Ajuntament de Barcelona
Institut Municipal d'Informàtica
Direcció d'Operacions i Sistemes

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE LA SUBSCRIPCIÓ DE PROGRAMARI DE DOBLE FACTOR D´AUTENTICACIÓ PER A L'AJUNTAMENT DE BARCELONA, AMB MESURES DE CONTRACTACIÓ SOSTENIBLE

ÍNDEX

1. INTRODUCCIÓ

1.1. ANTECEDENTS

Actualment les comunicacions estan esdevenint la realitat del dia a dia de gran part de la plantilla municipal. En aquest aspecte, cada cop més, els i les treballadores municipals accedeixen a la informació corporativa servirà través d'ordinadors i tauletes portàtils que fan que la gestió de les dades esdevingui crítica i s'hagi de mantenir en perfectes condicions, i s'hagin d'extremar les mesures de protecció d'aquesta informació Actualment, entorn al 85% dels atacs i les bretxes de seguretat tenen a veure amb credencials compromesos, pel que cal una solució que permeti:

- Reforçar l'accés amb protecció més sòlida que amb usuari i contrasenya
- Protegir als usuaris contra robatoris de credencials
- Protegir els recursos d'accessos no autoritzats.

Com a part d'aquest procés de millora s'ha iniciat un projecte doble factor d´autenticació. L'autenticació de doble factor proporciona un segon canal de seguretat per a qualsevol tipus d'inici de sessió que requereixi connectar amb altres aplicacions o serveis o bé connectar un dispositiu físic per iniciar aquesta sessió. Es tracta de doble factor perquè es requereix a més del seu usuari i la seva contrasenya. Per poder aplicar-lo, l'usuari final ha d'haver realitzat prèviament el procés de registre en què associï un dispositiu al seu compte d´usuari corporatiu.

1.2. SITUACIÓ ACTUAL

L'Ajuntament ha de disposar d'una solució que permeti autenticar l'accés dels usuaris i dispositius a les aplicacions mitjançant un sistema de "verificació en dos passos" o "multifactor", protegint així l'accés de tot el perímetre de l'Ajuntament. La solució ha de permetre verificar als usuaris abans de donar accés a aplicacions i recursos corporatius, i comprovar que tinguin una identitat confiable, i establir polítiques d'accés en funció d'aquesta verificació.

L'objectiu és que aquesta eina sigui la solució unificada de doble factor per a tots els serveis que ofereix l'Ajuntament i que requereixen autenticació d'usuari.

L'interès públic d'aquesta millora rau en proporcionar una millora considerable als i les treballadores públiques amb un augment de la seguretat de la connectivitat a la xarxa de dades i, conseqüentment, un augment de la seguretat en la capacitat de treball per tal d´atendre les necessitats de la ciutadania.

A més a és, aquest contracte promou l'eficiència i, a tal efecte, inclou els termes acordats en l'execució dels processos de contractació pública, afavorint l'agilització de tràmits, així, com la valoració de la incorporació de consideracions socials com aspectes positius en aquest procediment de contractació pública, fomentant alhora la participació de la petita i mitjana empresa, facilitant també l'accés sense cost a la informació.

2. OBJECTE

L'objecte del contracte és la subscripció del dret d'ús de llicències d'un programari de doble factor d´autenticació per a l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible.

Dintre de l'objecte del contracte s'inclouen determinats serveis que s'especifiquen en el punt 3 del present plec.

3. ABAST

L'abast d'aquest contracte inclou:

3.1. SUBMINISTRAMENTS I SERVEIS ASSOCIATS INCLOSOS

L'adjudicatari haurà d'incloure necessàriament els següents subministraments i serveis associats:

a) El lliurament i activació de les llicències objecte del contracte acreditant la vigència del dret d'ús i el servei de manteniment i suport de les mateixes.

b) El lliurament de la documentació que acrediti la vigència del servei de subscripció de les llicències lliurades.

