Ajuntament de Barcelona

PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL CONTRACTE DEL SERVEI DE SUPORT TÈCNIC, MANTENIMENT I DESENVOLUPAMENT DEL PROGRAMARI DE GESTIÓ I COMUNICACIONS DE LA CENTRAL D'OPERACIONS AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE.

CLAUSULA 1.- ANTECEDENTS

La Central d'Operacions és un servei permanent 24/7 dins del Centre de Serveis de Mobilitat i Espai Públic, format per operadors distribuïts en torns de matí, tarda i nit. Tanmateix, disposa d'un col·lectiu de Tècnics de Guàrdia que els donen suport per emergències greus amb la capacitat de desplaçar-se al lloc dels fets.

La Central té la funció de rebre avisos sobre incidències urgents a l'espai públic i la responsabilitat d'activar els equips d'intervenció urgent en aquells que així ho requereixin. A més realitza tasques de comunicació a l'activació i desactivació de plans d'emergència municipals.

La Central d'Operacions actualment disposa d'un programari que és una de les eines fonamentals del treball dels operadors i també del Tècnics Cap de Guàrdia ja que els dona suport en els processos de resolució d'incidències i els permet tenir concentrada, ordenada i actualitzada tota la informació relativa als protocols i comunicacions a realitzar en cas d'incidències de ciutat o activació de Plans d'Emergència Municipals.

El programari ha estat desenvolupat seguint la metodologia BPM (Bussiness Process Management) amb la plataforma Bonitasoft versió 7.11.4.Les principals funcionalitats que l'eina incorpora són:

- Gestió de processos per cada tipologia d'incidència.
- Gestió dels avisos via e-mail als contactes corresponents al procés de resolució.
- Consultes diverses.
- Assistent per cerca de telèfons per criteris de protocols, processos, temàtica, paraules clau,...
- Eines de manteniment de la informació corresponent (Protocols i Porcessos, Contactes, Documents, Plantilles,....)
- Control d'usuaris i perfils amb relació als protocols i processos.

Aquesta eina és utilitzada 24x7 i requereix un servei d'assistència tècnica per resoldre casos de caiguda del servei o d'errors inesperats, així com adaptacions a la millora dels protocols i processos de treball operatiu de la Central d'Operacions.

L'Ajuntament no pot realitzar els serveis inclosos en aquest contracte directament per no disposar dels mitjans materials i humans necessaris per portar-ho a terme. Per aquest motiu, es considera imprescindible la contractació externa.

CLAUSULA 2.- Objecte del contracte

L'objecte d'aquest contracte, és disposar d'un servei per donar suport tècnic als usuaris, manteniment preventiu i correctiu de l'eina i desenvolupament de millores del programari de gestió de processos d'operació i comunicacions de la Central d'Operacions.

CLAUSULA 3.- Serveis inclosos a l'abast del contracte

Com a eina fonamental de la Central d'Operacions, cal garantir la continuïtat de funcionament i l'adaptació operativa del programari de gestió i comunicacions de la Central d'Operacions a les seves necessitats.
Amb aquest objectiu, les tasques incloses dins l'abast del contracte de suport i manteniment del programari de la CdO són les següents:

- **Servei Tècnic d'Atenció a l'Usuari (STAU).**

  L'adjudicatari haurà de comptar amb els mitjans necessaris per donar aquest servei, facilitant número de telèfon de contacte i correu electrònic per enviar les possibles incidències del programari.

  Abast i horari: L'adjudicatari atendrà dubtes i problemes de funcionament de l'eina mitjançant correu electrònic i telèfon en dies laborables de 08:00 a 20:00. Fora d'horari, les sol·licituds quedaran registrades i s'atendran a partir de les 08:00 del següent dia laborable.

  Canals i traçabilitat:

  - Obertura i tancament de cada cas es faran sempre per trucada i correu electrònic per deixar constància.
  - El gestor de tiquets haurà de registrar a l'històric: data/hora d'obertura, data/hora del primer contacte, canal, persona contactada i actuació inicial; i adjuntar la còpia del correu de resposta (i, en tancament el mateix).

  SLA (Acords de nivell de servei)**— Temps de resposta STAU:**

  - **Definició:** minuts entre l'hora d'obertura del tiquet i la primera resposta per correu electrònic del tècnic especialista adscrit al servei (bots/auto respostes no compten).
  - **Compromís ofertat**: el licitador indicarà un valor **Tstau en hores** amb un màxim acceptable de 6 hores. Aquest valor quedarà incorporat com a SLA vinculant del contracte per aplicar criteris d'incompliment del servei.
  - **Còmput horari:** si la petició arriba fora de l'horari del servei, el temps comença a comptar a les 08:00 del proper dia laborable.

