PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SERVEI D'IDENTITATS I ACCESSOS (CAAA), AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE.

ÍNDEX

1. INTRODUCCIÓ

L'Ajuntament de Barcelona gestiona una ciutat d'1,6 milions de ciutadans, unes 200.000 empreses i un teixit associatiu format per més de 10.000 entitats.

Disposa d'una oferta de serveis molt amplia, emmarcada en diferents àmbits: serveis socials, mobilitat, educació, salut, cultura i oci, promoció econòmica, etc. sempre amb la vocació de servir a la ciutadania i a realitzar la gestió de la ciutat que te encomanada de forma òptima, àgil i eficient.

Aquests serveis, s'han d'oferir amb garanties i seguretat TIC pel ciutadà i per la pròpia ciutat, i això suposa, des de protegir la informació personal del ciutadà, garantir els serveis i protegir la pròpia gestió de la ciutat i de l'Administració Municipal.

La informació relativa a aquests serveis, es troba disgregada en un gran nombre de sistemes d'informació i fitxers legals diferents la qual cosa porta a la necessitat de disposar de serveis d'identificació, protecció, prevenció i reacció davant amenaces a què es troben exposades els sistemes d'informació i les infraestructures TIC i així reduir i minimitzar els riscos d'incidents de seguretat i ciberatacs.

A més, en un escenari en què el concepte i continguts de seguretat lògica o ciberseguretat avança i es troba en contínua i ràpida evolució, els serveis de ciberseguretat que requereix l'Ajuntament han de ser confiables i àgils, així com configurats amb la flexibilitat suficient per poder estar fent front als riscos que es presenten, sovint impredictibles.

L'Institut Municipal d'Informàtica (en endavant, IMI) té delegades les funcions de Seguretat en les Tecnologies de la Informació i Comunicació de l'Ajuntament de Barcelona, i exerceix de Responsable de Seguretat TIC, en funció de la seva organització interna, d'acord amb els preceptes, estàndards internacionals en matèria de seguretat TIC i en especial, amb els requeriments que l'Esquema Nacional de Seguretat (ENS) i la normativa de Protecció de Dades Personals estableix en els entorns automatitzats.

Dins d'aquest escenari, l'IMI ha definit **un Model de Gestió de la Seguretat** on s'hi desenvolupen els programes de Seguretat Corporatius del mandat. El marc hi encabeix el model de seguretat del NIST *framework* de Ciberseguretat (Identificar, Protegir, Detectar, Respondre i Recuperar) així com el de l'SGSI ISO 27001 i la seva interpretació en l'administració espanyola amb l'Esquema Nacional de Seguretat.

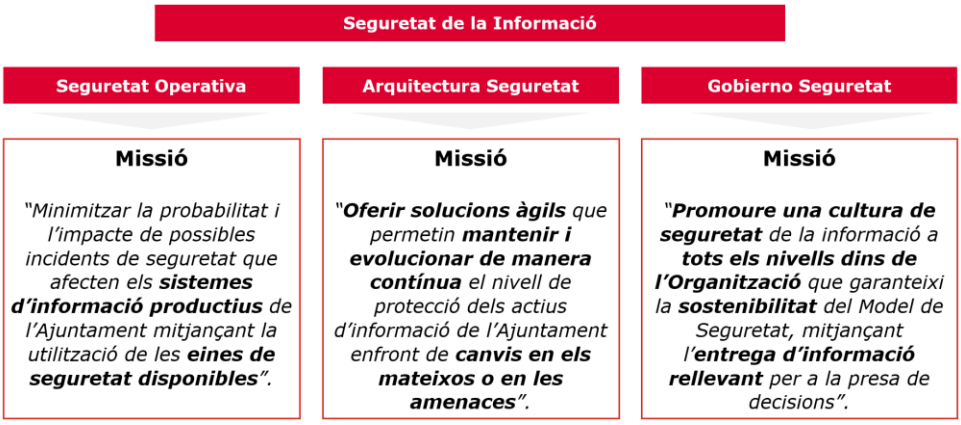
Aquest Marc de Seguretat estableix la base per definir el pla de seguretat que ha de desenvolupar el mandat, és a dir, les línies d'actuació, projectes i serveis a executar per donar resposta i sortida, en l'àmbit de protecció i seguretat, a les estratègies i plans d'actuació de l'Ajuntament, amb l'objectiu de:

- Incrementar els Serveis de seguretat TIC
- Dotar a l'Ajuntament d'una estructura que asseguri el compliment de la seguretat i la minimització dels riscos de Seguretat TIC corporatius.

- Assegurar un Marc Normatiu de referència per l'Ajuntament
- Garantir el compliment de la legalitat (ENS, RGPD, eIDAS, LPACAP...)
- Implantar Projectes de Seguretat per donar resposta a les necessitats TIC en matèria de seguretat i protecció
- Protegir els projectes del pla de digitalització: Establir a partir dels riscos els requeriments de seguretat dels projectes del Pla de transformació digital. Establir, implementar i governar el model i les condicions de seguretat per a tots projectes i iniciatives que se'n deriven del Pla de transformació Digital de l'Ajuntament de Barcelona.
- Tenir Govern dels accessos TIC a partir dels principis de mínim privilegi i necessitat de saber per tal de poder conèixer qui fa què i quan dins dels sistemes d'informació i infraestructures TIC de l'Ajuntament.
- Disposar de vigilància activa, reactiva i preventiva de la seguretat

Així doncs, l'IMI desenvolupa la funció de la seguretat dins d'un model de Gestió de la Seguretat a tres nivells o línies de defensa: Estratègic, Tàctic i Operatiu, i estableix 5 línies d'actuació sobre les que es desenvolupen els programes de seguretat del mandat.

Funció Seguretat Informació en tres línies de defensa



Marc de Seguretat : línies d'actuació

- **Govern de la seguretat de la informació:** Establiment d'una estructura i un model organitzatiu sòlid en l'àmbit de la seguretat, amb capacitat per a controlar i prendre decisions en totes aquelles accions que així ho requereixin
- **Control i divulgació de la normativa:** Disposar d'un marc normatiu actualitzat i alineat a l'estratègia de seguretat i exercir un control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat
- **Protecció dels sistemes d'informació**: Aplicació de mesures de seguretat per tal de mitigar els riscos que se'n puguin derivar com possibles fallides o atacs intencionats així com gestionar de manera ràpida i efectiva tots aquells incidents que es produeixin
- **Seguiment de la identitat digital:** Gestió de les seves credencials i control de la manera de compartir i accedir a la informació, tant a l'organització com al propi usuari i del ciutadà per tal de garantir la confidencialitat, l'autenticitat, l'autenticació, la integritat i el no repudi de la informació i les accions que realitzi.
- **Detecció, reacció i reducció d'amenaces:** Identificar les amenaces més rellevants per als sistemes d'informació de l'organització, sigui pel seu número o per l'impacte que puguin produir.
- **Millora de la resiliència de l'activitat:** Cal valorar el nivell de resistència dels sistemes d'informació en situacions adverses i detectar millores i mesures per augmentar o assegurar la capacitat per mantenir els sistemes en funcionament.

Les línies d'actuació donen cobertura a 4 de les 5 funcions del *framework* del NIST de Ciberseguretat: Identificar (Govern), Protegir (Arquitectura de Seguretat), Detectar i Respondre (operació de la seguretat). Deixant la funció de "Recuperar" en un marc d'actuació global més gran de l'organització fora de la seguretat.

Així doncs, l'IMI, per exercir aquesta funció delegada de la Seguretat Corporativa TIC i en la seva vocació d'oferir els millors serveis TIC a l'Ajuntament de Barcelona i al ciutadà, ha establert conjunt de serveis de seguretat TIC per cobrir els requeriments identificats i de futur en aquesta matèria:

En l'àmbit del **Govern de la Seguretat**:

- **Govern de la seguretat de la informació:** Establiment d'una estructura i un model organitzatiu sòlid en l'àmbit de la seguretat, amb capacitat per a controlar i prendre decisions en totes aquelles accions que així ho requereixin
- **Control i divulgació de la normativa:** Disposar d'un marc normatiu actualitzat i alineat a l'estratègia de seguretat i exercir un control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat

Estableix els serveis següents:

- **<u>Serveis de GRC</u>** (Govern Risc i Compliment). El servei engloba tota la Gestió i iniciatives de l'SGSI de Seguretat per garantir el tractament dels Riscos de seguretat

identificats amb l'objectiu de donar cobertura a la missió estratègica del govern de la seguretat.

En l'àmbit **d'Arquitectura de Seguretat** s'estableixen els següents serveis:

- **Protecció dels sistemes d'informació**: Aplicació de mesures de seguretat per tal de mitigar els riscos que se'n puguin derivar com possibles fallides o atacs intencionats així com gestionar de manera ràpida i efectiva tots aquells incidents que es produeixin

- **<u>Serveis d'Arquitectura i Projectes:</u>** Servei que ofereix solucions àgils i arquitectures enfront de noves tecnologies i reptes i que permetin mantenir i evolucionar de manera contínua el nivell de protecció dels actius d'informació de l'Ajuntament enfront de canvis en els mateixos o en les amenaces. Aquest Servei serà l'únic punt d'entrada de la resta d'equips de Projectes de l'IMI i de l'Ajuntament, i gestionarà la cartera de participació de seguretat en els projectes i coordinarà la participació dels altres equips de Seguretat.

- **Seguiment de la identitat digital:** Gestió de les seves credencials i control de la manera de compartir i accedir a la informació, tant a l'organització com al propi usuari i del ciutadà per tal de garantir la confidencialitat, l'autenticitat, l'autenticació, la integritat i el no repudi de la informació i les accions que realitzi.

- **<u>Serveis d'Identitats i Accessos</u>**: Control Autenticació, autoritzacions i Control d'Accés (CAAA). Aquest servei ha d'operar els processos d'identitats, credencials, autoritzacions i accessos de tot l'Ajuntament, amb l'objectiu de garantir la protecció requerida i proporcional de la informació i serveis TIC corporatius. Aquest és el servei objecte de licitació d'aquest plec.

En l'àmbit de **Seguretat Operativa** amb relació a la ciberseguretat:

- **Detecció, reacció i reducció d'amenaces:** Identificar les amenaces més rellevants per als sistemes d'informació de l'organització, sigui pel seu número o per l'impacte que puguin produir.

Estableix els serveis següents:

- **<u>Serveis de Preventiu.</u>** El servei de seguretat preventiva ha de disposar i ingerir múltiples fonts de ciberintel·ligència i realitzar proves d'intrusió d'infraestructures i

serveis amb la finalitat de garantir que les infraestructures o serveis siguin segurs i de realitzar la gestió completa del cicle de vida de les vulnerabilitats i posterior revisió. També ha d'assessorar en la definició de les arquitectures dels sistemes i tecnologies que té actualment l'IMI, que dintre de la seva funció de donar servei informàtic a l'Ajuntament de Barcelona, necessita per donar el correcte i segur servei, analitzant les millores que es poden implantar relacionat amb les novetats tecnològiques del mercat i els nous paradigmes d'atacs informàtics que es poden patir.

- **Serveis de Vigilància, detecció i Reactiu (SOC i Resposta a incidents).** Aquest servei inclou El Centre d'Operacions de Seguretat, per la vigilància i monitoratge dels esdeveniments de la seguretat, i el CSIRT, Centre de Seguretat de Resposta d'incidents, per al ràpid anàlisi i gestió de l'incident per tal de reduir o minimitzar l'impacte que pugui produir i establir les mesures preses per tal que no es torni a produir, es coordinarà amb el servei de preventiu per millorar, si fos el cas, la infraestructura de seguretat fent les propostes pertinents.

I per tal de fer un pas endavant, s'estableix en aquest contracte la licitació dels **"Serveis d'Identitats i Accessos"** dins del marc de governança i d'arquitectura d'identitats per a mitigar el risc d'accés indegut a la informació corporativa això com de manca de disponibilitat dels serveis corporatius.

Amb els riscos de ciberseguretat actuals, la creixent necessitat de teletreball, dispositius IOT i serveis al *cloud*, etc. està fent que les identitats i arquitectures d'accés passin a ser una de les eines principals per a protegir les organitzacions. Tot això implica adquirir dosis grans **d'agilitat al canvi** i a la implementació de noves formes d'accés i protecció. Aquests riscos porten a les organitzacions a necessitats de canviar tan operatives d'accés com a redefinir la seguretat d'accés en el disseny. Les tendències actuals plantegen una seguretat "**identitat cèntric**" on la identitat és el nou perímetre, plantegen també models d'accés segur en el núvol així com mecanismes de **seguretat adaptativa** segons escenari d'accés i models basats en accessos remots que ens van portant a seguretat **d'accés a la xarxa amb confiança zero** deixant d'alguna manera tothom fora de la xarxa corporativa.

Aquests serveis de governança i serveis d'arquitectes d'identitats i accessos han passat a ser una necessitat prioritària, per tal de dirigir com una orquestra totes les tecnologies i mecanismes d'accés perquè funcionin ordenadament en l'Ajuntament, de forma previsible, assegurin a l'Ajuntament la protecció adequada en relació amb els riscos assumibles i amb traces d'*accountability*.

L'IMI ha implantat un model de gestió dels accessos per **tal de que l'Ajuntament de Barcelona disposi d'una solució centralitzada i de futur en el control dels accessos** i autoritzacions que integra les identitats i recursos atorgats amb les capacitats d'accés ajustada a les múltiples formes de treball, ubiqüitat o mobilitat.

Aquest model contempla les solucions centralitzades i altres de particulars , els accessos interns i remots als diferents sistemes d'accés a serveis i informació de l'ajuntament així com diferents mecanismes de credencials per l'autenticació i autorització als recursos corporatius.

Aquest model de gestió d'accessos té els següents objectius:

Bon govern, transparència i relació amb ciutadans

- Protecció de la informació del ciutadà.
- Millorar el servei i la resposta al ciutadà.

Desenvolupament de negoci

- Garantir el bon funcionament de la gestió dels accessos i autoritzacions dels sistemes d'informació dels sectors, districtes i Instituts Municipals .
- Gestionar l'Ajuntament de forma eficaç i eficient.
- Simplificar els processos, reduir la burocràcia. Millorar l'eficiència i l'eficàcia dels serveis que reben actualment els departaments i els organismes de l'Ajuntament.
- Ajudar a l'assignació de tasques TIC en el desenvolupament laboral del personal corporatiu i de l'extern (contractes).
- Garantir el compliment de la normativa relacionada amb la LOPD, per la protecció i confidencialitat de la informació del ciutadà així com altres reglaments com són eIDAS, LPACAP, Llei ciber, etc.

Seguretat

- Preservar la confidencialitat, integritat, fiabilitat, autenticitat dels accessos als serveis TIC i a la informació corporativa.
- Garantir la seguretat i traçabilitat de les accions.

Estalvi econòmic i excel·lència TIC

- Plataforma única de gestió.
- Generar sinèrgies amb altres línies estratègiques.
- Integració amb la gestió d'identitats que proveeix l'IMI a l'Ajuntament de Barcelona.

La correcta gestió de les identitats i el control dels accessos permet assegurar i ajudar a governar els accessos TIC de l'Ajuntament de manera més eficient i amb la qualitat i seguretat esperada. Aquest fet redunda en la millora de la qualitat i seguretat de la prestació dels serveis oferts per l'Ajuntament a la ciutadania, entre els quals es troben entre d'altres, els d'Acció Social, Hisenda, Padró o el correu corporatiu.

1.1. SITUACIÓ ACTUAL

Actualment, en el marc del domini de de la ISO 27002 (CAAA - Control d'accés, autenticació i Autorització) **es disposa de**:

a) Una **gestió dels accessos i autoritzacions** que el doten d'un control d'accés de forma segura i centralitzada a les aplicacions i serveis TIC, permetent d'aquesta manera la transformació de l'organització, mitjançant la incorporació de les tecnologies mòbils i xarxes socials, el desplegament d'aplicacions en el núvol i la gestió d'accessos híbrids entre aplicacions residents a les nostres instal·lacions i altres residents en el núvol, preservant al mateix temps una experiència d'usuari sense fissures, administració centralitzada i amb el màxim rendiment i escalabilitat.

   Tot plegat s'ha realitzat amb una visió totalment integrada amb la Gestió d'identitats corporativa amb la finalitat de poder establir en el futur automatismes en els fluxos i tasques referents a la gestió dels permisos i amb funcionalitats d'autenticació adaptativa (adaptar els requeriments d'accés condicionat a l'origen i amb quines condicions d'entorn s'estableix), *Single Sign-on* federat i control afinat als clients de mòbil i als serveis en el núvol.

   El nucli d'aquesta solució corporativa són un conjunt d'eines que anomenem GIA i que es componen de:

   - GID, una solució de Gestió d'identitats que abasta la gestió del cicle de vida de la identitat (producte i estàndards de mercat : OIM ORACLE).
   - Pel que fa al Control d'accés es disposa d'una eina de control d'accés unificat (Producte i estàndards de mercat: OAM Oracle). Aquest control d'accés gestiona també la implementació publicació segura de serveis API d'ús corporatiu i públic.
   - De Sistema de gestió d'autoritzacions sustentat per un repositori/serveis de directori i un aplicatiu propi que gestiona les autoritzacions. Actualment, resten pendent la migració d'alguns aplicatius des d'un sistema antic desenvolupat fa més de 10 anys (anomenat CONTROLUSER) a aquest repositori d'autoritzacions sustentat per la Gestió d'Identitats.
   - Sistema d'autenticació i punt de control d'accés únic (SSO) per les extranets exposades a internet (Producte i estàndards de mercat: ENTRUST GetAccess)
   - Mecanismes de segon factor globals de l'organització i seguretat adaptativa.

b) Productes que realitzen controls d'accés a la xarxa corporativa, com són:

   - Sistemes d'Accés remot VPN IPSEc, VSSL, Virtualització ET, ...
   - SSO estació de treball
   - Solucions de PAM exigits a proveïdors
   - Accés a directori Actiu
   - Control accés OWA

- Futura implementació de NAC
- Accés a wifis ciutadà i corporatives.
- Etc.

