de la LAN;
- El canvi dels switches es farà en horari laborable, mirant de reduir al màxim el temps d'indisponiblitat;
- Cal presentar una Memòria de Projecte, incloent-hi: material, equipament (Model, SN, MAC), taula d'assignació de ports-lloc de treball i Visio actualitzat;
- El projecte és "claus en ma";

3.1 Aspectes particulars de cada seu

EDAR	Equip actual	Substituir per	F.Os/Latiguillos RJ45
Montcada	TRENDNET	Stack de 2 switches Cisco de 24 ports c.u. i 2 SPF MM 1Gbps	2 de 2m./24 de 2 m.
Prat	SP302-8 + SG500-	Stack de 2 switches Cisco de 48 ports c.u. i 4 SPF MM 1Gbps	4 de 2m./48 de 2 m.
Gavà	SFE2000P	Stack de 2 switches Cisco de 24 ports c.u i 2 SPF MM 1Gbps	2 de 2m./24 de 2 m.
Begues	No aplica	1 switch Cisco de 12 ports	0/6 de 2 m.
Sant Feliu	SFE2000P	Stack de 2 switches Cisco de 24 ports c.u i 2 SPF MM 1Gbps	2 de 2m./24 de 2 m.
Vallvidrera	No aplica	1 switch Cisco de 12 ports	0/6 de 2 m.

4. Condicions operatives per el desenvolupament del projecte.

4.1 Planificació del projecte i terminis d'entrega

En un termini no superior a **sis (6) mesos**, el Prestador del Servei haurà de posar a disponibilitat de AB la totalitat de les funcionalitats requerides, així com haver donat compliment a la totalitat dels requeriments tècnics definits.

Els licitadors hauran d'entregar en les seves ofertes una proposta de planificació per l'execució del projecte, amb l'objectiu de disposar de les millores fetes en el termini indicat anteriorment o inferior que s'oferti a comptar des de la signatura del Contracte.

L'esmentada planificació haurà d'incloure com a mínim les següents tasques:

1. Kick off

   Reunió d'inici del projecte en la que es concretarà el plà de treball

2. Disseny tècnic. El disseny tècnic ha d'especificar com es faran les tasques del projecte, les quals son:

   Instal·lació física dels equips en els armaris de comunicacions

   Configuració inicial dels equips seguint les instruccions del nostre proveïdor de gestió de xarxes informàtiques

   Connexionat dels nous equips amb la resta de la xarxa

   "Pentinat" del cablejat per deixar-lo perfectament ordenat

3. Construcció (per seus). A cada seu es repetiran les tasques incloses en el disseny tècnic.

4. Probes (detallant tipus de probes).

   Es faran les probes necessàries per certificar que els nous equips funcionen perfectament i que s'han integrat sense problemes amb la resta de la xarxa.

   Per aquells equips que s'instal·lin en stack i/o alta disponibilitat es comprovarà que el sistema és tolerant a la fallida d'un dels elements.

5. PaP y traspasso a servei. Documentació que ha d'incloure, com a mínim:

   Disseny gràfic dels equips dins del seu nou entorn

   Configuració inicial utilitzada

   Bitàcora de les tasques realitzades

6. Suport proporcionat durant el període de garantia.

En qualsevol cas, el licitador que resulti Adjudicatari haurà de construir l'equip de treball per l'execució del projecte objecte d'aquesta licitació, així com dur a terme la reunió de Kickoff prevista en el PPT, en un termini màxim de QUINZE (15) dies naturals a comptar des de la signatura del Contracte.

Els licitadors disposaran de un termini de **4 setmanes com a màxim**, a comptar des de la signatura del Contracte, per a subministrar i lliurar a les EDARS tot el material del projecte.

Un cop iniciat el projecte, el Prestatari del Servei s'haurà de coordinar amb AB la comunicació prèvia als usuaris als quals se'ls farà el canvi.

4.2 Lliurables Tècnics

Tant durant la durada del projecte con durant el període de garantia, s'haurà de generar i entregar, com a mínim, la següent documentació:

Abans de l'inici de les instal·lacions

- **Planificació del Projecte**, s'haurà de presentar a l'inici del projecte, durant el **Kickoff**.
- **Document d'inici de projecte** o **Kickoff**, que es presentarà als interessats (tant de negoci, de gestió de la demanda com l'equip intern de AB) en la reunió de formalització d'inici de projecte.