3.2. INFORMACIÓ DE LES LLICÈNCIES

L'adjudicatari haurà de lliurar, en l'inici del contracte i com a màxim una setmana després que s'hagin activat la vigència del servei de suport i manteniment de les llicències, un fitxer MS Excel® amb el següent format:

Descripció producte	Part Number o SKU	Unitats adquirides	Quantitat per unitat	Mètrica	Cost de compra unitari anual amb IVA	Data efectiva	Data finalització	Data primera adquisició / subscripció del producte	Número de contracte o contracte associat	Fabricant	Proveïdor

Omplint-la completament amb tantes files com productes siguin lliurats segons l'abast demanat en aquest apartat del plec.

La descripció dels camps a omplir és la següent:

Descripció producte: Nom del producte segons el fabricant del mateix.

Part Number o SKU: Identificador alfanumèric del producte donat pel fabricant del mateix.

Unitats adquirides: Unitats del producte adquirides segons es demana al plec.

Quantitat per unitat: Omplir quan la mètrica del producte correspongui a un paquet indicant quin és aquest valor (per exemple: 2 quan la mètrica sigui packs de dos processadors)

Mètrica: Descripció de la mètrica corresponent al producte (per exemple: packs de dos processadors o usuaris nominals en cloud)

Cost de compra unitari anual amb IVA: Cost del producte unitari anual amb IVA inclòs.

Data efectiva: Data d'inici de validesa del producte. És a dir, data en què el producte està disponible per a la seva utilització o data en què s'activa el corresponent dret d'ús o manteniment.

Data finalització: Data de fi de validesa del producte. És a dir, data en què el producte ja no està disponible per a la seva utilització o data en què s'acaba el corresponent dret d'ús o manteniment.

Data primera adquisició / subscripció del producte : Data del primer contracte per part de l'IMI de l'adquisició o subscripció del producte.

Número de contracte o contracte associat: És el codi o nom del contracte associat que l'adjudicatari signa o activa amb el fabricant i que conté els termes i condicions del programari.

Fabricant: Fabricant del producte.

Proveïdor: Adjudicatari del contracte.

Juntament amb aquest document en format MS Excel®, l'adjudicatari lliurarà els termes i condicions del programari que aplica pels productes demanats. Tant el fitxer en format MS Excel® com aquesta documentació no han de ser incloses juntament amb l'oferta, sinó quan el licitador esdevingui adjudicatari del contracte i els productes s'hagin activat i/o lliurat.

És requisit imprescindible que aquesta informació sigui lliurada correctament per poder presentar la facturació del contracte, podent ser motiu de penalitzacions si no es compleix el seu lliurament en el termini establert.

4. ORGANITZACIÓ I MODEL DE RELACIÓ

L'IMI gestiona totes les llicències de forma centralitzada per part d'un equip encarregat i especialitzat en aquest tema. Aquest equip serà l'interlocutor per part de l'IMI i tindrà la responsabilitat de validar el correcte lliurament dels productes demanats amb el licitador.

El licitador detallarà la seva proposta d'organització per assegurar de forma òptima els subministraments i serveis associats indicats a l'apartat 3. Com a mínim, oferirà un contacte tècnic expert en llicenciament de programari de doble factor d´autenticació i un contacte administratiu que es responsabilitzi dels aspectes comercials i administratius.

5. REQUERIMENTS TÈCNICS

El doble factor d´autenticació ha de recollir la informació mínima indispensable de l'usuari i del dispositiu associat i ha de tractar només aquella que és estrictament necessària pel seu correcte funcionament. S'evitarà recollir informació de dades personals (numero de telèfon mòbil, IPs, IMEI, etc) i en els casos en què es requereixi registrar alguna dada personal haurà de ser per un període curt de temps i previ a justificar la necessitat i el període de permanència d'aquesta que mai hauria de superar, excepte previsió legal al respecte, els 2 o 3 mesos des de la recollida de la dada.