I requereix les següents activitats:

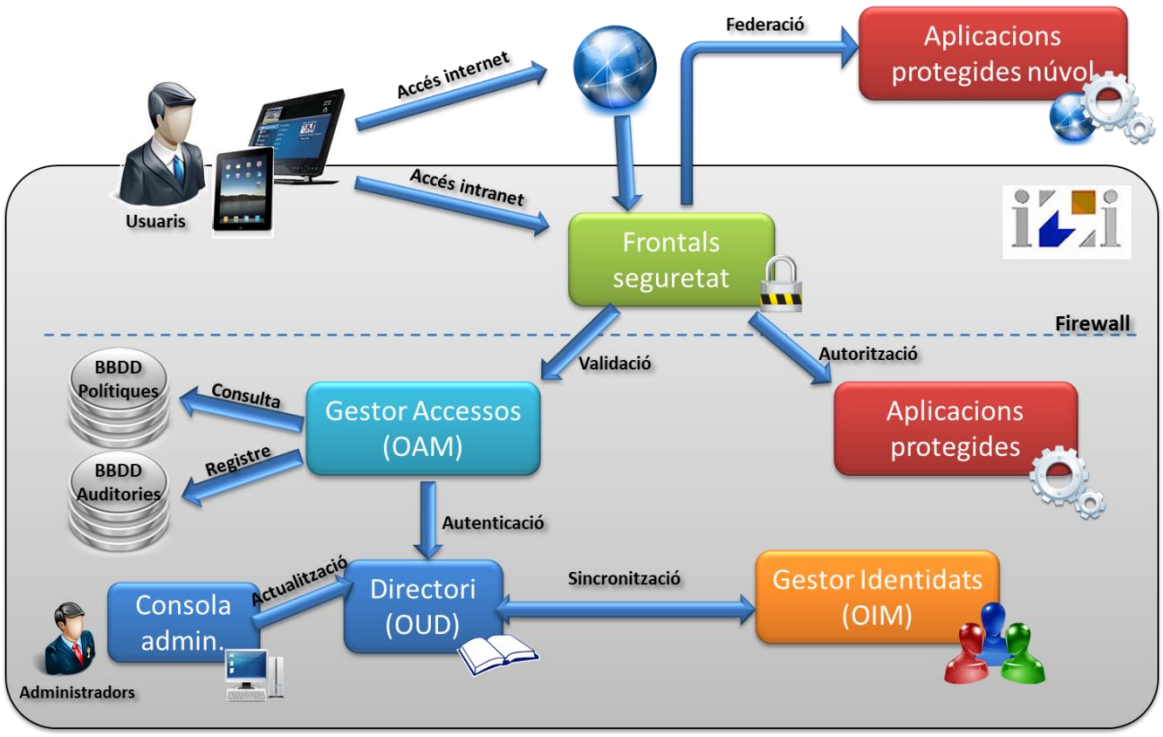
c) Control dels usuaris administradors també és una tasca principal del servei de governança i arquitectura d'identitats:
   - Administradors de Domini
   - Processos per la futura implementació d'eina de control d'usuaris administradors (PAM) per les àrees de operació, explotació i sistemes i desenvolupament.
   - Administradors en el núvol.

d) Coneixements de Tecnologies segures d'accés nativa en el núvol (SASE – Secure Access Service Edge).

e) Processos de recertificacions i de millora de la qualitat de repositoris:
   - Gestió de credencials
   - Qualitat de les autoritzacions (recertificacions)
   - Cicle de vida de les identitats
   - Canvis organitzatius
   - Canvis rellevants d'organigrama (Canvi de mandat)
   - Revisió d'accessos i monitoratge activa dels accessos
   - Informació a les gerències dels accessos dels seus sistemes d'informació
   - Etc.

1.1.1. Arquitectura nucli

La suite de productes que donen resposta central d'identitats i accessos es representa amb el següent diagrama:



En aquesta arquitectura s'identifiquen els següents components:

Directori (OUD): Repositori amb les credencials dels usuaris i els permisos.

Gestor d'identitats: S'encarrega de mantenir actualitzat els usuaris en el directori i sincronitza la seva pertinença a grups funcionals i perfils, així com la seva contrasenya.

Consola d'administració: Permet als administradors de la solució mantenir la informació continguda en el directori (aplicacions, grups funcionals, perfils, variables i la pertinença d'usuaris a aquests elements).

Gestor d'accessos: S'encarrega de donar resposta a les peticions de validació de credencials (autenticació) o de les URLs que pot visitar un usuari (autorització)

Frontals de seguretat: S'encarreguen de capturar el tràfic que va cap a les aplicacions i s'assegura que l'usuari que visita aquestes URLs està autenticat i autoritzat (consulta el ***Gestor d'accessos*** per resoldre aquestes consultes)

La suite de productes disposa de tres entorns (Desenvolupament, Preproducció i Producció).

Arquitectura redundada (Alta disponibilitat) i diversos frontals per a gestionar els accessos.

Altres productes secundaris

- Accés a extranet (GetAccess): gestor d'accessos addicional
- Solucions de segon factor d'autenticació

1.1.2. Model de protecció

El model de protecció d'OAM està basat en els següents conceptes:

- **Aplicació:** Representa l'aplicació (exemple: https://app.bcn.cat/aplicacioX), aquest concepte està representat com "unitats organitzatives" en el directori (OUD) de la solució.
- **Perfils:** Els perfils estan associats a una aplicació i poden ser assignats als usuaris, aquest concepte està representat com "grups" en el directori (OUD) de la solució.
- **Regles de protecció:** Els usuaris estan autoritzats a accedir a una aplicació en funció de si disposen algun perfil de l'aplicació. Aquest concepte està representat en la BBDD d'OAM com a polítiques d'autorització.

El manteniment d'usuaris de les estructures està organitzat de la següent forma:

- **Usuaris:** Es generen des de la Gestió d'Identitats implantada a l'IMI.
- **Associació d'usuaris a perfils:** Es realitza des de la consola d'administració que genera entrades en el directori (OUD) associat a la solució OAM. Els accessos a aquesta consola està limitat a usuaris que tenen un perfil determinat i els proporciona accés a aquesta gestió.

1.1.3. Gestió d'Identitats

El 2009 es va implantar a l'IMI l'eina de Gestió d'Identitats (en endavant GID) sobre un producte de Novell i el 2015 es va migrar a la plataforma d'Oracle IGS (Identity Governance Suite).

L'IMI disposa del producte d'Oracle EIS (Enterprise Identity Services), tot i que actualment no està totalment implementat, que suporta i dona resposta a les necessitats esmentades. Dins d'aquesta suite, l'IMI té desplegada i productiva la Gestió d'identitats (IGS) donant solució als següents processos de negoci:

- Gestió del cicle de vida de la identitat i els seus comptes associats.
- Gestió d'Accessos bàsics.
- Sincronització de contrasenyes amb els directoris i Bases de Dades corporatives on estan actualment delegades l'Autenticació i Autorització de les Aplicacions.
- Enviament d'informació a Sistemes no Integrats amb la Gestió d'Identitats.

Actualment no hi ha provisió automàtica amb fluxos d'autoritzacions pels col·lectius grans de l'Ajuntament (GUB, Atenció ciutadana, Centres de serveis socials, Uts Districtes, etc.) i manquen sincronismes bidireccionals amb sistemes que no empren el directori d'autoritzacions corporatiu.

1.1.4. GetAccess

A continuació es descriuen les principals característiques de la solució GetAccess implantada.

1.1.4.1. Components de l'arquitectura

A cada entorn (preproducció o producció) s'identifiquen els següents components que afecten directament a la protecció d'aplicacions:

- URL accés extern (noms de domini que es comuniquen als usuaris per accedir a les aplicacions)
- Runtime GetAccess: Servidor que fan les funcions de *proxy* invers per les aplicacions, comprova que l'usuari està autenticat i reenvia el tràfic al servidor corresponent, s'identifiquen 2 tipus de *runtimes* a l'entorn de l'IMI:
    - *Runtime* aplicacions WAS: Les aplicacions desplegades sobre servidors WAS tenen uns runtime dedicats implantats sobre servidors IHS.
    - *Runtime* aplicacions NO WAS: La resta d'aplicacions (.Net, Tomcat, JBoss,…) disposen de *runtimes* implantats sobre servidors Apache.
- Proxy formularis GetAccess: Per evitar que els formularis per introduir credencials siguin accessibles en clar, s'accedeixen mitjançant un servidor web que actua com *proxy* sota protocol segur HTTPS.
- *Backend* GetAccess: Consola d'administració en la qual configurar la protecció de les aplicacions.
- Repositori de polítiques: Base de dades Oracle on s'emmagatzemen els usuaris (amb la seva contrasenya) i les seves autoritzacions.

1.1.4.2. Model protecció

El model de protecció de GetAccess es basa en els següents conceptes:

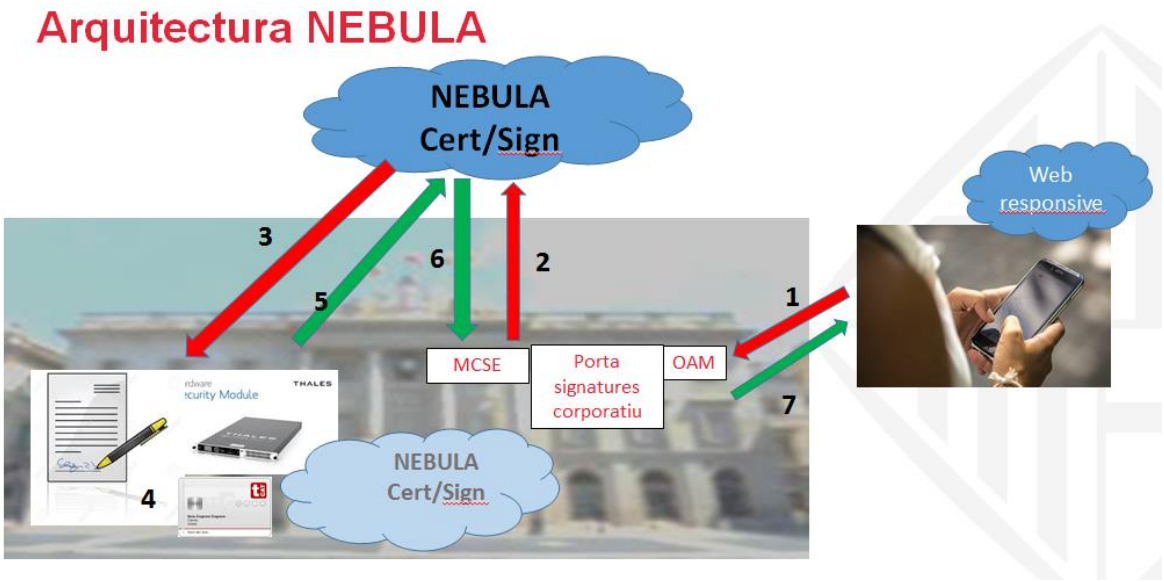
- **Recurs**: Representa l'accés a una aplicació, és una URL del tipus /APPS/<nom_aplicacio> També associats a un recurs es defineixen les URLs concretes de l'aplicació que estan protegides, és a dir, que requereixen que l'usuari estigui autenticat per poder visualitzar-les.
- **Rols de recurs**: Els recursos tenen associats rols, els usuaris han de pertànyer a algun d'aquests rols per poder visitar les URLs protegides d'un recurs.
- **Rol administrador de recurs**: També està associat a un recurs i permet accedir a la consola d'administració de GetAccess i assignar usuaris a rols de recurs.

Mitjançant la consola d'administració del producte, es creen i mantenen usuaris i se li associen els **rols de recurs** (aquesta tasca la poden realitzar els usuaris amb **rol d'administrador de recurs**). El producte GetAccess verifica que els usuaris que visiten URLs d'un **recurs** tenen un **rol de recurs** corresponent i permet o bloqueja l'accés en funció de la seva pertinença a aquest rol.

Quan un usuari està autenticat se li envia a l'aplicació una capçalera HTTP amb el nom "user" i com valor el nom d'usuari (*login*), l'aplicació pot fer servir aquesta capçalera per identificar l'usuari en el seu model de dades.

1.1.5. Certificats i Signatura centralitzada: Nebula

L'Ajuntament disposa d'una solució Nebula Suite de Vintegris Tech de custòdia de certificats i signatura centralitzada, que es composa d'un servei Nebula Cert/sign al Núvol per realitzar la gestió i signatures i un HSM (*Hardware Security Module* – Mòdul de Seguretat de Maquinari) on-premise per a l'emmagatzemament i custòdia de certificats corporatius, tant personals de TCAT-P o altres com de certificats d'Òrgan o d'encriptació d'informació.



NEBULA suite (CERT/SIGN) custodia els certificats ubicats on premise a HSM:

- Certificats de segell amb els que es fan Actuacions Administratives Automàtiques. Aquests certificats són els de proves, emesos per la imiCA i els d'òrgan municipal emesos per CATCert
- Certificats de l'empleat públic, t-cat p emesos per CATCert.
- Gestiona el cicle de vida dels certificats, avisa de la caducitat

Realitza signatures

- Amb els segells de forma automatitzada i amb els certificats d'empleat públic de governat per l'acció de l'empleat.

Compleix amb Reglament eIDAS eIDAS 910/2014

1.1.6. LinOTP, solucions de Segon Factor d'autenticació.

Solució d'autentificació de *token* d'un sol ús basada en LinOTP, una plataforma *open source* suportada per LSE, Leading Security Experts, GmbH i distribuïda sota llicència AGPLv3.

Aquesta solució permet accedir als serveis de l'IMI designats (gestionats a través d'un *appliance* Juniper) utilitzant contrasenyes generades per OTP (*tokens*).

També hi ha implementat el Segon factor que proporciona la Suite de EIS d'Oracle.

L'IMI es troba en procés de canvi pe què fa al Segon factor d'autenticació, el contracte haurà de gestionar i donar suport tècnic de Nivell 3 del eina/de OTP que tingui implementades.

2. OBJECTE

Aquest contracte té per objecte la prestació dels **SERVEIS D'IDENTITATS I ACCESSOS** (Identitats, Accessos, Autenticacions i Autoritzacions) que engloba els serveis de Govern i arquitectura d'identitats corporatives així com el suport de nivell 3 d'alguna eina que es requereix en aquest moment, mitjançant una oficina tècnica encarregada de garantir un alt nivell de seguretat dels serveis i sistemes d'informació corporatius de l'Ajuntament de Barcelona per a garantir l'accés adequat i establert, l'autenticitat, confidencialitat, integritat, disponibilitat i no repudi.

Aquest "**SERVEIS D'IDENTITATS i ACCESSOS"** (Identitats, Accessos, Autenticacions i Autoritzacions) inclourà:

a) Govern i Arquitectura d'identitats (Directrius, Model corporatiu i Tecnològic i evolució d'aquest model i orquestrat de les identitats i accessos).
b) Processos d'Identitats i accessos (Auditories i Qualitat): Processos de recertificacions i de millora de la qualitat de repositoris.
c) Evolutius, destinat a l'evolució de la solució de les identitats i gestió d'accessos, donant resposta a les peticions d'evolutius sota demanda relacionats amb tots els components de la solució.
d) GID Provisió automàtica recursos i autoritzacions i sincronismes bidireccionals, definir i implementar el model de provisió automàtica d'autoritzacions i recursos per perfilats i integració bidireccional de sistemes SAP, CRM, ADFS/AD, webs corporatives i serveis cloud.
e) Suport Tècnic 24x7 de Nivell 3 de GetAccess, Nebula (HSM) i solucions de segon factor d'autenticació. Es requereix el Suport tècnic de nivell 3 i l'operació en l'horari no laboral (horari que no es troba cobert actualment, que és de 18 hores fins a les 9 del mati i caps de setmana i dies festius).

L'objectiu principal del Servei serà dur a terme totes aquelles activitats que garanteixin determinar l'estratègia i tàctica del servei: definició de models, evolució, coordinació, control, gestió i

funcionament dels processos associats a les identitats i accessos TIC de l'Ajuntament de Barcelona, així com assegurar el seu correcte i òptim funcionament, aportar els plans de millores i evolucions que es requereixin dins del marc del domini de controls d'accés, autenticacions, autoritzacions i credencials (en endavant CAAA) de forma proactiva i reactiva.

També totes les tasques i activitats de suport necessàries per a garantir una correcta planificació i execució dels projectes de l'IMI relacionades amb les identitats i accessos amb el propòsit d'aconseguir l'objectiu final amb el temps establert i amb el nivell de qualitat exigit.

Definir i evolucionar els processos requerits per a garantir

Els serveis de Suport Tècnic fins a nivell 3 i serveis Operatius de la solució GIA (OIM, OAM i OUD) s'executen en la Direcció d'Explotació i Sistemes i per tant, queden fora de l'abast d'aquest contracte. D'igual manera totes les eines que incorporen controls d'accés com son els escriptoris virtuals, estacions de treball corporatives, accessos remots, productes específics,... quedant en relació a aquestes plataformes el govern i definició de millores a aplicar en pro de l'estratègia de govern de les Identitats i Accessos.

3. ABAST

A nivell de Govern, definició i suport de les arquitectures d'identitats i accessos destinats al ciutadà i empreses com pel personal intern corporatiu i extern de contractes, gestió d'identitats corporativa, accessos remots d'aquests o accés a aplicatius o productes. També entren la construcció d'evolutius de tots els sistemes de gestió d'identitats, d'autenticació, controls d'accés, d'autorització, credencials i 2FA corporatius destinats al personal intern corporatiu i extern de contractes, gestió d'identitats corporativa, accessos remots d'aquests o accés a aplicatius o productes.

Addicionalment entren a nivell de suport tècnic de nivell 3 del GetAccess, Nebula i solucions de segon factor d'autenticació en els horaris indicats i concrecions indicades en l'apartat corresponent d'aquest plec.

4. SERVEIS INCLOSOS

Identifiquem com a serveis d'identitats els serveis de govern i arquitectura d'identitats que estructurem amb els següents blocs:

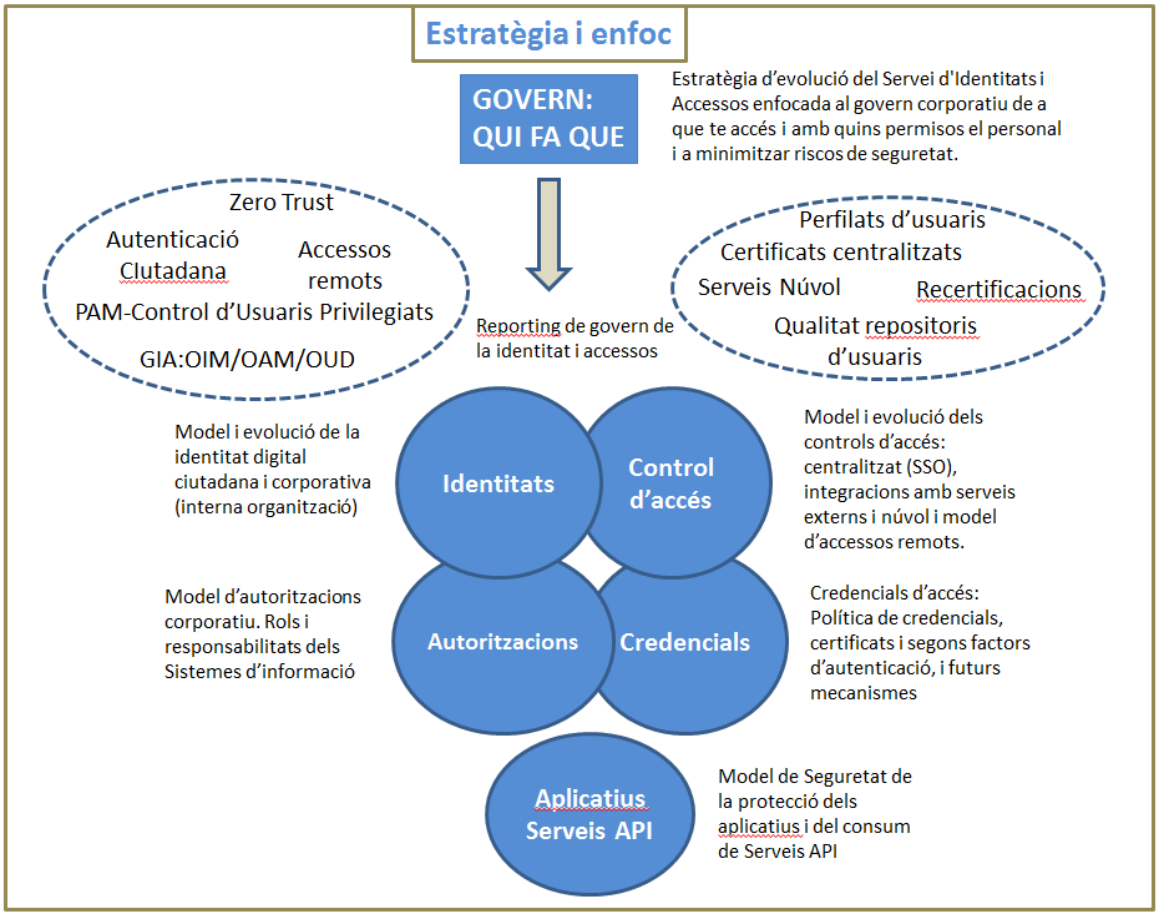
- Govern i Arquitectura d'identitats
- Processos d'Identitats i accessos (Auditories i Qualitat)
- Evolutius
- GID Provisió automàtica recursos i autoritzacions i sincronismes bidireccionals
- Assessoria i suport.
- Suport Tècnic 24x7 de Nivell 3 de Getaccess, Nebula (HSM) i solucions de SSO

Es posa a disposició un detall pràctic de tasques i activitats d'aquest servei en una visió vertical per objectes de protecció de seguretat (Identitats, accessos, autoritzacions, credencials, serveis API) s'incorporen al ANNEX 2.

