

PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT, INTEGRACIÓ, IMPLANTACIÓ, SUPORT I MANTENIMENT D'UNA APLICACIÓ MÒBIL I SISTEMA DE SEGURETAT CIUTADANA AL NÚVOL PELS AJUNTAMENTS DE TARRAGONA, REUS, CAMBRILS, MONT-ROIG DEL CAMP, CONSTANTÍ, LA CANONJA I EL CATLLAR

1. INTRODUCCIÓ

Els Ajuntaments de Tarragona, Reus, Cambrils, la Canonja, Constantí, Mont-roig del Camp i el Catllar, van aprovar un protocol de col·laboració signat el 18 de juny del 2024 amb l'objectiu d'establir un marc de col·laboració per dur a terme el desenvolupament d'un sistema digital de seguretat compartit entre els municipis. Fruit d'aquest protocol, es planteja contractar el subministrament, integració, implantació, suport i manteniment d'una aplicació mòbil i sistema de seguretat ciutadana al núvol pels ajuntaments indicats adherits a la present licitació.

La realització d'aquest contracte és necessari per poder comptar amb un sistema de comunicació bidireccional entre la ciutadania i la Policia Local, la Guàrdia Urbana o els Cos de Vigilants, així com una comunicació àgil entre els diferents cossos de seguretat que puguin disposar d'aquesta plataforma, amb l'objectiu de proporcionar un servei més eficient a la població del municipi, tot creant una xarxa de cooperació interterritorial als municipis que disposin d'aquesta aplicació, amb l'objectiu d'engegar un model de gestió de la seguretat urbana i ciutadana interterritorial, a més també altres principis i valors com:

- Sumar per optimitzar recursos i multiplicar l'èxit dels resultats esperats.
- Crear un sistema de transferència d'informació, de comunicació bidireccional i interterritorial, entre els ciutadans i les seves administracions municipals.
- Cooperar entre les policies locals, les guàrdies urbanes i els cossos de vigilants municipals donada la mobilitat natural dels ciutadans entre territoris.

Aquest sistema es basa en una aplicació ciutadana per a mòbils i tauletes intel·ligents i en un sistema de gestió i d'intercanvi d'emergències i alarmes entre els diferents cossos de seguretat del grup de forma àgil i segura.

2. OBJECTE DEL CONTRACTE

L'objecte del contracte és el següent:

- Subministrament, integració i implantació d'una aplicació mòbil i un sistema de gestió de seguretat ciutadana.
- Servei de suport, manteniment i actualització tècnica del sistema que garanteixi el seu funcionament i evolució tecnològica des del núvol.
- Millores del sistema posteriors a la implantació a través de consultories o programació que es vagin incorporant per necessitats municipals.

3. ABAST DEL PROJECTE

L'abast del contracte compren el subministrament de les llicències del programari, les integracions necessàries amb els sistemes municipals i la implantació i posada en funcionament d'un sistema de gestió interterritorial de seguretat ciutadana en el núvol, especialment vinculada amb els territoris limítrofs, per raons evidents d'eficiència en la mobilitat de la ciutadania.

Posteriorment a la implantació, es posarà en marxa un servei de suport, manteniment i actualització tècnica del sistema per garantir el seu funcionament i evolució tecnològica des del núvol i millores del sistema de forma contínua a través de consultories o programació per noves necessitats municipals no incloses en el servei de suport i manteniment.

Es tracta d'implantar un sistema de comunicació bidireccional d'innovació social i tecnològica en xarxa que faci possible la integració de les infraestructures públiques i privades tant local, com de manera interterritorial, amb la missió de fer possible l'augment de la sensació de seguretat i eficiència en les nostres inversions, obtenint, aquests objectius de manera cooperativa i per l'interès local.

El programari ha de permetre entre d'altres, un canal de comunicació directe i àgil entre la ciutadania, els serveis municipals, el teixit comercial i turístic, amb la Policia Local, les Guàrdies Urbanes i els cossos de Vigilants municipals, a més de les diferents comunicacions entre altres cossos policials. Aquest sistema permetrà relacionar-se de forma més àgil amb la policia dels municipis, i suposa una millora de l'eficiència i l'optimització dels recursos emprats en els serveis de la Policia Local, Guàrdia Urbana i del Cos de Vigilants del municipi.

Aquest sistema també dona resposta a la interactuació amb les càmeres de videovigilància ja instal·lades o que es tenen previst d'instal·lar, que permetrà controlar zones de la ciutat que tenen un alt grau d'incidència, i amb els perifèrics de control existents a la nostre població (obertura de portes, perifèrics de monitorització, etc).

Tanmateix el sistema permetrà tenir accés a la càmera i micròfon dels terminals mòbils de les persones usuàries i dels locals i establiments comercials que ho autoritzin.

4. REQUERIMENTS FUNCIONALS

El sistema a oferir ha d'existir com a solució comercial d'aplicació mòbil i sistema de seguretat ciutadana en el moment de presentar l'oferta ampliant si s'escau, amb les funcionalitats i les integracions requerides.

Es tracta de disposar d'eines de contacte ràpid entre la ciutadania i la seva administració local a través de les policies i vigilants del municipi que alhora, col·laboren en xarxa.

Tot i que cada ajuntament implanta el sistema de forma local, pot ser utilitzada des de qualsevol part del món per rebre i enviar informació d'interès per a la ciutadania allà on es trobi l'usuari/a.

L'aplicació ciutadana s'ha d'adaptar a diferents perfils (persones grans, joves, emprenedors, professionals de la salut, etc.) i usos ciutadans.