Abans d'iniciar el desplegament

- **Pla de Proves**. Aquest document s'entregarà en dos fases. En una primera entrega, sense executar, per poder validar les proves a fer. La segona entrega es farà per cada un dels equips instal·lats. Serà un documento viu que, si cal , s'actualitzarà durant el desplegament.
- **Pla de Implantació**. Haurà de ser revisat i aprovat per AB. S'haurà de fer un per cada seu a desplegar.
- **Documentació PaP.** Actualització de la documentació d'inventari (Marca, Model, MAC, SN) i altra documentació relacionada.

A la finalització del desplegament:

- **Fitxa de tancament del projecte**. Amb aquest document es podran valorar els objectius acomplerts i si el resultat ha sigut exactament el que s'esperava. També haurà de recollir aquelles lliçons apreses durant les diverses etapes del projecte. Es formalitzarà l'entrega del document que contengui l'As Built (dels nous equips, llicencies, programes i manual d'us i configuració) a una reunió i , amb la signatura de l'acta corresponent es donarà per finalitzat el projecte.

Durant la durada del projecte:

- **Informes de Seguiment**. Seran informes recurrents que haurà de presentar el Cap de Projecte en les reunions de seguiment del projecte. Hauran de recollir informació sobre l'estat del projecte, grau d'avenç, problemes trobats, riscos i mitigació **dels mateixos.** Es requerirà un informe cada 15 dies.
- **Informes de Desplegament**. Serà un informe per cada planta, en el qual es podran valorar els objectius acomplerts i si el resultat ha sigut exactament el que s'esperava. També haurà de recollir aquelles lliçons apreses durant el desplegament que puguin utiltitzar-se en desplegaments posteriors.

Durant el període de garantia:

- **Informe d'Incidències Significatives.** Una vegada posat en marxa el projecte fins la finalització de la garantia, de generar-se una incidència greu (tipificades com *Crítica* o *Alta*) sobre alguns dels processos o una indisponiblitat parcial o total del sistema, el licitador haurà de generar un informe d'Incidència Significativa, detallant el motiu pel qual s'ha

produït i el pla d'acció per la resolució. Aquest informe tindrà de ser entregat en un temps màxim de TRES (3) dies laborables des.de la comunicació de la incidència por part d'AB.

4.3 Ubicació

Els serveis es prestaran als centres de treball dins de l'àmbit territorial de l'Àrea Metropolitana de Barcelona, sense que això pugui suposar un increment de costos en els serveis.

4.4 Recepció, control, resolució i canalització d'Incidències

L'Adjudicatari haurà d'utilitzar les eines d'AB per al reporting i seguiment de les incidències.

4.5 Garantia

El període mínim que ha de tenir com a garantia el producte entregable serà de SIS (6) mesos, a contar des.de la posta en producció i activació dels mateixos (lliurament de la Fitxa de tancament de Projecte). Dins d'aquest període el proveïdor tindrà que solucionar las incidències que hi pugin sorgir relacionades amb el projecto sense cap cost afegit.

No obstant això, tal com s'indica a la clàusula 7 del "Plec de Condicions Particulars" (PCP), els licitadores podran oferir un augment del període de garantia respecto als SIS (6) mesos indicats.

4.6 Gestió i coordinació de l'execució

S'indiquen a continuació uns requeriments mínims de seguiment i control que haurà de complir el Prestatari del Servei

Rols i responsabilitats

El Prestatari del Servei haurà de nomenar com a mínim els següents rols, aportant recursos l'experiència i nivell de decisió dels quals s'adapti al seu nivell de responsabilitat: Responsable del Contracte i Cap de Projecte.

- ***Responsable del Contracte***

  Es la persona que tindrà la visió completa del Contracte i serà el principal interlocutor amb AB. Entre les seves funcions destaquen les següents:

  - Assegurar el compliment general dels acords de nivell de servei (ANS).
  - Assegurar la correcta assignació de recursos per el compliment dels objectius del projecte objecte de contractació y dels ANS.
  - Garantir la ràpida resolució y priorització de les incidències greus.
  - Assegurar el compliment de la Planificació general i dels compromisos de contracte en els diferents aspectes.
  - Assistir a las reunions de Comitè de seguiment.
  - Decidir o gestionar la decisió per part del Prestador del Servei sobre la validesa dels ANS mesurats i les penalitzacions que se'n puguin derivar.
  - Actuar com interlocutor principal per la gestió de les modificacions en l'abast del Contracte que pugui sorgir.