Dades a recollir pel doble factor d´autenticació:

Relacionada amb l'usuari

- El nom d'usuari (o username) del login, és a dir, inici de sessió des de Microsoft AD
- Zona horària, hora i data d'autenticació

Relacionada amb el dispositiu

- Tipus de dispositiu
- Versió del sistema operatiu
- Adreça IP obtinguda de forma dinàmica. Es requereix aquesta dada per a l'autenticació basada en riscos, que detecta i mitiga automàticament els patrons d'atac coneguts habitualment i les anomalies d'alt risc per proporcionar un nivell de seguretat més alt sense comprometre l'experiència de l'usuari final. (S'utilitza només quan hi ha un procés d'autenticació relacionat amb el telèfon/tauleta i només durant aquest procés.)
- Aplicació a la qual el dispositiu intenta accedir
    - UUID (*Universally Unique IDentifier*): és un identificador per aplicació i identifica una aplicació en un dispositiu. Sempre que l'usuari no elimini l'aplicació per complet, aquest identificador persistirà entre els inicis de l'aplicació i, almenys, li permetrà identificar el mateix usuari que fa servir una aplicació en particular en un dispositiu. Si l'usuari elimina per complet i després reinstal·la l'aplicació, la ID canviarà.

- Identificadors del dispositiu:
    - nom del dispositiu
    - identificador del processador
    - números de sèrie
    - UDID (*Unique Device Identifier*): és una seqüència de 40 caràcters hexadecimals que identifiquen de forma única un dispositiu. S'utilitza precisament per a identificar el dispositiu però només durant el procés d'enrolament/onboarding
- nom d'amfitrió DNS

El número de telèfon només s´ha d´obtenir si, en fer l'onboarding/enrolament, l'usuari selecciona Smartphone al principi del procés. Si l'usuari selecciona Tablet, llavors l´aplicació no ha de tenir visibilitat del seu número de telèfon.

Altrament, un usuari ha de poder demanar l'eliminació de les dades personals i aquestes seran purgades o anonimitzades de la següent forma:

Un client ha de poder sol·licitar l'eliminació de les dades personals en qualsevol moment enviant un avís a un correu electrònic. Quan un client sol·licita l'eliminació de les dades personals emmagatzemades per sistema de doble factor, aquest ha de purgar o anonimitzar les dades sol·licitades dels seus sistemes en la mesura que ho requereixi la llei aplicable i ha de poder conservar les dades administratives necessàries per a finalitats comercials legítimes (per exemple, registres de facturació).

5.1. REQUERIMENTS DE PROTECCIÓ DE DADES PERSONALS

El sistema proposat ha de recaptar, en la totalitat dels seus serveis per acomplir amb la 2FA, el mínim de dades de caràcter personal de l'usuari possible.

El sistema proposat ha de poder parametritzar els terminis d'esborrat automàtic de les dades amb caràcter personal per a un ús puntual (connexió d'un usuari ja registrat a una aplicació amb 2FA) des d'un mínim de 1 dia. Per exemple, ha de poder parametritzar que després de validar a un usuari, les seves dades de terminal, aplicació, IP de connexió, etc. s'esborrin abans de 24 hores posteriors a la connexió).

El sistema proposat ha de poder parametritzar l'eliminació o anonimització completa (no PSEUDOanonitmització!) automàtica amb avís previ a l'administrador del sistema, de les dades de registre d'usuari quan aquest hagi fet servir l'autenticació 2FA en un període que també es pugui parametritzar.

En cas que s'opti per l'anonimització, la proposta haurà d'explicar quin mecanisme s'utilitzarà per aconseguir l'anonimització completa, garantint que no es pugui en cap cas reidentificar a un usuari en particular.

En qualsevol cas, totes les dades de caràcter identificatiu, encara que de segon ordre -per exemple la matrícula AJB d'un usuari- s'emmagatzemaran encriptades a la base de dades.

L'administració del sistema recaurà en un perfil específic que gestionarà la resta de perfils i es podran generar diferents perfils segons les necessitats funcionals dels administradors o usuaris.

La proposta no podrà generar en cap cas llistats amb relacions d'usuaris o fitxes específiques dels mateixos amb les dades identificatives obertes. Qualsevol dada identificativa estarà anonimitzada en el llistat o fitxa.

Els mecanismes de Multi-Factor d'Autenticació (MFA) han de garantir que no es registri el telèfon mòbil si així ho considera l'IMI, en aquells casos que els mecanismes no requereixin el mòbil pel procés de MFA emprat.