4.1. SERVEI DE GOVERN I ARQUITECTURA D'IDENTITATS

Engloba els serveis de definició, coordinació, gestió i suport tècnic i implantació de processos de seguretat associats al control d'accés, autenticació i autorització (en endavant CAAA), en concret, el govern de les identitats, la seva seguretat, la gestió de les credencials, la gestió de les autoritzacions, la segregació de funcions, les evidències, els sistemes de control d'accés, accessos remots, els processos implementats, els indicadors associats, el seu cicle de vida, les polítiques i normes que les regulen, les noves necessitats que han de donar resposta i l'encaix el programa de Seguretat de l'IMI, són els objectius principals d'aquesta licitació.

El contracte en primera instància, ha de vetllar per la millora contínua del Servei de Identitats i Accessos, recollint l'estratègia i models establerts actuals, revisant i millorant els models i les estratègies a seguir, definint un pla de millores a executar dins del servei i amb les àrees operatives de l'IMI i fen propostes de projectes amb el seu objectiu, justificació de la oportunitat de millora, proposta de projecte o evolutiu en recursos, pla estimat d'execució, esforç i valoració.



Com a part cabdal dels serveis que es liciten, l'adjudicatari haurà de participar en tot procés de transformació i desplegament de serveis relacionats amb Identitats i Accessos (CAAA) de l'IMI, participant en la definició i fent seguiment de la correcta implementació dels requeriments que el departament de Seguretat l'IMI determini a tal efecte.

El Servei de Govern i Arquitectura d'identitats també definirà arquitectures d'identitats i Accessos i vetllarà per què els Projectes tecnològics de l'IMI i l'Ajuntament es construeixin amb les arquitectures i models definits.

En Concret el Servei seran:

4.1.1. Govern Identitats i Accessos

- Establir directrius de seguretat de processos relacionats amb el dominis de la ISO27002 de Identificació, Control d'accés i autorització (Normatives i guies d'estàndards d'identitats corporatives). Compliment ENS, LOPD i Seguretat corporativa.
- Establir/Revisar/Mantenir el Model corporatiu d'identitats i accessos global (serveis de xarxa i serveis al núvol, dispositius, IOTs, drons, accessos remots, etc.):
    - Model Global del CAAA

- Model del Govern de la Identitat:
  - Cicle de vida de les identitats,
  - Sincronització de credencials
  - Integracions amb directoris d'usuaris síncrones i en procés diferit.
  - Definició de Processos de recertificacions
  - Una vegada feta la reconciliació segons l'apartat 4.4.2 Sincronització bidireccional, és possible cercar patrons (usuaris amb característiques similars que tenen els mateixos drets d'accés) i generar funcions amb assignació automàtica, de manera que s'elimini la necessitat de sol·licitar permisos.
  - Descobriment de comptes orfes: Degut també a la reconciliació dels comptes segons l'apartat 4.4.2 Sincronització bidireccional, els comptes orfes es descobreixen en els sistemes.
  - Permisos amb risc associat: s'identificaran els permisos amb un gran risc associat (per exemple, Grup d'Administradors del Directori Actiu) i generar una funció/perfil que proporcioni aquests permisos per tal d'identificar els permisos assignats manualment i actuar en conseqüència.
  - Organismes Integrats. Incorporació de noves organitzacions, fonts autoritatives.
  - Visió dels recursos autoritzats
  - Perfilats i Identificació.
  - Assignació de recursos
  - Models d'integracions en el núvol i federacions d'identitats
  - Fluxos de treball per a l'assignació d'accessos, i dels actors que intervenen en aquests fluxos
- Model dels controls d'accessos:
  - Arquitectures dels controls d'accés i tipologies acceptades
  - Single Sign On (SSO)
  - Inventaris de controls d'accés corporatius
  - Accessos remots,
  - control d'externs i serveis en el núvol
  - Timmings: Timeouts de sessió, d'inactivitat, de login, ..
  - etc.
- Model de credencials:
  - Credencials acceptades pel ciutadà
  - Credencials corporatives
  - Política de contrasenyes corporativa
  - Segon Factor d'autenticació
  - Certificats centralitzats/HSM
  - Futures tecnologies: per exemple, *blockchain*.
- Model d'autoritzacions:
  - Identificació de Rols i Perfils,
  - Directori d'autoritzacions corporatiu
  - model d'autoritzacions (RBAC)

        - processos de revisió de la qualitat d'aquestes autoritzacions
        - model /tipus d'integració d'autoritzacions
        - Coordinació amb departament d'arquitectura de desenvolupament de l'IMI pels evolutius i manteniment de l'aplicatiu GIA (Aplicatiu que habilita que el personal i gerències municipals atorguin i treguin permisos/rols a les aplicacions i sistemes d'informació dels què en són "propietaris"/Responsables executius.
    - Model de protecció d'Aplicatius i serveis API:
        - Models acceptats de definició i configuració de perfils i rols d'autorització dels aplicatius.
        - càrrega de la configuració de perfils d'autorització dels aplicatius en la pipeline DEVSECOPS a través de l'aplicatiu SHIELD (desenvolupat pel departament d'arquitectura de desenvolupament de l'IMI).
        - Coordinació amb departament d'arquitectura pels evolutius i manteniment de l'aplicatiu Shield
- Tractar i incorporar en el model les noves necessitats de Identitats i Accessos.
- Gestió d'excepcions relacionades amb les identitats i accessos: acceptar i vetllar pel cicle de vida de les excepcions registrades en la Oficina de GRC.
    - Dins d'aquest apartat i durant el primer trimestre del contracte es farà una proposta d'evolutiu de millora en els processos d'identitats que ofereixi un salt qualitatiu en el govern de les identitats i les seves autoritzacions per tal de tenir el control de qui fa que en la organització i que minimitzi els riscos de ciberseguretat. Aquesta millora s'implementarà en 9 mesos com a màxim. La proposta s'acceptarà en el Comitè de Direcció del Servei. Aquesta petició s'engloba dins de la necessitat de prioritzar l'assegurament de que la organització pugui tenir la visió de a què accedeix el personal corporatiu i personal de contractes externs.
    - El contracte a l'inici del contracte revisarà les implementacions fetes i models documentats, identificarà les que necessiten revisió i les no implementades i es farà una relació un pla de millores identificant les tasques i/o Projectes de millora que es prioritzaran en el comitè de direcció del servei:
        - Es farà un especial focus en l'evolució de la identitat digital atenent a les necessitats de la Organització Municipal proposta d'evolució del sistema d'identitats cap a la governança: disposar de la visió de qui fa que qui fa que en la organització i quins processos i evolutius se'n deriven.
        - D'igual manera pels accessos interns i remots i credencials i models d'autenticació del ciutadà.
        - Finalment, evolució dels models d'autoritzacions a aplicatius i serveis API.

      => Les propostes tindran dos apartats, la de projectes que per el volum i recursos requerits o requeriments d'adquisició de productes queden fora de l'abast d'aquest contracte i s'han de configurar com un projecte i les millores continues que s'executaran dins del servei del contracte directament amb recursos del contracte i amb possibles gestions amb les àrees operatives per a la seva implantació.

- En 6 mesos haurà d'entregar els models d'identitats i accessos revisant i documentant per tal de que la Oficina de Govern de GRC els incorpori al cos normatiu i la oficina de Projectes les incorpori en la documentació d'arquitectures per què els projectes de l'IMI els emprin per el correcte desenvolupament dels projectes.

El licitador presentarà una proposta de plantejament dels factors a tenir en compte i com portarà a terme la revisió dels models existents i com presentarà la proposta d'evolució. Es valorarà com planteja aquestes tasques el licitador.

4.1.2. Arquitectura d'Identitats i Accessos

El servei d'arquitectura i accessos ha d'actuar com a referent de les arquitectures d'identitats que permetin assessorar als projectes en les implementacions especials, establir i revisar dissenys i arquitectures corporatives o integracions de fonts i vetllar perquè els models establerts s'implementin correctament en les diferents tecnologies, processos i integracions, tasques de arquitectura d'identitats com són:

- Consultoria Tecnològica d'identitats i accessos: Actuar com a **punt de referència tecnològic** per a la resta d'àrees de l'IMI i per extensió per a l'Ajuntament.
- Participar activament en la fase de disseny i dels **nous projectes de sistemes d'informació** amb requeriments especials amb relació a CAAA del Ajuntament de Barcelona per definir el disseny de les necessitats.
- Disseny Tecnològic d'arquitectura d'identitats i accessos. **Dissenyar i validar l'arquitectura dels sistemes** que donen serveis a les identitats i accessos (CAAA), a propostes de una nova plataforma tecnològica o evolutius i/o canvis que afectin als processos i funcionalitats del ecosistema corporatiu d'identitats i accessos., garantint els requeriments de seguretat establerts a l'IMI i la correcta integració amb les plataformes tecnològiques existents així com els de disponibilitat i operatius..
- Tasques de Gestió i Coordinació d'Evolutius de les plataformes que donen suport al servei d'identitats i accessos: Anàlisi d'impacte global de les problemàtiques diàries per definir solucions i aplicar-les.
- Prescripció, establir processos, revisió i participació en les Implementacions de Productes d'accessos o eines PAM per control de credencials i accessos d'administradors.
- Assessoria i suport a projectes i serveis (Guia d'estàndards d'identitats)
- Coordinació i orquestrador de les implementacions d'accessos en les àrees operatives.
- Arquitectura d'Integracions amb plataformes corporatives (SAP, AD, OUD, BBDD,HPSM,...)
- Assessoria i suport a projectes i serveis (Guia d'estàndards d'identitats)
- Auditories tecnològiques i revisió dels processos i procediments
- Implantació de polítiques de credencials.
- Exemples de temes que l'arquitectura i Projectes haurà de treballar:

- Identitats: Fonts autoritatives SAP para interns i fluxos per externs
- Federacions d'identitats i integracions amb Solucions al núvol
- Integracions de noves organitzacions Municipals i de confiança
- Integració de noves tecnologies d'accés
- Evolució del sistema de credencials cap a la seguretat adaptativa.
- Usabilitat de les credencials.
- Aplicatiu GIA/Shield de gestió d'autoritzacions i serveis.

4.1.3. Presentació d'informes per al Govern les Identitats i Accessos

Pel bon govern de QUI FA QUÈ I QUAN de l'Ajuntament, el servei requereix d'un sistema d'informes de les Identitats i Accessos, pel coneixement i control de la seguretat de la informació, de manera que les direccions i gerències de Ajuntament tinguin visibilitat i control sobre el personal i els sistemes d'Informació dels que en són responsables.

L'adjudicatari elaborarà i lliurarà com a mínim els següents informes de lliurament recurrent:

- Informe sota demanda de compliment de sistemes d'informació a Gerències de Ajuntament
- Informe mensual de compliment de la política de contrasenyes i d'altres credencials
- Informe mensual d'indicadors d'identitats i accessos.
- Informe mensual d'indicadors accessos remots
- Informe específic que se sol·liciti arrel d'alguna actuació que requereixi d'indicadors puntuals.
- Informe de l'evolució de l'estratègia d'evolució del servei de Identitats i Accessos.

El licitador ha de lliurar en la seva proposta tècnica una proposta d'informes per al govern del servei de CAAA, avaluable en els criteris d'adjudicació, que com a mínim inclourà els informes detallats al paràgraf anterior.

- Es valoraran també propostes que proporcionin un salt qualitatiu i millorin el control i vigilància dels accessos.
- Valoració dels informes que es proposen que millorin la proposta.

D'igual manera, models eficients de generació d'informes que consumeixin els mínims recursos i puguin ser consultats en qualsevol moment.

- Proposta d'informes que s'elaboraran durant al contracte i periodicitat.
- Als 3 mesos del contracte s'hauran de proporcionar 3 informes i als 9 mesos la resta dels mínims exigits en el plec. Es valoraran les millores a aquesta proposta ja sigui en informes addicionals que siguin rellevant per l'IMI com pel compromís d'entrega en temps d'aquests.

- Es farà una revisió anual dels informes i la seva idoneïtat o qualitat i s'aplicaran millores
- Al següent any del contracte així com en les possibles pròrrogues s'incorporaran dos informes nous anualment.
- Informes de necessitats concretes i específiques que es requereixin: 3 a l'any no contemplats ni en la proposta ni exigits en el plec.

4.2. PROCESSOS D'IDENTITATS I ACCESSOS (AUDITORIES I QUALITAT)

Aquest servei ha de mantenir i millorar els processos d'identitats i accessos i vetllar per la lògica de l'Ajuntament per garantir la qualitat, integritat i la fiabilitat de les identitats, accessos i autoritzacions perquè garanteixin la protecció real de l'Ajuntament en el desenvolupament de les seves competències. Això requereix vigilància activa, processos de recertificacions i de control i millora de la qualitat de repositoris:

- Integracions de GID amb sistemes i plataformes corporatives:
    i. Processos Background: SAP RH, SAP CUA, Easyvista, Webs DTI.
    ii. Online: Directori actiu.
- Processos de manteniment d'integritat d'identitats i accessos, revisions dels responsables
- Processos de gestió de credencials i implantació política corporativa
- Processos d'automatització d'assignació de recursos i perfilats
- Processos de qualitat de les autoritzacions (recertificacions) amb els responsables dels Sistemes d'informació.
- Processos de cicle de vida de les identitats (relacions amb departaments de RH i peticionaris T4).
- Processos de canvis organitzatius
- Processos de canvis rellevants d'organigrama (Canvi de mandat)
- Processos de revisió d'accessos i monitoratge actiu dels accessos
- Processos d'informació a les gerències dels accessos dels seus sistemes d'informació
- Processos d'eliminació de recursos i autoritzacions d'identitats eliminades
- Processos de segregació de funcions
- Processos de vigilància dels administradors de sistemes
- Auditoria de procediments d'accés físic a CPDs, de autoritzacions d'accés a Administradors de sistemes i desenvolupaments SAP.

El proveïdor farà una proposta de processos i priorització què es valorarà.

Com a mínim s'implantaran 4 processos anuals. Es farà una proposta d'enfoc general dels processos requerits i es decidirà quins s'implementen en el comitè de Direcció del servei.

4.3. EVOLUTIUS

El servei d'identitats, donada la situació de teletreball i els riscos de ciberatacs, exigeix molta agilitat a l'hora d'implementar millores de les funcionalitats existents o implementar noves funcionalitats de manera recurrent, tant per anar ajustant l'evolució del model d'identitats i accessos definit com per a minimitzar riscos emergents de ciberseguretat:

- Nous models requerits per minimitzar riscos emergents.
- Noves funcionalitats, integracions i processos.

En principi es consideraran 5 evolutius anuals de **nivell mig de complexitat**, amb un valor aproximat de **100 hores** cadascun. Es repercutiran proporcionalment però, cada evolutiu segons si aquest suposa mes o menys esforç, BAIX 50 hores, MIG 100 hores i ALT 150 hores, de manera que dos evolutius de nivell baix equivaldran a un de nivell mig i un de nivell alt equivaldrà a un i mig de nivell mig.

Donat el context altament volàtil de la ciberseguretat i donada la criticitat i urgència probable en la implantació d'aquests evolutius, cal preveure que hi hagi demandes addicionals, ja sigui per l'interès sobrevingut concret d'un projecte que te requeriments específics no previst al pla anual d'evolutius, o per si es requereixen mes evolutius dels establerts al pla anual d'evolutius. En ambdós casos cal preveure que es puguin executar dins del marc d'aquest contracte a través d'ampliacions contemplades en aquest mateix contracte..

- Es puntuaran les propostes dels licitadors que millorin el nombre mínim d'evolutius a realitzar anualment. En cas de millora oferta per part de l'adjudicatari, serà aquesta la que prevaldrà.

L'adjudicatari haurà de definir el pla de millores del contracte, proposant a l'inici del contracte i revisant aquest pla anualment. Quan hi hagi canvis de les millores proposades al pla es presentaran amb la seva justificació al Comitè de Direcció del Servei per ser aprovades.

L'adjudicatari del servei s'encarregarà de la planificació, gestió i execució dels evolutius. La tipologia de evolutius que s'executaran seran:

- Funcionalitats, integracions i processos de Identitats.
- Funcionalitats, integracions i processos de Controls d'accés.
- Funcionalitats, integracions i processos d'autoritzacions.
- Funcionalitats, integracions i processos de credencials.
- Funcionalitats, integracions i processos de model de protecció d'aplicatius i serveis API.

A mode d'exemple, els evolutius més comuns que es demanaran en aquest servei són:

- Desplegament de la implementació de millores sobre l'aplicatiu corporatiu GIA/SHIELD.
- Implantació de nous factors d'autenticació o credencials.
- Nous mecanismes d'autenticació: Mecanismes alternatius o complementaris (segons factors) per autenticar l'usuari (ex. enviament de OTP, certificats electrònics, ...).
- Incorporació de nous atributs d'usuari: En el cas que es faci necessari publicar nous atributs dels usuaris caldrà modificar el connector del gestor d'identitats per enviar els nous atributs al directori de la solució.
- Integracions especials de noves aplicacions en el núvol o proveïdors de serveis (*Service Provider*): Integrar aplicacions o sistemes que no s'ajusten als models d'integració estandarditzats.
- Migració d'aplicatius GetAccess a OAM.
- Automatització de processos o canvi rellevant.
- Integració de noves fonts d'identitats o creació de connectors nous per integrar repositoris interns o serveis al núvol. Canvi rellevant en el cicle de vida de les identitats.
- Implementacions de segons factors d'autenticació.
- Migracions d'aplicatius a OAM.
- Construcció de nous informes: Capturar noves dades associades al servei i presentar informes amb l'analítica corresponen.
- Implementació de nous processos d'identitats o recertificacions.
- Integració de Certificats centralitzats amb els mecanismes d'autenticació establerts corporatius i amb la gestió d'identitats.
- Implementacions de evolutius Evolució del model de autoritzacions.
- Evolució portals d'autoservei.
- Sincronitzacions de directoris i fonts.
- Solucions particulars per donar sortida a necessitats puntuals.

