Institut Municipal Barcelona Innovació i Tecnologia

Direcció de Serveis de Tecnologia i Transformació Digital de Serveis Corporatius

Plec de prescripcions tècniques per a la contractació del subministrament de pantalles i software de gestió de continguts digitals (cartelleria digital) en diferents edificis municipals de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible

Índex

1. INTRODUCCIÓ

L'Institut Municipal Barcelona Innovació i Tecnologia (en endavant BIT) és l'organisme autònom de l'Ajuntament de Barcelona responsable de subministrar tots els serveis de les tecnologies de la informació i comunicació (TIC) a l'Ajuntament de Barcelona i els seus organismes autònoms.

Concretament, BIT participa en el disseny i execució de l'estratègia TIC de l'Ajuntament de Barcelona, ofereix assessorament i suport en tots aquells projectes o programes de l'Ajuntament que requereix una estratègia de sistemes d'informació i telecomunicacions i impulsa i executa projectes tecnològics de diversa índole. Entre aquests, la implementació d'un sistema de gestió de continguts digitals de cartellera en els edificis municipals ha de ser referent en la transformació digital de l'Administració per tal d'alliberar al personal municipal de tasques mecàniques i manuals que possibilitin la dedicació del seu temps a tasques de major valor afegit.

Els sistemes de gestió de continguts digitals o cartelleria digital permeten la publicació de manera centralitzada de continguts, el monitoratge i manteniment de tots els elements d'un circuit digital (programari i maquinari) i la creació de continguts a través d'eines internes, en pantalles de visualització distribuïdes en diferents localitzacions dins dels edificis municipals.

D'aquesta manera, els sistemes de gestió de continguts digitals aconsegueixen:

- Gestionar diferents tipus de continguts: Text, vídeos, imatges
- Gestionar en un únic sistema diferents continguts en un mateix edifici i en diferents edificis de manera descentralitzada, es a dir, que diferents gestors de continguts puguin crear i mantenir els continguts del seu àmbit
- Gestionar diverses pantalles de visualització amb el mateix contingut per un únic usuari o multiusuaris
- Capacitat per recollir dades de sondes connectades i mostrar la temperatura i humitat, o altres dades recollides per elements connectats dins de l'edifici
- Integrar-se amb sistemes corporatius amb informació a visualitzar
- Possibilitat de configurar els continguts tant en vertical com en horitzontal
- Monitoritzar remotament el contingut que s'està visualitzant en les pantalles en temps real

En definitiva aquesta tecnologia permet disposar d'una eina corporativa única on definir el contingut a visualitzar en les diferents localització d'un edifici, i en tots els edificis on es decideixi instal·lar les pantalles de visualització, segons diferents perfils d'usuari, on la gestió es més eficient i amb millor qualitat, a part de l'alliberament de temps de l'usuari que aquest pot dedicar a tasques més estratègiques augmentant la seva motivació.

Addicionalment, amb l'aplicació d'aquesta tecnologia, s'augmenta la homogeneïtzació dels continguts a visualitzar seguint criteris corporatius per a tots els edificis municipals.

En aquest àmbit, BIT conjuntament amb la Direcció de Serveis d'Edificis Municipals (en endavant, DSEM), decideixen gestionar els continguts digitals de manera remota i centralitzada, gestió que actualment es realitzen de forma manual i de manera local en cada pantalla de visualització (amb un alt cost en dedicació), fet que permetria afegir valor i eficiència al servei així com alliberar temps i recursos.

2. OBJECTE DEL CONTRACTE

L'objecte d'aquest contracte es el subministrament de pantalles i software de gestió de continguts digitals (cartelleria digital) en diferents edificis municipals de l'Ajuntament de Barcelona, així com els serveis accessoris de suport i manteniment dels equips, amb mesures de contractació pública sostenible.

3. ABAST

Totes les activitats es duran a terme segons criteri de l'Ajuntament de Barcelona i s'executaran sota les directrius i procediments que definirà, coordinarà i supervisarà la Direcció de Serveis de Tecnologia i Transformació Digital de Serveis Corporatius del BIT.

L'abast del contracte comprèn els següents subministraments i serveis:

- Subministrament de les pantalles professionals i garantia
- Etiquetatge i gestió de l'inventari de les pantalles professionals
- Instal·lació física de les pantalles professionals
- Implantació i configuració del software de gestió de continguts digitals
- Llicència d'ús i suport del software (Manteniment correctiu del programari)
- Manteniment preventiu i correctiu dels elements de la instal·lació
- Garantia de les pantalles de visualització professionals
- Suport i gestió del canvi (formació)

A continuació es detallen els subministraments i serveis inclosos en l'abast del contracte.

3.1. Subministrament de les pantalles professionals i garantia

Subministrament de 38 pantalles d'ús professionals de visualització amb reproductor integrat i compatibles amb el software de gestió de continguts digitals que resulti adjudicat, aptes per a funcionament vertical i horitzontal, i dissenyades per a ús professional 18/7 o 24/7.

Les pantalles inclouen:

- Elements de protecció per evitar manipulacions no autoritzades.
- Els suports físics, ancoratges, així com tots els elements i accessoris necessaris per a la seva instal·lació.
- Fonts d'alimentació, cablejat i elements de canalització necessaris per a la seva instal·lació.
- Garantia mínima obligatòria de tres anys.

La distribució prevista de les pantalles en els edificis municipals es la següent:

Edifici	**Número de Pantalles**	**Tipus de pantalla**
Novíssim	8	Pantalla professional 43''
Novíssim	2	Pantalla professional 50''
Nou	12	Pantalla professional 43''
Vell	5	Pantalla professional 43''
Via Laietana 8-10	5	Pantalla professional 32''
Via Laietana 8-10	1	Videopantalla LED 110''
Creatic (Carrer Sancho de Ávila 125)	4	Pantalla professional 43''
Creatic (Carrer Sancho de Ávila 125)	1	Videopantalla LED 110''

Durant l'execució del contracte, BIT podrà modificar aquesta distribució entre edificis municipals.

Així mateix, per criteris estrictament tècnics i d'adequació a l'espai físic disponible, es podrà autoritzar que alguna pantalla instal·lada sigui d'un mida equivalent o lleugerament diferent a la prevista inicialment, sempre dins de les prestacions contractades i sense que aquesta adequació suposi cap modificació de contracte, del nombre d'unitats, ni de l'import del contracte, amb autorització prèvia i expressa de BIT.

Especificacions tècniques mínimes requerides.

Pantalles professionals

- Resolució Full HD o superior.
- Brillantors de 350 nits o superior.
- Connexió a xarxa per WIFI i cable Ethernet.
- Funcionament vertical i horitzontal.

3.2. Etiquetatge i gestió d'inventari de les pantalles professionals

L'adjudicatari haurà d'etiquetar els elements de servei que el BIT consideri per tal de facilitar un sistema d'inventari dels mateixos. Aquesta activitat es durà a terme generalment a les instal·lacions de l'Ajuntament de Barcelona.

BIT facilitarà la informació necessària per a l'etiquetatge dels equips que permeten el seu inventari amb un el codi unívoc de dispositiu, i l'adjudicatari procedirà a col·locar les etiquetes en un lloc visible de l'equipament.

Respecte al parc actualment existent, que es troba identificat amb etiquetes impreses, no es preveu inicialment un re etiquetatge del mateix.

Serà responsabilitat de l'adjudicatari les altes i les baixes a l'eina d'inventari, que determini el BIT, d'aquells dispositius que es posin en servei. Aquesta alta a l'inventari de BIT haurà de fer-se en tot moment seguint les directrius que es donin des de BIT o qui ell designi.

Aquest inventari serà de caràcter obligatori i no es considerarà un element correctament posat en servei fins a la incorporació del mateix a l'inventari de manera completa.