El Responsable del Contracte haurà de tenir un interlocutor per part de AB amb qui mantindrà la comunicació, interlocució i resolució de problemes.

- ***Cap de projecte***

  Es la persona que tindrà la visió completa del projecte i serà el principal interlocutor amb AB en tot el relacionat amb el detall de l'esmentat projecte. Entre les seves funcions destaquen les següents:

  - Fer el seguiment de les fites i l'avanç del projecte
  - Assegurar la qualitat i compliment amb els objectius del projecte, terminis establerts, entregues i ANS.
  - Validar, finalitzar i fer arribar a AB els entregables segons la planificació.
  - Identificar possibles riscos i implementar accions mitigadores.
  - Assegurar la correcta atenció de les incidències detectades, segons la prioritat assignada a cada una.
  - Gestionar la ràpida resolució i priorització de les incidències greus (tipificades com Crítiques o Altes).
  - Coordinar l'equip de projecte assignat al projecte per el Prestatari de Servei.
  - Supervisar que el personal integrant de l'equip de treball desenvolupa correctament les funcions que te encarregades.
  - Coordinar amb AB les activitats en les quals existeixen relacions entre els dos, per la correcta execució del projecte.
  - Participar en las reunions d'inici, seguiment i tancament del projecte, sota requeriments de AB, així com elaborar les actes de reunió corresponent.
  - Informar al Responsable de Projecte de AB de qualsevol circumstància que pogués afectar al desenvolupament correcte del projecte (retards en la planificació, estat en el tancament de les incidències, nivell d'avanç, etc.).
  - Actuar com interlocutor principal per la gestió de les modificacions en l'abast del projecte que puguin sorgir.
  - Elaborar la Fitxa de Tancament de Projecte.
  - Recolzar al Responsable del Contracte en la seva funció d'informar a AB sobre la marxa del projecte.

  El Cap de Projecte haurà de tenir el seu corresponent interlocutor per part de AB amb el qual mantindran la comunicació, interlocució i resolució de problemes. En aquest sentit, AB fixarà un Responsable de Projecte que actuarà com interlocutor principal del Cap de Projecte designat per el Prestatari del Servei. D'igual manera aquest Responsable del Projecte establirà les coordinacions necessàries amb els Responsables d'altres projectes vinculats o amb impacte amb el que és objecte del present Plec.

  Aigües de Barcelona designarà un cap de projecte que coordinarà el projecte amb el cap de projecte adjudicatari i amb la resta de projectes vinculats.

Comitè de Seguiment del Contracte

S'establirà un Comitè de Seguiment que es reunirà amb caràcter periòdic bimestral o amb la freqüència superior que raonablement es consideri necessària o després de TRES (3) dies laborables després d'una petició de qualsevol de les parts.
El Comitè de Seguiment estarà compost per les persones que el **Prestador del Servei** (almenys, el Responsable del Contracte) i AB designin per cada part.

En qualsevol cas, el Comitè de Seguiment del Contracte serà informat de l'evolució del projecte.

Les funcions del Comitè de Seguiment, es cenyiran a les que es refereixen a l'execució del projecte, a saber:

- Presentació per part del **Prestador del Servei** de l'informe de seguiment dels diferents Serveis i les mesures dels ANS definits.
- Seguiment global del projecte.
- La revisió del compliment dels corresponents indicadors de nivell de servei i l'ajust d'aquests indicadors a la realitat, així com l'establiment de les penalitzacions que puguin derivar-se del nivell de compliment d'aquests indicadors.
- Aprovació formal per ambdues parts dels ANS calculats i de les penalitzacions corresponents, si hi haguessin, alliberant el procés de facturació associat.
- L'anàlisi i resolució de les incidències o discrepàncies que puguin sorgir en la prestació del servei, que no hagin pogut ser resoltes, i hagin sigut escalades al Comitè de Seguiment.
- Qualsevol qüestió relacionada amb la variació del perímetre o abast del Servei.
- L'anàlisi de qualsevol modificació o adaptació del Contracte, de conformitat amb aquelles que s'han previst de forma expressa en el PCP o bé aquelles considerades sobrevingudes.
- Qualsevol altre funció que es consideri per a l'execució exitosa del Projecte.

Comitè de Seguiment Operatiu

S'establirà un Comitè de Seguiment Operatiu que mantindrà reunions de seguiment (almenys amb caràcter periòdic quinzenal o amb la freqüència superior que raonablement es consideri necessari en funció de l'evolució del projecte o després de DOS (2) dies laborables després d'una petició de qualsevol de les parts) així com revisions tècniques, entre l'equip de coordinació d'AB i el Cap de projecte designat per el Prestador del Servei i amb la part de l'equip de projecte la participació de la qual es consideri necessària.