Les dades personals que es registrin per ciberseguretat han d'estar eliminades amb un temps curt, el mínim necessari i justificat per evitar atacs.

5.2. FUNCIONALITATS

Tot seguit es detallen les característiques i funcionalitats que caldrà que tingui el programari de Doble Factor d'Autenticació:

- Suport del doble factor per Microsoft OWA

Integració amb Microsoft OWA per a permetre múltiple factor d´autenticació en la autenticació de OWA sense canviar de font d´autenticació ni utilitzant *reverse proxy*.

- Integració amb SIEM/QRADAR i ELK

Els esdeveniments de la solució s'han de poder integrar amb el ELK i el SIEM corporatiu de l'organització.

- Suport de múltiple factor d´autenticació per a Microsoft Logon i RDP

Integració amb Microsoft Windows per permetre múltiple factor d´autenticació a l'autenticació a Windows en local o via RDP. Ha de ser compatible per a Windows 8.1 o posteriors, i Windows Server 2012 o posteriors.

- Múltiples mètodes d'autenticació

Capacitat i flexibilitat per fer servir múltiples mètodes d'autenticació de diferent fortalesa en funció del risc i per la usabilitat i adaptació a la realitat del client. Ha d'incloure: WebAuth, Biometrics, Tokens, OTP/TOTP/HOTP, SMS, trucada, Mobile Push i Passcodes.

- Idiomes

Suport de múltiples idiomes tant a l'aplicació del mòbil/tablet com als prompts d'autenticació múltiple factor d´autenticació. Ha d'incloure castellà i català.

- Passwordless

Suport passwordless amb suport a Windows i OS X, podent utilitzar com el mòbil/tablet com a autenticador passwordless.

- Single Sign On des del núvol

Capacitat de SSO integrat per reduir la fricció amb l´usuari. Aquesta ha de ser allotjada pel fabricant i 100% cloud.

- APIs

Disponibilitat d'APIs per a: Configuració de polítiques, monitorització del sistema i resposta a incidents. Els administradors poden integrar les aplicacions dels clients mitjançant API i SDK sense cap mena de servei professional.

- SDKs

Disponibilitat de SDKs per integrar el múltiple factor d´autenticació directament a l'aplicació. El producte ha d'incloure SDKs amb documentació per a l'ús a les plataformes de desenvolupament més comunes, incloent-hi plataformes d'aplicacions mòbils natives.

- Registes (enrollment)

La solució ha de permetre el registre del MFA per diversos fluxos: registrant-lo al primer accés a una aplicació (en cas de que l'usuari no el tingui registrat), via correu enviat a l'usuari, etc.

- Federació

La solució ha de permetre la federació amb altres proveïdors d'identitat (IDP) via protocols estàndards (SAML2, WS-Fed, WS-Trust, OpenID Connect), delegant l'autenticació del primer factor en aquest IDP i aplicant la solució el mecanisme de MFA corresponent.

- Consola unificada forense

Consola unificada per simplificar la investigació i resposta a incidents. Aquesta consola haurà de permetre:

  - Integracions: la integració de forma nativa d´altres solucions (protecció de correu, navegació, NGFW, NGIPS…) del mateix fabricant o de tercers.
  - Automatismes: l'execució de playbooks predefinits o propis que permetin automatitzar tasques de tiquet, resposta a incidents
  - Col·laboració: compartir informació de recerca amb altres eines i entre investigadors forenses.

- Capacitats de reduir el risc distingint si el dispositiu personal és gestionat o no, podent aplicar polítiques diferenciades com per exemple:
  - Bloquejar accessos des de dispositius no corporatius
  - Fer *bypass* del DFA quan es tracta d'un dispositiu corporatiu
- Capacitats mitjançant upgrade o ampliació de llicenciament

El producte ha de ser capaç de suportar mitjançant upgrade de llicenciament les següents capacitats i característiques :

- Capacitat d'intel·ligència a l'hora de poder capturar les adreces IP utilitzades per un usuari per accedir i verificar les IP no estan identificades en algun dels possibles atacs (de força bruta, etc.) detectats entre altres clients del fabricant. L'avaluació s'ha de fer a la fase d'autenticació prèvia per evitar el bloqueig de l'usuari.
- Capacitat de seguretat adaptativa, es a dir, d'autenticació adaptativa gràcies a la personalització de la resposta segons el context. Creació de polítiques intel·ligents basades en la xarxa, el dispositiu, la ubicació i el context de risc que limitin la necessitat d'identificació als intents d'inici de sessió amb risc.