L'empresa adjudicatària haurà de realitzar les següents activitats lligades a l'inventari físic dels elements del servei:

- Revisar el conjunt de l'inventari del tipus d'equipament objecte del contracte, existent en les dependències municipals, en el moment de planificar, revisar o instal·lar cada equipament o elements del servei.
- Afegir l'equipament que s'instal·li a l'inventari i eliminar l'equipament que es retiri de l'inventari.
- Un cop realitzada la instal·lació, s'ha de subministrar en format electrònic al responsable del contracte designat pel BIT el llistat de números de sèrie i el seu corresponent número d'inventari BIT de l'equipament que s'hagi instal·lat o retirat.
- En el cas de la substitució d'un equip, en el llistat anterior també s'haurà d'indicar el model i el número d'inventari BIT substituït.

3.3. Implantació i configuració del software de gestió de continguts digitals

Software as a Service que permeti la gestió de continguts multimèdia (imatge, vídeo, so, text), per publicar directoris digitals, anuncis i altres continguts de cartelleria digital.

A més de la gestió de continguts bàsica, el software ha de complir els següents requeriments funcionals i no funcionals:

- **Gestió descentralitzada de les pantalles**: diferents gestors de continguts podran administrar la informació amb permisos i condicions definides.
- **Facilitat d'ús**: el software ha de ser intuïtiu, requerint una formació mínima per als usuaris sense experiència tècnica ni coneixements informàtics avançats.
- **Gestió de múltiples pantalles**: el software ha de permetre la possibilitat de mostrar elements comuns i específics segons ubicació.
    - Per exemple, un directori d'una planta alterna imatges específiques per aquell aparell/planta, amb imatges corporatives que son comuns a un grup més gran de pantalles.
- **Integració amb IoT**: el software ha de recollir dades de sensors connectats com temperatura i humitat, i mostrar-les en pantalla.

- **Compatibilitat amb web i intranet**: possibilitat de mostrar a les pantalles el contingut de webs externes o intranets de l'Ajuntament.
- **Orientació de pantalla**: el software ha de permetre la visualització en format tant vertical com horitzontal.
- **Monitorització**: el software ha de permetre verificar el contingut emès en cada dispositiu en temps real.
- **Integració amb el mòdul corporatiu d'autenticació**: el software ha d'integrar-se amb proveïdor d'identitats corporatiu (IDP) per a l'autenticació dels usuaris (consultar l'apartat 7.14 del present plec).

El proveïdor haurà de configurar i integrar el software per tal de permetre el funcionament de les pantalles un cop instal·lades.

El llicenciament cobrirà la gestió dels dispositius de reproducció subministrats i de la plataforma de continguts, i inclourà usuaris il·limitats (editors i administradors). A efectes d'estimació, es preveu una ràtio aproximada d'1 editor per pantalla, sense caràcter limitatiu.

3.4. Instal·lació física de les pantalles professionals i posta en marxa

A petició de BIT, el proveïdor haurà d'atendre la instal·lació i posada en marxa de les pantalles, d'acord amb els estàndards, sistemes i xarxa de l'Ajuntament de Barcelona. La instal·lació inclourà totes les tasques necessàries perquè quedin totalment operatives i integrades amb el software de gestió de continguts digitals (descrit a l'apartat 3.3).

Les pantalles hauran de mostrar el contingut multimèdia configurat al software SaaS, d'acord amb els estàndards, sistemes i xarxa de l'Ajuntament de Barcelona.

La instal·lació del equipament inclou les següents tasques mínimes:

- Revisió i acceptació de la planificació del desplegament.
- Direcció i execució de la instal·lació.
- Desplaçaments de tècnics a qualsevol edifici amb presència de l'Ajuntament de Barcelona.
- Instal·lació i configuració de l'equipament de maquinari i programari segons planificació i les guies d'instal·lació. Ordenació del cablejat.
- Posada en marxa i realització de les proves de funcionament especificades en els estàndards de BIT per certificar el bon funcionament de l'equip, així com confirmar amb l'usuari que s'han realitzat totes les accions.
- Traspàs d'informació i parametrització personal de l'equipament antic al nou en cas de canvi o trasllat.

El responsable del contracte designat pel BIT i la persona referent designada per l'adjudicatari, planificaran definitivament la instal·lació, identificant l'usuari (nom complert, telèfon, correu i identificació corporativa) i la localització física. Aquesta activitat pot fer-se en una única operació o en blocs.

Per a la instal·lació i posada en marxa de la pantalla, l'usuari receptor del mateix haurà d'estar present, o la persona en qui es designi que farà les mateixes activitats que l'usuari receptor.

Amb la finalitat de facilitar les activitats anteriors s'emprarà una ordre d'instal·lació d'una plantilla formalitzada i que com a mínim constarà de:

- Nom de les dependències municipals on s'ha de fer la instal·lació.
- L'adreça completa, planta i descripció de la ubicació del punt de muntatge.
- Nom i cognoms de la/les persona/es responsables.
- Número de telèfon de contacte i horari.
- Altres indicacions de l'ordre de d'instal·lació.

Les ordres d'instal·lació poden referir-se a una unitat (un sol equip) o a vàries unitats destinades a una mateixa ubicació i han de ser ateses en un termini no superior **als 5 dies laborables**.

L'empresa adjudicatària haurà de realitzar les següents activitats lligades a la retirada dels residus generats durant la instal·lació:

- Desembalatge de l'equipament o elements del servei.
- Retirada dels residus que s'originin en les actuacions d'instal·lació i retirada de les pantalles.

L'adjudicatari retirarà i eliminarà de manera sostenible els residus de l'embalatge (plàstics, cartrons, Porexpan, palets, etc.) en un punt verd oficial. El procés ordinari de retirada dels residus s'haurà de dur a terme el **mateix dia de la instal·lació**. Només a petició de BIT es durà a terme més endavant, i aquesta retirada no podrà excedir del termini màxim de 3 dies laborables una vegada feta la sol·licitud per escrit. Per tant, l'adjudicatari del contracte aportarà la seva capacitat d'emmagatzematge i logística.

Totes les ubicacions implicades en l'activitat de retirada de residus estan situades a la ciutat de Barcelona. Tots els costos de desplaçament han d'estar inclosos en l'oferta econòmica presentada i no implicaran cap cost afegit per BIT.

3.5. Llicència d'ús i suport del software (Manteniment correctiu del programari)

El servei de manteniment correctiu té per objecte garantir la disponibilitat i el correcte funcionament del software de gestió de continguts digitals en modalitat SaaS, posat en marxa i configurat per l'empresa proveïdora en el marc del present contracte. S'hi inclou la recepció de la incidència, la diagnosi, la correcció o parametrització necessària, la verificació i el tancament amb comunicació a la persona interlocutora designada per BIT.

Canals i horari.

- L'atenció d'incidències es realitzarà de dilluns a divendres, de 8:00 a 18:00h, excepte els dies festius a la ciutat de Barcelona.
- El canal de comunicació serà telefònic i/o correu electrònic definit per BIT.

- El proveïdor registrarà cada incidència (data/hora, descripció, classificació, estat i data de tancament) i quan sigui requerit remetrà a BIT un resum del detall d'incidències i nivells de servei assolits.

Classificació d'incidències.

- **Greu**: indisponibilitat total del servei o bloqueig d'una funcionalitat crítica que impedeix la gestió/publicació/visualització de continguts a nivell general.
- **Normal**: incidència amb un impacte acotat que permet mantenir l'operativa amb alternatives o bé no comporta una indisponibilitat total del servei.

Les incidències es donen d'alta per defecte com a Normal i es re classifiquen com a Greu o Urgent durant la diagnosi inicial, si escau.

Acord de Nivell de Servei (hores laborables dins l'horari base).

En avisos fora d'horari, el còmput s'inicia a les 8:00 del següent dia laborable.