Donat el context altament volàtil de la ciberseguretat i donada la criticitat i urgència probable en la implantació dels evolutius, cal preveure que hi hagi demandes addicionals, ja sigui per l'interès sobrevingut concret d'un projecte que te requeriments específics no previst al pla anual d'evolutius, o per si es requereixen més evolutius dels establerts al pla anual d'evolutius. En ambdós casos cal preveure que es puguin executar dins del marc d'aquest contracte a través d'ampliacions contemplades en aquest mateix contracte..

L'adjudicatari haurà d'implementar o millorar funcionalitats, implementacions tecnològiques, integracions i processos en els diferents solucions d'identitats i accessos-CAAA (Control d'accés

(OAM), single sign on, Sistema d'autoritzacions, federacions d'identitats, *clouds identity*, Segon factor d'autenticació, accessos remots, Gestió d'identitats, etc.). L'Evolutiu es realitzarà seguint les fases d'implantació que s'executarà amb el perfil d'un "Tècnic sènior especialista en evolutius i integracions":

- Realitzar la presa de requisits, tot identificant els casos d'ús i el detall dels mateixos.
- Participar en les tasques d'anàlisi i proposta d'alternatives.
- Realitzar les proves funcionals del sistema.
- Disseny d'interfícies d'usuari.
- Disseny i realització les proves funcionals i d'acceptació del sistema.
- Donar suport funcional als usuaris.
- Definir els continguts dels cursos i validar el contingut de la documentació lliurada.
- Implementar la proposta d'arquitectura del sistema d'acord amb les especificacions del projecte i l'arquitectura de referència de l'IMI.
- Documentació i traspàs a producció.

Dins d'aquest servei els evolutius es definiran i s'implementaran en entorns de test i preproducció i es documentaran i traspassaran (si aquests estan operats per la direcció d'explotació i sistemes) a la Direcció d'operació i sistemes que porten els serveis de GIA o altres plataformes.

- Dins d'aquest apartat i durant el primers 2 mesos de cada any contractual l'adjudicatari presentarà la proposta dels evolutius a executar en base a les necessitats d'evolucionar o millorar el model global d'identitats i accessos. Aquesta proposta portarà el nom de l'evolutiu, descripció esforç necessari i temps d'execució. Els evolutius es definiran i executaran en el marc d'un any tot i que si es requereix podran establir-se fins a de 2 anys)
- Revisió anual dels evolutius proposats.

4.4. GID PROVISIÓ AUTOMÀTICA DE RECURSOS I AUTORITZACIONS I SINCRONISMES BIDIRECCIONALS

El Servei haurà de definir i implementar en el període d'un any i mig la segona fase de la gestió de les identitats (GID). Aquesta fase ha d'avançar amb els perfilats dels usuaris, la implementació de fluxos d'autoritzacions per a la provisió dels recursos i les autoritzacions d'una manera automàtica. També s'haurà de sincronitzar amb sistemes com SAP, CRM, ADFS/AD, webs corporatives i sistemes cloud. També el model àgil pels col·lectius que mantenen i desenvolupen les webs.

4.4.1. Provisió automàtica de recursos

Alguns col·lectius, degut a la seva casuística, tenen usuaris amb perfils molts semblants, com succeeix, per exemple a Acció Social, Guàrdia Urbana (GUB), Districtes, Oficines d'Atenció Ciutadana (OAC), etc.

La provisió d'aquests tipus d'usuari ha de ser quasi automàtica i ràpida. L'automatització es basarà en emprar una plantilla bàsica amb els recursos propis dels usuaris. A més, s'ha de tenir en compte que poden haver-hi algunes modificacions:

- Incloure automatitzacions en els càlculs de certs atributs/permisos dels usuaris.
- Incloure nous atributs en el procés de càrrega.
- Canviar la tecnologia / tipus d'integració amb la font mestra, etc.
- Perfilat en base a categories de llocs de treball i posicions.
- Workflows d'autoritzacions per organigrama i resposables dels Sistemes d'informació.

4.4.2. Sincronització bidireccional

El licitador presentarà una proposta detallada de la provisió automàtica de recursos i autoritzacions i integracions de sistemes SAP, CRM, ADFS/AD i webs corporatives DTI. Es valorarà el nivell d'enteniment del licitador de les tasques que derivin amb una bona proposta.

En quant a la sincronització:

- Provisió: Hi ha connectors que en l'actualitat no estan realment integrats ja que només deixen un fitxer a una carpeta i el sistema final els recull i actualitza el seu model de dades. En aquests cas es desplegarà el connector real que permetrà actuar directament sobre el sistema final. Aquesta provisió és molt important ja que, sense ella no es pot saber si s'han fet les actualitzacions i no es poden prendre mesures ràpides (per exemple, inhabilitar usuaris per compromís de credencials).
- Reconciliació: Actualment els connectors són unidireccionals, des de l'OIM fins al sistema final. Per aquesta raó, OIM no sap els permisos que l'usuari té en el sistema final i tampoc no identifica comptes orfes. Per resoldre això, s'ha implementar la capacitat de conciliació dels sistemes origen i final. D'aquesta manera OIM sabrà els recursos i permisos que l'usuari té a tots els sistemes. Això és especialment important al Directori Actiu (*Active Directory*) ja que és aquí on els grups representen l'accés a moltes aplicacions. I accessos a ADFS.

4.5. ASSESSORIA I SUPORT

Per tal de garantir govern de les identitats i els accessos (CAAA), el servei d'identitats i accessos oferirà a la resta d'àrees i departaments de l'Ajuntament i de l'IMI un servei d'atenció i resolució

de dubtes o de suport tècnic especialitzat en matèria de Seguretat de les identitats i accessos (CAAA). Suposa proporcionar un servei d'assessorament per a la implementació tecnològica, procedimental i organitzativa de CAAA en general, amb el qual es resoldran dubtes que és puguin despendre tant conceptual, de processos i procediments o tècnic.

Dins d'aquest suport donarà suport al Suports tècnics de Nivell 3 de les diferents plataformes que s'administren i operen en la direcció de operacions i sistemes.

En especial, es donarà suport per recolzar les integracions d'aplicatius complexes, que s'encallen per algun motiu, especials o no definides en els models d'integració a la Direcció d'Operacions i Sistemes. Les integracions les implementarà producció amb els serveis operatius d'aquesta direcció. Per aquest suport, si convé s'empraran els arquitectes d'identitats i accessos d'aquest servei i/o d'evolutius sempre i quan sigui aprovat en el comitè de direcció del servei.

També entren en l'abast la prestació de suport als suports tècnics de Nivell 3 i als projectes de GetAccess, solucions de API Manager, OPT i del desplegament d'aplicatiu d'autoritzacions (GIA/SHIELD):

- Suport a les aplicacions per definir i integrar-se amb GetAcces.
- Suport a les aplicacions per definir i integrar-se amb *One Time Password*.
- Suport a les aplicacions per definir i integrar-se amb Microserveis i API Manager.
- Suport a les aplicacions per definir i integrar-se amb Processos de Aplicatiu GIA i de l'Aplicatiu SHIELD per la configuració d'aplicatius (DEVSECOPS).

Per al desenvolupament d'aquest servei es duran a terme les següents tasques regulars de suport:

- Atenció a la bústia de consultes i peticions associades al servei d'identitats i accessos de peticions directes i d'escalats de tickets de SAU.

  El proveïdor oferirà un mecanisme per comptabilitzar el consum de temps i tickets gestionats, acordat amb el responsable del contracte de l'IMI i que reportarà mensualment en el comitè de direcció del servei.

  L'adjudicatari destinarà un mínim de **100 hores** anuals en el servei regular de gestió de les entrades de peticions i tickets de seguretat escalats de SAU i en la gestió d'incidències operatives del servei abast d'aquest plec.

  Es valorarà l'increment de les hores dedicades a aquest servei a l'oferta del licitador.

- Assessories i suports: servei d'atenció i resolució de dubtes o de suport tècnic especialitzat en matèria de Seguretat de les identitats i accessos:
  - Suport orientatiu de funcionament de processos i procediments dels serveis.
  - Servei de consultoria orientativa de temes puntuals.
  - Incidències i canvis que derivin en tasques del servei.
  - Serveis d'ajuda al diagnòstic d'incidents, problemes i canvis que derivin en tasques del Servei de CAAA. Suport al Suport de Nivell 3 que es troba en àrees operatives.

  - Resolució de dubtes o consultes sobre la interpretació o aplicació del marc normatiu de seguretat.

- El proveïdor oferirà un mecanisme per comptabilitzar el consum de temps en assessories o consultories gestionades, acordat amb el responsable del contracte de l'IMI i que reportarà mensualment en el comitè de direcció del servei.
  - Lliurament mensual de l'informe de les accions de suport realitzades i dedicació, especificant com a mínim el nombre de tickets, l'estat, i la dedicació.

4.6. SUPORT TÈCNIC NIVELL 3 I OPERACIÓ DE PLATAFORMES:

Els serveis de suport tècnic són aquells que s'executaran amb la finalitat de garantir el correcte funcionament dels Serveis i Plataformes , GetAccess, Nebula/HSM – Certificats centralitzats i Solucions de One Time Password. Queda exclòs (no forma part de l'abast del contracte) el Suport tècnic de GID/OAM i OUD. Aquesta part del servei inclou activitats pròpies dels serveis TIC com la resolució de peticions, incidències i problemes i activitats d'administració així com l'estandardització dels procediments i la gestió dels actius i de les seves configuracions.

- **Suport Tècnic de Nivell 3** de la plataformes i serveis **GetAccess** i **solucions de One Time Password (OTP)** segon factor d'autenticació 10x5.
- **Operació de la Solució i administració en horari no laboral** del servei de Certificats centralitzats - **Nebula (CERT/SIGN i HSM)** (temps de resposta, diagnòstic i resolució es compta sobre l'horari de 18:00. a 8:00 del dia següent de dilluns, i de 00:00 a 24 hores dissabtes, diumenges i festius. Actualment ja es disposa d'un servei 10x5 que cobreix dies laborals de 8 a 18 hores. S'hauran de coordinar aquests dos serveis per garantir un 24x7 i incorporar les tasques mínimes de resolució d'incidències de Suport Tècnic de Nivell 3 que es precisin per donar continuïtat a aquest servei 24x7.

4.6.1. Incidències i Problemes (Suport Tècnic Nivell 3)

L'empresa adjudicatària posarà a disposició de l'IMI un servei de suport estructurat en un únic nivell (nivell 3 de suport) per atendre les incidències i problemes detectats tant en el sistema d'informació objecte del contracte com en la part que li correspongui pel què fa a les integracions amb altres sistemes d'informació de la corporació.

Es consideren els següents tipus d'incidències:

- Incident: interrupció no planificada o reducció de qualitat d'algun servei proporcionat pel programari.
- Problema: causa subjacent d'una sèrie d'incidències o incidència aïllada d'importància significativa.

Les incidències podran ser de tipus tècnic i funcional. Estan incloses en l'abast del contracte les tasques derivades de la solució dels incidents i problemes, que derivaran en tasques de manteniment correctiu, així com el suport en la instal·lació i implantació del producte o de les noves versions i pegats d'aquest en els entorns on estigués ja implantat. De forma més detallada:

- Serveis de resolució d'incidències tècniques, que resoldrà les qüestions tècniques que planteja l'ús del producte i les seves integracions dins de l'entorn tècnic de l'IMI i els sistemes d'informació que puguin estar involucrats en el futur.
- Servei de resolució d'incidències funcionals en l'aplicació, o en les seves integracions. Es resoldran les incidències que puguin sorgir amb l'ús del sistema i les seves integracions.
- Servei de suport per a la instal·lació i posada en producció de les noves versions i pegats del sistema derivats de la resolució d'incidències. Comprèn tots els processos de parametrització, migració de dades, proves i validació de les versions en els diferents entorns afectats.

L'adjudicatari haurà de garantir l'atenció a incidències i resolució de problemes de codi i dades sobre tots els elements tecnològics que formen la solució (descrits a l'apartat 3.1 Plataforma Tecnològica GIA), tenint en compte que l'adjudicatari ha de donar servei sense interrupció i garantir el correcte funcionament de la solució.

Aquest servei té com a objectiu principal garantir la màxima disponibilitat de la solució de gestió d'accessos, localitzar i eliminar els possibles defectes del programari o en les dades que genera.

L'adjudicatari haurà d'especificar el circuit i atenció proposades, tot i que haurà d'adoptar les directrius que li siguin indicades per l'IMI, per tal d'integrar-se en el procés i eines corporatives de gestió d'incidències i problemes.

Es valorarà la precisió a l'hora d'abordar els aspectes clau de l'Operació del Servei de la plataforma objecte del contracte.

4.6.2. Definició de suport de tercer nivell

Habitualment els sistemes de manteniment es gestionen amb un màxim de tres nivells, sent el tercer nivell, el de més capacitat per resoldre problemes, arribant a aquest nivell, els problemes tècnics de major calat o de resolució més avançada.

És sinònim de nivell 3, suport de back-end, la línia de suport 3, el suport d'alt nivell, i diverses altres denominacions que denoten els mètodes de solució de problemes a nivell d'experts i d'anàlisi avançat. Els individus assignats a aquest nivell, són experts en els seus camps i són responsables, no només per ajudar tant al personal de nivell 1 i 2, sinó també per a la investigació i desenvolupament de solucions als problemes nous o desconeguts. Els tècnics de Nivell 3 tenen la mateixa responsabilitat que els tècnics de nivell 2 en la revisió de l'ordre de treball i avaluar el temps ja complert amb el client perquè es doni prioritat a la gestió del temps.

4.6.3. Canals de recepció d'incidències

S'ha de tenir en compte que l'Ajuntament disposa d'una sèrie de serveis i canals que poden rebre o bé originar incidències relacionades amb la gestió d'accessos. Els actors que poden generar incidències són per tant:

- **Servei de monitorització:** Es tracta d'un primer nivell d'atenció i monitorització de sistemes amb sondes. En cas que es detecti un problema crític en el servei o algun dels seus components s'escalarà una incidència a aquest servei.
- **Servei d'atenció al usuari (SAU):** Primer nivell d'atenció a usuari, escalaran la incidència a aquest servei.
- **El propi servei d'operació de la gestió d'accessos:** El propi servei d'operació, dintre de les seves tasques de revisió d'indicadors clau o manteniment preventiu pot detectar incidències o comportaments erronis.

L'eina per a gestionar les incidències serà la que l'IMI determini en el moment oportú, HP/SM o Easyvista i en el cas que el servei d'incidents rebi incidències per altres canals (via telefònica o e-mail), les reflectirà en l'eina.

4.6.4. Informació estat de la incidència

En el servei incidental, l'adjudicatari es responsabilitza de donar feedback en tot moment tant del diagnòstic com sobre l'estat de la incidència a l'emissor de la mateixa, així com altres serveis que es poden veure afectats. El total d'incidències, estat i ANS es reportarà en els comitès corresponents tal i com s'explica en el punt 5.

4.6.5. Garantir la disponibilitat

El servei incidental ha d'atendre amb la màxima celeritat possible les incidències que provoquin una disrupció important o bé una aturada del servei. Aquest servei ha d'atendre i resoldre incidències segons el ANS que es detalla més endavant.

4.6.6. Correcció als defectes de programari o de dades

Quan sigui necessari modificar el programari o dades de la solució, l'adjudicatari s'encarregarà de:

- Aplicar les correccions necessàries al codi desenvolupat
- Provar la solució en els entorns pre productius (desenvolupament i pre producció)
- Fer les passes necessàries per distribuir la solució
- Documentar la solució aplicada

En cas que es tracti d'un problema de dades o que l'incident hagi provocat una corrupció de les mateixes, s'executaran totes les passes necessàries per restablir la consistència de les dades, incloent si fos necessari la recuperació de còpies de seguretat.

4.6.7. Modificacions dels components base

En cas que l'incident requereixi d'un evolutiu i/o el suport del fabricant per modificar qualsevol dels components base de la solució, l'adjudicatari escalarà aquesta situació al responsable del servei de l'IMI i gestionarà aquesta eventualitat fins la seva resolució, proposant els "workarounds" necessaris per pal·liar o minimitzar l'impacte de l'incident. Concretament l'adjudicatari gestionarà:

- Actualització de les versions del software base
- Solució d'incidents dels productes
- Seguiment de desenvolupaments (evolutius) que solucionin la incidència
- Suport in situ pel diagnòstic i, si fos necessari per garantir la disponibilitat, aquest suport es podrà prestar fora d'horari d'oficina.

4.6.8. Acord de nivell de servei (ANS)

La resolució d'incidències i el suport al SAU relacionades amb els serveis inclosos:

Serveis de la Plataforma GetAccess, Nebula (horaris no laborables) i OTP.
Addicionalment, la Operació del Producte Nebula en horaris no laborables.

Es farà segons els següents nivells de servei:

Resolució d'incidències	Temps de resposta	Temps de diagnòstic	Temps de resolució	Perfil mínim de suport assignat
Incidència crítica	2 hora	6 hores	10 hores	Analista funcional sènior
Incidència greu	4 hores	10 hores	24 hores	Analista funcional sènior
Incidència normal	6 hores	18 hores	40 hores	Analista funcional sènior

Tipus d'incidències:

- Incidència crítica: El sistema no funciona o una de les funcionalitats bàsiques no funciona. Implica una aturada en l'operativa normal de funcionament de l'aplicació.
- Incidència greu: El sistema o una de les seves funcionalitats té una anomalia important però no impedeix l'operativa normal de l'aplicació.
- Incidència normal: El sistema o una de les seves funcionalitats té una incidència normal

Franges de temps:

- Temps de resposta. És el temps transcorregut des que la incidència és comunicada a l'adjudicatari fins que un tècnic qualificat es posa en contacte amb el responsable de l'aplicació o la persona que es designi.
- Temps de diagnòstic. És el temps transcorregut des que la incidència és comunicada a l'adjudicatari fins que aquest fa un diagnòstic del problema.
- Temps de resolució. És el temps transcorregut des que la incidència és comunicada a l'adjudicatari fins que es considera tancada pel responsable de l'aplicació o la persona que es designi.

El temps de resposta, diagnòstic i resolució es compta sobre l'horari de 8:00 a 18:00 de dilluns a divendres. Notar que en el cas de les incidències, el temps de resposta és acumulatiu: és a dir, que tots els temps comencen a comptar des de l'inici de la comunicació de la incidència. En aquest cas, una millor resposta en un temps, dóna més marge en els temps de resposta posterior.

4.7. SERVEIS NO INCLOSOS

Els següents serveis estan exclosos de l'abast del projecte:

- L'adquisició de llicències de software.

4.8. ALTRES REQUISITS

4.8.1. Idioma

Obligatòriament l'adjudicatari desenvoluparà els sistemes i interfícies d'usuari externes en català.