  Exclusions. No computen: aturades programades aprovades; incidències atribuïbles a tercers fora del control de l'adjudicatari (degudament justificades al tiquet); duplicats i proves internes.

Escalat a incidència greu (STCRI). Si durant l'atenció es detecta afectació crítica del servei, el cas s'escalarà immediatament al procediment STCRI 24×7, amb el règim de resposta per trucada de veu definit al servei STCRI.

- **<u>Servei Tècnic davant d'incidències greus (STCRI).</u>**

  L'adjudicatari haurà de comptar amb els mitjans necessaris per donar servei d'assistència davant de fallides crítiques del sistema i procurar el seu re establiment operatiu.

  L'adjudicatari haurà de facilitar número de telèfon de contacte i correu electrònic per comunicar les incidències greus del sistema i principalment en relació a l'enviament de d'avisos d'emergències.

  Abast i horari. L'adjudicatari prestarà servei 24×7 per atendre incidències greus del sistema. És defineix incidència greu la que impedeixi l'enviament d'avisos i/o la consulta dels protocols definits, o qualsevol contingència que, per decisió de la Sala de Control, suposi una impossibilitat d'ús del sistema de forma adequada.

  Aquest servei inclou l'atenció de la incidència i les actuacions derivades (reinici del sistema, revisió comunicacions amb altres sistemes i recuperació de backups) per restaurar el sistema. Les actuacions seran coordinades amb el responsable del servei .

  Referència de volum (no limitativa).

  Al llarg dels darrers 12 mesos, s'han registrat unes 6 incidències d'aquest tipus. Aquesta dada serveix només per a dimensionament i no limita l'abast del servei.

  Canals i traçabilitat:

  - Obertura i tancament de cada cas es faran sempre per trucada i correu electrònic per deixar constància.
  - El gestor de tiquets haurà de registrar a l'històric: data/hora d'obertura, data/hora del primer contacte, canal, persona contactada i actuació inicial; i adjuntar la còpia del correu de resposta (i, en tancament, el mateix).

  SLA — Temps de resposta STCRI:

  - **Definició:** minuts entre l'hora d'obertura del tiquet i la primera intervenció a l'entorn de producció per resoldre la incidència o la solució de la mateixa (el registre d'incidència o bots/autorespostes no compten).
  - **Compromís ofertat**: el licitador indicarà un valor **Tstcri en minuts,** inferior als 120 minuts que es consideren el temps màxim de resposta. Aquest valor quedarà incorporat com a SLA vinculant del contracte per aplicar criteris d'incompliment del servei i valorar la oferta.

  Mitjans i coordinació. Guàrdies 24×7, procediments d'escalat i recursos per a fallides crítiques i reestabliment operatiu (incloses actuacions posteriors a talls elèctrics i reinicis de plataforma o altres canvis a l'entorn de sistemes).

  Exclusions. No computen en l'SLA: aturades programades aprovades.

- **<u>Manteniment del programari i d'actualització de les versions de software necessàries.</u>**

  Aquest servei de manteniment del programari de base inclou:
  - Garantir l'emmagatzematge de backups de tot l'entorn de producció amb una periodicitat diària d'acord als mecanismes que IMI estableixi per tal de garantir el backup extern.
  - Manteniment preventiu del servidor on està ubicat el programari, realitzant neteja de fitxers de log. i altres aspectes que calgui ajustar pel correcte rendiment del servidor. 1 revisió complerta anual.
  - Actualització de la versió del programari de base Bonita amb la darrera versió i pegats corresponents i adaptació de la personalització i aplicació que funciona damunt de Bonita, per tal de que funcioni correctament amb la nova versió del sistema. 1 revisió complerta anual.
  - Mantenir actualitzada la documentació tècnica i funcional del programari per qualsevol tipus de modificació del programari així com els manuals de perfil usuari i administrador.

- **<u>Adaptació i millora:</u>**

  Adaptació i millora de funcionalitats del programari que garanteixi el correcte funcionament a les noves necessitats de la CdO, i/o aportin valor afegit al seu funcionament.

  La modalitat d'aquest servei serà un bossa d'hores de 160h/anuals, a executar sota demanda i planificació del gestor del contracte per part de l'Ajuntament de Barcelona.