Prioritat	Resposta	Diagnosi inicial	Resolució
Greu	≤ 4h	≤ 8h	≤ 24h
Normal	≤ 8h	≤ 16h	≤ 48h

- **Resposta**: temps fins a l'acusament de recepció i assignació tècnica.
- **Diagnosi inicial**: temps fins disposar d'un informe breu dels símptomes, abast i properes accions.
- **Resolució**: temps fins la recuperació del servei o mesura provisional que permeti operar fins a la correcció definitiva.

Penalitzacions.

En cas de tall total del servei superior a 48 hores naturals consecutives, per causes imputables a l'empresa adjudicatària, s'aplicarà una penalització de 200 €.

Aquesta penalització es descomptarà, amb caràcter preferent, de la següent factura pendent de pagament. En cas que no existeixi, la penalització adquirirà la consideració d'import líquid exigible per l'Institut, que l'empresa adjudicatària haurà de satisfer en els termes que determini BIT.

Fora d'abast.

No formen part d'aquest servei la creació/edició de continguts, evolutius o noves funcionalitats.

3.6. Manteniment preventiu i correctiu de les pantalles professionals

El servei de manteniment preventiu i correctiu té per objecte garantir la continuïtat operativa, la seguretat física, i el correcte funcionament de les pantalles professionals instal·lades, els seus suports, elements de protecció o altres elements associats subministrats en el marc del present contracte. Aquest servei inclou totes les actuacions necessàries per a la revisió, detecció, diagnosi i resolució d'incidències relacionades amb les pantalles, així com la gestió de la garantia del fabricant quan aquesta sigui aplicable.

Manteniment preventiu.

L'empresa adjudicatària realitzarà, amb la periodicitat que sigui requerida per BIT o segons recomanacions del fabricant, les accions de manteniment preventiu orientades a garantir la durabilitat i bon estat de les pantalles i dels seus elements d'instal·lació.

A requeriment de BIT l'empresa adjudicatària haurà de tenir documentat la relació d'accions realitzades relacionades amb aquest manteniment.

Aquestes accions podran incloure, entre d'altres:

- Revisió visual de l'estat físic de la pantalla, suport i carcassa de protecció.
- Verificació de la correcta fixació dels suports i elements d'ancoratge.
- Neteja tècnica bàsica, amb productes i procediments adequats segons el fabricant, limitada a les reixetes i obertures de ventilació de la pantalla, si escau.
- Comprovació de connexions elèctriques i de xarxa, presència de tensió i estat general del cablejat.
- Detecció de riscos potencials relacionats amb vibracions, sobreescalfaments o degradació d'elements físics.

Servei de suport (Manteniment correctiu).

L'empresa adjudicatària serà responsable de la tramitació, gestió i seguiment de les incidències relacionades amb les pantalles professionals instal·lades, així com la resolució de consultes que puguin sorgir durant el seu funcionament.

En el cas d'incidències cobertes per la garantia del fabricant de les pantalles o dels seus components, l'empresa adjudicatària realitzarà les següents accions:

- Comunicació amb el fabricant o distribuïdor per a l'obertura del cas de garantia.
- Coordinació logística amb BIT i amb el fabricant per a la retirada, transport i eventual reubicació temporal de l'equip afectat.
- Reposició o reparació de la pantalla o del component corresponent, d'acord amb les condicions de garantia establertes pel fabricant.
- Reinstal·lació i verificació del funcionament de l'equip reparat o substituït, i tancament formal de la incidència amb comunicació a BIT.

El temps invertit en aquestes gestions no comportarà cap cost afegit per a BIT.

Canals i horari.

- L'atenció d'incidències es realitzarà de dilluns a divendres, de 8:00 a 18:00h, excepte els dies festius a la ciutat de Barcelona.
- El canal de comunicació serà telefònic i/o correu electrònic acordat entre BIT i l'empresa adjudicatària.
- El proveïdor registrarà cada incidència (data/hora, descripció, classificació, estat i data de tancament) i quan sigui requerit remetrà a BIT un resum del detall d'incidències i nivells de servei assolits.

Acord de Nivell de Servei.

Atenció en 8h i tramitació de la resolució en 48h en horari laborable, sempre i quan les actuacions depenguin exclusivament de l'empresa adjudicatària.

En cas que, davant d'una avaria d'una pantalla, la tramitació de la garantia amb el fabricant per a la seva reparació o reposició superi les 48 hores laborables, i sempre que BIT consideri necessari disposar d'una solució temporal, l'empresa adjudicatària haurà de subministrar i instal·lar provisionalment una pantalla de substitució fins a la resolució definitiva del cas.

3.7. Gestió del canvi i formació

L'objecte d'aquest apartat és garantir l'adopció efectiva del sistema de cartelleria digital per part dels col·lectius implicats, assegurant l'autonomia en la publicació de continguts i la correcta administració de la plataforma.

Abast de la prestació

- Sessió de formació pràctica per a personal no tècnic orientada a publicar i gestionar continguts de manera autònoma.
- Sessió de formació per a administradors tècnics, incloent la gestió d'usuaris, plantilles i altres funcionalitats d'administració.
- Manual o guies ràpides d'ús en format digital que recullin els procediments bàsics i els fluxos habituals de treball.

En finalitzar la formació, les persones usuàries han de poder publicar continguts de forma autònoma, i els administradors tècnics han de poder configurar i administrar el sistema d'acord amb les necessitats de BIT.

4. CONDICIONS ESPECÍFIQUES DEL CONTRACTE

4.1. Organització de les prestacions i model de relació

El Model de Relació té com a objectiu definir les funcions i responsabilitats de l'adjudicatari i de BIT per tal d'assegurar el compromís d'acompliment de les respectives obligacions. El Model de Relació contempla un marc que permet acordar el contingut i nivell de prestació del servei per part de l'adjudicatari, així com articular un seguiment de la prestació del servei.

L'adjudicatari pot ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb BIT així com els mecanismes de control propis del servei.

4.2. Equip de treball

Per tal de poder atendre de forma adient les activitats descrites en el punt 0, l'adjudicatari haurà de garantir un equip de professionals suficientment qualificats i que s'haurà d'ajustar als següents perfils professionals:

Perfil	Funcions i experiència
Personal tècnic d'instal·lació, manteniment preventiu i correctiu de les pantalles professionals	Instal·lació física de les pantalles professionals Posta en marxa de les pantalles Manteniment preventiu i correctiu de les pantalles professionals Es requereix 2 anys o més d'experiència en la instal·lació i manteniment de pantalles professionals
Personal tècnic de manteniment i suport del software	Implantar i configurar el software de gestió de continguts digitals Atendre i resoldre consultes i incidències relacionades amb el software de gestió de continguts digitals i la configuració de la plataforma Formació del software Es requereix 2 anys o més d'experiència en manteniment i suport del software
Persona interlocutora i responsable del contracte	Un dels tècnics serà el responsable de la interlocució del servei, entre la persona responsable de BIT i la resta de l'equip tècnic de l'adjudicatari, especialment en allò relacionat amb les tasques de seguiment i control del contracte Es requereix 2 anys o més d'experiència en tasques com a responsable de contracte de similars característiques

L'empresa adjudicatària, per temes de seguretat i control, haurà de lliurar a BIT la relació actualitzada dels professionals assignats a les prestacions del contracte amb les dades que els puguin identificar.

Amb l'objectiu d'establir un model de relació àgil i efectiu BIT designarà una persona del departament com a responsable del procés que serà l'encarregat de supervisar la qualitat tècnica de les prestacions i aquesta serà la persona a la que aquest equip de professionals reportarà la seva activitat.

BIT es reserva el dret de verificar les capacitats del personal que participa en el contracte 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.

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 BIT i les persones que substitueixin al personal sortint han de complir els mateixos requeriments que l'equip inicial, a més hauran de rebre l'aprovació de BIT per a la seva incorporació.