A continuació, s'indiquen de forma no exhaustiva ni limitativa, les tasques d'aquest Comitè de Seguiment Operatiu:

- Reunió d'Inici de projecte (Kickoff);
- Reunions de seguiment de desenvolupament (periodicitat setmanal);
- Tractament dels Informes de Seguiment;
- Aprovació de la Planificació del projecte;
- Aprovació del Pla de Proves i del Pla d'Implantació;
- Aprovació tancament de projecte;
- Coordinació amb altres projectes relacionats en curs d'AB;
- Elevar al Comitè de Seguiment del Contracte possibles riscos o canvis significatius que impactin en l'abast del projecte.

En qualsevol cas, s'organitzaran tantes sessions de treball, o les reunions que siguin necessàries per assegurar la correcta coordinació i correcta consecució dels objectius del projecte a desenvolupar i implantar.

Es sol·licita als licitadors que detallen en la seva proposta la metodologia concreta que proposen utilitzar en la gestió del projecte, incloent l'especificació de procediments, reunions, periodicitats, mecanismes de control i seguiment, etc.

4.7 Recursos Materials requerits

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

No obstant l'anterior, Aigües de Barcelona proporcionarà als Prestadors dels Serveis les següents eines:

- Software a instal·lar amb els seus codis de llicència
- Maquinari per les renovacions i actualitzacions
- Usuaris locals o de domini amb els permisos necessaris
- Eines de reporting i seguiment de les incidències detectades: en l'actualitat el JIRA o el BMC Remedy.

5. Annex 1- Normes de seguretat IT d'Aigües de Barcelona.

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

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

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

5.1 Intercanvi d'informació i software SI-N-07-02/01

L'intercanvi d'informació o software qualificats com d'ús intern, restringit o confidencial que realitzi AB amb altres organitzacions, ha d'estar formalitzat en acords, validats per la Direcció Jurídica, que han d'establir les condicions en les que es realitzaran aquests intercanvis.

Quan, per raons d'urgència i eficiència del servei, sigui impossible la formalització prèvia de dit 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'etiquetat de la informació que es faci durant dit 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 xifrat que impedeixin la divulgació no autoritzada.

En els acords s'han d'establir els mecanismes oportuns per facilitar la gestió d'aquests intercanvis i plasmar les responsabilitats i obligacions legals quan es portin a terme, especialment les relaciones 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 les responsabilitats i obligacions legals relatives al intercanvi, especialment aquelles derivades de l'intercanvi de dades de caràcter personal amb altres entitats, cessionàries 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 TI identificar els mecanismes especials requerits per protegir actius crítics, amb les de xifrat indicats anteriorment o l'ús de solucions de no-repudi, amb la finalitat d'assegurar la recepció de la informació per part del destinatari.

5.2 Configuració i administració segura

5.2.1. 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 les credencials d'autentificació 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 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 a les utilitats de gestió i administració del sistema que requereixin 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: "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'activen per defecte durant la instal·lació i en que 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 inactives.
- 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'AB o que utilitzin algoritmes d'encaminament dinàmics, hauran d'usar-se mecanismes d'autentificació 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 LOPD.

5.2.2. 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 a que les credencials d'aquest usuari administrador viatgin 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, 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'AB, que corregeix 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 les normatives legals vigents en matèria de protecció de dades de caràcter personal (LOPD).

5.2.3. Identificació i autentificació d'usuaris

Tots els sistemes d'informació no públics de les unitats i societats operatives d'AB hauran de disposar de mecanismes que verifiquen la identitat dels usuaris que els utilitzen, de tal manera que es restringeixen els recursos als que deuen accedir cada usuari.

Els usuaris disposaran d'un únic identificador 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 de l'apartat "Identificació d'usuari".

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

- Software de control d'accés inherent al propi sistema.
- Eina de software de control d'accés agregat al sistema.

L'autentificació, 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'autentificació hauran de ser supervisats per la Direcció de Seguretat TI, que verificarà la correcta parametrització de la normativa de seguretat relativa a l'autentificació d'usuaris.

L'autentificació en el sistema haurà de garantir que l'usuari solament tingui accés als recursos que necessiti per al acompliment de les seves funcions, no disposant de permisos d'accés a les eines pròpies del sistema, excepte 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 modo 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 Cap de Seguretat de la Informació de la entitat a la que pertanyi.