Les aplicacions han de ser pròpies i independents de cada territori. No obstant això, a qualsevol municipi de la xarxa de ciutats que formin el Sistema, es podrà rebre el mateix nivell de servei que a la va pròpia població.

L'aplicació estarà basada en el principi de «pertinença a un territori» en una població, si bé permet que no s'hagi de «canviar d'aplicació» quan l'usuari/a te una incidència fora de la seva població. D'aquesta forma els Ajuntaments i els serveis de policia/vigilants dels municipis disposaran d'una eina potent per donar suport als conciutadans més enllà de la frontera territorial.

La cooperació interterritorial de persones ciutadanes i professionals de moltes diverses disciplines amb vocació de servei fan, cada dia possible, la singularitat del Sistema i estant a l'avantguarda mundial en matèria de seguretat.

Per a això es fa necessari solucions que permeti a la ciutadania explorar i controlar tot el potencial de serveis que el seu Ajuntament pot oferir-los per mitjà de la connectivitat IOT (Internet de les Coses) generant una visió i una percepció del que és viure en un veritable ecosistema "Safe Smart City" (Ciutat Intel·ligent Segura) que faci dels nostres municipis un millor lloc per viure, la qual cosa, comporta oferir el següent:

- Canal de comunicació directa entre les persones ciutadanes i la seva policia de proximitat (Policia Local, la Guàrdia Urbana o el Cos de Vigilants Municipals) del

seu municipi (i tercers), a través d'una interfície "amigable" i "personalitzable" segons les necessitats específiques que es defineixin.

- Videovigilància per a la seguretat ciutadana
- Videovigilància per al control de trànsit
- Gestió d'accessos a infraestructures públiques i / o privades
- Monitorització de perifèrics.
- Seguretat per al teixit comercial, industrials i turístic
- Serveis per persones en situació de risc (ordres d'allunyament, violència de gènere, etc)

El sistema ha de connectar a la ciutadania amb la seva administració pública local, especialment amb les àrees de seguretat ciutadana i urbana, mitjançant diferents plataformes i tecnologies com poden ser dispositius mòbils intel·ligents, tauletes intel·ligents, ordinadors personals i d'altres sistemes connectables que puguin aparèixer, com poden ser polseres o rellotges intel·ligents.

El servei inclourà un nucli de gestió per la interconnexió de diferents subsistemes, que permeti:

- a) Disposar d'un canal de comunicació directe i àgil entre la ciutadania i la Policia Local, la Guàrdia Urbana o el Cos de Vigilants Municipal, utilitzant dispositius mòbils, ordinadors personals i tauletes intel·ligents que permetin comunicar situacions d'emergències, alarmes i d'altres comunicacions de seguretat de forma segura i geolocalitzades, sense necessitat de realitzar una trucada.
- b) Disposar d'un canal d'intercanvi d'emergències i alarmes entre diferents cossos de policia de forma segura i àgil, que permeti derivar de manera immediata a d'altres poblacions limítrofs els missatges i avisos.
- c) Disposar d'un canal de comunicació bidireccional entre els diferents departaments de l'Ajuntament i els ciutadans incorporant, entre d'altres, els missatges "push" directes a un ciutadà o específics per diferents segments de població, rols socials, col·lectius de risc o professionals. Aquestes alertes són oficials i arriben en segons a milers de persones, i de forma immediata permet a usuaris/es saber que han de fer en cada situació.
- d) Realitzar trucades ràpides d'emergències, comunicar incidències i denúncies a diferents policies locals i forces de seguretat en funció de la geolocalització o voluntat dels ciutadans, i que puguin ser ateses.
- e) Disposar d'una plataforma en línia per la gestió de tot el conjunt de dades rebudes i per a les comunicacions a realitzar.

D'altra banda, la plataforma serà totalment oberta de cara a la integració de nous dispositius maquinari de 3ers fabricants com ara: càmeres, smartphones, smartwatches, botons d'assistència, sensors, pilons, wearables, programari de gestió policial, etc .. i qualsevol altre element que els usuaris de sistema considerin que sigui necessari incorporar.

L'escalabilitat del sistema serà il·limitada a llarg termini podent-se incorporar a la mateixa tants dispositius captadors d'informació com sigui necessari.

4.1. FUNCIONALITATS GENERALS

Amb caràcter general la plataforma de gestió ha de complir les següents funcionalitats:

- Enviar i rebre missatges per comunicar situacions d'emergències i alarmes entre diferents cossos de policia de forma segura i àgil.
- Enviar i rebre missatges avisos de la ciutadania, de departaments municipals i de Protecció Civil.
- Obtenir dades de la ciutadania, únicament per a la finalitat de seguretat ciutadana i urbana.
- Localitzar geogràficament els missatges d'emergència rebuts sense necessitat de realitzar una trucada.
- Realitzar trucades ràpides d'emergències a la Policia Local, la Guàrdia Urbana o el Cos de Vigilants municipals, amb geolocalització, transferència de dades personals i aquelles que puguin ser claus
- Multiidioma: L'aplicació ha de permetre que la personal usuària pugui seleccionar en quin idioma es mostra la interfície de l'aplicació i, com a mínim, han de poder triar entres les següents llengües: català, castellà i anglès. En base a les necessitats que tinguin les administracions, es podran anar incorporant més idiomes.
- Multicomunitat: El sistema ha de proporcionar la capacitat perquè les persones usuàries puguin accedir amb rols de comunitat diferents i rebre els avisos categoritzats per rol (ciutadania, comerços, turisme, restaurants, etc.)
- Perfil d'usuàries del portal de gestió: El portal ha de permetre diferents perfils d'ús amb rols diferents que permetin realitzar tasques d'administració, publicació, edició, etc.
- Perfil d'usuaris de l'aplicació: El Sistema ha de permetre la segmentació d'usuàries per perfils i categories com: ciutadania, comerç local, empreses,

professionals sociosanitaris, educadors, persones en situació de vulnerabilitat, etc.