4.3. Lloc de prestació del contracte

Totes les ubicacions on s'hauran de realitzar la instal·lació i suport presencial de les pantalles professionals son edificis municipals de l'Ajuntament de Barcelona i estan situats a la ciutat de Barcelona.

El servei no presencial es prestarà des de dependències de l'empresa adjudicatària, o des d'aquelles que aquesta designi. En cap cas es realitzarà en dependències municipals.

Tots els costos de desplaçament derivats de l'execució del contracte hauran d'estar inclosos en l'oferta econòmica presentada i no implicaran cap cost afegit per a l'Ajuntament de Barcelona.

4.4. Calendari i horaris del servei

L'empresa adjudicatària prestarà les prestacions descrites en aquest plec de dilluns a divendres, de 8:00 a 18:00h, sempre i quan siguin dies laborables a la ciutat de Barcelona. L'empresa adjudicatària prestarà aquest horari considerant que la jornada laboral dels integrants de l'equip assignat és de com a màxim 8 hores diàries.

L'empresa adjudicatària ha de contemplar que, ocasionalment, es pot ampliar fora de l'horari laboral habitual per atendre circumstàncies específiques. Exemples de suports excepcionals poden ser: incidències de llarga durada, incidències sobrevingudes en horari no laboral, esdeveniments puntuals com processos electorals, etc. Aquest fet no podrà ser objecte de facturació addicional.

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

4.5. Eines de gestió de les prestacions

A continuació es detallen algunes de les eines de les quals disposa BIT per a la gestió i operació de la prestació:

- **Eina de gestió de peticions, de configuració i inventari**: Aplicació web/intranet mitjançant la qual BIT gestiona el catàleg de serveis TIC, la CMDB (*Configuration Management Database*) i les peticions.
- **Base de dades inventari**: El proveïdor haurà de mantenir actualitzada la informació d'inventari i estat de les prestacions en la base o bases de dades de configuració segons BIT determini.

Respecte a l'ús de les eines s'hauran de complir els següents punts:

- L'adjudicatari haurà d'usar les eines proposades per BIT en les condicions que aquest estableixi i es farà càrrec (en cas que hi hagi) dels costos associats a l'ús d'aquestes eines (accés i integració amb altres eines).

- L'adjudicatari podrà proposar modificacions a les eines per obtenir una millor eficiència i qualitat en el servei. Qualsevol petició de canvi haurà d'estar documentada prèviament perquè BIT pugui analitzar la conveniència de la seva implantació.
- L'adjudicatari podrà fer ús d'eines addicionals, però això no l'eximeix del compliment i de l'ús de les eines que hagi determinat BIT. Aquestes eines no poden posar en risc la continuïtat del servei després de la finalització de la relació contractual.
- BIT es reserva el dret de modificar aquestes eines amb el previ avís suficient perquè els proveïdors puguin adaptar-se a les mateixes:
  - BIT podrà evolucionar les eines escollides en qualsevol moment de la durada del contracte.
  - BIT es reserva el dret d'incorporar noves eines. En qualsevol cas, es donarà un preavís als proveïdors d'un mínim de dos mesos abans de la seva implantació.
- La informació continguda en les eines haurà de coincidir amb la realitat dels treballs. BIT no tindrà en consideració cap informació que no estigui continguda en les eines que determini BIT.
- La correcta actualització de la informació és requisit del servei, processos i solucions. Qualsevol defecte en la informació es considerarà un defecte del propi servei.

4.6. Idioma

Obligatòriament l'adjudicatari elaborarà en català la documentació de gestió i documentació tècnica requerida i lliurada durant l'execució del contracte.

4.7. Repositori de documentació

BIT posarà a disposició de l'adjudicatari un repositori on intercanviar la documentació referent a la provisió del servei. En aquesta eina l'adjudicatari desarà també els documents lliurables resultants de l'execució del servei.

L'adjudicatària serà la responsable de mantenir la informació actualitzada i seguint les polítiques, nomenclatura i control de versions determinats per BIT.

5. FACTURACIÓ

Fita	Any facturació	Data límit	Import de facturació
Fita núm. 1-2026	2026	15 desembre 2026	Compra i posta en marxa de les pantalles
Fita núm. 2-2026	2026	15 desembre 2026	Subscripció i suport
Fita núm. 1-2027	2027	15 desembre 2027	Subscripció i suport

Durant l'execució del contracte l'adjudicatari facturarà l'import corresponent a cada fita quan assoleixi cada fita de les descrites a la taula anterior. Cada fita es descriu a continuació:

- Fita núm. 1-2026: El servei d'instal·lació i posta en marxa de les pantalles s'ha executat.

- Per motius d'organització interna, BIT podrà decidir que la d'instal·lació i posta en marxa es realitzi de forma esglaonada en el temps. En aquest cas, la fita es considerarà assolida quan pantalles es trobin a disposició de l'Ajuntament, ja sigui a les instal·lacions municipals o bé custodiades per l'empresa a petició de BIT.

- Fita núm. 2-2026: El software de gestió de continguts està implantat a l'Ajuntament i operatiu per funcionar amb les pantalles. La llicència anual comença a ser efectiva.
- Fita núm. 2027: Renovació de la subscripció de la llicència del software de gestió de continguts i servei de suport.

S'entén que qualsevol fita és assolida quan ha estat validada i formalment acceptada pel responsable de contracte de BIT.

6. PROPOSTA TÈCNICA I ECONÒMICA

Els licitadors presentaran la seva proposta d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen 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.

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 presentarà un sobre electrònic**, el sobre electrònic AC**, on s'inclourà la documentació administrativa i 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'ha 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.

7. CLÀUSULES GENERALS DE SEGURETAT

7.1. Seguretat dels sistemes d'informació, protecció de dades i compliment normatiu

BIT 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.

BIT, 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 del REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, 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 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat.

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 BIT indistintament. De conformitat als seus estatuts s'ha d'entendre que BIT 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.

7.2. Conformitat amb l'esquema nacional de seguretat

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 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS).

Donada la naturalesa del contracte, l'empresa adjudicatària haurà de donar compliment als requeriments establerts a l'ENS pel **nivell MIG.**

D'igual manera per qualsevol obligació legal que recaigui en l'Ajuntament, el proveïdor haurà de donar compliment per la part que li correspongui segons l'abast del contracte.

L'empresa adjudicatària haurà d'acreditar la conformitat amb l'ENS mitjançant alguna de les vies previstes a l'art. 38 de l'ENS, entre les que es troben les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.
- Informe d'auditoria de compliment. L'empresa adjudicatària serà responsable de disposar d'un informe d'auditoria (en el que l'ENS formi part del seu abast) de compliment on es detalli que els productes de seguretat, equips, sistemes i aplicacions compleixen amb totes les mesures aplicables de l'Esquema Nacional de Seguretat.

L'empresa adjudicatària garantirà l'accés per part de BIT a auditar tota la informació necessària per donar compliment a aquestes regulacions (procediments, anàlisi de riscos, registre d'incidents, pla d'adequació, etc.).

D'igual manera, en el cas que es subcontracti, totalment o parcial, les prestacions objecte del present contracte, les empreses subcontractades quedaran a totes les mesures de seguretat d'aplicació a l'empresa adjudicatària dins de l'abast dels servis subcontractats. És responsabilitat de l'empresa adjudicatària assegurar-se que l'empresa subcontractada compleix amb el nivell de l'ENS corresponent, així com amb el conjunt de mesures de seguretat determinades en aquest clausulat de seguretat.

7.3. Responsable de seguretat

L'empresa adjudicatària 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 BIT 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 BIT.
- Assegurar que tot el personal de l'empresa adjudicatària 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.