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

Amb la finalitat d'evitar l'accés no autoritzat, el procés d'identificació i autentificació 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 altre originada per el 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 de que l'identificador d'usuari bloquejat sigui el de correu electrònic, el superior jeràrquic de l'usuari implicat haurà de sol·licitar, per els 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.

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

5.2.4. Identificació d'usuari

L'accés a qualsevol dels sistemes d'informació d'AB 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 com la persona física.

L'accés a qualsevol dels sistemes d'informació d'AB es realitzarà utilitzant un identificador d' usuari convenientment autoritzat ([UserID]). L'identificador d'usuari haurà d'estar assignat a una persona física y 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 al que pertany i del sistema al que es connecta. L'identificador d'usuari romandrà associat al seu propietari d'AB amb independència dels canvis de destí o de categoria que pugues 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'AB han de rebre identificadors que segueixin els mateixos processos d'aprovació que per els nous empleats. Els drets d'accés dels usuaris que no pertanyen a AB deuen d'atorgar-se solament per el període de temps estrictament necessari i hauran de ser revaluats periòdicament.

No estarà permesa la creació o utilització d'usuaris genèrics excepte en aquells casos en els que sigui estrictament necessari per raons operatives, funcionals, etc., que, per la seva naturalesa, aconsellen o obliguen a 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 coneixen, en tot moment, el grup d' usuari que l'utilitzen. Quan la necessitat d'usar l'usuari genèric per un usuari del grup finalitzi, s'haurà de modificar la contrasenya d'accés compartida per fer efectiva la sortida de dit 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 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.

5.3 Gestió de contrasenyes i credencials de clients

Per evitar la possible esbrinament de les 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 d'usuaris no hauran de tenir una longitud inferior a 6 (sis) caràcters alfanumèrics, incloent almenys dos caràcters numèrics i dos 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 sintaxis que

impediran, per exemple, que la contrasenya coincideix amb l'identificador d'usuari, o correspongui a una seqüencia 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 les que s'utilitzi.

Els sistemes han de permetre a l'usuari el canvi de la seva contrasenya de forma autònoma quan aquest ho estimi oportú. Així mateix, quan s'accedeixi per primer cop 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 a 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 de que ha perdut el caràcter de secreta i no disposi de l'opció per canviar-la o desconeguin 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 de inhabilitar l'identificador associat fins la seva inicialització o desbloqueig.

Els sistemes d'informació d'AB 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 las aplicacions.
- Protegir la informació i les aplicacions d'accessos realitzats per personal no autoritzat.
- Autentificar a tots els usuaris abans de 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 referencia, 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. Exceptuant excepcions prèviament autoritzades per la Direcció de Seguretat TI. La Direcció de Seguretat TI haurà de definir mecanismes de control d'accés alternatius que efectuïn controls no coberts per els sistemes de control d'accés instal·lats en els entorns, així com avaluar els avantatges i debilitats de les noves versions i/o productes alternatius o complementaris.

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

5.4 Comunicació dels incidents de seguretat

En el cas de detecció d'un incident greu de seguretat (mitjançant sistemes de detecció d'intrusions, anàlisis de logs, comunicació d'un tercer, alarmes de seguretat, etc.), la Direcció de Seguretat AB haurà de ser informada amb la major brevetat 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 sigut identificades, la qual la seva participació sigui necessària en la resolució de l'incident. Aquesta elecció es farà en funció de la criticitat de l'incident, el grau de coneixement necessari o els sistemes als que afecti.

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

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'AB en front d'incidents de seguretat.

El reporting d'informació sobre incidents de seguretat quedarà restringit únicament a aquelles persones absolutament necessàries. Qualsevol divulgació d'aqueta 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 sigut informades de cada incident amb la finalitat de detectar una possible divulgació no autoritzada.

Tant els empleats de las entitats d'AB 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-ho igualment.

6. Annex 2 – Mesures de seguretat a complir durant l'execució del contracte

L'adjudicatari del present Contracte, donat que ostentarà la condició d'encarregat de tractament de dades per compte d'AB, haurà de complir, durant l'execució del Contracte, les següents mesures de seguretat:

6.1 Mesures de seguretat mínimes aplicables a tractament en paper.

6.1.1. Criteris d'arxiu.

L'arxiu dels suports o documents es realitzarà d'acord amb els criteris previstos en la seva respectiva legislació. Aquests criteris hauran de garantir la correcta conservació dels documents, la localització i consulta de la informació i possibilitar l'exercici dels drets dels interessats.