- Validació de persones usuàries: El sistema ha de permetre el registre i validació de les persones per evitar els robots o usuàries anònimes.

- Disposar d'eines per guiar l'ús de la plataforma: com enregistrar-se, associar dispositius, etc.

- Eines de publicació: La plataforma ha de disposar d'una eina de publicació fàcil i amigable.

- Edició: La plataforma de gestió ha de permetre el rol per editar i moderar els continguts, així com bloquejar l'accés a usuàries no autoritzades. Aquest bloqueig ha de ser reversible.

- Registres d'activitat: El sistema ha de registrar totes les accions rellevants realitzades per les gestores de la plataforma segons els seus nivells de permís.

4.2.FUNCIONALITATS ESPECÍFIQUES

4.2.1 GESTIÓ DE LES EMERGÈNCIES

El fonament del sistema residirà en l'anomenat "principi de comunicació" que es basa a identificar l'usuari que genera la informació i el rol, i la comunicació de les emergències i la seva gestió.

Els serveis d'emergència municipal podran enviar missatges massius a la ciutadania per comunicar incidents rellevants, activacions i actuacions en Plans d'Emergències, mesures d'autoprotecció, consells de seguretat, etc.

4.2.2 AVISOS D'EMERGÈNCIES

L'App disposarà d'un botó d'avís per enviar un missatge d'alerta davant d'una emergència ciutadana per informar a la Policia Local o Cos de Vigilants Municipals que la persona es troba en una situació de perill en tan sols 3 segons i només prement un botó.

Els usuaris correctament registrats podran enviar una emergència directa a la Policia Local o Cos de Vigilants del municipi al qual pertanyen i alhora també, cap a aquells territoris en què es trobin en un determinat moment per geolocalització, en tant que aquests disposin a la seva vegada del sistema.

D'altra banda, si la persona es trobés de viatge fora de la seva localitat de residència (a l'estranger per exemple) i tingués una emergència, a través de l'App podria fer ús del botó d'avís. Així, l'alerta i el seu geoposicionament arribaria a la Policia de la seva localitat i seria aquesta última qui intentaria contactar amb les autoritats locals del lloc on es trobés la persona per auxiliar-la i prestar-li la deguda assistència. Quan es procedeix a la intervenció per l'avís d'emergència, aquesta actuació queda registrada al sistema per tal de poder tenir una traçabilitat i un registre d'històrics amb tots els avisos generats per una persona determinada.

Aquesta funcionalitat també pot ser molt útil per dur-la el personal dels serveis municipals que de vegades poden ser objecte d'algun tipus d'agressió física o verbal per part dels usuaris, i permet saber qui és la persona que ha activat l'alerta i el lloc on es troba.

El protocol d'actuació davant l'emergència serà coordinat i dirigit remotament per la Policia Local a través de l'aplicatiu client "BackOffice" que es descriurà més endavant.

El temps màxim que l'aplicació trigarà a iniciar el procés d'enviament de l'avís serà de 3 segons per evitar falses alertes/errors.

També serà possible enviar l'avís d'emergència mitjançant un Widget sense necessitat d'obrir l'App.

La catalogació d'una situació específica que està tenint lloc com a emergència estarà sempre subjecta a criteri del ciutadà i no caldrà identificar-ne el tipus prèviament per llançar l'avís, simplement s'activarà el Widget (Botó SOS). No obstant això, la funció disposarà també d'un menú amb la tipificació d'emergències següent:

- Mèdiques
- Assetjament o Violència de Gènere
- Atracament
- Incendi
- Accident de trànsit
- Emergència petroquímica (tenint en compte que les sales de comandament de les petroquímiques també podran ser usuaris)
- Altres

La catalogació d'una emergència facilita la tasca policial i optimitza els temps de resposta en l'activació dels protocols específics adequats a cada situació.

4.2.3 WIDGET PER ACCÉS RÀPID EN CAS D'EMERGÈNCIA

També serà possible enviar l'avís d'emergència mitjançant un Widget sense necessitat d'obrir l'App.

Per a protocols (accions) enfocats a col·lectius amb un alt grau de vulnerabilitat, el sistema haurà de poder recollir una emergència enviada per l'App fins i tot amb el telèfon bloquejat tal com s'especifica a l'apartat 4.2.5 "Alerta davant de violència de gènere".

4.2.4 POLSADOR DE TRUCADA D'EMERGÈNCIA

El sistema disposarà d'un botó que permeti fer una trucada d'emergència i encaminar-la a la Policia Local més propera a la ubicació on trobi el ciutadà en el moment de la mateixa perquè incorporará la funcionalitat de geolocalització. Això vol dir que si la persona es desplaça fins a un altre municipi i necessita tornar a fer una trucada d'emergència, aquesta darrera seria dirigida cap a la Policia Local, la Guàrdia Urbana o el Cos de Vigilants Municipals d'aquest darrer municipi.

En cas de no tenir activat el GPS al telèfon intel·ligent en el moment de fer la trucada, aquesta serà dirigida a la Policia Local del municipi que va indicar l'usuari en el moment d'efectuar el seu registre a l'App.

4.2.5 ALERTA DAVANT DE VIOLÈNCIA DE GÈNERE

L'aplicatiu ha de permetre que una persona que es trobi en una situació d'assetjament o violència de gènere, pugui comunicar-ho a la policia de proximitat per formar part del protocol contra la violència de gènere.