  La millora i adaptació funcional a nous requeriments i necessitats del CdO, es realitzarà seguint una metodologia de treball AGILE, amb definició, valoració i seguiment iteratiu quinzenal, per tal de poder adaptar l'eina als procediments de treball de la CdO i incorporar noves funcionalitats.
  S'han identificat i analitzat les següents millores que es preveu abordar durant la durada del contracte:

  - **Implementació de nous procediments :** Com a resultat del procés de millora continua dels Protocols de ciutat i els Protocols d'actuació amb els diferents serveis de la Gerència, cal realitzar constantment tasques de millora dels procediments implementats per l'eina, així com afegir-ne de nous.
  - **Millores funcionals identificades** i que caldrà realitzar a banda d'altres que s'identifiquin al llarg de la durada del contracte hi ha les següents:
    - Millora integració amb el sistema IRIS.
    - Millora del sistema d'enviament d'avisos via e-mail.
    - Component d'ajuda a determinar números de contactes de serveis i resolutors segons l'adreça de la incidència.

- Customització de l'aplicació pel perfil d'usuari Tècnic Cap de guardia, limitant les funcionalitats i afegint informació referent al llibre de guàrdia i les incidències obertes.

- **Adaptacions tecnològiques:** Com a sistema integrat amb altres plataformes de l'Ajuntament de Barcelona i en particular amb sistemes de l'IMI, aquest servei inclou realitzar adaptacions tecnològiques requerides per canvis a altres sistemes i comunicacions.
- **Incorporació de informes i exportacions de dades:** La incorporació i millora de les funcionalitats d'exportació de dades referents a l'activitat dels usuaris amb l'eina, així com la confecció d'informes, és un aspecte rellevant per millorar la informació que es disposa sobre l'activitat i events gestionats per la CDO. Cal incorporar noves funcionalitats a aquest àmbit i millorar els existents.

- **Reunions de seguiment**

  El seguiment del servei i d'evolució de les feines, es realitzarà quinzenalment. Les reunions es convocaran per part del departament responsable municipal del contracte.

  Aquesta freqüència es podrà modificar en funció de les necessitats de l'Ajuntament de Barcelona.

  - L'adjudicatari haurà de mantenir actualitzat i lliurar un informe de gestió quinzenal que reculli els següents conceptes:
    - Recull d'incidències de ateses al serveis STAU i STCRI que inclogui sol·licitud i resolució, data i hora. Per les STCRI, caldrà aportar un pla d'actuació per evitar la seva repetició.
    - Planificació i seguiment de les tasques de manteniment preventiu.
    - Taula de seguiment d'evolutius i planificació temporal setmanal de tot el contracte:
      - Tasques realitzades i previstes per cada un dels serveis del contracte, amb una projecció a la durada del contracte.
      - Estat de cada una de les tasques (en curs, pendent, realitzada).
      - Hores previstes a cada tasca planificada.
      - Hores realitzades per cada tasca en curs i realitzades.
      - Per cada una de les tasques realitzades, una memòria executiva que reculli la feina prevista i/o realitzada.

- **Retorn del servei**

  Servei sota demanda destinat a fer un traspàs útil i pràctic del coneixement necessari per realitzar els serveis objecte del contracte a l'equip tècnic que el responsable del servei per part de l'Ajuntament de Barcelona designi.
  Aquest servei correspondrà a una dedicació no inferior a 20h. distribuïdes al llarg del darrer mes del contracte.

CLAUSULA 4.- DOCUMENTACIÓ A LLIURAR DURANT EL CONTRACTE

Documentació inicial

- L'adjudicatari realitzarà una comprovació inicial de l'estat del programari i del sistema de hardware que el suporta. Detectant els punts crítics així com proposant millores per a un funcionament més eficaç i eficient del mateix.
- De la mateixa manera farà la proposta calendaritzada dels serveis objecte del contracte que servirà de base com a document de seguiment.

Informe quinzenal

- Document que reculli:
  - Planificació global de tots els serveis del contracte amb detall a setmana.
  - Tasques realitzades i previstes.
  - Hores imputades i previstes per cada feina dins el servei de Millora funcional de l'eina.
  - Llista de consultes realitzades mitjançant el servei STAU.
  - Llista d'incidències ateses mitjançant el servei STCRI, adjuntant anàlisi , solució i pla de millora per prevenció.

Documentació final

- L'adjudicatari farà lliurament de tota la documentació actualitzada a final de contracte tant a nivell de versions de software, documentació tècnica i funcional actualitzada, backups, i tota la documentació que l'Ajuntament consideri necessaria per que el manteniment del programari sigui factible i eficient.