7.4. Clàusula de propietat intel·lectual

Tot i reconeixent l'autoria de les persones que els hagin elaborat, la propietat intel·lectual dels treballs realitzats a l'empara d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió de la mateixa ni es permet el seu ús sense autorització expressa d'aquest ajuntament.

L'empresa adjudicatària accepta expressament que els drets d'explotació dels productes derivats d'aquest plec corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, transformació o

modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

7.5. Confidencialitat

L'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària 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.

7.6. Clàusula programari i metodologia de desenvolupament

L'empresa contractada, disposarà del programari necessari i farà servir la metodologia implantada pel BIT per al desenvolupament de les prestacions contractades.

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'empresa adjudicatària.

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 adjudicatària, 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.

L'empresa adjudicatària 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 les prestacions contractades.

7.7. Delegat de protecció de dades

Si l'empresa adjudicatària ha anomenat un delegat de protecció de dades, procedirà a comunicar les seves dades de contacte a l'Oficina del Delegat de Protecció de Dades de l'Ajuntament perquè es puguin establir els circuits de comunicació establerts en el Reglament General de Protecció de Dades. En cas de no haver definit aquesta figura, s'haurà de proporcionar el contacte de la persona encarregada del tractament de dades personals.

7.8. Auditoria

BIT es reserva el dret d'auditar que l'empresa adjudicatària vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

- Auditoria de seguretat periòdica/planificada: BIT podrà realitzar auditories de seguretat planificades per verificar el compliment dels requeriments de seguretat, de l'oferta de l'empresa adjudicatària.
- Auditoria sobrevinguda: addicionalment BIT podrà efectuar més auditories que les planificades respecte el servei que s'està prestant.

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

L'empresa adjudicatària proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per BIT.

La realització de l'auditoria en cap moment eximirà l'empresa adjudicatària del compliment dels compromisos derivats de la prestació del contracte.

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

7.9. Gestió d'incidents

L'empresa adjudicatària informarà a la Direcció de Serveis de Seguretat de la Informació de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per BIT.

L'empresa adjudicatària ha de disposar d'un procediment de notificació i gestió d'incidents de seguretat, on es registrin tots els incidents de seguretat que es produeixin.

L'empresa adjudicatària col·laborarà amb el Departament de Seguretat de BIT en la resolució de qualsevol incident produït en el seu entorn, i que afecti als sistemes d'informació o a les dades subjectes a l'aplicació del present contracte, proporcionant totes les evidències requerides.

En cas que l'incident afecti els sistemes i els recursos propietat de l' adjudicatari, serà responsabilitat d'aquest realitzar les accions de contenció i resolució necessàries per restaurar el servei.

L'empresa adjudicatària haurà de documentar els incidents de seguretat i indicar el tipus d'incidència, moment en que es produeix, moment en que s'ha detectat, persona que fa la notificació, a qui es comunica, els efectes d'aquesta, moment en que se soluciona, descripció de la solució i persona que ho realitza. A l'esmentat registre s'han d'establir, a més, els procediments realitzats de recuperació de la informació, persona que executa el procés i la informació restaurada.

La documentació d'un incident de seguretat de la informació i la investigació i resposta consegüent s'han de preparar mitjançant informes de forma cronològica i lliurar-se a al Departament de Seguretat de BIT, en el cas que hi hagi hagut afectació al servei prestat.

7.10. Còpies de seguretat

L'empresa adjudicatària haurà de comptar amb procediments i mecanismes per fer còpies de seguretat de la informació. Aquests procediments han de tenir en compte els processos per fer les còpies de seguretat, la periodicitat, els mètodes d'emmagatzematge i custòdia, els processos de restauració, etc. de manera que garanteixin la recuperació de la informació davant d'una situació de pèrdua o destrucció d'aquesta.

L'empresa adjudicatària ha de garantir que les còpies de seguretat es facin com a mínim amb una periodicitat setmanal.

L'empresa adjudicatària ha d'emmagatzemar còpies de seguretat de la informació en una ubicació alternativa d'aquella en què es processa habitualment.

A més, l'empresa adjudicatària haurà de disposar de mecanismes per a la realització periòdica de proves de restauració de les dades i les aplicacions. Hauran de ser capaços de restaurar les dades a partir de la darrera còpia de seguretat i de fer de manera periòdica aquestes proves amb dades reals.

7.11. Seguretat física i de l'entorn

7.11.1. Accés físic a les instal·lacions de processament de dades

L'empresa adjudicatària garanteix que disposa de mecanismes d'autenticació i control per garantir que únicament el personal autoritzat accedeixi a les instal·lacions i a les zones de dintre les dependències.

L'empresa adjudicatària haurà de contemplar, en funció de les seves necessitats, la implantació de les mesures de seguretat següents:

- Emissió d'autoritzacions per accedir a ubicacions físiques i a les diferents dependències.
- Mesures de dissuasió i vigilància (per exemple: càmeres de videovigilància).
- Mesures de monitorització i alertes de seguretat davant d'intrusions.
- Mesures de protecció contra accessos no autoritzats físics (per exemple: panys amb clau física o digital, etc.)
- Altres mesures de seguretat (per exemple: vigilants de seguretat).

7.11.2. Accés físic a les Zones de Seguretat

L'empresa adjudicatària identificarà dins de les seves instal·lacions les zones que requereixin mesures de seguretat addicionals (per exemple: el CPD) i implementarà els controls necessaris que permetin identificar i només deixar passar les persones autoritzades. S'ha de garantir que l'accés es faci de forma individual i s'han de guardar els registres de les entrades i sortides en aquestes àrees.

7.11.3. Seguretat del cablejat

L'empresa adjudicatària implementarà mesures per garantir la seguretat del cablatge als seus centres y dependències.

7.12. 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 BIT 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 BIT posa a disposició.

Autenticació interna
Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per BIT basats en protocols estàndards de seguretat. L'empresa

proveïdora haurà d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant, IDP) per a l'autenticació dels usuaris.

La integració amb la solució IDP es podrà fer mitjançant les següents opcions:

- Integració mitjançant l'estàndard OpenID Connect (OAuth 2.0), utilitzant el flux d'autenticació de codi d'autorització amb PKCE (intercanvi de clau codificada)
- En cas de que l'aplicació no suporti l'ús del protocol OpenID Connect, la integració es farà mitjançant l'estàndard SAML 2.0.

Autenticació externa

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

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació (2FA), requerint així una verificació de la identitat de l'usuari que sol·licita accés. L'empresa adjudicatària aplicarà el mateix 2FA que sigui d'aplicació a l'Ajuntament i, en cas de no ser possible haurà de justificar aquesta impossibilitat tècnica, tot aplicant un 2FA diferent que haurà de ser validat per BIT.

7.13. Autorització dels usuaris als sistemes

BIT disposa d'un repositori centralitzat d' autoritzacions dels usuaris corporatius, basat en un directori actiu, que és d'on recull les autoritzacions el IDP corporatiu. L'empresa adjudicatària haurà d'assegurar que les autoritzacions es troben delegades en aquest repositori central d'autoritzacions.

En cas que l'empresa adjudicatària no pugui delegar l'autorització per impediments greus del sistema, com a mínim, hauran d'integrar-se amb l'eina de gestió i govern de les identitats per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els rols funcionals definits a GID (capa de negoci).

Aquesta integració podrà ser de dos tipus:

- Integració directa amb la GID, si l'aplicació pot publicar els usuaris i perfils a través d'un servei web que es pugui consumir mitjançant un connector des de l'eina de gestió d'identitats.
- En cas de no ser possible la connexió directa amb la GID, l'aplicació haurà d'enviar un fitxer diari a la GID i configurar un connector de processament de fitxers per tal de representar les autoritzacions a l'eina.

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.

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 la Direcció de Seguretat de la Informació de BIT.

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 rols de seguretat, entenent com a rol una entitat que dona accés a una sèrie d'operacions.