En aquells casos en els que existeixi norma aplicable, el responsable del tractament haurà d'establir els criteris i procediments d'actuació que hagin de seguir-se per l'arxiu.

6.1.2. Dispositius d'emmagatzematge.

Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin la seva apertura (per exemple, calaixos amb clau). Quan les característiques físiques d'aquells no permetin adoptar aquesta mesura, el responsable del tractament adoptarà mesures que impedeixin l'accés de persones no autoritzades.

6.1.3. Emmagatzematge de la informació.

1. Els armaris, arxivadors o altres elements en els que s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal hauran de trobar-se en àrees en les que l'accés estigui protegit amb portes d'accés dotades de sistemes d'apertura mitjançant clau o altre dispositiu equivalent. Aquestes àrees hauran de romandre tancades quan no sigui precís l'accés als documents inclosos en el fitxer.

2. Si, ateses les característiques dels locals de que disposés el responsable del tractament, no fos possible complir lo establert en l'apartat anterior, el responsable adoptarà mesures alternatives que, degudament motivades, es documentaran.

6.1.4. Còpia o reproducció.

1. Els armaris, arxivadors o altres elements en els que s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal hauran de tronar-se en àrees en les que l'accés estigui protegit amb portes d'accés dotades de sistemes d'apertura mitjançant clau o altre dispositiu equivalent. Aquestes àrees hauran d'estar tancades quan no sigui precís l'accés als documents inclosos en el fitxer.

2. Si, ateses les característiques dels locals de que disposés el responsable del tractament, no fos possible complir lo establert en l'apartat anterior, el responsable adoptarà mesures alternatives que, degudament motivades, es documentaran.

6.1.5. Accés a la documentació.

1. L'accés a la documentació es limitarà exclusivament al personal autoritzat.

2. S'estableixen mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris.

3. L'accés de persones no incloses en el paràgraf anterior haurà de quedar adequadament registrat d'acord amb el procediment establert a l'efecte per escrit.

6.1.6. Trasllat de documentació.

Sempre que es procedeixi al trasllat físic de la documentació continguda en un fitxer, hauran d'adoptar-se mesures dirigides a impedir l'accés o manipulació de la informació objecte de trasllat.

6.2 Mesures de seguretat mínimes aplicables a tractament automatitzats.

6.3.1. Funcions i obligacions del personal.

1. Les funcions i obligacions de cadascun dels usuaris o perfils d'usuaris amb accés a les dades de caràcter personal i als sistemes d'informació estaran clarament definides i documentades.

També es definiran les funcions de control o autoritzacions delegades pel responsable del tractament.

2. S'adoptaran mesures necessàries perquè el personal conegui d'una forma comprensible les normes de seguretat que afectin el desenvolupament de les seves funcions així com les conseqüències en que pogués incórrer en cas d'incompliment.

6.3.2. Registre d'incidències.

1. Haurà de fer-se constar, si succeeix una incidència, el tipus d'incidència, el moment en que s'ha produït, o en el seu cas, detectat, la persona que realitza la notificació, a qui se li comunica, els efectes que s'haguessin derivat de la mateixa i les mesures correctores aplicades.

2. En el registre hauran de consignar-se, a més, els procediments realitzats de recuperació de les dades, indicant la persona que va executar el procés, les dades restaurades i, en el seu cas, quines dades han estat necessàries gravar manualment en el procés de recuperació.

3. Serà necessària l'autorització del responsable del tractament per l'execució dels procediments de recuperació de les dades.

6.3.3. Control d'accés.

1. Els usuaris tindran accés únicament a aquells recursos que precisin per al desenvolupament de les seves funcions.

2. Haurà d'existir una relació autoritzada d'usuaris i perfils d'usuaris, i els accessos autoritzats per a cadascun d'ells.

3. S'establiran mecanismes per evitar que un usuari pugui accedir a recursos amb drets diferents dels autoritzats.

4. Exclusivament el personal autoritzat per allò podrà concedir, alterar, anular l'accés autoritzat sobre els recursos, conforme als criteris establerts pel responsable del tractament.

5. En cas de que existeixi personal aliè al responsable del tractament que tingui accés als recursos haurà d'estar sotmès a les mateixes condicions i obligacions de seguretat que el personal propi.