- Característiques de la reducció del risc:
  - Posture: Capacitat de detectar la higiene del dispositiu usat (tant gestionat com no gestionat) amb agent i sense. Aquesta capacitat ha d'incloure tot el cicle de vida del compliment de posture: visibilitat i remediació, podent aplicar polítiques diferenciades bloquejant accessos des de dispositius desactualitzats
  - Comportament: Capacitat de detectar la desviació del comportament de l'usuari en base a un baseline d'aplicacions accedides, fingerprinting de wifi, localització d'accés, mètode d'autenticació, etc.

5.3. REVISIÓ PRÈVIA A L'ADJUDICACIÓ

Amb caràcter previ a l'adjudicació del contracte, l'IMI podrà requerir a l'empresa candidata a ser la contractada a lliurar, en un termini no superior a 5 dies hàbils des del requeriment, un "entorn de proves", així com tota la documentació que es consideri oportuna.

Un cop verificades les característiques del producte i la seva plena adequació a l'oferta presentada, aquest entorn quedarà com a entorn de Pre-producció on poder validar l'impacte dels futurs upgrades.

En cas que algun dels productes oferts no s'ajusti a les característiques tècniques exigides en el present plec, l'empresa podrà ser exclosa d'aquest procediment per no complir els requeriments tècnics del contracte i es procedirà a requerir "entorn de proves" al següent licitador segons l'ordre en què hagin quedat classificades les ofertes.

5.4. REQUERIMENTS DE LLICENCIAMENT I D'ENTORN DEL PRODUCTE

El licitador presentarà una proposta de llicenciament basat en un model de subscripció amb suport 24x7 del fabricant.

La solució aportada pel licitador ha de contemplar la construcció de 2 entorns: entorn de preproducció i entorn de producció.

A nivell de característiques, es demana que la solució i el llicenciament proposats compleixin els següents requisits:

- El llicenciament de la solució s'ha de fer per usuari, essent vàlida la mateixa llicència d'usuari per protegir diversos serveis.
- Integració amb Microsoft OWA per permetre MFA en la autenticació de OWA sense canviar de font d'autenticació ni ús d'un reverse Proxy.
- Integració amb Microsoft Windows per permetre MFA en l'autenticació de Windows en local o via RDP. Ha de ser compatible amb Windows 8.1 en endavant, I Windows Server 2012 en endavant.
- Disponibilitat de diferents opcions per a l'enrolament dels usuaris. Ha d'incloure enrolament automàtic (amb integració amb AD, LDAP o Azure), auto-enrolament, i importació d'usuaris a través d'un .csv o via REST API.
- En el cas de l'autoenrolament, cal garantir que el procés és senzill i àgil per l'usuari. Els usuaris han de poder gestionar múltiples dispositius.
- Capacitat de fer server múltiples mètodes d'autenticació per adaptar-se millor a la realitat de l'IMI. Ha d'incloure WebAuth, biomètrics, Tokens físics, SMS, trucada telefònica i Passcodes. En el cas de les trucades telefòniques i SMS, la proposta ha d'incloure un pool global mínim de 20 trucades o SMS nacionals per usuari/any, ampliable en cas necessari.
- Suport de múltiples idiomes tant en l'aplicació mòbil/tablet, com en els prompts d'autenticació MFA. Ha d'incloure, com a mínim, català i castellà.
- Suport passwordless per Windows i OS X, podent fer servir el mòbil/tablet com autenticador passwordless.
- Capacitat de SSO integrat per unificar l'experiència d'usuari en l'autenticació. Aquesta capacitat ha de ser hostatjada en la solució i 100% cloud.
- La solució proposada ha de tenir capacitat d'integració amb altres aplicatius i sistemes amb l'objectiu d'establir una autenticació única (SSO) basat en estàndards moderns d'autenticació, autorització i federació d'identitats (per exemple, SAML v1.1 i v2.0, WS-Fed, WS-Trust, OpenID Connect, OAUTH, etc.).
- La solució proposada ha de tenir capacitat d'integració amb aplicacions i sistemes per establir l'SSO basat en mètodes d'autenticació reconeguts per la indústria i que possibilitin la integració d'aplicacions legacy i sistemes on-prem (per exemple, Radius i LDAP).
- Disponibilitat d' APIs per configuració de polítiques, monitorització del sistema i resposta a incidents. Els administradors han de poder integrar les aplicacions de l'IMI mitjançant API i SDK, sense dependre dels serveis professionals del fabricant.