Això inclou també la documentació de gestió i documentació tècnica requerida i lliurada durant l'execució del projecte. Aquesta documentació, com tota la que es generi durant el contracte, haurà de fer servir les plantilles proporcionades per l'IMI.

5. MODEL DE PRESTACIÓ DEL SERVEI

Amb caràcter general, l'IMI controlarà, mitjançant la figura d'un Cap de Servei, el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte.

La relació amb el client final (Ajuntament) la gestionarà l'IMI, i determinarà el model i figures que actuaran com interlocució i lligam entre l'IMI i l'organització interna del proveïdor. Aquest model de relació establirà les figures i determinarà les responsabilitats del responsable del contracte, i establirà responsables de blocs de serveis o agrupacions de serveis en base a la seva dimensió i/o funcionalitat que cobreixin, així com la responsabilitat de transformació del servei cap al model proposat.

5.1. MODEL DE RELACIÓ IMI/ADJUDICATARI

El model de relació defineix les funcions i responsabilitats del proveïdor i de l'IMI en un marc d'actuació comú, per assegurar el compliment de les obligacions de cadascuna de les parts. És un marc de relació que permet acordar el contingut i nivell de la prestació dels serveis, així com el seguiment de la prestació real en els aspectes estratègics, contractuals, tàctics i operatius.

L'adjudicatari pot ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb l'IMI, així com els mecanismes de control propis de cada servei i funció transversal. L'equip de treball dels proveïdors, haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les tasques assignades.

L'adjudicatari haurà de plantejar de forma explícita i el més exhaustiva possible un model de relació amb l'IMI, dissenyat de manera que s'asseguri el correcte acompliment de les seves funcions.

L'esmentat model de relació haurà de fer explícits els rols i responsabilitats del contracte, els nivells de relació i l'estructura i funcionament dels Comitès de relació i coordinació que siguin precisos per mantenir una interlocució permanent amb els actors involucrats en el procés.

Hi haurà d'haver, com a mínim, els **òrgans de govern** següents que s'indiquen a continuació:

- Comitè de direcció del servei
- Comitè de Seguiment operatiu del servei.

L'organització del servei haurà d'ajustar-se als requisits mínims que s'especifiquen als següents apartats.

5.1.1. Comitè de Direcció

L'Institut anomenarà un Comitè de Direcció que assumirà les funcions de supervisió de l'execució del contracte així com la presa de decisions que afectin a l'objectiu i abast del mateix, especialment per definir i encarregar tasques sota demanda de nous projectes o iniciatives no identificades inicialment. L'àmbit executiu és el nivell màxim de seguiment del contracte i la prestació del servei.

Aquest comitè farà un seguiment exhaustiu de l'execució dels serveis tecnològics i de negoci i del contracte. S'assegura el compliment dels mateixos de control global i s'elevaran a l'àmbit executiu aquells aspectes que puguin originar la modificació del contracte o contractes.

Aquest Comitè es reunirà mensualment, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

Aquest Comitè definirà les directius i assumirà els canvis de contractes o resoldrà conflictes contractuals:

- Revisar compromisos de serveis i visió global dels mateixos.

- Des d'aquest àmbit s'elevaran a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.
- Marcar les directius estratègiques.
- Visió holística i estratègica del servei: Indicar objectius del mes següent en relació als objectius globals, esdeveniments o activitats que es detecten que vindran, constraints (limitacions) repetitius i assoliments generals.
- Realitzar el seguiment tàctic de les activitats realitzades i l'assoliment d'objectius plantejats en el Pla de Seguretat del Servei.
- Gestionar i identificar de canvis o modificacions d'objectius o canvis d'abast, modificacions de contracte, condicions econòmiques.
- Definir el catàleg de Serveis.
- Proposta del règim sancionador.

El Comitè de Executiu estarà format com a mínim per les següents persones:

- Responsable de Seguretat
- Responsable del Contracte en l'IMI
- Responsable del contracte empresa adjudicatària

5.1.2. Comitè de Seguiment Operatiu

L'IMI anomenarà un Comitè de seguiment que s'encarregarà de la gestió del dia a dia de l'execució del contracte. També resoldrà les incidències i conflictes menors que apareguin al llarg de la vida d'aquest contracte.

Es reunirà quinzenalment.

El Comitè de Seguiment està format com a mínim pel responsable del contracte de l'empresa adjudicatària i el responsable del contracte per part de l'IMI. Quan calgui, es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip de projecte necessaris per a tractar en profunditat determinats temes. El responsable del contracte (empresa adjudicatària) és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Li correspon al comitè de seguiment les funcions de control de l'execució del contracte

- Validació de la feina
- Verificació operativa de l'acompliment del contracte
- La resolució dels conflictes que puguin sorgir en l'execució del contracte
- Detecció d'incompliments i escalat

L'IMI controlarà, mitjançant la figura d'un Responsable el contracte de l'IMI, el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte .

El Comitè de Executiu estarà format com a mínim per les següents persones:

- Responsable del Contracte en l'IMI.
- Responsable del Servei empresa adjudicatària.
- Opcionalment, responsable del Lloc de treball de les àrees operatives.

Cal que els licitadors detallin a les seves propostes quina és l'organització que proposen per a l'execució del contracte, tenint en compte que hauran de dotar el personal necessari per assegurar les funcions de governança que són objecte d'aquest contracte i permeti mantenir un model fluid amb els agents que participen en el procés.

5.2. SEGUIMENT DEL SERVEI

L'adjudicatari haurà de presentar un model de seguiment del servei exposat en el plec.

En això, serà obligatori convocar una reunió de Kick-off o llançament de servei amb els principals membres del projecte (Equip de l'adjudicatari i Equip de l'IMI).

L'adjudicatari proposarà indicadors clau per a poder fer seguiment de l'acompliment del contracte així com el model de compliment dels compromisos associats i una proposta esquemàtica de reporting dels mateixos pel seguiment, control i gestió del servei. El proveïdor però, s'ajustarà al model de l'IMI que determini poder fer el seguiment del bon funcionament del Servei contractat.

Els licitadors, juntament amb la proposta tècnica i dintre del plantejament general i tècnic del contracte que es demana al sobre B, hauran de presentar un plantejament previ d'aquest model de seguiment, tal com s'indica a la clàusula 8a del present plec. Es valorarà la proposta que millor garanteixi el bon funcionament del servei i que més s'ajusti a les maneres de treballar corporatives.

Obligatòriament l'adjudicatari haurà de presentar com a mínim en la temporalitat que s'especifica en cada apartat els següents **informes de comunicació i seguiment**:

Informe de feina en curs i prioritats establertes: (setmanal)

- Estat de cada una de les tasques o serveis que s'estan realitzant. Per cada una d'elles:
    - Estat actual.
    - Passos que s'han realitzat fins la data actual.
    - Passos pendents per tal de finalitzar-ho.
    - Detecció i proposta de resolució de problemes.
    - Revisió segons planificació i dates previstes d'execució.
- Tasques futures previstes.

Informe de seguiment de l'avenç: (mensual)

- Estat general de les tasques o serveis que s'estan realitzant:

- Estat actual.
- Passos que s'han realitzat fins la data actual.
- Passos pendents per tal de finalitzar-ho.
- Detecció i proposta de resolució de problemes.
- Revisió segons planificació i dates previstes d'execució.

- Tasques futures previstes.

Informe d'indicadors de seguretat:

- Registre de Seguretat (Peticions/Incidents)
- Temes a ressaltar que s'han produït durant el mes.
- Incidències rellevants produïdes. Indicar quines s'han registrar al registre d'incidències.
- Informe actuacions preventives realitzades.
- Riscos Vigents i Vulnerabilitats.

Tanmateix la composició dels informes es consensuarà amb l'IMI a l'inici del contracte i podrà variar durant la prestació del mateix en funció de les necessitats del gestor del contracte per part de l'IMI.

Les actes de totes les reunions hauran de ser elaborades per l'empresa adjudicatària seguint les plantilles proporcionades per l'IMI.

Es valorarà les propostes que millorin el contingut i estructura dels informes previstos en aquest apartat. I en especial les millores en l'accessibilitat a la informació i el quadre de comandament proposat.

5.3. PLA DE SERVEI

El servei es desplegarà seguint les següents fases:

5.3.1. Llançament del Servei

Es validaran amb la Direcció de l'IMI els assistents als comitès del servei i es planificaran els primers comitès.

Es realitzaran les tasques de comunicació interna i externa per informar del pla d'acció de l'oficina i dels actors que hi participaran en la Direcció de Qualitat i Seguretat.

5.3.2. Execució del Servei

Es realitzaran les tasques identificades en aquest plec d'acord amb els referents del contracte del Departament de Seguretat.

Es planificaran els comitès de seguiment del servei.

Es continuaran les accions de comunicació interna i externa per informar dels resultats del servei i per comunicar properes passes.

5.3.3. Resolució del Servei

Es definiran les tasques necessàries per realitzar el traspàs del servei exposat a l'IMI o al següent adjudicatari.

Es validarà amb la Direcció de l'IMI la transferència de coneixement dels lliurables, tasques i accions del servei.

Es realitzaran les tasques de comunicació interna i externa per informar dels resultats del servei.

5.3.4. Pla de devolució del servei

Li correspon a l'adjudicatari elaborar el Pla de devolució del servei sobre el coneixement del tasques d'operació i millora contínua. que s'han executat dins el contracte

En el Pla de devolució dels serveis s'hauran d'incloure totes les activitats de transferència del servei i del coneixement a l'IMI o a un tercer proveïdor, en els casos en el quals així es decideixi per part de la Direcció de l'IMI.

En cas de cessament o finalització del contracte, el proveïdor estarà obligat a tornar el control del serveis objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb la prestació del servei, sense cost addicional per l'IMI.

Tanmateix el Pla de devolució del servei haurà de complir com a mínim els següents principis i continguts:

- El termini d'execució serà de màxim un mes abans de la finalització del contracte.
- Inclourà la metodologia de transferència de coneixement dels aspectes fonamentals d'operació i, com a mínim, descriurà: - Suport al nou adjudicatari, formació i documentació sobre els procediments del servei.
- L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat per l'adjudicatari o l'IMI en la provisió del servei.
- La formació pràctica tutelada, en la qual el personal designat pel l'IMI realitzi els treballs propis de cada procés o funcionalitat tutelats pel personal de l'adjudicatari.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència l'IMI, o a terceres parts anomenades per aquest.
- L'adjudicatari assegurarà un correcte traspàs de tots els entregables, assegurant-ne la completesa i que estigui tot actualitzat.
- L'adjudicatari haurà d'oferir un pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, l'IMI i/o altres adjudicataris.

- Presentarà el pla de devolució del servei que millor aprofiti la feina implementada a les eines en us i menys disruptiu sigui per l'IMI.
- Durant el període de devolució del servei, l'adjudicatari ha de complir els acords de nivell de servei. El pla de devolució no ha de causar cap discontinuïtat en el servei.
- L'IMI no assumirà una dedicació significativa de recursos propis de l'Ajuntament en les activitats de devolució.
- S'establirà el pla per devolució de la migració de la informació de les eines emprades pel servei per tal de ser incorporades en el nou servei. El projecte definirà en el plec el pla i compromís de devolució.

El pla s'executarà dins el termini del contracte.

Els licitadors detallaran en la seva oferta un pla de devolució del servei, indicant les tasques que assegurin el tancament correctament, la qualitat dels lliurables finals, i de traspassar completament tota la informació a l'IMI. Aquest Pla es presentarà amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa i previsible de la seva realització material.

5.4. PLA DE QUALITAT

L'adjudicatari haurà de definir i documentar, durant el primer mes de la vigència del contracte, segons els punts que s'indiquen a continuació, un Pla de Qualitat específic que asseguri la qualitat dels serveis oferts.

El Pla de Qualitat inclourà tots els requisits definits en el present plec per part de l'IMI.

Els punts que s'indiquen a continuació seran els índexs que, com a mínim, ha d'emplenar l'adjudicatari:

- Cicle de Vida d'un servei:
  - Kick off
  - Checkpoints.
  - Rols responsables de cada tasca o activitat.
- Gestió de la Configuració: Assegurar que els canvis no afectin els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- Procediments que assegurin que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Gestió de la documentació i dels requeriments del servei.
- Regles i procediments que garanteixin la millora contínua del servei.
- Planificació de les auditories internes que asseguren l'adequada documentació dels resultats i accions dutes a terme.
- Mètriques i indicadors.

Els rols responsables de l'execució de les activitats detallades en el Pla de Qualitat, l'Assegurament de la Qualitat i Auditories internes han d'estar reflectits en l'apartat corresponent a recursos.

Els licitadors han de presentar aquest Pla de Qualitat en el conjunt de documentació tècnica que es detalla al punt "Proposta Tècnica", amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa.

6. RECURSOS HUMANS

Cal que els licitadors detallin a les seves propostes quina és l'organització que proposen per al contracte, tenint en compte que hauran de dotar al personal necessari per assegurar les funcions que són objecte d'aquest contracte i que permeti mantenir un model de relació fluid amb els agents que participen en el procés.

El contracte contempla, per les necessitats que requereix aquest servei, una dedicació del 30% del Cap de Servei, la dedicació plena del perfil de Consultor de CAAA i d'arquitecte d'identitats, una dedicació del 50% del Tècnic sènior especialista en evolutius i integracions i una dedicació del 60% del Tècnic de Nivell 3 (GETACCES i Nebula horaris no laborals).

Fet aquest aclariment, en l'oferta presentada s'indicarà, un compromís d'adscripció en cas de resultar adjudicatari dels recursos inclosos amb especificació de les dedicacions i condicions proposades.

L'adjudicatari haurà de presentar un detall exhaustiu de l'equip que proposarà amb els compromisos de l'oferta detallats amb la concreció i acreditació de l'experiència, certificacions i formació requerides en aquest apartat i que hagin estat proposades pel mateix.

No obstant això, l'IMI considera que **es necessiten com a mínim els següents perfils que es detallen a continuació**, i exigirà que aquests hi participin amb les dedicacions que s'expliciten:

Les prioritzacions del servei s'establiran dins del marc dels comitès del Servei (model de relació). S'estima necessària la implicació d'un equip de 2-3 persones considerant que una persona de perfil d'arquitecte d'identitats ha de tenir una dedicació específica i propera a l'IMI i amb dedicació quasi exclusiva (mínim 80% del temps setmanal) per tal de realitzar una bona gestió de totes les necessitats diàries del servei.

Els serveis de Suport Tècnic de Nivell 3 es tractaran com un servei i es deixa sota la decisió del contracte establir com vol gestionar el servei. Tot i això, en la presentació de l'oferta detallarà com planteja el servei i amb quina dedicació estimada.

- **Funcions per Perfil professional**

El proveïdor proposarà un equip de treball adequat per a l'execució dels serveis i n'assegurarà la seva estabilitat mentre estigui vigent el contracte. Al document de l'oferta s'indicaran de forma detallada els recursos inclosos. No obstant això, l'IMI considera que **es necessiten com a mínim els següents perfils, que es detallen a continuació**, i exigirà que aquests hi participin amb les dedicacions que s'expliciten:

6.1. FUNCIONS PER PERFIL

A continuació s'identifiquen i es descriuen els perfils a proporcionar per l'adjudicatari:

Perfil	Responsabilitat
Cap de Projecte / Responsable del servei	És el màxim responsable de dur el servei a bon port i actuarà com a punt de contacte i interlocutor únic. Per tant serà responsable de la gestió del servei en les condicions descrites en aquest plec, de la provisió en temps i qualitat dels serveis inclosos en aquest plec. Gestiona l'adequació dels recursos humans, i gestiona riscos, desviacions, peticions fora de l'abast inicial, etc. Les seves principals tasques són: • Controlar i gestionar els recursos del contracte. Acreditarà les skills necessàries per dur a terme tasques arquitectòniques en l'àmbit tècnic i de gestió. • Realitzar i actualitzar les tasques derivades del servei contractat. Especialment: grau d'avenç de les activitats del servei, calendari, riscos, desviacions, recursos i involucració dels participants. Centrarà la seva activitat en el control de terminis i costos dels projectes i vetllarà pel compliment dels projectes en Qualitat i Termini. • Interlocutor a alt nivell amb els responsables de l'IMI. • Definició del catàleg de serveis • Participació al Comitè Tècnic del Servei fent reporting de l'evolució del servei als responsables del servei de l'IMI. • Aplicació de les bones pràctiques en la gestió de serveis TIC • Monitorar mitjançant el pla del servei • Gestionar accions correctives a les incidències. • Gestionar els canvis. • Assegurament el compliment del Pla de Qualitat. • Elaboració de quadres de comandament. És important que tingui experiència dilatada en projectes de gestió d'identitats en organismes o empreses amb més de 10.000 identitats diferents.
Consultor/Arquitecte d'Accessos i Identitats	Les seves principals tasques són: • Establir directrius de seguretat de processos relacionats amb identitats i accessos (Normatives i guies d'estàndards d'identitats

	corporatives). Compliment ENS, LOPDGDD i Seguretat corporativa. • Vetllar pel model corporatiu d'identitats i accessos global (serveis de xarxa i serveis núvol dispositius, IOTs, drons, accessos remots, etc.) • Gestió i Coordinació d'Evolutius de les plataformes que donen suport al servei de identitats: Anàlisi d'impacte global de les problemàtiques diàries per definir solucions i aplicar-les. • Mantenir els processos d'identitats i accessos: cicle de vida de les identitats, credencials, organismes, recursos, Accessos remots, control d'externs, etc. • Disseny Tecnològic d'arquitectura d'identitats i accessos. • Participar en projectes per determinar requeriments per les Implementacions de Productes d'accessos o eines PAM per control de credencials i accessos d'administradors • Coordinació i orquestrador de les implementacions d'accessos en les àrees operatives. • Model d'Integracions amb plataformes corporatives (SAP, AD, OUD, BBDD,HPSM, etc.). • Assessoria i suport a projectes i serveis (Guia d'estàndards d'identitats). • Auditories tecnològiques i revisió dels processos i procediments. • Implantació de polítiques de credencials. • Model d'autoritzacions corporatiu. Rols i responsabilitats dels Sistemes d'informació. • Actuar com a punt de referència tecnològic per a la resta d'àrees de l'IMI.
Tècnic sènior especialista en evolutius i integracions	Haurà d'implementar integracions i processos en els diferents solucions de CAAA (Control d'accés (OAM), single sign on, Sistema d'autoritzacions, federacions d'identitats, clouds identity, Segon factor d'autenticació, accessos remots, Gestió d'identitats, etc) • Realitzar la presa de requisits, tot identificant els casos d'ús i el detall dels mateixos. • Participar en les tasques d'anàlisi i proposta d'alternatives. • Realitzar les proves funcionals del sistema. • Disseny d'interfícies d'usuari. • Disseny i realització les proves funcionals i d'acceptació del sistema.