CLAUSULA 5.- METODOLOGIA de treball

Per dur a terme les feines descrites, es preveu treballar seguint els següents mecanismes:

Reunions de direcció:

- Caldrà fer un seguiment mensual a nivell de direcció del projecte, que contingui com a mínim:
  - Objectius clarament definits del proper període
  - % d'assoliment de cada un dels objectius
  - Calendari aproximat per completar-los
  - Problemes i solucions

- Proposta de certificació dels serveis realitzats

Reunions de seguiment (operatives)

- Reunió setmanal o quinzenal (segons les necessitats municipals) amb els components de l'equip, per tal de:
  - Revisar els serveis realitzats, problemes sorgits i solucions.
  - Properes tasques i revisió del pla de serveis
  - Gestió d'agendes per properes reunions tècniques.
  - Resoldre dubtes i dificultats.

Reunions tècniques (de consultoria)

- Reunions temàtiques amb personals intern o extern que caldrà planificar i gestionar.

Tasques de manteniment preventiu , correctiu i evolutiu

Les tasques de modificació del sistema en producció s'hauran:

- Totes les actuacions a realitzar a les instal·lacions de l'Ajuntament de Barcelona, hauran de ser provades prèviament a l'entorn privat del proveïdor per tal de garantir el correcte resultat de la seva execució.
- Posteriorment, el proveïdor farà el desplegament a l'entorn de PreProducció de l'Ajuntament per tal de que els usuaris puguin validar el correcte funcionament. Aquest entorn haurà de contenir dades reals actualitzades a un nivell que sigui operatiu i vàlid realitzar les proves.
- Un cop aprovat el funcionament a l'entorn de preproducció, es planificarà l'actualització, per part del proveïdor, a l'entorn de producció per tal de generar el menor impacte possible. Les actualitzacions es realitzaran a horari de 12x5.

Repositori de documentació

Tota la documentació generada (Gestió del manteniment, Material de Reunions, Actes, etc) estarà disponible a un repositori digital actualitzat, securitzat adequadament, estructurat i accessible per qualsevol dels components de l'equip del projecte.

CLAUSULA 6.- DIRECCIÓ I SEGUIMENT DEL PROJECTE

L'impulsor del contracte serà el **Centre de Serveis de Mobilitat i Espai Públic** de la Gerència d'Àrea de Mobilitat, Infraestructures i Obres (GAMIO), el qual designarà a la responsable que actuarà com a coordinadora i que vetllarà per l'acompliment de les expectatives i els objectius fixats en el projecte.

L'adjudicatari designarà com a cap de l'equip a un Director, tècnic superior competent per al desenvolupament dels treballs que són objecte del contracte el qual exercirà la representació de l'Assistència Tècnica davant l'Ajuntament de Barcelona.

Per a la realització de les seves funcions, el Director disposarà de les atribucions necessàries que permetin al seu equip donar l'assistència tècnica que la GAMISU demani sobre aquells temes que tinguin incidència en el normal desenvolupament dels serveis per a dur a terme les tasques d'aquest contracte.

CLAUSULA 7.- CONTROL DELS TREBALLS DE L'EQUIP

El Director Tècnic de l'equip del licitador, presentarà mensualment un informe de gestió que inclourà les tasques desenvolupades en aquell període, l'estat i evolució de la planificació, i les perspectives de tasques per al mes següent.

El responsable designat pel Departament de Centre de Serveis de Mobilitat i Espai Públic definirà el número de reunions de treball i seguiment que s'hauran de realitzar a les oficines del Departament o de manera telemàtica, que seran un mínim de 1 quinzenal.

L'informe de gestió mensual així com el resum es considera la documentació obligatòria pel control del servei i per la certificació mensual mateix. Per aquest motiu aquests documents s'enviaran pel Departament de **Centre de Serveis de Mobilitat i Espai Públic** el dia 20 de cada mes.

CLAUSULA 8.- EQUIP MATERIAL I HUMÀ

L'equip consultor posarà a disposició de l'Ajuntament de Barcelona els següents recursos:

Equip material

L'equip material mínim necessari per al desenvolupament del contracte i que l'adjudicatari destinarà a la realització dels serveis descrits sense cap cost per l'Ajuntament de Barcelona durant la seva durada és:

- Un entorn de desenvolupament que permeti replicar el funcionament del software ProCDO idèntic al de la CDO per tal de poder realitzar la validació funcional de les millores, així com la replicació d'errors del software detectades, sense necessitat d'interactuar ni desplegar a infraestructures de l'Ajuntament de Barcelona.

  Aquest entorn està conformat per :

  - Bonita-7.11.4
  - JavaScript
  - AngularJS
  - Groovy
  - Java
  - Sistema Operatiu CentOS Linux 7 (Core)

- Tanmateix, haurà de realitzar totes les tasques necessàries per configurar l'accés securitzat via VPN als entorns de preproducció i producció , seguint les indicacions de l'IMI.
- Totes les eines necessàries (mail, telèfon , ordinadors...) de cada un dels components de l'equip dedicat, per tal de que realitzin les tasques assignades amb la màxima eficiència i que permetin la més fluida comunicació amb l'equip del projecte (format per Ajuntament – proveïdor).