Sota la premissa d'aquests criteris generals, l'empresa adjudicatària 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'empresa adjudicatària per incloure nous punts a tractar o adaptacions dels punts existents.

7.14. Inventari d'actius

L'empresa adjudicatària 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.

7.15. Configuració de seguretat

L'empresa adjudicatària 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.

7.16. Manteniment

L'empresa adjudicatària haurà de mantenir l'equipament físic i lògic que constitueix el sistema i/o infraestructura administrada.

L'empresa adjudicatària haurà de mantenir actualitzats els productes utilitzats en l'abast del plec d'acord a la política acordada amb BIT.

La política d'actualitzacions està basada en el nivell de criticitat de la vulnerabilitat valorada segons l'última versió publicada de l'estàndard públic CVSS (Common Vulnerability Scoring System), segons el nivell de CVSS les actualitzacions per la correcció de vulnerabilitats s'hauran de produir dins d'uns terminis específics (en funció del nivell d'exposició, la criticitat de la vulnerabilitat i la criticitat de l'actiu afectat), detallats en la taula següent:

		Nivell d'exposició			
		Exposat a internet		**No exposat a internet**	
		Criticitat de l'actiu		**Criticitat de l'actiu**	
		Crític	**No crític**	**Crític**	**No crític**
Criticitat vulnerabilitat	**CVSS <=3**	20 dies	40 dies	40 dies	40 dies
	3 < CVSS <= 6	5 dies	1 mes	20 dies	20 dies
	6 < CVSS <=8	1 dia	5 dies	5 dies	5 dies
	CVSS > 8	1 dia	2 dies	1 dia	5 dies

El proveïdor s'haurà d'involucrar en tot el cicle de vida de les vulnerabilitats, des de la seva detecció fins a la mitigació d'aquesta. Haurà de tenir un seguiment proactiu de les vulnerabilitats que es puguin produir amb un seguiment continu del anunci de defectes, mantenint el contacte amb els fabricants per tenir coneixement de les possibles solucions que aquest proposin per corregir-les.

7.17. 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 la Direcció de Seguretat de la Informació de BIT, qui ha d'assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament i 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 la Direcció de Seguretat de la Informació de BIT i/o seguir els estàndards i normes de BIT.

7.18. Certificats

La Direcció de Seguretat de la Informació de BIT serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de la Direcció de Seguretat de la Informació de BIT. 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 per la Direcció de Seguretat de la Informació de BIT 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.

7.19. Antimalware

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

BIT 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.

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

7.20. Còpies de seguretat

L'empresa adjudicatària 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 BIT.

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, BIT es reserva el dret de demanar el xifrat de les dades. L'abast de les còpies inclou:

- Informació de treball de BIT.

- 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.

A banda de ser responsable de la generació de les còpies de seguretat, l'empresa adjudicatària serà responsable de garantir que aquestes son perfectament funcionals, per mitjà de la realització d'exercicis periòdics de recuperació de backups. Els exercicis han de poder donar cobertura a tots els actius sota el present contracte dins d'un termini màxim de 1 any.

7.21. Control d'accés

Segregació de funcions i tasques

L'empresa adjudicatària 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.

7.22. Explotació

7.22.1. Gestió de la configuració

L'empresa adjudicatària 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.

7.22.2. Gestió de canvis

L'empresa adjudicatària 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.

7.22.3. Protecció de claus criptogràfiques

- L'empresa adjudicatària utilitzarà programes avaluats o dispositius criptogràfics certificats.
- S'empraran algoritmes acreditats pel "Centre Criptològic Nacional".

7.23. Protecció dels serveis

7.23.1. Protecció enfront de la denegació de servei

L'empresa adjudicatària establirà mesures preventives i reactives enfront d'atacs de denegació de servei (DoS Denial of Service). Per tal de garantir-ho:

- 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.

7.24. Estàndards, polítiques i procediments de seguretat

L'empresa adjudicatària durant la prestació del servei estarà obligada a complir i aplicar la normativa de seguretat de BIT, així com tots els procediments operatius definits per aquest. En aquest sentit, BIT posarà a disposició les esmentades normatives de seguretat i procediments a través dels canals habilitats a aquest efecte.

L'empresa adjudicatària haurà de tenir elaborada una normativa interna en matèria de seguretat de la informació i estar subjecta a revisions periòdiques.

L'empresa adjudicatària haurà de fer difusió entre el seu personal de les normes que els afectin i de les conseqüències del seu incompliment.

7.25. Gestió del personal

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.

Signatura de clàusules de confidencialitat

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.

Formació i conscienciació

L'empresa adjudicatària 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'empresa adjudicatària 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'empresa adjudicatària ha realitzat sobre el personal assignat a l'execució del contracte.

7.26. Control d'accés

Accés local

L'empresa adjudicatària 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.

Accés remot

L'empresa adjudicatària 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 BIT per als sistemes de l'Ajuntament.

7.27. 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'empresa adjudicatària 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 BIT.

7.28. Dimensionament/gestió de capacitats

L'empresa adjudicatària disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada.

7.29. Anàlisis forenses

L'execució d'anàlisis forenses és responsabilitat exclusiva de la Direcció de Seguretat de la Informació de BIT. L'empresa adjudicatària 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 la Direcció de Seguretat de la Informació de BIT i l'empresa adjudicatària.

7.30. Clàusula de comunicacions externes

L'empresa adjudicatària 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'empresa adjudicatària 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.

7.31. Xifrat en dispositius

Els dispositius (com ara: ordinadors de taula, portàtils, telèfons mòbils, tauletes electròniques, etc.) propietat de l'empresa adjudicatària han de disposar d'una solució de xifratge del disc dur per salvaguardar les dades en cas de pèrdua o robatori.

7.32. Protecció del lloc de treball

Lloc de treball buit

L'empresa adjudicatària 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.

Protecció d'equips

L'empresa adjudicatària 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'empresa adjudicatària 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 comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a BIT.

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 trànsit entrant a l'equip al mínim necessari.

7.33. Protecció dels suports informàtics

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

Etiquetat

L'empresa adjudicatària 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.

Transport

L'empresa adjudicatària garantirà que els dispositius romanen sota control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'empresa adjudicatària 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.

Esborrat i destrucció

L'empresa adjudicatària haurà de seguir els estàndards i normes de BIT 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.

Periòdicament i segons les necessitats de recurrència d'aquestes activitats, s'haurà d'informar i lliurar al responsable del contracte el certificat de destrucció corresponent, on quedarà especificat com a mínim, el identificador dels actius, el mètode d'esborrat i/o destrucció emprat, la data de l'activitat i el destí dels actius.

7.34. Protecció de la informació

Neteja de documents

L'empresa adjudicatària 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.

Protecció del correu electrònic

En el cas de que l'empresa adjudicatària 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'empresa adjudicatària.
- 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'empresa adjudicatària 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*.

El responsable del contracte de l'Ajuntament avaluarà si el contracte ha de gestionar informació sensible, especialment protegida en relació a la protecció de dades personals, confidencial de l'Ajuntament o de les tecnologies municipals (adreces IP, usuaris, credencials,...)

En cas afirmatiu, l'Ajuntament facilitarà a l'empresa adjudicatària un correu electrònic de l'Ajuntament (@ext.bcn.cat) el qual es convertirà en la via de comunicació entre l'empresa adjudicatària i l'Ajuntament.

Aquesta mesura vol evitar que les empreses externes retinguin informació confidencial de l'Ajuntament en servidors de correu aliens a l'entorn municipal, durant i sobretot, un cop finalitzat el contracte.

7.35. Protecció de les instal·lacions

Les instal·lacions de l'empresa adjudicatària 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.