6. Exclusivament el personal autoritzat podrà tenir accés a llocs on es trobin instal·lats els equips físics que donin suport als sistemes d'informació.

6.3.4. Registre d'accessos.

1. De cada intent d'accés es guardaran, com a mínim, la identificació de l'usuari, la data i l'hora en el que es va realitzar, el fitxer accedit, el tipus d'accés i si ha estat autoritzat o denegat.

2. En el cas de que l'accés hagi estat autoritzat, serà precís guardar la informació que permeti identificar el registre accedit.

3. Els mecanismes que permetin el registre d'accessos estarà sota el control directe del responsable de seguretat competent sense que hagin de permetre la desactivació ni la manipulació dels mateixos.

4. El període mínim de conservació de les dades registrades serà de dos anys.

5. El responsable de seguretat s'encarregarà de revisar al menys un cop al mes la informació de control registrada i elaborarà un informe de les previsions realitzades i els problemes detectats.

6.3.5. Gestió de suports i documents.

1. Els suports i documents que continguin dades de caràcter personal hauran de permetre identificar el tipus d'informació que continguin, ser inventariats i només hauran de ser accessibles pel personal autoritzat per allò. S'exceptuen aquestes obligacions quan les característiques físiques del suport impossibilitin el seu compliment, quedant constància motivada d'allò per escrit.

2. La sortida de suports i documents que continguin dades de caràcter personal, inclosos els compresos i/o annexos a un correu electrònic, fora dels locals sota el control del responsable del tractament haurà de ser autoritzada pel responsable o trobar-se degudament autoritzada per escrit.

3. En el trasllat de la documentació s'adoptaran les mesures dirigides a evitar la substracció, pèrdua o accés indegut a la informació durant el seu transport.

4. Sempre que s'hagi de rebutjar qualsevol document o suport que contingui dades de

caràcter personal haurà de procedir-se a la seva destrucció o esborrat, mitjançant l'adopció de mesures dirigides a evitar l'accés a la informació continguda en el mateix o la seva recuperació posterior.

5. La identificació dels suports que continguin dades de caràcter personal que la organització considerés especialment sensibles es podrà realitzar utilitzant sistemes d'etiquetat comprensibles i amb significat que permetin als usuaris amb accés autoritzat als citats suports i documents identificar el seu contingut, i que dificultin la identificació per la resta de persones.

6. Haurà d'establir-se un sistema de registre d'entrada de suports que permeti, directa o indirectament, conèixer el tipus de document o suport, la data i hora, l'emissor, el número de documents o suports inclosos en l'enviament, el tipus d'informació que continguin, la forma d'enviament i la persona responsable de la recepció que haurà d'estar degudament autoritzada.

7. Igualment, es disposarà d'un sistema de registre de sortida de suports que permeti, directa o indirectament, conèixer el tipus de document o suport, la data i hora, el destinatari, el número de documents o suports inclosos en l'enviament, el tipus d'informació que continguin, la forma d'enviament i la persona responsable del lliurament que haurà d'estar degudament autoritzada.

8. La identificació dels suports s'haurà de realitzar utilitzant sistemes d'etiquetat comprensibles i amb significat que permetin als usuaris amb accés autoritzat als citats suports i documents identificar el seu contingut, i que dificultin la identificació per la resta de persones.

9. La distribució dels suports que continguin dades de caràcter personal es realitzarà xifrant aquestes dades o bé utilitzant un altre mecanisme que garanteixi que aquesta informació no sigui accessible o manipulada durant el seu transport.

Així mateix, es xifraran les dades que continguin els dispositius portàtils quan aquests es trobin fora de les instal·lacions que estan sota el control del responsable del fitxer.

10. Haurà d'evitar-se el tractament de dades de caràcter personal en dispositius portàtils que no permetin el seu xifrat. En cas de que sigui estrictament necessari es farà constar motivadament en el document de seguretat i s'adoptaran mesures que tinguin en compte els riscos de realitzar tractaments i entorns desprotegits.

6.3.6. Identificació i autenticació.

1. El responsable del tractament haurà d'adoptar les mesures que garanteixen la correcta identificació i autenticació dels usuaris.

2. El responsable del tractament establirà un mecanisme que permetrà la identificació de forma inequívoca i personalitzada de tot aquell usuari que intenti accedir al sistema d'informació i la verificació de que està autoritzat.

3. Quan el mecanisme d'autenticació es basi en l'existència de contrasenyes existirà un procediment d'assignació, distribució i emmagatzematge que garanteixi la seva confidencialitat i integritat.