Requisits de l'equip humà

L'adjudicatari designarà un equip de treball de mínim **3** perfils amb la dedicació que consideri òptima.

Requisits addicionals

- Tots els integrants de l'equip s'hauran d'expressar amb total correcció oral i escrita en les dues llengües oficials: castellà i català, i tenir coneixements a nivell d'usuari d'Ofimàtica (processador de textos, full de càlcul, base de dades, presentacions) i Internet.
- Les reunions de seguiment es realitzaran a les oficines de l'Ajuntament de Barcelona, ja sigui a la pròpia Central d'operacions, altres dependències municipals que designi el responsable del contracte, o amb mitjans telemàtics si la Direcció del projecte per part de l'Ajuntament així o estableix.

Equip humà

L'equip humà haurà d'estar format per un mínim de 3 perfils amb les següents capacitats i experiència.

FUNCIÓ	PERFIL	MÍNIMA EXPERIÈNCIA REQUERIDA
Consultor Cap de projecte (Dedicació 6%)	Enginyer en informàtica, amb perfil de Consultor de processos BPM.	Experiència en els darrers 5 anys, en automatització de processos amb fluxes de treball amb metodologia BPM (Bussines Process Management) per la gestió de tickets.
Consultor Bonita Senior (Dedicació 10%)	Enginyer en informàtica amb perfil en consultor de processos BPM.	Experiència en els darrers 2 anys, en automatització de processos amb fluxes de treball amb metodologia BPM (Bussines Process Management) per la gestió de tickets.
Consultor Bonita (Dedicació 23%)	Enginyer en informàtica amb experiència en desenvolupar sobre Bonita.	Experiència en els darrers 2 anys, en desenvolupar i configurar solucions sobre el producte Bonita(v6 en endavant).

CLAUSULA 9.- Organització del servei

- Responsable del contracte: Assignar una persona encarregada de ser el punt d'interlocució principal amb el client, gestionant calendaris, autoritzacions i informes.
- Personal especialitzat en Processos i BPM: L'equip haurà de comptar amb un dissenyador funcional en processos amb experiència i especialització en l'entorn BONITA, capaç de dissenyar solucions orientades a la gestió de tiquets i incidències.
- Personal especialitzat en desenvolupament: L'equip haurà de comptar amb els perfils necessaris especialitzats i amb experiència per desenvolupar sobre les tecnologies i entorn del programari de la CdO (PROCdO) descrit a l'apartat anterior.
- Equip de suport i desenvolupament: Comptar amb un equip tècnic qualificat per al manteniment i desenvolupament del software creat amb BONITA, assegurant-se que el software compleix els requeriments operatius.
- El servei de Servei Tècnic davant d'incidències greus (STCRI) ha de tenir una disponibilitat de 24h. x 7 dies , tots els dies de l'any.
- Capacitat d'evolució i adaptació: Equip tècnic capacitat per implementar millores i adaptar el software als nous requeriments i necessitats del client de manera àgil i eficient.
- L'adjudicatari ha de garantir i assegurar la continuïtat de l'equip durant tot el termini d'execució del contracte, preveient les suplències necessàries per al manteniment del servei en els casos de vacances, baixes per malaltia o qualsevol altre circumstancia de

tipus laboral.

- Qualsevol canvi en els integrants del servei de consultoria haurà d'ésser autoritzat prèviament per l'Ajuntament de Barcelona. Tanmateix, l'Ajuntament, es reserva la facultat de modificar en qualsevol moment les persones que formen l'Equip Consultor per tal d'aconseguir una millora en l'acompliment del servei.
- L'Ajuntament de Barcelona, a través del Departament de **Centre de Serveis de Mobilitat i Espai Públic** pot ajustar les dedicacions i les funcions dels tècnics de l'equip a la càrrega de treball existent en cada moment, comunicant-ho amb 7 dies d'antelació.
- L'equip haurà de tenir flexibilitat horària per tal d'assistir a reunions amb d'altres departaments o òrgans de govern.

CLAUSULA 10.- SUBCONTRACTACIÓ

No es podran subcontractar les tasques següents:

Les reunions de seguiment, el retorn del servei i l'adaptació i millora de funcionalitat, descrites en la clàusula 3 del PPT."

CLAUSULA 11.- AUDITORIA DEL CONTRACTE

L'Ajuntament de Barcelona es reserva el dret d'auditar els recursos realment aportats així com la metodologia utilitzada per l'adjudicatari en l'exercici del Contracte.