- Disponibilitat de SDKs per integrar el MFA directament amb l'aplicació.
- Consola que permeti la investigació i resposta a incidents, que s'integri de forma nativa amb altres solucions de seguretat (protecció del correu, navegació, NGFW, NGIPS...) del mateix fabricant o de tercers. Aquesta consola també haurà de permetre l'execució de playbooks predefinits per automatitzar tasques de tiqueting o resposta a incidents.
- El sistema ha de disposar de mecanismes per auto-protegir-se d'atacs contra la pròpia solució.

5.5. REQUERIMENTS DE DISPONIBILITAT DEL PRODUCTE

Per a la simplicitat d'implementació i minimitzar els requisits d'infraestructura, la solució proposada ha d'estar basada en un model de solució SaaS (Software as a Service) de fabricant.

Totes les capacitats i les funcionalitats que s'indiquin als diferents requeriments han de ser suportades per una única solució SaaS. A més, tots els components/mòduls de la solució SaaS s'han de poder gestionar des d'una única consola d'administració accessible via web.

Els DataCenters (CPD) han d'estar ubicats dins de la Unió Europea en compliment de la normativa de protecció de dades aplicable.

Donada la importància que tindrà la solució, serà especialment important assegurar la disponibilitat de la plataforma. Per això, la solució haurà de garantir per defecte i contractualment un nivell de disponibilitat del servei de 99,9%, aportant evidències d'almenys 2 anys de temps d'activitat per al seu servei; amb estadístiques del percentatge de caiguda del servei sobre el temps total.

Cal assegurar la inexistència de parades o talls planificats per a finestres de manteniment (Zero Downtime).

La solució ha d'incloure un directori d'usuaris amb la possibilitat d'escalar milers d'usuaris i centenars de milers d'autenticacions mensuals.

La solució ha de permetre la sincronització d'usuaris cap a ella a partir d'un directori extern (per exemple, un directori actiu).

6. EVOLUCIÓ DE LA SOLUCIÓ

Per tal d'alinear la solució amb l'estratègia de seguretat de l'IMI a mig/llarg termini, basada en una estratègia Zero-Trust i la seguretat adaptativa amb un alt nivell de visibilitat i control de usuari/dispositiu/aplicació, a nivell d'evolució del servei de multifactor dins l'Ajuntament es valorarà que l'eina proposada permeti les següents característiques (amb llicenciament addicional si s'escau):

- Capacitat d'autenticació adaptativa gràcies a la personalització de la resposta segons el context. Creació de polítiques intel·ligents basades en la xarxa, el dispositiu, la ubicació i el context de risc que limitin la necessitat d'identificació als intents d'inici de sessió amb risc
- Capacitat de distingir dispositius personals i dispositius corporatius (incloent tot el cicle de vida dels certificats), podent aplicar polítiques diferenciades.
- Capacitat de detectar la higiene d'un dispositiu, gestionat o no gestionat, amb o sense agent. Aquesta capacitat ha d'incloure tot el cicle de vida de compliment de la postura de seguretat: visibilitat i remediació, podent aplicar polítiques diferenciades bloquejant accessos a dispositius desactualitzats, jailbroken...
- Capacitat de detectar la desviació en el comportament d'usuari. Això ha d'incloure, com a mínim, baseline d'aplicacions usades, petjada de Wifi, localització d'accés (país origen), mètode d'autenticació... podent aplicar polítiques diferenciades per bloquejar accessos d'usuaris amb comportaments anòmals.
- Capacitat d'exposar aplicacions internes, IaaS i SaaS, en un portal en el núvol amb accés condicional en base a identitat, dispositius confiables i postura de seguretat dels dispositius.