	• Donar suport funcional als usuaris. • Definir els continguts dels cursos i validar el contingut de la documentació lliurada. • Implementar la proposta d'arquitectura del sistema d'acord amb les especificacions del projecte i l'arquitectura de referència de l'IMI. * Documentació i traspàs a producció.
Tècnic de Nivell 3 (GETACCES i Nebula horaris no laborals)	Les seves principals tasques són: • Gestió tècnica i operativa de la plataforma tecnològica. • Suport de tècnic resolució enfront incidències i problemes del servei. • Suport de Nivell 3 del servei de GetAcces i del Nebula/HSM (Nebula fora d'horaris laborals). • Suport de tècnic resolució enfront incidències i problemes amb PKI de Microsoft. • Suport tècnic en OTP (One Time Password).

L'IMI podrà sol·licitar en qualsevol moment a l'adjudicatari el llistat de persones que formen part de l'equip de projecte.

6.2. CARACTERÍSTIQUES PROFESSIONALS

El número de perfils mínims, així com la seva dedicació i l'experiència mínimes que s'estima per poder realitzar les tasques objecte del contracte seran les següents:

% Dedicació	Perfil	Experiència/Coneixements
15 %	**Cap de Projecte / Responsable del servei**	Titulació universitària (enginyeria, grau o llicenciatura) Certificacions: - Certificació ITIL (a partir de la versió 3) Experiència: - Almenys 3 anys d'experiència, dels quals al menys 3 anys (dels darrers cinc) implementant projectes d'Accessos i Identitats, degut a la complexitat tecnològica. - Experiència mínima en gestió de contractes TIC d'un valor total no inferior a 100.000,00 euros (en almenys un contracte), degut a la complexitat tecnològica.

75 %	**Consultor/Arquitecte d'Accessos i Identitats**	Experiència mínima de 3 anys fent tasques d'analista funcional/consultor i, com a mínim 3 anys en els següents àmbits d'actuació: • Gestió d'identitats • Control d'Accés • Sistemes d'autoritzacions • Credencials i segons factors d'autenticació.
75 %	**Tècnic sènior especialista en evolutius i integracions**	Experiència mínima de 3 anys, dels quant al menys 3 anys fent tasques d'analista funcional/consultor com a mínim en els següents àmbits d'actuació: • Gestió d'identitats • Control d'Accés • Sistemes d'autoritzacions • Credencials i segons factors d'autenticació. Disposar d'una de les següents certificacions: • Certificació Oracle Identity Governance Suite PS3 Certified Implementation Specialist. • Certificació Oracle Access Management Suite Plus 11g Implementation Specialist (o versió superior d'Oracle Access Management). En cas de què l'Ajuntament canviï l'OAM, el tècnic haurà d'adquirir els coneixements necessaris per a poder seguir donant servei.
40 %	**Tècnic de Nivell 3 (GETACCES i Nebula horaris no laborals)**	Experiència mínima de: • 3 anys fent tasques de suport tècnic de nivell 3 en tecnologies en serveis de gestió d'identitats i accessos. • Capacitat per a portar l'eina GetAccess (es valoraran certificacions). La capacitat es basa en tenir experiència amb haver portat eines de Controls d'accés i Single Sign On. • Capacitat per a portar l'eina Nebula (es valoraran certificacions). La capacitat es basa en tenir experiència en eines de certificats centralitzats. • Capacitat per a portar solucions de OTP. La capacitat es basa en tenir experiència en solucions implementades i desplegades de segons factor d'autenticació i seguretat adaptativa a nivell de suport tècnic.

Els licitadors, mitjançant una declaració responsable en la forma que s'indica en el plec de clàusules administratives particulars, acreditaran que disposen de l'equip de treball amb l'experiència professional exigida i amb coneixements dels entorns tecnològics requerits i que el posaran a disposició del contracte, en cas de resultar adjudicataris.

L'adjudicatari haurà d'acreditar que l'equip que s'adscrigui al contracte disposa dels coneixements anteriorment demanats dels entorns tecnològics mitjançant els certificats dels cursos exigits en el punt de capacitat, aptitud i solvència dels licitadors del document de clàusules administratives. És a dir, els certificats aportats per acreditar la solvència tècnica han d'estar expedits a les persones assignades a l'equip de treball de l'adjudicatari per aquest projecte.

L'IMI es reserva el dret de verificar les capacitats del personal que participa en el projecte en qualsevol moment i rebutjar-lo en cas que no compleixin amb els requisits exigits. Les despeses que es derivin com a conseqüència de canvis en l'equip de projecte aniran a càrrec de l'adjudicatari.

L'empresa adjudicatària haurà de mantenir l'equip de treball adscrit al contracte durant tota la vigència d'aquest. En cas que s'hagi de produir la substitució d'algun membre de l'equip, que no sigui per causes de força major, l'adjudicatari ho comunicarà a l'IMI i la substitució s'haurà de fer per un perfil que com a mínim tingui les mateixes característiques professionals i tècniques que les exigides en aquesta clàusula; en cas contrari i sense el consentiment de l'IMI aquest fet serà susceptible de sanció.

A més, en cas de substituir algun membre de l'equip de treball, s'exigirà el següent:

- La substitució d'una persona clau haurà d'estar consensuada amb l'IMI i s'haurà de comunicar amb un preavís de 15 dies naturals.

- Un període de formació, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.

- Un període de coexistència, d'un mínim de 15 dies, entre la persona que causa baixa i la persona que s'incorpora.

7. CONDICIONS D'EXECUCIÓ

A continuació es detallen les condicions d'execució del present contracte.

7.1. LLOC DE PRESTACIÓ DEL CONTRACTE

L'equip humà aportat per l'adjudicatari durà a terme els serveis des de les seves pròpies instal·lacions, però en qualsevol moment es pot requerir pel responsable del contracte de l'IMI que el servei s'executés en les dependències de l'IMI, en un màxim del 60% d'aquest contracte. En cas de ser necessari degut a força major (com en el cas actual de pandèmia), tots els serveis es portaran des de les instal·lacions de d'adjudicatari.

En les ocasions que ho requereixin, es podrà demanar el desplaçament a les oficines de l'IMI per a la prestació d'aquell servei que sigui necessari, essent obligació de l'adjudicatari l'aportació de les eines que siguin necessàries per a la prestació d'aquest.

Les reunions que es derivin d'aquest contracte, ja siguin comitès, reunions tècniques o d'usuaris es podran fer en qualsevol dependència municipal de la ciutat de Barcelona, tot i que es prioritzaran les oficines de l'Institut Municipal d'Informàtica.

7.2. HORARI DE PRESTACIÓ DEL SERVEI

L'adjudicatari haurà de cobrir els horaris de servei els dies laborables de 9:00h a 18:00h, excepte el tècnic de Nivell 3 de Nebula horaris no laborals, que treballarà fora de l'horari d'oficina, de tal manera que es doni un suport 24x7 a l'Ajuntament.

Pel cas de tasques d'implantació d'evolutius, l'horari és l'indicat a excepció de 25 hores anuals fora d'horari laboral per a donar suport a implementacions especials d'evolutius que requereixen de horaris especials o incidències.

Es consideren "dies laborables", els dies que siguin laborables a qualsevol dels centres de treball de l'IMI.

Per la gestió de peticions i canvis es considera l'horari de "dies laborables amb possibilitat d'execució fora d'horari laboral" qualsevol horari amb planificació prèvia consensuada amb l'IMI.

Si durant l'execució del contracte, l'IMI o l'adjudicatari detecten la necessitat de modificar l'horari de servei d'algun dels processos descrits en aquest plec, l'IMI i l'adjudicatari consensuaran de forma conjunta la modificació.

Les hores dedicades als serveis previstos en aquest contracte es prestaran en horari laboral de l'IMI, tot tenint en compte el calendari de festes de Catalunya i el municipi.

7.3. INFRAESTRUCTURA NECESSÀRIA PER LA PRESTACIÓ DEL SERVEI

El proveïdor haurà d'aportar medis logístics suficients per a la prestació del servei des de les seves instal·lacions.

La connexió amb l'IMI es podrà fer amb les següents alternatives:

- Mitjançant un enllaç dedicat amb algun dels operadors existents en el mercat. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol actuació necessària per a la posada en marxa de la connexió: esteses de fibra i electrònica addicional, manipulacions de connexions de fibra a la via pública, etc.
- A través d'una connexió al servei Macrolan o VPN de l'adjudicatari actual o del contracte del GIX municipal i amb una connexió d'ample de banda suficient per a garantir un adequat rendiment. L'enllaç a establir serà una connexió Ethernet amb separació i translació d'adreces

en el costat de l'adjudicatari. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol adquisició o actuació necessària per a la posada en marxa de la connexió. També serà al seu càrrec la quota mensual de la línia a contractar.

- Alternativament, mitjançat solució VPN (lan-to-lan, si son servidors) o VPN-Client si es per a usuaris remots, sobre l'accés a Internet existent a les dependències de l'IMI d'acord amb la normativa establerta per l'IMI per a l'accés remot als seus sistemes d'informació. És responsabilitat de l'adjudicatari la contractació i manteniment del seu accés a Internet així com disposar d'un equip que suporti aquest tipus de connexions i d'un ample de banda suficient en aquesta línia.

Si hi ha dificultats per a l'establiment d'aquest circuit, l'IMI es reserva el dret de comprovar, amb equips de la seva propietat, la causa del problema amb l'objectiu de determinar responsabilitats en la resolució de qualsevol incidència.

Sempre que hi hagi urgències o no s'hagi pogut establir la connectivitat el adjudicatari tindrà la responsabilitat de prestar el servei amb els mitjans que consideri oportuns, podent fer ús temporalment de zones de treball per a tal.

Per a realitzar les tasques de desenvolupament requerides caldrà realitzar la instal·lació d'un software a les estacions del client (aquest software està garantit sobre plataformes Windows). Aquest software permetrà accedir a unes màquines de desenvolupament remot que estaran a la seu del IMI. Igualment s'hauran de instal·lar uns certificats de persona per al correcte funcionament.

El firewall cal configurar-lo amb les opcions estàndard que indicarà l'IMI. L'accés a la màquina o màquines de desenvolupament assignades es farà mitjançant un o més noms DNS que l'IMI subministrarà. Per a la resolució d'aquests noms cap a una adreça IP també es facilitarà l'adreça d'un servidor DNS de l'IMI capaç de resoldre correctament els noms d'estació. És responsabilitat de l'adjudicatari configurar les estacions o els servidors DNS interns perquè les peticions puguin arribar fins als servidors de l'IMI.

Cada estació de desenvolupament només admet una connexió remota. És responsabilitat del client garantir que cada usuari utilitzi una màquina diferent de les que l'IMI els ha assignat.

Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

7.4. FACTURACIÓ

Els serveis es facturaran per mesos vençuts.

L'import a facturar de la part corresponen al servei regular serà el resultat de dividir el preu ofert per aquest servei per l'adjudicatari entre els 12 mesos del contracte, amb excepció de la primera i darrera factura si el contracte no ha estat formalitzat el primer dia del mes. En aquest cas, el primer i últim termini de facturació contindrà l'import corresponent des del primer dia de servei del contracte fins al darrer dia de servei del mes en curs.

Només es facturaran els mesos de servei realment prestats.

A cada factura es farà constar la relació de serveis realitzats dintre del període concret de facturació.

7.5. PERÍODE DE GARANTIA

L'adjudicatari es responsabilitzarà dels serveis prestats i donarà servei de garantia durant un període mínim de sis mesos posteriors a la seva implantació en l'entorn de producció. Durant aquest període l'adjudicatari estarà obligat a resoldre les anomalies detectades imputables a l'adjudicatari.

Aquesta garantia inclourà la correcció d'errors detectats posteriorment per mal funcionament o perquè no s'han cobert les funcionalitats requerides, que es posin de manifest en el funcionament de les aplicacions o que es descobreixin posteriorment, així com la correcció de la que tingui deficiències.

Els productes lliurats com a conseqüència de la correcció d'errors, es faran de conformitat amb el present plec, i per tant gaudiran d'un nou període de garantia.

La resolució d'incidències relacionades amb la garantia, corresponents al suport tècnic de nivell 3 i operació de plataformes (Serveis de la Plataforma GetAccess, Nebula (horaris no laborables) i OTP; addicionalment, l'Operació del Producte Nebula en horaris no laborables), es farà segons els nivells de servei indicats a l'apartat 4.6.8 del present plec.

8. PROPOSTA TÈCNICA

Els licitadors presentaran la seva oferta tècnica de realització del contracte tant per fer comprensible la seva proposta com per facilitar i fer possible la seva valoració d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen per aquesta contractació.

El licitador haurà de presentar la seva oferta en format electrònic, on tots els arxius han d'estar signats digitalment cadascun d'ells i en format Word, Excel, Power Point, MSProject o Acrobat de conformitat amb l'establert al plec de clàusules administratives particulars.

El licitador pot adjuntar tota la informació complementària que consideri d'interès, tot i això haurà de presentar uns continguts mínims i estar obligatòriament estructurada de la forma següent:

Es presentaran dos sobres electrònics, el **sobre B** on s'inclourà la documentació tècnica i aquella que haurà de ser valorada segons els criteris de judici de valor assenyalats en les clàusules del plec de clàusules administratives particulars, i el **sobre C** que haurà de contenir la oferta econòmica i la resta de documentació que haurà de ser valorada segons els criteris avaluables de forma automàtica assenyalats en les clàusules del plec de clàusules administratives particulars que regeixen per aquesta contractació.

A cada sobre s'ha d'incorporar una relació, en arxiu independent, dels documents que hi conté ordenats numèricament, especialment en el **sobre B** ja que aquest ha de respondre a les explicacions i compromisos sobre tots i cadascun dels criteris de valoració subjectius definits.

En el sobre B s'inclourà la documentació següent **indexada de manera que faciliti la seva localització**. Per a cada apartat i entre parèntesi s'ha indicat el nombre màxim de pàgines de què pot constar i amb tipus de lletra **Arial o Times New Roman, grandària 12 i interlineat simple**.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines per document.

- **Resum executiu** (màxim 3 pàgines)

  Resum per a la direcció dels continguts més significatius de la proposta del projecte, destacant-ne els recursos i les propostes de valor afegit.
- **Plantejament general i tècnic del contracte (màxim 10 pàgines)**

  En aquesta secció el licitant ha d'exposar el seu enteniment del servei i les línies principals de la seva estratègia per afrontar-lo tenint en compte els requeriments exposats en el plec de prescripcions tècniques. El licitador presentarà els diagrames i esquemes que cregui necessaris i que ajudin a visualitzar el grau de comprensió de la solució.
- **Model d'estratègia i definició dels models del Govern de les Identitats i Accessos** (màxim 10 pàgines)

  En aquesta secció el licitant ha d'exposar l'estratègia proposada a l'organització en la definició del Govern de les Identitats i Accessos. Ha de ser de tal manera que minimitzi els riscos en matèria de ciberseguretat.
- **Proposta d'evolutius** (màxim 5 pàgines)

  En aquesta secció el licitant ha d'exposar com gestionarà els evolutius que se'ls demanin i que minimitzi els riscos emergents de ciberseguretat.
- **Proposta d'arquitectura d'identitats i accessos** (màxim 5 pàgines)

  En aquesta secció el licitant ha d'exposar la seva proposta d'arquitectura d'identitats i accessos. L'arquitectura ha de ser el màxim compatible amb l'actual de l'organització.
- **Informes de govern del servei CAAA** (màxim 5 pàgines)

  En aquesta secció el licitant ha d'exposar els informes de govern del servei CAAA d'una manera clara, indicant la periodicitat, el seu públic objectiu i la interacció entre ells per al govern del servei. Els informes han de ser el més automatitzats possibles i han d'aportar un gran valor per a poder governar el servei CAAA.
- **Model de seguiment del servei CAAA** (màxim 5 pàgines)

  En aquest document licitadors han de documentar un plantejament previ de com es farà el seguiment del servei. Un cop adjudicat el contracte, l'adjudicatari haurà de presentar un document de manera definitiva i amb totes les garanties segons s'estableix a l'apartat 5.2 Seguiment del servei.

- **Pla de Qualitat** (màxim 5 pàgines)

  En aquesta secció el licitant ha de proposar una descripció d'alt nivell dels punts descrits en l'apartat corresponent del present plec per als serveis prestats en l'ordre exposat en el present plec.

- **Pla de Devolució del Servei** (màxim 5 pàgines)

  El Pla de Devolució del Servei ha de detallar correctament la transferència de coneixement dels treballs previstos en el contracte en la hipòtesi de canvi d'operador a la finalització d'aquest contracte o de les seves pròrrogues. És important que es detalli el % de dedicació de cadascun dels perfils en funció del pressupost del contracte.

En el sobre C s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.

9. CLÀUSULES GENERALS DE SEGURETAT

9.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU

L'IMI ha adoptat com a marc de referència per a la Seguretat dels Sistemes d'Informació el conjunt de bones pràctiques internacionalment reconegudes que desenvolupa la norma ISO-27002:2013.

L'IMI, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven de la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia de Drets Digitals, de la Llei 39/2015 en tot allò que fa referència a l'accés dels ciutadans als serveis públics, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 3/2010 de 8 de gener pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel què fa referència a la protecció de dades de caràcter personal.

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i IMI indistintament. De conformitat als seus estatuts s'ha d'entendre que l'IMI actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les que no sigui directament titular.

9.2. RESPONSABLE DE SEGURETAT

L'adjudicatari nomenarà un Responsable de Seguretat, el qual haurà de vetllar pel compliment dels següents requeriments:

- Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.
- Garantir que tots els serveis prestats pel proveïdor a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per l'IMI i seguint la normativa de seguretat vigent.
- Garantir i liderar dins la seva organització la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives i jurídiques), així com les directrius en matèria de seguretat establertes per l'IMI.
- Assegurar que tot el personal de l'adjudicatari que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.
- Informar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en les polítiques i instruccions de l'Administració Municipal en cas que els sigui d'aplicació i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.
- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

9.3. CONFIDENCIALITAT

L'adjudicatari s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Ajuntament.

L'adjudicatari queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Ajuntament, així com qualsevol altre producte obtingut com a resultat del present contracte.

9.4. CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT

L'empresa contractada, disposarà del programari necessari i farà servir la metodologia implantada pel Institut Municipal d'Informàtica (IMI) per al desenvolupament dels serveis contractats.

Si l'Administració Municipal ho considera necessari, es podrà instal·lar programari en els equips de l'empresa contractada, sempre sota la responsabilitat de l'empresa contractada, amb la finalitat d'obtenir una correcta prestació dels serveis contractats. Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

L'Administració Municipal continuarà essent la propietària o, en el seu cas, titular dels drets de propietat intel·lectual que el corresponen sobre el programari i bases de dades instal·lat en les màquines de l'empresa contractada, sense que la corresponent llicència d'ús suposi transferència o cessió, total o parcial de la titularitat, ni autorització per la seva utilització amb una finalitat diferent a la definida en el contracte de prestació de serveis.

L'empresa contractada donarà a conèixer a tot el personal adscrit a la prestació dels serveis, el contingut d'aquesta clàusula respecte al programari, sistemes operatius i bases de dades cedides per l'Administració Municipal, la seva obligació respecte a:

- No reproduir-los.
- No transmetre'ls a un altre sistema.
- No modificar, adaptar, cedir, ni realitzar qualsevol altre activitat sobre el programari cedit, sense l'autorització de l'Administració Municipal.
- No divulgar, publicar, ni posar a disposició d'altres persones diferents a les autoritzades.
- Fer ús única i exclusivament per les tasques encomanades, incloses en els serveis contractats.