El resultat de l'auditoria pot modificar la certificació mensual d'acord amb els recursos realment aportats.

CLAUSULA 12.- CONDICIONS GENERALS DE REALITZACIÓ

Confidencialitat

La informació tractada és de propietat Municipal i l'adjudicatari del concurs ha d'adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat i confidencialitat de les dades i evitin la seva alteració, pèrdua, tractament o accés no autoritzat.

La difusió d'informació a qualsevol altre entitat o persona física aliena a la Gerència d'Àrea de Mobilitat, Infraestructures i Obres haurà de tenir sempre la conformitat de la responsable del contracte designada per l'Ajuntament.

El personal que intervé en la gestió de la informació estarà obligat al secret professional respecte de la mateixa i en haver de guardar-lo, obligació que subsistirà fins i tot després de finalitzar l'actual contracte.

L'adjudicatari del contracte serà el responsable de la custòdia i arxiu de la informació facilitada per a l'execució dels treballs i a la finalització dels treballs haurà de retornar-la a l'Ajuntament de Barcelona, i destruir totes les còpies que en tingui.

En el supòsit que l'Ajuntament indiqués la destrucció d'una part de la documentació, aquesta s'haurà de realitzar per una empresa acreditada, i fer-se càrrec d'aquesta destrucció l'empresa adjudicatària.

Propietat dels treballs

La propietat intel·lectual dels treballs i desenvolupaments informàtics realitzats a l'empara d'aquest contracte pertany a l'Ajuntament de Barcelona. La documentació generada no podrà ser utilitzada sense la deguda autorització prèvia.

La consultoria contractada accepta expressament que els drets dels productes derivats d'aquest plec correspon única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractant cedeix amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, distribució, transformació o modificació i qualsevol d'altres dret susceptible de cessió exclusiva, d'acord amb la legislació sobre drets de la propietat intel·lectual.

La cessió dels drets d'autor que es fa en aquest contracte és sense perjudici dels drets morals que conserva l'autor, i ho és fins el moment què arribin a domini públic.

La cessió de drets té caràcter d'exclusiva i és per l'àmbit territorial de qualsevol país del món.

La retribució per la cessió de drets s'entén inclosa en la retribució establerta en el contracte.

CLAUSULA 13.- CERTIFICACIÓ DE TREBALLS

La facturació del contracte es realitzarà mensualment segons els treballs recollits a la darrera memòria quinzenal.

No es tramitarà la certificació sense el darrer informe quinzenal del mes, aprovat.

La certificació es realitzarà de la part proporcional de cada servei pel total del contracte, a banda del servei de Millores i Evolutius, que es certificarà per hores emprades en la realització d'evolutius validats i desplegats en producció.

Penalitzacions:

Els Serveis de suport STAU i STCRI, incorporen penalitzacions a la certificació mensual per incompliment dels temps Tstau i Tstcri.

Si en algunes de les sol·licituds d'aquests serveis s'ha incomplert aquests temps descrit al SLA corresponent, l'Ajuntament de Barcelona es reserva el dret contractual d'aplicar una penalització sobre el 1% del contracte.

ANNEX 1: SEGURETAT I SISTEMES INFORMACIÓ

D'acord amb Real Decret 311/2022, de 3 de maig, pel qual es regula el Esquema Nacional de Seguretat (ENS), es té per objectiu determinar les polítiques de seguretat adients que estableixin els principis bàsics i requisits mínims per a la protecció dels sistemes d'informació i la informació continguda en ells als quals es troba sotmesa l'Administració pública.

1. Condicions de seguretat generals i accés a sistemes d'informació

Atenent a serveis prestat per terceres parts a l'Ajuntament de Barcelona emprant els sistemes propis de l'Ajuntament, s'estableixen els següents requeriments per garantir el compliment del Esquema Nacional de Seguretat.

a) **Dret d'auditoria**: per tal de vetllar per la qualitat del servei, el departament de Seguretat es reserva el dret d'auditar el servei prestat per l'empresa adjudicatària. Es contemplen tant auditories de seguretat periòdiques com auditories sobrevingudes si es considerés necessari. En qualsevol cas, si la realització de l'auditoria es realitzés en les instal·lacions de l'empresa adjudicatària, aquest haurà de garantir l'accés necessari, incondicional i irrevocable als documents necessaris a l'abast.

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

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

- L'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. Es podrà verificar que el pla d'acció s'ha implementat correctament.

b) **Gestió d'incidents**: l'empresa adjudicatària informarà al Departament de Seguretat de l'IMI de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert.

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

c) **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.