A més, disposarà d'un accés directe que es pot configurar per enviar emergències, que permetin a la policia conèixer la ubicació de la víctima en el moment dels fets, i fins i tot, si té el permís de l'usuari, activar el seu telèfon (encara que el telèfon estigui bloquejat) per escoltar el que està passant i fins i tot activar la càmera per gravar vídeo i poder-ho aportar com a prova.

Per facilitar l'enviament de l'alerta a la policia, ja que la persona que podria estar sent víctima d'aquesta situació sovint no té temps ni tan sols per obrir l'App en el

moment que l'està patint, disposarà d'una funció que permeti enviar l'emergència sense haver d'obrir l'aplicació.

Funcionarà mitjançant un Widget específic (només per a aquest propòsit) i diferent del Widget (Botó SOS). Se'n farà ús per part de l'usuari de l'App sense més que desbloquejar el telèfon i activar-lo.

4.2.6 ALERTES PER PERSONES VULNERABLES

Es tracta d'un sistema d'alertes pensada per al seu ús per part dels familiars/tutors/cuidadors o persones de l'entorn d'altres persones que es troben en situació d'especial vulnerabilitat: ancians, persones dependents, menors, etc. i servirà per associar el telèfon mòbil de l'usuari amb el de la persona vulnerable.

La funció oferirà un menú a l'usuari per fer una petició de cerca de l'altra persona amb què l'usuari hagi vinculat el telèfon mòbil si es considera que es troba en una situació de risc.

En aquest cas, es tracta d'un tipus d'emergència especial on l'objectiu serà facilitar tot el possible l'enviament de l'alerta i activar l'actuació policial tan ràpidament com sigui possible.

Per poder tenir activada aquesta funció a l'App, es requerirà un registre presencial previ a les dependències policials per facilitar les dades de la persona que es considera "especialment vulnerable" i un consentiment exprés d'aquesta perquè el seu familiar/tutor /cuidador o persona que designi llanci la petició de cerca. Quan la Policia validi aquest registre, es produirà l'habilitació d'aquesta funció a l'App de l'usuari per fer-ne ús.

4.2.7 ALERTES PREVENTIVES

La funció d'alerta preventiva podrà fer-la servir qualsevol persona registrada al sistema que tingui instal·lada l'App al telèfon mòbil i amb un perfil que hagi estat validat per fer-ne ús.

Aquesta funcionalitat està destinada a aconseguir seguretat de les persones en aquelles situacions habituals, sense companyia, que comporten risc o senten por, en què el ciutadà consideri que necessita avisar.

A títol d'exemple, el/la ciutadana que realitzarà un cert trajecte que pot comportar al seu parer cert risc d'algun tipus. En aquests casos, aquesta funció permetrà establir i desar al telèfon intel·ligent el temps que dura el trajecte, activar l'alerta en iniciar-lo i desactivar-la en arribar a la destinació. El ciutadà decidirà els minuts/hores que durarà l'alerta preventiva.

L'alerta preventiva una vegada activada funcionarà fins i tot amb el telèfon intel·ligent bloquejat, la qual cosa és fonamental si la persona preveu que durant el temps que dura l'alerta podria estar en una probable situació de perill.

Si no es cancel·la una alerta preventiva que hagués estat activada prèviament transcorregut el temps establert, l'App enviarà un missatge d'emergència a les persones que l'usuari hagi registrat prèviament a l'App com aquelles a qui avisar en cas d'una situació així. També, hi haurà opció de seleccionar com a destinataris del missatge a la Policia Local/Cos de Vigilants, cas en què, l'App enviarà el missatge d'emergència també al cos de seguretat del municipi.

4.2.8 ASSOCIACIÓ DE DISPOSITIUS

Amb aquesta funcionalitat, l'aplicació, permetrà informar les persones de l'entorn que es troba l'usuari/a en una situació d'emergència, per tal que el/la puguin ajudar, i es permetrà indicar a l'App si es vol informar un o més destinataris de l'entorn d'aquell que s'ha produït aquest fet.

La persona que sigui usuària de l'aplicació també pot ajudar a un altre usuari del seu entorn.

L'aplicació ha de permetre associar el dispositiu i crear una xarxa de contactes mitjançant els seus usuaris.

Si s'activa una alerta, aquesta només arribarà als contactes que decideixi el ciutadà.

4.2.9 COMUNICACIÓ DE INCIDÈNCIES

Responent a la premissa fonamental de cooperació i la corresponsabilitat entre els ciutadans i el cos de seguretat del municipi, el mateix ciutadà serà una peça fonamental del mecanisme global que representa la gestió de la seguretat a la seva ciutat. Per aquest motiu, l'App permetrà mitjançant aquesta funció la comunicació amb la Policia Local, la Guàrdia Urbana o el Cos de Vigilants Municipals de diferents tipus d'incidències:

Ciutadanes/comerç

Atracaments, robatoris, agressions, discussions, baralles, situacions d'assetjament de qualsevol tipus podran ser notificades.

Mobilitat

Accidents o infraccions de trànsit, problemes amb la senyalització així com consultes/denúncies en relació amb les restriccions de mobilitat.

Infraestructures

Anomalies de la via pública, estat de la calçada, problemes en edificis, parcs, jardins o problemes relacionats amb les normatives de sanitat i higiene als espais públics.

Pèrdues i denúncies

Pèrdua de persones, animals o objectes, així com denúncies i/o suggeriments de diversa índole.