La utilització de la metodologia a utilitzar per al desenvolupament i que està inclosa en el punt 7 del present plec.

9.5. AUDITORIA

L'IMI auditarà que l'adjudicatari vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

- Auditoria de seguretat periòdica/planificada: l'IMI podrà realitzar auditories de seguretat planificades per verificar el compliment dels requeriments de seguretat, de l'oferta de l'adjudicatari.

- Auditoria sobrevinguda: addicionalment l'IMI podrà efectuar més auditories que les planificades respecte el servei que s'està prestant.

En tots aquells casos en què l'IMI decideixi la realització d'una auditoria des de les instal·lacions de l'adjudicatari, aquest haurà de garantir a l'IMI l'accés necessari, incondicional i irrevocable als documents existents que estiguin relacionats amb l'abast de l'auditoria.

L'adjudicatari proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per l'IMI.

La realització de l'auditoria en cap moment eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis.

A la finalització de l'auditoria, es revisaran els resultats i s'elaborarà un pla d'acció per corregir les desviacions i/o observacions detectades. El conjunt del resultat serà signat per ambdues parts.

L'adjudicatari, d'acord amb el calendari establert al pla d'acció, es compromet a portar a terme les activitats establertes en el pla d'acció. L'IMI podrà verificar que el pla d'acció s'ha implementat correctament.

9.6. GESTIÓ D'INCIDENTS

L'adjudicatari informarà a l'IMI-Seguretat de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per l'IMI.

L'adjudicatari col·laborarà amb l'IMI-Seguretat en la resolució de qualsevol incident produït en el seu entorn, proporcionant totes les evidències requerides.

9.7. CONFIDENCIALITAT

L'adjudicatari s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Ajuntament.

L'adjudicatari queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir

l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Ajuntament, així com qualsevol altre producte obtingut com a resultat del present contracte.

9.8. DIMENSIONAMENT/GESTIÓ DE CAPACITATS

El proveïdor disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada.

9.9. ACCÉS A LA INFORMACIÓ

Si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, o si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, l'adjudicatari té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per l'IMI.

9.10. ANÀLISIS FORENSES

L'execució d'anàlisis forenses és responsabilitat exclusiva de l'IMI-Seguretat. L'adjudicatari haurà de col·laborar proporcionant la informació requerida i el coneixements de les plataformes i tecnològics que facin falta. Les peticions de col·laboració es realitzaran a través dels procediments que s'acordin entre IMI-Seguretat i el Proveïdor.

9.11. CONTROL D'ACCÉS

9.11.1. Accés local

L'adjudicatari haurà de protegir les estacions de treball i es compromet a complir les següents condicions:

- La informació revelada a qui intenta accedir ha de ser la mínima imprescindible. Els diàlegs d'accés proporcionaran únicament la informació indispensable.
- El nombre d'intents permesos serà limitat, bloquejant l'oportunitat d'accés una vegada efectuats un cert nombre de fallades consecutives.
- Es registraran els accessos amb èxit, i els fallits.
- El sistema informarà a l'usuari de les seves obligacions immediatament després d'obtenir l'accés.
- S'informarà a l'usuari de l'últim accés efectuat amb la seva identitat.

9.11.2. Accés remot

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Ajuntament, sent els costos de connexió a càrrec de l'empresa adjudicatària.

La connexió remota als sistemes de l'Ajuntament es realitzarà seguint els protocols establerts per l'IMI per als sistemes de l'Ajuntament.

9.12. GESTIÓ DEL PERSONAL

9.12.1. Deures i obligacions del personal

El Cap de Projecte de l'empresa adjudicatària durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.

L'empresa adjudicatària està obligada a implantar i donar a conèixer al seu personal els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat, integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

El Cap de Projecte de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte i formar al seu personal en la política i instruccions de l'Ajuntament que els sigui d'aplicació.

El Cap de Projecte haurà d'informar a tothom que presti serveis dins del marc del contracte, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat de la informació i protecció de dades de caràcter personal, especificant les mesures disciplinàries al fet que pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El Cap de Projecte de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Ajuntament, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al Cap de Projecte de l'Ajuntament, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

Es contemplarà el deure de confidencialitat respecte de les dades a les que tingui accés, tant durant el període de duració del contracte, com posteriorment a la seva terminació.

L'empresa adjudicatària haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

9.12.2. Formació i conscienciació

L'adjudicatari realitzarà les accions necessàries per conscienciar regularment al personal sobre el seu paper i responsabilitat respecte a la seguretat dels sistemes. Es recordarà regularment:

- Instrucció sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona.
- Normativa de seguretat relativa al bon ús dels sistemes.
- Normativa d'identificació i comunicació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat.

L'adjudicatari haurà de formar regularment al personal en aquelles matèries que requereixin per a l'acompliment de les seves funcions, en particular en relació a configuració de sistemes, detecció i reacció a incidents, i gestió de la informació i dades personals en qualsevol tipus de suport.

L'Ajuntament podrà demanar evidències de les diferents accions de formació i conscienciació que l'adjudicatari ha realitzat sobre el personal assignat a l'execució del contracte.

9.13. CLÀUSULA DE COMUNICACIONS EXTERNES

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'adjudicatari serà el responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús del certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

9.14. PROTECCIÓ DEL LLOC DE TREBALL

9.14.1. Lloc de treball buit

L'adjudicatari haurà d'establir una política de "taules netes" respecte a la documentació de l'Ajuntament. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

El material haurà de quedar guardat en un espai tancat quan no s'estigui utilitzant.

9.14.2. Bloqueig del lloc de treball

L'adjudicatari garantirà que els seus equips es bloquejaran al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de l'usuari per reprendre l'activitat.

9.14.3. Protecció d'equips

L'adjudicatari es compromet a que els equips que surtin, o puguin sortir de l'empresa adjudicatària, estaran protegits adequadament contra accessos no autoritzats en cas de pèrdua o robatori.

Sense perjudici de les mesures generals que els afectin, es requereix a l'adjudicatari que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Els usuaris hauran de disposar d'un canal de de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a l'IMI.

S'evitarà, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que habilitin un accés a altres equips de l'organització, o unes altres de naturalesa anàloga.

Addicionalment, els equips hauran de disposar:

- Solució antivirus actualitzada a la última versió i configurada per a que realitzi anàlisis regulars de l'equip.
- Política d'actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant aquelles actualitzacions crítiques.
- *Firewall* habilitat restringint el tràfic entrant a l'equip al mínim necessari.

9.14.4. Medis alternatius

L'adjudicatari garantirà l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius hauran d'estar subjectes a les mateixes garanties de protecció. Igualment, s'haurà d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

9.15. PROTECCIÓ DELS SUPORTS INFORMÀTICS

L'adjudicatari haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

9.15.1. Etiquetat

L'adjudicatari es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

9.15.2. Criptografia

Qualsevol informació corporativa que requereixi ser xifrada a la seva ubicació d'emmagatzemament, en particular a tots els dispositius extraïbles del tipus CD, DVD, discos USB, o uns altres de naturalesa anàloga, han de seguir els estàndards de seguretat, custòdia i protecció de les claus establerts per IMI-Seguretat.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'adjudicatari haurà de presentar-les per ser validades per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

9.15.3. Transport

L'adjudicatari garantirà que els dispositius romanen baix control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'adjudicatari garantirà que es segueix el procediment de transport, de manera que s'haurà de disposar d'un registre de sortida que identifiqui al transportista que rep el suport per al seu trasllat i d'un registre d'entrada que identifiqui al transportista que el lliura, conjuntament amb un procediment rutinari que quadri les sortides amb les arribades i elevi les alarmes pertinents quan es detecti algun incident.

9.15.4. Esborrat i destrucció

L'adjudicatari haurà de seguir els estàndards i normes de l'IMI respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut. S'hauran de destruir de forma segura els suports en cas de que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, fent us dels productes certificats per l'IMI.

9.16. PROTECCIÓ DE LA INFORMACIÓ

9.16.1. Neteja de documents

L'adjudicatari disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura serà especialment rellevant quan el document es difongui àmpliament, com quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

9.16.2. Protecció del correu electrònic

En el cas de que l'adjudicatari faci ús del seu correu electrònic corporatiu per gestionar informació de l'Ajuntament, l'haurà protegir enfront d'amenaces que li són pròpies:

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'adjudicatari.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:
    - Correu no sol·licitat (*spam*)
    - Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
    - Codi mòbil de tipus *applet*.

L'adjudicatari establirà polítiques d'ús del correu electrònic que inclourà com a mínim:

- Limitacions a l'ús com a suport de comunicacions privades.
- Realitzar activitats de conscienciació i formació relatives a l'ús del correu electrònic per al seu personal, per exemple per detectar casos de *malware* o *phishing*.

Si l'Ajuntament considera que la informació tractada pel contracte és prou sensible, facilitarà a l'adjudicatari un correu electrònic de l'Ajuntament el qual es convertirà en la via de comunicació entre l'adjudicatari i l'Ajuntament.

9.17. PROTECCIÓ DE LES INSTAL·LACIONS

Les instal·lacions de l'adjudicatari hauran de disposar de certes condicions de seguretat física:

-
- En cas de emmagatzemar informació de l'Ajuntament de Barcelona, disposar de les mesures de seguretat pertinents per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació.

- Garantir que la informació de l'Ajuntament de Barcelona no pugui ser visible i/o audible des de l'exterior de les instal·lacions.

9.18. GESTIÓ D'EXCEPCIONS

Qualsevol excepció als anteriors apartats no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials a IMI-Seguretat per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

Aquestes clàusules tenen per objecte establir requeriments sobre aquells projectes on **l'administració del sistema** es trobi dintre del seu abast.

9.19. GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuaris, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants.

L'empresa proveïdora haurà de validar i revisar accessos dels usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades. Els comptes d'usuari estaran integrats amb l'eina que l'IMI posa a disposició.

Autenticació interna

Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el repositori central per a l'autenticació dels usuaris. La solució d'autenticació corporativa utilitzada per l'IMI és l'Oracle Access Manager (OAM) que proveeix el Single Sign On corporatiu.

La integració amb l'OAM es podrà fer mitjançant les següents opcions:

- Integració mitjançant capçaleres.
- Integració mitjançant l'estàndard SAML 2.0.
- Integració mitjançant l'estàndard OAuth 2.0.

Autenticació externa

Els usuaris externs (fora de l'àmbit municipal, empreses i altres persones físiques - clients de l'aplicatiu) hauran d'autenticar-se mitjançant la solució corporativa (Mòdul Comú d'Autenticació).

9.20. AUTORITZACIÓ DELS USUARIS ALS SISTEMES

L'IMI disposa d'un mecanisme d'autorització d'usuaris corporatiu basat en el producte Oracle Unified Directory (OUD). L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en el repositori central d'autorització (OUD).

En cas que l'adjudicatari no pugui delegar l'autorització per impediments greus del sistema, com a mínim, hauran d'integrar-se amb GID (eina de gestió d'identitats corporativa basada en Oracle Identity Manager) per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els funcionals definits a GID (capa de negoci).

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats. El temps dedicat normalment a integrar un connector estàndard amb una BBDD Oracle és aproximadament 80 hores d'un tècnic.

Perfilat d'usuaris

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i per IMI-Seguretat.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
- Mínim privilegi, els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir les seves obligacions.
- Necessitat de Conèixer, els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.
- Capacitat d'autorització, només i exclusivament el personal amb competència d'autorització, podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.

La gestió de permisos haurà de ser en base a perfils i rols, podent un usuari tenir múltiples perfils. Els usuaris només podran accedir a aquelles funcions que tinguin expressament autoritzades. La implementació ha de permetre la implementació de matrius de segregació de funcions i l'agilitat en l'administració d'aquests permisos.

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant perfils (rols) de seguretat. Entenent com a perfil o rol una entitat que dona accés a una sèrie d'operacions.

Sota la premissa d'aquests criteris generals, l'adjudicatari haurà de dissenyar el joc de permisos i autoritzacions requerits pels sistemes d'informació implementats, en base al document 'Pla d'Autoritzacions'. Aquest document serà revisat i actualitzat per l'adjudicatari per incloure nous punts a tractar o adaptacions dels punts existents.

9.21. CONTROL D'ACCÉS

9.21.1. Segregació de funcions i tasques

L'adjudicatari s'encarregarà de que el sistema de control d'accés s'organitzi de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.

En concret, se separaran almenys les següents funcions:

- Desenvolupament d'operació. Garantint, com a mínim, que els desenvolupadors únicament disposin d'accés a l'entorn de preproducció i desenvolupament. La configuració dels entorns productius l'haurà de realitzar persones o equips diferents.
- Configuració i manteniment del sistema d'operació.
- Auditoria o supervisió de qualsevol altra funció.

9.22. INVENTARI D'ACTIUS

L'adjudicatari haurà de mantenir un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa i identificant al seu responsable; és a dir, la persona que és responsable de les decisions relatives al mateix.

9.23. CONFIGURACIÓ DE SEGURETAT

L'adjudicatari haurà de configurar els equips prèviament a la seva entrada en operació, de manera que:

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
    - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.
    - No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
    - S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.
- S'aplicarà la regla de "seguretat per defecte":

- Les mesures de seguretat seran respectuoses amb l'usuari i protegiran a aquest, tret que s'exposi conscientment a un risc.
- Per reduir la seguretat, l'usuari ha de realitzar accions conscients.
- L'ús natural, en els casos que l'usuari no ha consultat el manual, serà un ús segur.

9.24. MANTENIMENT

L'adjudicatari haurà de mantenir l'equipament físic i lògic que constitueix el sistema, per això tindrà que aplicar el següent:

- S'atendrà a les especificacions dels fabricants quant a instal·lació i manteniment dels sistemes.
- S'efectuarà un seguiment continu dels anuncis de defectes.
- Es disposarà d'un procediment per analitzar, prioritzar i determinar quan aplicar les actualitzacions de seguretat, pegats, millores i noves versions. La priorització tindrà en compte la variació del risc en funció de l'aplicació o no de l'actualització.

9.25. XIFRATGE DE DADES

Qualsevol informació corporativa que requereixi ser xifrada en la seva ubicació d'emmagatzemament (i per tant, queda exclòs l'encriptació per transit en les comunicacions) ha de seguir els estàndards de seguretat i la custòdia i protecció de les claus estableix IMI-Seguretat. IMI-Seguretat ha de assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. IMI-Seguretat custodiarà les claus de xifratge.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser validades per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

9.26. SIGNATURA ELECTRÒNICA

Qualsevol requeriment de signatures digitals que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser valides per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

Per la signatura electrònica s'empraran els mecanismes aprovats per l'IMI, en cas que hagin de ser uns altres, s'haurà de justificar, documentar tècnicament i haurà d'estar validat per IMI-Seguretat. En tot cas s'ha de complir la política de signatura electrònica de l'ajuntament de Barcelona.

9.27. CERTIFICATS

L'IMI-Seguretat serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de l'IMI-Seguretat. S'entén per certificats digitals corporatius: els de servidor segur, els d'aplicatiu per autenticació o signatura digital, de signatura de codi, de xifratge, etc.

Tots els certificats hauran de ser sol·licitats a través del procediment establert en l'IMI-Seguretat per al seu control i gestió.

El proveïdor haurà de seguir l'estàndard establert per la protecció i custòdia dels certificats digitals a l'hora d'incorporar el certificat pel seu ús.

9.28. ANTIMALWARE

L'adjudicatari serà responsable de la instal·lació i actualització de programes de protecció antimalware de les màquines que suporten serveis de l'IMI segons es recull al marc normatiu del l'IMI.

L'IMI obtindrà indicadors de la bona gestió de proteccions antimalware i en qualsevol moment tindrà accés i visió de l'estat de la seguretat global de les proteccions.

L'IMI seguretat tindrà accés en consulta a la consola de gestió d'aquests programaris del proveïdor.

9.29. EXPLOTACIÓ

9.29.1. Gestió de la configuració

L'adjudicatari s'encarregarà de gestionar de forma continua la configuració dels components del sistema de manera que:

- Es mantingui a tot moment la regla de "funcionalitat mínima".
- Es mantingui a tot moment la regla de "seguretat per defecte".
- El sistema s'adapti a les noves necessitats, prèviament autoritzades.
- El sistema reaccioni a vulnerabilitats reportades.
- El sistema reaccioni a incidents.

9.29.2. Gestió de canvis

L'adjudicatari s'encarregarà de mantenir un control continu de canvis realitzats en el sistema, de manera que:

- Tots els canvis anunciats pel fabricant o proveïdor seran analitzats per determinar la seva conveniència per ser incorporats, o no.

- Abans de posar en producció una nova versió o una versió amb un pegat, es comprovarà en un equip que no estigui en producció, que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per al treball diari. L'equip de proves serà equivalent al de producció en els aspectes que es comproven.
- Els canvis es planificaran per reduir l'impacte sobre la prestació dels serveis afectats.
- Mitjançant anàlisi de riscos es determinarà si els canvis són rellevants per a la seguretat del sistema. Aquells canvis que impliquin una situació de risc de nivell alt seran aprovats explícitament de forma prèvia a la seva implantació.

9.29.3. Protecció de claus criptogràfiques

- L'adjudicatari utilitzarà programes avaluats o dispositius criptogràfics certificats.
- S'empraran algoritmes acreditats pel "Centro Criptológico Nacional".

9.30. PROTECCIÓ DELS SERVEIS

9.30.1. Protecció enfront de la denegació de servei

L'adjudicatari establirà mesures preventives i reactives enfront d'atacs de denegació de servei (DoS Denial of Service). Per a això:

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.
- Es desplegaran tecnologies per prevenir els atacs coneguts.

9.31. DIMENSIONAMENT/GESTIÓ DE CAPACITATS

El proveïdor disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada.

9.32. CÒPIES DE SEGURETAT

L'adjudicatari serà responsable de realitzar còpies de seguretat als sistemes dels quals és administrador per tal de poder recuperar les dades en cas de pèrdua accidental o intencionada. La freqüència de les còpies de seguretat vindrà donada pel nivell de sensibilitat de les dades que conté, segons el recollit a les guies de l'IMI.

El nivell de seguretat d'aquestes dades ha de ser un reflex del de les dades originals a tots els nivells (integritat, confidencialitat, autenticitat y traçabilitat). Per tal de garantir la confidencialitat, l'IMI es reserva el dret de demanar el xifrat de les dades. L'abast de les còpies inclou:

- Informació de treball de l'IMI.
- Aplicacions en explotació, incloent els sistemes operatius.
- Dades de configuració, serveis, aplicacions, equips o d'altres anàlegs.
- Claus emprades per conservar la confidencialitat de la informació.

9.33. PROTECCIÓ DE LES APLICACIONS I SERVEIS WEB

L'adjudicatari garantirà que els subsistemes dedicats a la publicació de la informació hauran de ser protegits front a les amenaces que li siguin pròpies:

- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
    - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
    - Es previndran atacs de manipulació de URL.
    - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pagina web a traves del seu navegador, a petició del servidor de la pagina, conegut en la terminologia anglesa com a "cookies".
    - Es previndran atacs d'injecció de codi.
- Es previndran intents d'escalat de privilegis.
- Es previndran atacs de "cross site scripting".
- Es faran servir certificats d'autentificació de llocs web d'acord amb les polítiques establertes per IMI-Seguretat.