7.36. Clàusules de seguretat per a la prestació de serveis SaaS no exclusius

El present punt recull les mesures de seguretat que l'empresa adjudicatària haurà de complir per al servei en la seva modalitat SaaS (Software as a Service), el qual no és d'ús exclusiu de l'Ajuntament. Aquestes mesures seran d'obligat compliment durant tota la vigència del contracte i s'aplicaran a tots els components, sistemes, entorns i personal implicats en la prestació del servei objecte de l'acord.

7.36.1. Infraestructura del servei

L'arquitectura del servei estarà dissenyada en tres capes diferenciades: presentació o front-end, aplicació o middleware, i dades o back-end. Cadascuna d'aquestes capes s'implementarà en servidors físics o lògics independents. En particular, el servidor de base de dades s'instanciarà en un sistema separat del d'execució de l'aplicació, garantint l'aïllament entre les capes de processament i d'emmagatzematge.

La comunicació entre l'aplicació i la base de dades estarà xifrada en tot moment i es realitzarà mitjançant un usuari genèric d'aplicació d'ús exclusiu per al servei prestat a l'Ajuntament. Tota la informació de l'Ajuntament emmagatzemada a la plataforma de l'empresa adjudicatària romandrà xifrada en repòs a les bases de dades.

L'empresa adjudicatària aplicarà mecanismes de xifrat robust tant en repòs com en trànsit. Per al xifrat en repòs s'utilitzarà AES-256 o un algorisme equivalent reconegut com a segur per les autoritats i organismes de referència en la matèria. Per a les comunicacions en trànsit s'emprarà el protocol TLS en la seva versió 1.2 o superior. En cas que l'evolució dels estàndards criptogràfics determini la obsolescència d'algun dels algorismes o protocols indicats, l'empresa adjudicatària els substituirà per les versions actualitzades que siguin considerades segures, comunicant-ho prèviament a l'Ajuntament.

La xarxa sobre la qual es desenvolupa el servei es trobarà aïllada de la xarxa interna de l'empresa adjudicatària. No es permetrà l'ús d'entorns compartits entre clients sense que existeixi un aïllament lògic complet que impedeixi qualsevol accés o filtració de dades entre ells.

No es permet l'ús de dades reals en entorns que no siguin de producció. Per a la realització de proves s'hauran d'utilitzar exclusivament conjunts de dades ficticis. En el cas excepcional que fos necessari realitzar una còpia de les dades de l'entorn de producció, aquestes hauran de ser prèviament emmascarades o sotmeses a un procés d'alteració irreversible que impedeixi el reconeixement de la informació original.

Tots els sistemes implicats en la prestació del servei que puguin ser afectats per programari maliciós hauran de disposar de protecció antivirus o antimalware operativa i permanentment actualitzada, tant en les signatures de detecció com en el motor d'anàlisi.

7.36.2. Seguretat en les connexions i comunicació

7.36.2.1. Connexions entre l'Ajuntament i l'empresa adjudicatària

Per a la connexió des d'una aplicació corporativa de l'Ajuntament al servei de l'empresa adjudicatària es requerirà l'aplicació conjunta de les mesures de seguretat següents: control d'adreça IP d'origen, de manera que el servei sigui accessible exclusivament des de les adreces autoritzades per l'Ajuntament; control de sessió única per evitar accessos concurrents no autoritzats; control en destinació que garanteixi que l'aplicació només sigui accessible des de l'aplicació corporativa d'origen; autenticació mitjançant credencials i certificat d'origen, amb missatges signats pel certificat emès per l'Autoritat de Certificació de l'Ajuntament; i comunicació mitjançant protocol HTTPS amb certificat digital emès per una Autoritat de Certificació reconeguda.

S'implementarà validació mútua de certificats entre ambdues parts i control d'integritat en totes les comunicacions per garantir que la informació no ha estat alterada durant el trànsit.

7.36.2.2. Intercanvi d'informació

Les connexions amb l'empresa adjudicatària s'iniciaran sempre des de l'Ajuntament.

L'intercanvi massiu d'informació, incloent-hi qualsevol càrrega inicial de dades, es realitzarà mitjançant SFTP, EDITRAN xifrat o un mitjà equivalent que garanteixi la confidencialitat i la integritat de la informació transmesa. Els intercanvis puntuals d'informació que es produeixin fora de les aplicacions implicades en el servei, com ara l'enviament de suports o comunicacions per correu electrònic, hauran de ser prèviament formalitzats i acordats per escrit entre l'Ajuntament i l'empresa adjudicatària, establint-se les mesures de protecció adequades per a cada cas.

Queda prohibit l'ús de canals no xifrats per a qualsevol intercanvi d'informació entre ambdues parts, inclòs el correu electrònic convencional sense mecanismes de xifrat.

7.36.3. Detecció d'intrusions i prevenció de fuita de dades

L'empresa adjudicatària utilitzarà eines de detecció i prevenció d'intrusions de xarxa per identificar i bloquejar de manera proactiva activitats malicioses o accessos no autoritzats als sistemes implicats en la prestació del servei.

Així mateix, s'implementaran solucions de prevenció de fuita de dades que permetin detectar i bloquejar qualsevol intent d'exfiltració no autoritzada d'informació de l'Ajuntament, ja sigui de forma intencionada o accidental, a través de qualsevol canal de comunicació o dispositiu.

7.36.4. Retenció i disposició de dades

L'emmagatzematge de dades i el temps de la seva retenció es limitaran a la quantitat estrictament exigida pels requisits legals, reglamentaris i de negoci aplicables en cada moment. La base de dades associada al servei, els fitxers i les còpies de seguretat es dimensionaran per donar compliment a aquests requisits. Amb caràcter general, el temps de retenció s'estableix en cinc anys, sens perjudici de les obligacions legals específiques que poguessin exigir un termini diferent en funció de la tipologia de les dades tractades.

L'empresa adjudicatària disposarà de processos documentats per a l'eliminació segura de les dades quan deixin de ser necessàries per a la prestació del servei o quan finalitzi el període de retenció establert. Aquests processos garantiran que la informació eliminada no pugui ser recuperada per cap mitjà.

Un cop finalitzat el contracte per qualsevol causa, l'empresa adjudicatària lliurarà a l'Ajuntament la totalitat de les dades en format xifrat i en un format estàndard que permeti la seva reutilització sense dependència del proveïdor. Posteriorment, procedirà a l'eliminació de totes les còpies de dades que romanguin en el seu poder, incloent-hi les còpies de seguretat, en un termini màxim de trenta dies naturals. L'eliminació s'haurà de realitzar mitjançant tècniques segures, com l'esborrat criptogràfic o la destrucció certificada de suports. Finalitzat el procés, l'empresa adjudicatària emetrà i lliurarà a l'Ajuntament un certificat formal de destrucció que acrediti que cap dada de l'Ajuntament roman en els seus sistemes o en els de tercers implicats en la prestació del servei.

7.36.5. Localització i custodia de les dades

Totes les dades de l'Ajuntament vinculades a la present prestació de servei hauran de residir i ser processades exclusivament dins de l'Espai Econòmic Europeu durant tota la vigència del contracte. Aquesta obligació abasta, amb caràcter enunciatiu i no limitatiu, les dades d'aplicació, les metadades, els registres d'auditoria, els fitxers adjunts, les configuracions, les còpies de seguretat i qualsevol altra informació derivada de l'ús del servei.

Les dades emmagatzemades tant en la infraestructura del proveïdor de solucions al núvol com en els sistemes propis de l'empresa adjudicatària estaran ubicades en centres de dades situats al territori de l'Espai Econòmic Europeu. Aquests centres hauran de disposar, com a mínim, de certificació Tier III de l'Uptime Institute o equivalent acreditat, capacitat de manteniment

concurrent sense interrupció del servei i redundància en els components d'infraestructura garantint l'alta disponibilitat i la continuïtat operativa.