4. Per escrit s'establirà la periodicitat, que en cap cas serà superior a un any, amb la que han

de ser canviades les contrasenyes que, mentre siguin vigents, s'emmagatzemaran de forma inintel·ligible.

5. El responsable del fitxer o tractament establirà un mecanisme que limiti la possibilitat d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

6.3.7. Copies de suport i recuperació.

1. Hauran d'establir-se procediments d'actuació per a la realització com a mínim setmanal de còpies de suport, excepte que en aquest període no s'hagués produït cap actualització de dades.

2. Així mateix, s'establiran procediments per a la recuperació de les dades que garanteixin en tot moment la seva reconstrucció en l'estat de que la pèrdua o destrucció afectés a fitxers o tractaments parcialment automatitzats, i sempre que l'existència de documentació permeti arribar a l'objectiu al que es refereix el paràgraf anterior, s'haurà de procedir a gravar manualment les dades quedant constància motivada d'aquest fet per escrit.

3. El responsable del fitxer s'encarregarà de verificar cada sis mesos la correcta definició, funcionament i aplicació dels procediments de realització de còpies de suport i de recuperació de dades.

4. Les proves anteriors a la implantació o modificació dels sistemes d'informació que tractin fitxers amb dades de caràcter personal no es realitzaran amb dades reals, excepte que s'asseguri el nivell de seguretat corresponent al tractament realitzat i es documenti la seva realització.

Si està previst realitzar proves amb dades reals, prèviament haurà d'haver-ser realitzat una còpia de seguretat.

5. Haurà de conservar-se una còpia de suport de les dades i dels procediments de recuperació dels mateixos en un lloc diferent d'aquell en el que estiguin els equips informàtics que els tracten, que hauran de complir en tot cas les mesures de seguretat exigides en aquest títol, o utilitzant elements que garanteixin la integritat i recuperació de la informació, de forma que sigui possible la seva recuperació.

6.3.8. Responsable de seguretat.

Hauran d'assignar-se per escrit un o varis responsables de seguretat encarregats de coordinar i controlar les mesures definides en el mateix. Aquesta designació pot ser única per tots els fitxers o tractaments de dades de caràcter personal o diferenciada segons els sistemes de tractament utilitzats, circumstància que haurà de constar clarament per escrit.

6.3.9. Auditoria.

1. A partir del nivell mig, els sistemes d'informació i instal·lacions de tractament i emmagatzematge de dades es sotmetran, al menys cada dos anys, a una auditoria interna o externa que verifiqui el compliment del present títol.

Amb caràcter extraordinari haurà de realitzar-se aquesta auditoria sempre que es realitzin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment

de les mesures de seguretat implantades amb l'objectiu de verificar l'adaptació, adequació i eficàcia de les mateixes. Aquesta auditoria inicia el còmput de dos anys assenyalat en el paràgraf anterior.

2. L'informe d'auditoria haurà de dictaminar sobre l'adequació de les mesures i controls a la legislació aplicable, identificar les seves deficiències i proposar les mesures correctores o complementàries necessàries. Haurà, igualment, d'incloure les dades, fets i observacions en que es basin els dictàmens assolits i les recomanacions proposades.

3. Els informes d'auditoria seran analitzats pel responsable de seguretat competent, que elevarà les conclusions al responsable del tractament perquè adopti les mesures correctores adequades.

6.3.10. Telecomunicacions.

La transmissió de dades de caràcter personal a través de xarxes públiques o xarxes sense fils de comunicacions electròniques es realitzarà xifrant aquestes dades o bé utilitat qualsevol mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers.

Tenint en compte l'estat de la tècnica, els costos d'aplicació, i la naturalesa, l'abast, el context i les finalitats del tractament, així com els riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, s'aplicaran mesures tècniques i organitzatives apropiades addicionals a les anteriorment exposades per garantir un nivell de seguretat adequat al risc, que en el seu cas inclogui, entre altres:

a) la pseudonimització i el xifrat de dades personals;

b) la capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament;

c) la capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en cas d'incident físic o tècnic;

d) un procés de verificació, avaluació i valoració regulars de la eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

Al avaluar l'adequació del nivell de seguretat es tindran particularment en compte els riscos que presenti el tractament de dades, en particular com a conseqüència de la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o accés no autoritzats a aquests fitxers.

S'hauran d'aplicar també les polítiques de protecció de dades personals de la companyia.