4.2.10 PERFIL MODE AGENT DE POLICIA

Tindrà definit un mode funcional específic de l'App per al cas que els usuaris siguin els Agents de Policia. S'anomenarà "mode agent" i el seu perfil de registre els oferirà accés a informació confidencial sobre la seguretat ciutadana i a poder fer ús de funcions addicionals a les del perfil estàndard.

4.2.11 VISUALITZACIÓ DE CONTINGUTS D'UTILITAT CIUTADANA

L'App contindrà diferents seccions amb informació ciutadana en funció de la ubicació:

- Mapa ciutat destacant les farmàcies de guàrdia i la xarxa de desfibril·ladors
- Telèfons i directori d'interès
- Recomanacions de la Policia
- Consells de primers auxilis
- Campanyes de mobilitat
- Notícies i agenda de l'Ajuntament
- Activacions de plans d'emergència.
- Comunicats del CECAT
- Altres

4.2.12 APP D'ESCRITORI

L'aplicatiu de seguretat tindrà una versió d'escriptori del client del sistema pensada per ser desplegada entre d'altres a:

- Comerços del municipi
- Farmàcies
- Col·legis
- Centres de salut
- Instal·lacions municipals i esportives

4.2.13 MAPA VIRTUAL

El sistema tindrà una GIS (Geographical Information System) Interactiu i Interterritorial d'acord als requisits d'integració. Aquest programari no funcionarà de manera aïllada sinó que interactuarà amb la resta d'aplicatius a través de les diferents capes programari del nucli principal de servidors.

4.2.14 BACK OFFICE AGENT LOCAL I INTERTERRITORIAL

Serà el client del Sistema que s'instal·larà als llocs d'operador de la Sala de Comandament de la Policia Local del municipi o municipis que despleguen la plataforma.

També serà factible instal·lar aquest programari a qualsevol altre dispositiu connectat a la xarxa LAN del Centre de Control: portàtils, tauletes, etc.

Les funcionalitats que oferirà són:

- Des del nucli de la plataforma digital per mitjà d'una connexió VPN tots els avisos d'emergències, alertes i incidències registrades pels ciutadans del municipi a través de l'App. Un cop rebuts, es podrà a través de la interfície d'usuari de Back Office Agent dur a terme la coordinació i l'activació dels protocols d'actuació corresponents.
- Generació i tramesa d'alertes ciutadanes: Sota aquesta denominació els agents de policia/vigilants del Centre de Control podran:
 - Generar i enviar les denominades alertes push que contindran informació d'interès per a la seguretat dels ciutadans com ara:
 - Avisos sobre l'estat de les carreteres
 - Ús de sistemes d'avís acústic davant d'emergències
 - Alertes de frau, furt
 - Consells de primers auxilis
 - Etc.
 - Les “alertes push” podran ser de dos tipus:

- Locals: només arribaran als ciutadans registrats al Sistema com a residents al municipi al que pertany la Policia Local que genera l'alerta
- Interterritorial: arribaran als usuaris de tots els municipis que utilitzen el mateix sistema

4.2.15 VÍDEO VIGILÀNCIA NO INVASIVA PER LA SEGURETAT CIUTADANA

La Gestió de la Videovigilància de la seguretat ciutadana serà no invasiva, mitjançant la integració "nativa" de la plataforma programari de gestió de vídeo i enregistrament.

4.2.16 GESTIÓ DE LA GRAVACIÓ DE LES CCTV

Els aspectes més destacables que ha de complir el sistema són:

- Gestió integral de CCTV: permet una quantitat il·limitada d'usuaris, dispositius, servidors i llocs, amb capacitats d'alta disponibilitat, operació de Vídeo Wall intel·ligents i integració en dispositius mòbils.
- Qualsevol tipologia de càmera amb protocol ONVIF o RTSP podrà ser gestionada pel sistema. Això ha de possibilitar incorporar a la gestió de la videovigilància qualsevol càmera propietat de l'Ajuntament.
- S'ha de basar en una arquitectura client servidor, que suporta multioperadors, i disposar de definició de perfils d'accés al sistema amb diversos perfils configurables.
- Amb els diferents perfils s'ha de controlar i restringir l'accés a certes funcionalitats com ara visualitzar càmeres, accedir al vídeo-Wall, moviment de les càmeres, parametrització dels codificadors, creació de seqüències, creació de posicionaments preestablerts, etc.
- El sistema ha de suportar la creació de seqüències generals que només l'administrador podrà eliminar o canviar i seqüències de perfil. El sistema també suportarà la creació de preposicions de perfil, les generals estan protegides i només podran ser creades, codificades i eliminades per l'administrador.
- El servidor ha de servir com a unitat de sincronisme per a tots els dispositius de captació d'imatges, ja siguin els sensors de les càmeres, o els que estan per separat. Igualment, el sistema ha de suportar la implementació dels protocols de telemetria per al control de càmeres PTZ que calguin.
- L'accés al sistema es farà i es registrarà a través del servidor. Totes les ordres es gestionen mitjançant aquest que controla en tot moment l'estat de tots els elements.

- El servidor també permet aplicar polítiques de nivell d'accés a les càmeres. Hi ha diversos nivells d'accés, i davant de conflictes entre perfils d'usuaris amb diferents nivells, la gestió d'una càmera queda en mans del que tingui el nivell superior, i en cas de conflicte es poden treure la gestió l'un a l'altre en temps real i sense restriccions.