Es garantirà la redundància geogràfica mitjançant l'ús de, com a mínim, dos centres de dades situats en ubicacions geogràfiques diferenciades dins de l'Espai Econòmic Europeu, de manera que es pugui assegurar la continuïtat del servei davant d'incidències que afectin un dels centres.

No es permetrà cap transferència de dades fora de l'Espai Econòmic Europeu, ni tan sols amb caràcter temporal o transitori, sense l'autorització prèvia, expressa i per escrit de l'Ajuntament. Aquesta restricció s'aplica igualment a les dades en repòs, a les dades en trànsit, a les dades en processament i als accessos remots per part de personal tècnic o de suport. Queda expressament prohibit que personal ubicat fora de l'Espai Econòmic Europeu pugui accedir a les dades de l'Ajuntament, llevat d'autorització expressa i per escrit d'aquest i sempre que es compleixin les garanties exigides pel Reglament General de Protecció de Dades.

7.36.6. Continuïtat de negoci

L'empresa adjudicatària disposarà d'una política de continuïtat de negoci documentada i actualitzada que constitueixi el marc de referència per garantir la continuïtat dels serveis prestats a l'Ajuntament. Aquesta política establirà els objectius, l'abast i el compromís ferm de l'empresa adjudicatària amb la continuïtat del servei.

7.36.6.1. Identificació d'activitats essencials i anàlisi d'impacte

S'identificaran les activitats essencials i els recursos necessaris que sustentin el servei prestat a l'Ajuntament. Per a això, l'empresa adjudicatària disposarà d'un inventari d'actius i recursos necessaris per a la prestació del servei, classificats segons la seva tipologia i criticitat, incloent-hi maquinari, programari, comunicacions i instal·lacions.

S'elaborarà una Anàlisi de l'Impacte del Negoci que estableixi les estratègies, prioritats i temps de recuperació davant de les possibles interrupcions que poguessin produir-se. Es determinaran i categoritzaran els impactes d'aquestes interrupcions en funció dels temps i nivells de servei acordats, identificant per a cada escenari si és possible mantenir l'execució de les activitats crítiques amb normalitat i sense impacte en els nivells de servei, o si únicament és possible mantenir-les de forma limitada durant un període de temps determinat.

7.36.6.2. Anàlisi de riscos

L'empresa adjudicatària elaborarà una anàlisi de riscos que contempli les amenaces, vulnerabilitats i impactes que afecten el servei prestat a l'Ajuntament. Disposarà d'una metodologia d'anàlisi de risc documentada que permeti identificar, avaluar i tractar de manera sistemàtica els riscos als quals estan exposats els sistemes i la informació vinculats al servei.

7.36.6.3. Estratègies de recuperació

Es definiran estratègies de recuperació a seguir en cas d'incidents significatius. Aquestes estratègies hauran de detallar l'opció de recuperació seleccionada i els recursos necessaris per a la seva execució, incloent-hi els mètodes de còpia de seguretat, els centres alternatius,

l'equipament necessari i el personal crític. L'empresa adjudicatària haurà de garantir el compliment dels objectius de temps de recuperació i de punt de recuperació acordats contractualment.

7.36.6.4. Plans de resposta i proves

S'elaboraran plans de gestió i resposta davant incidents que proporcionin una gestió eficaç i oportuna de les possibles interrupcions del servei. L'empresa adjudicatària realitzarà proves tecnològiques, de manteniment i de continuïtat de negoci amb caràcter anual, incloent-hi simulacres complets de desastre, per verificar el correcte funcionament i l'efectivitat dels plans de continuïtat, així com el compliment dels nivells de disponibilitat establerts en els acords de nivell de servei.

7.36.7. Seguretat en serveis al núvol

Per a tots els serveis publicats a Internet, l'empresa adjudicatària proporcionarà mesures actives de prevenció i mitigació contra atacs de denegació de servei distribuïts. S'implementarà un tallafocs d'aplicacions web que protegeixi els serveis exposats contra les amenaces més comunes, així com monitoratge en temps real del trànsit i els accessos per detectar i respondre de forma immediata davant de qualsevol anomalia o intent d'atac.

L'empresa adjudicatària acreditarà la implementació de mesures de seguretat específiques per a entorns de computació en núvol mitjançant certificacions reconegudes en la matèria, com les emeses per la Cloud Security Alliance o organismes equivalents, des de la infraestructura on subministra el servei. Aquestes certificacions hauran de mantenir-se vigents durant tota la durada del contracte.

7.36.8. Seguretat en APIs

Les interfícies de programació d'aplicacions exposades per l'empresa adjudicatària com a part del servei estaran protegides mitjançant un tallafocs d'aplicacions web integrat que inspeccioni i filtri el trànsit dirigit a les APIs per bloquejar peticions malicioses o no autoritzades.

Es disposarà de mecanismes de protecció contra atacs de denegació de servei i contra atacs de força bruta, incloent-hi la limitació del nombre de peticions per segon i per origen, de manera que es previngui la saturació del servei i els intents d'accés no autoritzat per repetició massiva de peticions.

7.36.9. Gestió de tercers i subcontractistes

7.36.9.1. Control d'accés de tercers

L'accés de tercers a dades o sistemes de l'Ajuntament quedarà limitat al mínim imprescindible per a l'execució de les tasques que tinguin encomanades, aplicant en tot moment el principi de mínim privilegi. Tot accés de tercers requerirà autorització expressa i documentada per part de l'Ajuntament, identificació individual i nominativa de cadascun dels usuaris que hi accedeixin —sense que es permetin en cap cas comptes genèriques o compartides—, mecanismes

d'autenticació robusta mitjançant doble factor i registre complet d'activitat amb plena traçabilitat.

L'empresa adjudicatària mantindrà un registre actualitzat de tots els accessos de tercers a les dades i sistemes de l'Ajuntament, el qual estarà a disposició d'aquest en tot moment.

7.36.9.2. ***Avaluació i supervisió***

L'empresa adjudicatària realitzarà avaluacions de seguretat sobre tots els tercers implicats en la prestació del servei amb una periodicitat mínima anual. Aquestes avaluacions comprendran la verificació del compliment de les mesures de seguretat establertes contractualment, la revisió de les certificacions vigents, l'anàlisi de vulnerabilitats i riscos identificats, i la revisió dels incidents de seguretat reportats durant el període avaluat.

Els resultats de cada avaluació es recolliran en un informe executiu que es posarà a disposició de l'Ajuntament en un termini màxim de quinze dies laborables des de la seva finalització. L'Ajuntament es reserva el dret de sol·licitar avaluacions addicionals en qualsevol moment o de realitzar les seves pròpies auditories sobre els tercers implicats, ja sigui directament o a través d'un auditor independent designat a tal efecte.

7.37. 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 al Departament de Seguretat de BIT per al seu corresponent tractament i valoració.

Sr. Josep Puy Castells
Cap del Departament SD Serveis Generals i Coordinació Territorial

Nuria Lara Arana
Directora de Serveis de Tecnologia i Transformació Digital de Serveis Corporatius

8. Annex

8.1. Annex 1: Informació addicional / aclariments

Si és de l'interès de les empreses licitadores sol·licitar informació addicional per a la presentació de l'oferta, ho podran fer a través de la Plataforma de Serveis de Contractació Pública (PSCP).

Les consultes rebudes dins dels 3 dies hàbils anteriors a la data de finalització del termini de presentació de proposicions es respondran i es publicaran a la mateixa plataforma, al perfil del contractant de l'I.M. Barcelona Innovació i Tecnologia:

https://contractaciopublica.cat/ca/perfils-contractant/detall/15990903

Així mateix, s'indica que, inicialment, no es convocarà sessió informativa per a aquesta licitació. Malgrat això, si alguna de les empreses licitadores estigués interessada a realitzar-la, pot fer-ne la petició a través d'aquesta mateixa via."