7. CONDICIONS D'EXECUCIÓ

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

7.1. LLOC DE PRESTACIÓ DEL CONTRACTE

La prestació de la totalitat de l'abast del contracte es durà a terme des de les instal·lacions de l'adjudicatari i, per tant, aquest haurà d'aportar els medis logístics suficients per a la citada prestació. De manera excepcional, l'IMI podrà demanar el desplaçament de l'adjudicatari 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 necessàries per a la prestació.

Es considera que no serà necessària la connectivitat amb l'IMI per a la prestació del servei.

7.2. GARANTIA

S'aplicarà la garantia estàndard del fabricant pels productes contractats.

8. OFERTA ECONÒMICA

Els licitadors presentaran la seva oferta econòmica (IVA exclòs) a **preu unitari** d'acord amb el model d'oferta econòmica que s'adjunta al plec de clàusules administratives particulars.

En cas que es requereixi algun llicenciament o producte addicional necessari per tal que les llicències objecte del present contracte siguin 100% funcionals en les condicions que es requereix en el present plec (llicències de servidors, suport addicional, etc) els costos d'aquests elements hauran d'estar inclosos en el preu unitari ofert.

9. FACTURACIÓ

L'adjudicatari lliurarà a l'inici del contracte les llicències en els termes que s'indiquen en el punt 3 i concordants del present plec. Una vegada les llicències estiguin activades en el sistema, l'adjudicatari facturarà el contracte d'acord amb les següents instruccions:

- La primera factura serà per l'import corresponent resultat d'aplicar els preus unitaris oferts pel número de llicències que correspongui efectivament activades en el sistema per a l'any 2023 i, en tot cas, de com a màxim, el 75% del preu de licitació. Aquesta factura serà presentada durant l'últim trimestre de l'any 2023. Si l'import a abonar pel nombre de llicències efectivament activades en el sistema per a l'any 2023 fos superior a l'equivalent al 75% del preu de licitació, l'import excedent que correspongui s'abonarà en la segona factura.
- La segona factura serà per l'import corresponent resultat d'aplicar els preus unitaris oferts pel número de llicències que correspongui efectivament activades en el sistema per a l'any 2024 més, en el seu cas, l'import que correspongués per l'excedent de les llicències efectivament activades en el sistema per a l'any 2023 no abonades en la primera factura i, en tot cas, de com a màxim, el 25% del preu de licitació. Aquesta factura serà presentada durant el primer trimestre de l'any 2024.

Per a la presentació de la primera factura serà necessari que les llicències hagin estat validades pels serveis tècnics de l'IMI. També serà necessari per poder emetre aquesta factura s'hagi lliurat l'Excel i la documentació demanada a l'apartat 3 del present plec.

10. 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.

Els licitadors l'hauran de presentar a través de la plataforma electrònica, conforme s'estableix al plec de clàusules administratives que regeix la present licitació. A l'oferta en suport electrònic tots els arxius hauran d'estar en format **Open Document (odt o odp) o pdf obligatori**, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.

Els licitadors podran 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 tancats:

- **El sobre electrònic A** on s'inclourà la documentació administrativa requerida a la clàusula 8 "Documentació que han de presentar les empreses licitadores" del plec de clàusules administratives particulars.

- **I el sobre electrònic BC** que haurà de contenir l'oferta econòmica d'acord amb el model que s'annexa al plec de clàusules administratives particulars que regeixen per aquesta contractació així com la 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 l'interior del sobre s'haurà d'incorporar una relació, en arxiu independent, dels documents que hi conté ordenats numèricament.

També s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.

11. CLAUSULES GENERALS DE SEGURETAT

11.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ I PROTECCIÓ DE DADES

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.