4.2.17. ANALÍTICA DE DADES DE L'ÚS APP:

El sistema ha de permetre recollir dades de l'ús de l'app tipus google analytics o similar (a banda del que es recull en les pròpies botigues de publicació Google Play d'android i Apple Store d'iOS) i disposar d'un sistema d'informes que es pugui filtrar entre dates que permeti analitzar:

- Quines són les opcions o serveis més utilitzats
- Quina tipologia de persones usuàries l'utilitzen
- Quina valoració té l'app de forma general o en concret d'un servei o informació.

Aquests informes han de ser exportables almenys en format CSV i també via API per importar-ho als sistemes municipals de forma automatitzada.

També ha de disposar d'un dashboard que permeti amb una visió ràpida i per un període indicat i per un o tots els perfils de persones usuàries, saber:

- Persones usuàries que l'han utilitzada
- Persones que la tenen instal·lada
- Top ten de serveis i informacions més utilitzades o consultades
- Valoració mitja de l'aplicació
- Top ten de millors valoracions d'informacions o serveis
- Top ten de pitjors valoracions d'informacions o serveis

Tota aquesta informació d'analítica de dades de l'aplicació amb el màxim detall haurà de ser accessible via API des dels sistemes municipals de forma remota i automatitzable per importar-la periòdicament i carregar-la als sistemes d'analítiques municipals o Bussiness Intelligent per poder generar més analítiques amb eines específiques des de la corporació municipal.

4.2.18. ACCESSIBILITAT I DIVERSITAT FUNCIONAL:

L'aplicació ha de complir els màxims estàndards d'accessibilitat i el públic amb diversitat funcional s'ha de tenir present des del primer moment per facilitar la seva inclusivitat.

Amb l'ús de recursos tecnològics accessibles, s'ha d'acostar la informació a les persones amb disfuncions visuals o auditives i en especial complir el Real Decret 1112/2018, de 7 de setembre, sobre accessibilitat dels llocs web i aplicacions per dispositius mòbils del sector públic ja sigui per l'aplicació mòbil o per la versió web.

També cal que sigui accessible per a infants d'educació especial i per a persones amb discapacitat psíquica

5. REQUERIMENTS D'INTEGRACIÓ

El sistema a implantar haurà de complir els següents requeriments d'integració en el moment de posada en marxa i durant la durada del contracte gràcies a que els sistemes a integrar tenen APIs obertes i documentades que podrà accedir el contractista per fer les integracions:

5.1. SISTEMA DE QUEIXES I INCIDÈNCIES: Haurà de permetre integrar-se amb el sistema de queixes, incidències i suggeriments de cada municipi. En el cas de l'Ajuntament de Reus i Tarragona amb els seus sistemes propis via la seva API i en el cas de l'Ajuntament de La Canonja amb l'aplicació <https://www.appajuntaments.cat> amb la seva API. La resta no disposa d'aplicació però s'haurà de contemplar integració via API amb servei propi si en tenen.

5.2. APLICACIÓ CIUTADANA: ha de permetre l'accés a l'app general ciutadana en el cas que l'Ajuntament en tingui facilitant un accés destacat des de l'aplicació per saltar d'una a l'altre.

5.3. VALID: l'autenticació de la persona usuària es realitzarà de forma nativa amb el servei VALID del consorci AOC (<https://www.aoc.cat/serveis-aoc/valid>).

En el cas que l'autenticació de VALID sigui per idCat Mòbil (opció que es recomanarà en l'app de forma destacada), la persona usuària ha d'haver indicat en la configuració del seu perfil el seu dni, nie o passaport i, el número de mòbil que l'agafa automàticament del dispositiu. Quan s'autentiqui amb idCat Mòbil, es rebrà al mòbil el codi SMS com a clau d'un sol ús que l'app capturarà automàticament sense intervenció de la persona i li donarà acceptar; caldrà que l'app sol·liciti els permisos per capturar el SMS al instal·lar-se o quan la persona es vulgui identificar.

5.4. REPRESENTA: l'autenticació de la persona usuària ha de permetre seleccionar si representa una altre persona integrant-se de forma nativa amb el servei REPRESENTA del consorci AOC (<https://www.aoc.cat/serveis-aoc/representa/>) com poden ser comerços, empreses, entitats, etc.

Una vegada autenticada la persona, el sistema preguntarà la primera vegada si vol actuar en el seu nom (opció per defecte) o en representació d'una altre persona ja sigui física o jurídica o sense personalitat jurídica (entitats); des de la configuració es podrà canviar en tot moment si actua en el seu nom o representa una altre. En cas que esculli en representació, el sistema haurà de consultar el registre d'apoderaments del servei REPRESENTA del consorci AOC i si la persona autenticada té poders generals per una altre, se li mostrarà aquestes persones i podrà escollirà de tal manera que s'autenticarà com a persona representant d'una altre.

També es consultarà el registre d'entitats de l'Ajuntament en qüestió via servei web municipal si la persona presideix o és secretari/a d'una entitat i per tant representant d'una entitat municipal.

Una vegada autenticat, el sistema consultarà un WS de l'Ajuntament en qüestió per recuperar totes les dades d'aquesta persona si actua en el seu nom o de la persona representada en cas que actua en representació. Aquest WS recuperarà tota la informació necessària de la base de dades de persones de l'Ajuntament que inclou persones empadronades, contribuents, empreses, entitats, persones interessades en qualsevol expedient, tràmit, activitat o servei municipal, Això és un requisit d'integració amb la base de dades de persones municipal descrit més endavant.

Es recuperaran almenys les següents dades de la persona: dni/nie/passaport/nif, nom i cognoms o raó social, dades de contacte (correu electrònic i/o mòbil i/o telèfon fix), adreça postal, sexe, gènere i data naixement. En el cas que representi una entitat, també es retornarà informació de la pròpia entitat del registre d'entitats municipal.