9.34. ACCEPTACIÓ I POSTA EN SERVEI

L'adjudicatari ha de comprovar el correcte funcionament de l'aplicació, per tal de garantir que:

- Es compleixen els criteris d'acceptació en la matèria de seguretat.
- No es deteriora la seguretat d'altres components del servei.

Addicionalment per al nivell mitjà, l'adjudicatari realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisis de vulnerabilitats.

- Test de penetració.

9.35. DADES DE PROVES

L'adjudicatari es compromet a assumir tota la responsabilitat en la creació de dades de proves per testejar els serveis. En cap cas s'utilitzaran dades de l'entorn de producció per fer proves.

En cas que sigui necessari copiar dades de l'entorn productiu, aquestes seran les mínimes necessàries i hauran de ser sotmeses a un procés d'ofuscació. L'adjudicatari es farà càrrec del desenvolupament dels procediments de tractament de dades (ofuscació, truncament, etc.) en cas que fossin necessaris.

Tota manipulació de dades de l'entorn de producció haurà de ser informada i aprovada pel propietari de les mateixes.

En cas que s'hagi de realitzar una migració de dades entre sistemes, l'adjudicatari haurà de presentar un pla de migració de les dades on es detallin les operacions necessàries.

Aquest pla de migració s'adequarà al procediment establert per seguretat per tal de minimitzar l'exposició de les dades productives.

9.36. PLA DE TRACES

Les aplicacions o productes que permeten realitzar operacions sobre les dades de negoci han de proporcionar informació sobre les accions i accessos realitzats en aquesta informació. Tant la criticitat de les dades i els criteris del negoci, com els requeriments legals marcaran la informació que cal recollir i el temps de retenció dels logs.

L'adjudicatari haurà de configurar el sistema per recollir les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició l'IMI a l'inici del contracte. Dins d'aquest registre, s'ha d'incloure:

- Qui realitza l'activitat (tant usuaris com operadors i administradors en especial), quan i el sistema en qüestió.
- Registre d'activitats realitzades amb èxit i les rebutjades.
- Les activitats concretes subjectes a ésser registrades vindran determinades per l'anàlisi de riscos del sistema.

Un cop configurades les traces s'hauran d'incorporar en els documents estàndards de seguretat: 'Pla mestre de Traces' (on s'avaluen els requeriments de les traces, el disseny i es determina l'inventari de traces necessàries) en la fase d'anàlisi i el document 'Pla de Traces' (on s'aporten detalls i mostres de cadascuna de les traces) en fase de proves i/o pas a producció

Aquest plec de prescripcions tècniques ha estat emès per la Sra. Neus Bellavista Arimany, tècnica responsable del contracte, adscrita a la Direcció de Qualitat i Seguretat de l'IMI, amb el vistiplau de,

Sra. Ana Bastida Vilà
Directora de Qualitat i Seguretat de l'IMI

10.ANNEX 1: PLATAFORMA TECNOLÒGICA GIA

Els components tecnològics que forma part de l'abast d'aquest plec són tots els components de la Plataforma tecnològica amb l'excepció de la Gestió d'Identitats (OIM):

Gestor Accessos (Oracle Access Manager)

La suite Oracle Access Manager proporciona la funcionalitat de gestió d'accessos, autenticació i autorització:

- ***Autenticació:*** Realitza els processos d'autenticació de l'usuari, actualment estan configurats 3 mecanismes:
  - ***Kerberos:*** Les estacions de treball que han iniciat sessió en el domini de l'Ajuntament fan login automàtic en el gestor d'accessos
  - ***Usuari/Password:*** Per situacions en què l'estació de treball no té sessió en el domini de l'Ajuntament.
  - ***Google Authenticator:*** Aquest cas complementa els anteriors, es fa servir com segon factor d'autenticació en funció del risc, per exemple per connexions des d'Internet o per aplicacions amb dades crítiques.
- ***Single Sign On:*** Manté la sessió de l'usuari un cop autenticat i no es tornen a demanar credencials.
- ***Autorització:*** Definició de polítiques per permetre o denegar accessos a recursos web en funció dels rols dels usuaris.
- ***Inter operació:*** Gestiona diferents protocols para facilitar la interoperació amb tercers, actualment es gestionen els següents:
  - ***Capçaleres HTTP:*** És el mecanisme més bàsic, l'aplicació protegida rep un conjunt de capçaleres HTTP (nom, cognoms, e-mail,...) de l'usuari autenticat.
  - ***SAML:*** Protocol que genera les dades de l'usuari en format XML (amb sintaxis definida pel protocol SAML) i signades per un certificat de l'Ajuntament.
  - ***OAuth:*** Protocol que genera les dades de l'usuari en format JSON, es descarreguen per l'aplicació (l'aplicació també s'identifica per fer la descàrrega)
- ***Auditoria:*** Registre de les accions realitzades pels usuaris (autenticació correcta o fallida, autorització correcta o fallida) amb detall per ser explotades per sistemes d'informació.

Directori (Oracle Unified Directory)

El directori conté la informació associada als processos d'autenticació, autorització, accessos i credencials, concretament es mantenen les següents dades:

- ***Dades usuari:*** Dades bàsiques com nom, cognoms, e-mail, tipus d'usuari, i altres atributs.

- ***Credencials:*** Credencials associades a l'usuari
    - ***Contrasenya:*** Contrasenya de l'usuari
    - ***Google Authenticator:*** Claus associada a l'usuari per validar el tokens TOTP generats per l'usuari
- ***Aplicacions:*** Aplicacions protegides sota la solució, per cada aplicació es defineixen els següents conceptes
    - ***Funcions:*** Identifiquen una funcionalitat bàsica en l'aplicació
    - ***Perfils:*** Agrupen un conjunt de funcions i també rols de productes (veure el següent punt)
    - ***Grups:*** Permeten agrupar usuaris per altres criteris funcionals (ex. districte, oficina,...)
- ***Productes:*** Representen APIs (Application Programming Interface) de serveis web (veure apartat **DevOps**). De forma similar a les aplicacions, els productes defineixen els següents conceptes:
    - ***Serveis:*** Els serveis web unitaris que ofereix un producte
    - ***Rols:*** Agrupen serveis dintre del producte

Perfilat automatitzat - DevOps

Dintre dels processos de **DevOps** per cada API definida, en el moment dels seu desplegament s'executen processos que alimenten el **Directori (Oracle Unified Directory)** per modelar aquestes APIs com nous **productes**.

El model de seguretat definit a l'Ajuntament no permet consumir directament ***productes***, sinó que aquests sempre s'han de consumir mitjançant una ***aplicació***. Així el procés natural per oferir una **API** als usuaris consisteix a alt nivell en els següents passos:

1. Desenvolupar l'API i integrar-la en els processos de **DevOps**
2. Automàticament aquesta API apareixerà modelada com **producte** i disponible per ser assignada a **aplicacions**
3. A la consola d'autoritzacions (veure següent apartat) es realitzen 2 tasques realitzades per rols separats:
    a. Els **administradors d'aplicacions** defineixen una nova aplicació o modifiquen una existent per assignar-li el nou **producte** (apareixeran nous **perfils** que representen els **rols** del producte)
    b. Els **administradors d'usuaris** assignen usuaris als perfils de l'aplicació i així obtenen permisos per consumir el **producte** (quan el perfil assignat està vinculat a un rol del producte).

Consola autoritzacions

La consola d'administració és una eina d'alt nivell orientada a usuaris administradors, de forma que poden governar les autoritzacions sense entrar en les complexitats tècniques associades.

Es defineixen principalment 2 rols amb permisos segregats en aquesta consola:

- **Administradors d'Aplicacions:** Poden gestionar i definir aplicacions així com les seves estructures associades (perfils, grups, funcions i associació a productes), però **no** poden definir productes (es fa pels processos de **DevOps**) i **no** poden assignar usuaris als perfils (és una tasca que es realitza amb el rol **administrador d'usuaris** descrit a continuació)
- **Administradors usuaris:** Poden gestionar la vinculació d'usuaris a perfils d'una aplicació, però **no** poden definir els perfils ni les estructures associades als mateixos (funcions, productes,...).

Frontal Seguretat

Els frontals de seguretat són servidors web (ex. Apache, IHS, OHS) que actuen com a proxy invers de les aplicacions protegides. Aquests servidors incorporen el mòdul **"Webgate**" de la solució de gestió d'accessos Oracle Access Manager, de forma que revisen el tràfic i presenten a l'usuari el formulari d'autenticació, si encara no ha iniciat una sessió o li permeten o bloquegen el pas en cas que l'usuari no tingui els permisos adients.

L'arquitectura actualment desplegada en l'Ajuntament, consta dels següents components:

- **Frontals corporatius:** Són frontals que es fan servir per protegir aplicacions que no són crítiques i no tenien prevista en la seva arquitectura un frontal de seguretat. Existeixen frontals per aplicacions exposades només a la xarxa interna (normalment aplicacions *.ajuntament.bcn) i frontals en una DMZ per aplicacions exposades a Internet (normalment *.bcn.cat). Pel cas d'aplicacions desplegades fora de l'entorn de l'Ajuntament, els frontals corporatius exposen la funcionalitat per iniciar sessions de forma remota (gestió dels protocols SAML i Oauth).
- **Frontals WAS:** El cas d'aplicacions desplegades en els servidors WAS corporatius, es disposa d'un conjunt de frontals que proporcionen la capa de seguretat a aquestes aplicacions.
- **Frontal dedicats:** Algunes aplicacions necessiten infraestructura dedicada, ja sigui per la seva criticitat o volumetria, en aquests casos disposen de frontals de seguretat (servidor web + Webgate) dedicats. Actualment es troben en aquesta situació 2 peces importants:
    - **Intranet:** Aplicació amb dades internes pels empleats de l'Ajuntament
    - **API Manager:** Publicador de serveis webs, protegits per la solució de gestió d'accessos.

10.1. ENTORNS DE TREBALL

L'IMI disposa de 3 entorns per a l'execució d'aplicacions. 2 d'aquests entorns estan dedicats a la fase de construcció i proves d'integració.

L'IMI utilitza tres entorns per garantir que els sistemes s'integren en els servidors/hosts de l'IMI de manera segura i sense interferir en l'operativa diària de l'Ajuntament de Barcelona.

A l'entorn de Desenvolupament s'instal·len els nous components en primera instància per permetre identificar els errors d'integració amb d'altres components de l'arquitectura de l'IMI.

Una vegada depurats els errors d'integració, els mòduls i components s'instal·len a pre-producció. L'entorn de pre-producció es idèntic a l'entorn de producció i permet comprovar d'una manera fiable que el sistema funcionarà correctament quan s'instal·li en producció. Les proves de càrrega es fan en aquest entorn. A la plataforma del mainframe, de moment, no hi tenim entorn de pre-producció, les proves de càrrega es fan a l'entorn de desenvolupament.

L'entorn de Producció és el definitiu, en el que treballa l'usuari. Els tres entorns, Desenvolupament, Pre-Producció i Producció es consideren entorns de treball productius.

En concret aquests entorns són els següents:

- **Entorn desenvolupament**: en aquest entorn s'instal·len en primera instància les aplicacions i serveis. Permet identificar els errors d'integració amb els components de l'arquitectura de l'IMI.
- **Entorn de pre-producció**: una vegada depurats els errors d'integració, les aplicacions s'instal·len en aquest entorn. És idèntic a l'entorn de producció i permet comprovar que les aplicacions funcionaran correctament quan s'instal·lin en producció.
- **Entorn de producció**: aquest és l'entorn definitiu en què treballa l'usuari i on s'han de deixar instal·lades les aplicacions.

Tots els components que formin part de la solució s'han gestionar i administrar en aquests tres entorns.

11. ANNEX 2: SERVEIS D'IDENTITATS

El detall de serveis de govern a arquitectura d'Identitats, serveis de coordinació, gestió i suport tècnic i de processos de seguretat associats són els Següents:

CAAA - GESTIÓ D'IDENTITATS

Activitats per donar resposta a les necessitats de gestió i supervisió envers la governança de la identitat digital.

- Tasques de Gestió i Coordinació d'Evolutius de la plataforma: Anàlisi d'impacte global de les problemàtiques diàries per definir solucions i aplicar-les.
- Tasques de Gestió i Coordinació de Projectes d'integració i automatització de processos de les entitats i organismes que necessiten de la Gestió de Identitats.
- Tasques de Suport relacionades amb la integració de nous repositoris i normalització dels actuals.
- Tasques de Suport relacionades amb l'aplicació de la lògica de negoci de l'Ajuntament.
- Tasques d'Anàlisi d'implantació de controls per millorar la qualitat de la informació als repositoris integrats a la Gestió de Identitats i identificar patrons que no compleixin amb les polítiques corporatives.
- Tasques de Gestió i Coordinació per portar a terme el desplegament de la política de contrasenyes corporativa.
- Tasques de auto provisió perfilats de sectors específics de l'Ajuntament.
- Revisió de la qualitat dels repositoris d'identitats corporatiu.
- Establir processos de re certificació.
- Valoracions i disseny de propostes d'evolutius de les identitats.
- Nous connectors i noves integracions.
- Gestió de les operacions de canvis i incorporacions de noves fonts autoritatives (nòmines).

CAAA - GESTIÓ D'ACCESOS

Aquestes activitats treballen per controlar l'accés als sistemes de informació (Autenticació i Autorització) de manera que es **garanteixi la seguretat de la informació i es disminueixin els riscos** de robatori d'informació i accés indegut a aquesta.

- Tasques d'Anàlisi i Suport relatives a la definició del nou model d'autenticació mitjançant SSO i federació de les aplicacions corporatives i de tercers.
- Tasques d'Anàlisi i suport sobre les propostes d'implementacions d'ADFS.
- Supervisió i validació de les implementacions d'autenticacions i controls d'accés, accessos remots, segons factors d'autenticació i SSOen altres eines corporatives com són:
  - Sistemes d'Accés remot VPN IPSEc, VSSL, Virtualització ET, ...
  - SSO estació de treball

- Accés a directori Actiu
- Control accés OWA
- Futura implementació de NAC
- Accés a wifis ciutadà i corporatives.
- etc

- Gestió funcional del servei d'accessos extranet – Serveis interns exposats a Internet. El servei haurà de gestionar totes les tasques i projectes que se'n derivin del seguiment i control de la identitat digital, les seves credencials, l'autenticació, les autoritzacions i els controls d'accés als sistemes d'aquestes identitats. Es tracta de liderar i coordinar, així com de gestionar i millorar els processos i tecnologies que proporcionen que es compleixin les normatives i estàndards d'accés.

CAAA - GESTIÓ DE LES AUTORITZACIONS

Aquestes activitats treballen per controlar gestió (assignació i eliminació o transformació) dels rols i perfils d'accés als sistemes de informació (Autorització) de manera que es garanteixi que el personal accedeixi als recursos necessaris pel desenvolupament de la seva feina.

- Tasques d'Anàlisi i Suport relatives al desplegament i la definició del nou model d'autorització de les aplicacions corporatives.
- Tasques de Suport d'implementació de l'actual model d'autorització i autenticació sobre noves aplicacions corporatives complint el marc normatiu definit per seguretat.
- Procediments i processos segurs de creació, gestió d'autoritzacions.
- Revisions sistemes d'autoritzacions particulars.
- Requeriments d'autoritzacions de projectes.
- Revisió de disseny de perfils i rols de Projectes de nous SSII.
- Validació dels Plans d'autorització definides en els projectes

CAAA - GESTIÓ DE CREDENCIALS

El control de les credencials ha de fomentar-se en unes **polítiques adequades i revisades** a les necessitats de l'organització, respecte tant a activitat com a gestió de persones, i als corresponents nivells de seguretat.

En base a les polítiques que s'estableixin i als constants canvis en els sistemes d'informació, és necessari **disposar de l'inventari d'usuaris, els seus permisos i els seus accessos i fer-ne control i seguiment** de la seva evolució.

- Implantació i esmenes a la política de contrasenyes corporativa.

- Supervisió de polítiques i normatives de qualsevol tipus de credencials, tokens, Claus criptogràfiques, etc.
- Procediments segurs de creació, gestió i entrega de credencials.
- Implantar canvis en les polítiques de contrasenyes graduals.
- Inventari dels usuaris amb accés a les aplicacions crítiques de l'organització.
- Centralització del control i gestió de credencials. Gestió d'identitats.
- Revisió periòdica de credencials.
- Processos i Sistemes de custòdia de credencials i certificats centralitzats.
- Processos i serveis de PKI internes IMI.
- Avaluació de polítiques de credencials.
- Formació de normativa i bones pràctiques sobre credencials.

CAAA - GESTIÓ DEL GOVERN DELS SERVEIS API

- Tasques de definició de processos i procediments de publicació segura de serveis API d'ús corporatiu i públic.
- Establir el model de Govern de la seguretat associada al consum de serveis API. El model que proposi l'adjudicatari ha de tenir en compte tant els serveis a publicar a Internet com els serveis interns, tan a nivell de criteris de publicació com de configuracions de seguretat de les passarel·les (*gateways*) de publicació i configuracions de xarxes entre els diferents entorns de desenvolupament, preproducció i producció. Es valorarà la proposta que el licitador faci envers el procés de govern dels serveis API que permeti tenir un millor control dels serveis API publicats i dels criteris de publicació interns.
- Tasques de controls i reporting d'aquest govern: totes les tasques orientades a la recopilació, generació i distribució d'informació en aquesta activitat, incloent informes d'estat, indicadors de grau d'avenç i previsions. Això inclou:
  - Elaborar informes de seguiment mensual del contracte que proporcionin informació sobre el seu avenç, pressupost, qualitat i riscos, així com la seva comunicació als interessats.
  - El registre i actualització de les dades de seguiment que estableixi l'Ajuntament en cadascun dels apartats.

11.1. ANNEX 2: INFORMACIÓ ADDICIONAL / ACLARIMENTS

Si és de l'interès dels licitadors sol·licitar informació i aclariments per la presentació de l'oferta, l'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: : **nbellavista@bcn.cat**

En l'assumpte del correu indicar:

*Contracte CAAA: [**Número d'expedient del contracte**]*

S'atendran les sol·licituds d'informació i/o aclariments fins a 3 dies laborables abans de la data límit de presentació d'ofertes.

La sessió informativa presencial, on es dona resposta a totes les consultes rebudes per correu electrònic, podrà resultar anul·lada, amb motiu de les mesures organitzatives que se n'adoptin a causa de la COVID-19, determinades pel Comitè de Seguiment de l'Ajuntament de Barcelona en coordinació amb l'Agència de Salut Pública de Barcelona.

En cas que es pugui convocar aquesta sessió informativa, aquesta sessió es celebrarà a partir dels 5 dies hàbils posteriors al dia següent de la data de publicació de l'anunci de licitació a la plataforma de contractació pública del perfil del contractant. El lloc, el dia i l'hora d'aquesta sessió es publicarà a l'anunci de licitació en el perfil del contractant.https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903