11.2. CLÀUSULA DE PROPIETAT INTEL·LECTUAL

La propietat intel·lectual dels productes correspon al fabricant dels mateixos.

11.3. 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.

11.4. CLÀUSULA PER ACCESSOS POTENCIALS

En aquesta contractació no es preveu tractament de dades personals per part de l'empresa contractista.

Per a l'execució de les prestacions derivades del compliment de l'objecte d'aquest contracte, el personal de l'empresa contractista no pot accedir a les dades de caràcter personal que figuren als arxius, documents i sistemes informàtics de l'òrgan de contractació.

No obstant, el que estableix el paràgraf anterior, quan el personal de l'empresa contractista accedeixi a les dades personals incidentalment, estarà obligat a guardar secret fins i tot després de la finalització de la relació contractual, sense que en cap cas pugui utilitzar les dades ni revelar-les a tercers.

L'empresa contractista ha de posar en coneixement dels seus treballadors els deures i obligacions establerts anteriorment.

L'empresa contractista ha de posar en coneixement de l'òrgan de contractació, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de les dades de caràcter personal. Aquesta incidència s'haurà d'anotar al Registre d'incidències.

L'incompliment del que s'estableix en els apartats anteriors pot donar lloc a l'empresa contractista sigui considerada responsable del tractament, als efectes d'aplicar el règim sancionador i de responsabilitats previst a la normativa de protecció de dades.

11.5. CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT

L'adjudicatari 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'adjudicatari, sempre sota la responsabilitat de l'adjudicatari, 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'adjudicatari 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.

11.6. 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'adjudicatari.

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

L'adjudicatari serà 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.

11.7. CLÀUSULA DE SEGURETAT DELS EQUIPS, PROGRAMES I INFORMACIÓ

L'adjudicatari es compromet a vetllar per la seguretat dels equips on es trobin instal·lats els programes, bases de dades i informació de l'Administració Municipal, així com per la seguretat en els canals de comunicació emprats. Per tant, prestarà els seus serveis guardant estrictament les mesures de seguretat necessàries, amb la finalitat d'evitar la pèrdua d'informació, així com danys, pèrdua o deteriorament dels programes i bases de dades utilitzades i que són propietat de l'Administració Municipal.

11.8. CLÀUSULA DE PERSONAL EXTERN

El/La 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/La 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/La 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/La 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/la 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.

11.9. 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.

11.10. 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, custòdia i protecció de les claus que estableix el Departament de Seguretat de l'IMI. El Departament de Seguretat de l'IMI ha d'assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. El Departament de Seguretat de l'IMI 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 pel

11.11. INVENTARI D'ACTIUS

S'haurà de poder mantenir un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa.

Aquest informe de necessitat ha estat emès pel Sr. Miquel Matavacas Bayés, tècnic responsable del contracte, adscrit a la Direcció d'Operacions i Sistemes de l'IMI, amb el vistiplau de,

Amparo Rodríguez Rodríguez
Directora d'Operacions i Sistemes de l'IMI.

12.ANNEXOS

12.1. ANNEX 1. INFORMACIÓ ADDICIONAL / ACLARIMENTS

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

En l'assumpte del correu caldrà indicar:

Contracte: DFA

En cas de no obtenir resposta els licitadors podran trucar per telèfon al departament tècnic de l'IMI per fer les consultes tècniques pertinents:

- José Manuel Velilla Balaguer 932918358
- Miquel Matavacas Bayés 932918472 – 639344966

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

No es convocarà una sessió informativa per aquesta licitació. Per tal que els licitadors interessats en presentar oferta, puguin aclarir tots els dubtes que els hi sorgeixin, l'IMI posa a disposició dels licitadors la bústia de correu abans indicada per qüestions tècniques i la de imi_gestio_contractacio@bcn.cat, per consultes de caire administratiu.

Les consultes rebudes dins dels 3 dies hàbils anteriors a la data de finalització d'entrega de les proposicions seran solucionades i publicades al perfil del contractant de l'IMI:

(https://contractaciopublica.gencat.cat/perfil/BCN_IMI/customProf).