Aquestes dades es guardaran al perfil de configuració de l'app i si la persona realitza qualsevol canvi de dades personals en l'app, aquesta haurà de fer-ho de forma segura prèvia autenticació i aquests canvis s'enviaran als WS municipals perquè s'actualitzin les dades a la base de dades municipal de persones. En cas

que actuï en representació, només podrà canviar dades de contacte i adreça postal de la persona representant.

En el cas que no consti registrada aquesta persona física que es vol autenticar en els sistemes municipals, l'app demanarà totes les dades necessàries al igual que ho fa el tràmit telemàtic d'alta a la base de dades de persones com el cas de l'Ajuntament de Reus en <https://seu.reus.cat/seu/carpetaCiutadana/tramit/29515> i ho enviarà via WS als sistemes municipals pel seu registre i si es confirma l'alta, l'app li donarà accés com persona registrada i identificada. Si la persona a la que representa, no està en els sistemes municipals, l'aplicació donarà un error i no podrà donar-li accés de representació.

En el seu perfil de dades, la persona podrà configurar si actua en el seu nom (per defecte) o actua en representació d'una altre que hagi pogut escollir de REPRESENTA o pel registre d'entitats municipals de tal manera que pugui anar intercanviant el seu perfil d'identificació quan ho consideri oportú.

Totes les autenticacions hauran de ser registrades en un log local de la pròpia app així com en el sistema al núvol de tal manera que els administradors del sistema pugui tenir un registre d'autenticacions que pugui consultar, filtrar i exportar en format CSV almenys per tipus d'identificació, núm. identificació (dni/nie/passaport/nif), data i hora en segons, geolocalització (si ha donat la seva autorització la persona), idioma, IP del terminal, identificador únic del terminal, sistema operatiu i versió del terminal.

5.5. Identificació mitjançant la integració amb un Wallet conforme al European Digital Identity (EUDI) Wallet (millora opcional): Es valorarà que el sistema permeti la identificació mitjançant la integració amb un Wallet conforme al European Digital Identity (EUDI) Wallet com a sistema més àgil i futur d'identitat digital europea.

Aquest requisit és una millora opcional i en cas de presentar-la, caldrà acreditar-la i oferir-la en el sobre C on es valorarà i en cap cas en el sobre B.

5.6. Base de dades de persones BDP municipal: per obtenir o actualitzar les dades d'una persona registrada als sistemes municipals via els WS municipals.

En el cas de l'Ajuntament de Reus i Tarragona s'integrarà amb la solució T-Systems TAO 2.0 BDT i Epob, en el cas de la Canonja amb padró habitants de diputació de Tarragona, en el cas de Cambrils amb Audifilm i en el cas de Mont-roig del Camp amb Absis i la resta estan per definir amb integració via WS.

5.7. Agenda municipal: per obtenir l'agenda municipal filtrant si s'escau per dates, temàtica i paraules via feed RSS:

Reus - <https://www.reus.cat/noticies/feed>

Tarragona-<https://www.tarragona.cat/seguretat/seguretat-ciutadana/noticies/noticies/RSS>

Cambrils - feed RSS

La Canonja - <https://www.lacanonja.cat/noticies/rss>

Mont-roig del Camp - <https://mont-roig.cat/agenda/feed/>

Constantí - feed RSS

El Catllar - <https://www.elcatllar.cat/agenda/>

5.8. Notícies municipals: per obtenir les notícies municipals filtrant si s'escau per dates, àrea i paraules via feed RRSS:

Reus - <https://www.reus.cat/noticies/feed>

Tarragona-<https://www.tarragona.cat/seguretat/seguretat-ciutadana/noticies/noticies/RSS>

Cambrils - feed RSS

La Canonja - <https://www.lacanonja.cat/noticies/rss>

Mont-roig del Camp - <https://mont-roig.cat/tematica/noticies/feed/>

Constantí - feed RSS

El Catllar - <https://www.elcatllar.cat/noticies/>

5.9. Directori de contactes i localitzacions: per obtenir els contactes i localitzacions d'interès públic via WS:

Reus - <https://www.reus.cat/directori>

Tarragona - <https://www.tarragona.cat/la-ciutat/municipals>

Cambrils - <https://www.cambrils.cat/ca/atencio-ciutadana>

La Canonja - <https://www.lacanonja.cat/viure-a-la-canonja/serveis-contactes-interes>

Mont-roig del Camp - <https://mont-roig.cat/municipi/informacio-util/>

Constantí - WS per determinar

El Catllar - <https://www.elcatllar.cat/viure-al-catllar/telefon-d-interes/>

5.10. Xarxes socials: accedir a totes les xarxes socials actuals o futures de cada Ajuntament que interessi:

Reus - <https://www.reus.cat/ajuntament/lajuntament-les-xarxes-socials>

Tarragona - <https://www.tarragona.cat/governobert/comunicacio/xarxes-socials>

Cambrils - <https://www.cambrils.cat/ca/actualitat/xarxes-socials>

Mont-roig del Camp - <https://mont-roig.cat/comunicacio-i-premsa/>

La Canonja - <https://www.lacanonja.cat/viure-a-la-canonja/Xarxes-socials>

Constantí – per determinar

El Catllar - <https://www.elcatllar.cat/ajuntament/xarxes-socials/>

5.11. Mapa ciutat/GIS municipal: accedir als serveis de mapa, ubicació i geolocalització de cada municipi segons la seva geoAPI