- L'empresa adjudicatària serà responsable de les violacions del deure de secret que es puguin produir per part de les persones 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 de les persones participants 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.

- El deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

d) **Accés a la informació**: tant si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, com 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 l'IMI.

e) **Control d'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'accés una vegada efectuats un cert nombre de fallades consecutives.
- S'hauran de enregistrar els accessos amb èxit i els fallits.
- El sistema informarà a la persona usuària de les seves obligacions immediatament després d'obtenir l'accés.

f) **Control d'accés remot**: l'empresa adjudicatària haurà de disposar dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Ajuntament, sent els costos de connexió a càrrec de l'empresa adjudicatària.

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

g) **Gestió de les persones, deures i obligacions**: el/la Cap de Projecte de l'empresa adjudicatària durà a terme de forma correcta la gestió de les persones 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.

- 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.

h) **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 instruccions sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part de les persones 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 les persones assignades a l’execució del contracte.

i) **Protecció del lloc de treball:** quan el lloc de treball sigui 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.

- En relació a la 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. Les persones usuàries 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 l’IMI.

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

- Addicionalment, els equips hauran de disposar de: solució d’antivirus actualitzada a la última versió i configurada per realitzar anàlisis regulars de l’equip; política d’actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant les crítiques; Firewall habilitat restringint el trànsit d’entrada a l’equip al mínim necessari.

j) **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 la 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.

k) **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. Les persones usuàries han d'estar capacitades 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 l'IMI respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut.

l) **Protecció de la informació**: s'hauran de contemplar els següents camps d'aplicació.

- **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 s'ha de protegir tant en el cos com els annexes; s'haurà de protegir la informació d'encaminament de missatges i establiment de connexions; no es permetrà la redirecció a dominis de correu públics fora del correu corporatiu de l'empresa adjudicatària; s'ha de protegir el correu electrònic front spam, programes nocius i codi de mòbil de tipus applet.

  - Dins de les polítiques d'ús del correu electrònic s'inclou la limitació a l'ús com a suport de comunicació privada i el realitzar activitats de conscienciació i formació relatives a l'ús del correu personal per detectar 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.

m) **Protecció de les instal·lacions**: les instal·lacions de l'empresa adjudicatària hauran de disposar de certes condicions de seguretat física per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació i per garantir que la informació de l'Ajuntament no pugui ser visible i/o audible des de l'exterior de les instal·lacions.

n) **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 al Departament de Seguretat de l'IMI per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

Són d'obligat compliment les clàusules de l'apartat anterior conjuntament amb les descrites a continuació:

a) **Dimensionament**: l'empresa adjudicatària ha de garantir que disposa de les persones necessàries i amb les qualificacions professionals adients per garantir la correcta prestació del servei.

b) **Anàlisis forenses**: l'execució d'anàlisis forenses serà responsabilitat exclusiva del Departament de Seguretat de l'IMI. 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 i canals establerts entre el Departament de Seguretat de l'IMI i l'empresa proveïdora.

c) **Control accés local**: sumat a les obligacions anteriors, s'haurà de informar a la persona usuària de l'últim accés efectuat amb la seva identitat.

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

e) **Protecció dels suports informàtics**: addicionalment a les obligacions establertes anteriorment:

- **Esborrat i destrucció**: en cas de que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, s'hauran de destruir de forma segura els suports fent us dels productes certificats per l'IMI.

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

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

2. Clàusules administració de sistemes d'informació

2.1. Gestió d'identitats, autenticació d'usuaris

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuaris, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants.
L'empresa proveïdora haurà de validar i revisar accessos dels usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades. Els comptes d'usuari estaran integrats amb l'eina que l'IMI posa a disposició.

Autenticació interna
Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el 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'adjudicatari 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 l'IMI.

2.2. Autorització dels usuaris als sistemes

L'IMI 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'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en aquest repositori central d'autoritzacions.

En cas que l'adjudicatari 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 (eina de gestió d'identitats corporativa basada en Oracle Identity Manager) per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els 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 l'IMI.

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

2.3. Inventari d'actius

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

2.4. Configuració de seguretat

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

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
    - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.
    - No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
    - S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.
- S'aplicarà la regla de "seguretat per defecte":
    - Les mesures de seguretat seran respectuoses amb l'usuari i protegiran a aquest, tret que s'exposi conscientment a un risc.
    - Per reduir la seguretat, l'usuari ha de realitzar accions conscients.
    - L'ús natural, en els casos que l'usuari no ha consultat el manual, serà un ús segur.

2.5. Manteniment

L’adjudicatari haurà de mantenir l’equipament físic i lògic que constitueix el sistema i/o infraestructura administrada.

L’adjudicatari haurà de mantenir actualitzats els productes utilitzats en l’abast del plec d’acord a la política acordada amb l’IMI.

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.

2.6. 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 l'IMI, 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 pel Departament de Seguretat de l'IMI i/o seguir els estàndards i normes de l'IMI.

2.7. Certificats

La Direcció de Seguretat de la Informació de l'IMI 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 l'IMI. 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 l'IMI 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.

2.8. Antimalware

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

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

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

2.9. Còpies de seguretat

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

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

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

A banda de ser responsable de la generació de les còpies de seguretat, l'adjudicatari 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.

2.10. Control d'accés

Segregació de funcions i tasques

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

En concret, se separaran almenys les següents funcions:

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

2.11. Explotació

Gestió de la configuració

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

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

Gestió de canvis

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

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

Protecció de claus criptogràfiques

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

2.12. Protecció dels serveis

Protecció enfront de la denegació de servei

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

3. Clàusules desenvolupament de sistemes d'informació

3.1. Desenvolupament segur

L'adjudicatari es compromet a adequar les seves polítiques i procediments de desenvolupament de programari de tal forma que el seu cicle de desenvolupament de software garanteixi la seguretat en els productes desenvolupats al llarg de tot el cicle de vida, incloent normes de programació segura.

Els següents elements seran part integral del disseny del sistema:

- Els mecanismes d'identificació i autenticació.
- Els mecanismes de protecció de la informació.
- La generació i tractament de pistes d'auditoria.

El prestador està obligat a realitzar una revisió del codi font per a tots els desenvolupaments que siguin lliurats, ja sigui per al desenvolupament d'un aplicatiu, manteniment del mateix o desenvolupaments correctius, amb l'objecte de verificar si existeix alguna vulnerabilitat o amenaça en el desenvolupament realitzat, i si s'escau, procedir a la reparació de la mateixa.

L'IMI en qualsevol moment podrà realitzar una revisió del codi font. Si es detectés algun tipus de vulnerabilitat es comunicarà a l'adjudicatari per tal que procedeixi a arreglar les mancances detectades.

Per a millorar el procés de desenvolupament segur d'aplicacions, l'adjudicatari haurà de realitzar accions addicionals per a garantir la qualitat i seguretat del producte final. Aquestes accions són:

- Emprar una eina d'anàlisi de codi estàtic (SAST) per trobar vulnerabilitats de seguretat al codi font i garantir els bons estàndards de codificació. La periodicitat dels anàlisis hauran de ser acordats conjuntament amb el responsable del contracte. El software emprat al IMI correspon a l'eina SonarQube amb la modalitat OWASP, sent aquesta la tecnologia desitjable a emprar per l'adjudicatari.
- Per al cas particular d'aplicacions conteneritzades, l'adjudicatari haurà de fer ús d'un software d'anàlisis d'imatges Docker. La tecnologia emprada a l'IMI i la preferent d'ús per part de l'adjudicatari és Anchore.

En cas de emprar softwares diferents als plantejats anteriorment, hauran de ser comunicats i justificats degudament al responsable del contracte.

3.2. Acceptació i posta en servei

Abans de passar a producció l'adjudicatari comprovarà el correcte funcionament de l'aplicació es comprovarà que:

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

Addicionalment, l'adjudicatari realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisis de vulnerabilitats.
- Test de penetració.
-

3.3. Protecció de les aplicacions i serveis web

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

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

3.4. Dades de proves

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

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

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

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

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

3.5. 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 la Direcció de Seguretat de la Informació de l'IMI, que 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 l'IMI i/o seguir els estàndards i normes de l'IMI.

3.6. Signatura electrònica

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

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

3.7. Certificats

La Direcció de Seguretat de la Informació de l'IMI 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 l'IMI. S'entén per certificats digitals corporatius: els de servidor segur, els d'aplicatiu per autenticació o signatura digital, de signatura de codi, de xifratge, etc.

Tots els certificats hauran de ser sol·licitats a través del procediment establert en el Departament de Seguretat de l'IMI 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.

3.8. Pla de traces

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

L'adjudicatari haurà de dissenyar les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició l'IMI a l'inici del contracte.

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

L'IMI es reserva el dret de poder demanar en qualsevol moment del contracte la integrabilitat amb els sistemes corporatius destinats a la monitorització de traces, on actualment es contempla el sistema SIEM QRadar i/o ELK.

3.9. Informe de seguretat

El proveïdor elaborarà a petició de la Direcció de Seguretat de la Informació de l'IMI un informe on es detallaran tots els aspectes rellevants sobre Seguretat del seu contracte.