Reus - <https://geoportal.reus.cat>

Tarragona – <https://geoportal.tarragona.cat>

Cambrils – <https://mapes.cambrils.cat> (Nexus Geografic)

La Canonja – <https://gis.lacanonja.cat/canonjagp>

Mont-roig del Camp – GIS només d'accés intern (Nexus Geografic)

Constantí – geoAPI per determinar

El Catllar - <http://carrerer.elcatllar.cat/>

5.12. Serveis de mobilitat: per publicar serveis de mobilitat municipals via WS com talls de trànsit, estat del trànsit, aparcaments i places lliures, transport públic bus, bici pública, punts de recàrrega elèctrica, zones accés restringit, zones de baixes emissions,

5.13. Autenticació backoffice amb el IdP municipal: per l'autenticació d'usuaris i agents policials municipals al backoffice i per garantir l'aplicació de polítiques de seguretat de cada Ajuntament i l'accés amb les mateixes claus, cal que el sistema de backoffice s'autentiqui amb el sistema IdP municipal que serà:
Reus - redhat SSO (solució basada en el projecte de codi obert <https://www.keycloak.org/>) amb els protocols oberts SAML o OpenID

Tarragona – Microsoft AD

Cambrils – Microsoft AD. També disposa de SAML mitjançant FortiAuthenticator.

La Canonja – Microsoft AD

Mont-roig del camp – Microsoft AD

Constantí - Microsoft AD. També disposa de SAML mitjançant FortiAuthenticator

El Catllar – Microsoft AD

5.14. Integració correu electrònic: per l'enviament de correus electrònics del sistema quan sigui necessari s'integrarà amb el sistema de correu municipal enviant amb el correu electrònic que indiqui cada ajuntament amb el seu domini integrant amb:

Reus – mailrelay.com via SMTP

Tarragona - mailrelay.com via SMTP

Cambrils – Exchange 365, però es possible que es faci per mailrelay.com.

La Canonja - mailrelay.com via SMTP

Mont-roig del Camp – Exchange 365

Constantí - Exchange 365

El Catllar – smtp.altanet.org via SMTP

5.15. Integració SMS: per l'enviament de SMS del sistema si s'utilitza s'integrarà amb el sistema de SMS municipal que indiqui cada ajuntament via API WS:

Reus – WS Rest API Vodafone

Tarragona – WS Rest API Vodafone

Cambrils – API Vodafone

La Canonja – Movistar

Mont-roig del Camp - WS Rest API Vodafone

Constantí – WS Rest API per determinar

El Catllar - WS Rest API Vodafone

5.16. Integració amb totes les càmeres a la via pública, de trànsit o d'edificis municipals: el sistema haurà integrar-se i suportar qualsevol càmera que suporti protocols ONVIF o RSTP tenint en compte que cada Ajuntament disposa de:

Reus – càmeres AXIS o HIKVISION

Tarragona – càmeres Samsung i AXIS

Cambrils – diversos fabricants, entre altres DAHUA, Sony i AXIS

La Canonja – DAHUA

Mont-roig del Camp - DAHUA, Sony i AXIS

Constantí - càmeres AXIS

El Catllar – No hi ha

5.17. Integració amb el sistema de gestió operativa de la Policia Local: el sistema haurà d'integrar-se per enviar les alertes o incidències rebudes automàticament al sistema de gestió operativa i d'emergències de la Policia Local perquè des d'aquest sistema puguin assignar i enviar els recursos policials corresponents àgilment d'acord al següent:

Reus – DRAG

Tarragona – Gespol però està pendent nova licitació.

Cambrils – DRAG

La Canonja – DRAG

Mont-roig del Camp – DRAG

Constantí - DRAG

El Catllar - DRAG

5.18. Integració amb el sistema de telefonia de la policia local i 092 si en disposa: el sistema haurà d'integrar-se amb els sistemes de telefonia de cada

polícia local de cada Ajuntament quan calgui establir trucada entre la persona usuària i la policia local d'acord a:

Reus – Asterisk (freepbx) amb trunk SIP

Tarragona – Alcatel amb trunk SIP però està pendent nova licitació.

Cambrils – iPBX al núvol basada en Asterisk i trunk SIP.

La Canonja – Centraleta cloud Movistar

Mont-roig del Camp - Centraleta cloud Vodafone

Constantí – Avaya/Grandstream - Trunk SIP Movistar / Adamo

El Catllar - Vodafone

En el cas que alguna dels sistemes a integrar indicats anteriorment es modifiquin o canviïn perquè un Ajuntament contracta un altre sistema, el licitador haurà de realitzar les adequacions i integracions necessàries dins del preu fix ofert de servei de suport i manteniment.

5.19. API PRÒPIA COMPLETA AMB TOTES LES POSSIBLES FUNCIONALITATS QUE SIGUIN NECESSÀRIES:

A més de les integracions indicades, el sistema haurà de tenir totes les funcionalitats de consulta, gestió i transacció amb API de tal manera que qualsevol funcionalitat que disposa es pugui usar interactivament o per integració de forma automatitzada. Caldrà que el licitador detalli per valorar la seva API, la documentació tècnica d'aquesta, la definició, exemples d'ús i de crides.

6. REQUERIMENTS I CARACTERÍSTIQUES TÈCNIQUES

El sistema haurà de complir els següents requisits tècnics abans de la finalització completa de la implantació i durant la durada del contracte:

6.1. Requeriments i característiques generals i d'arquitectura tecnològica

- La seva arquitectura haurà de ser resilient, àgil, flexible i robusta basada amb alta disponibilitat, redundància i microserveis.

- L'aplicació serà tant nativa per android com per iOS suportant sempre les seves últimes dues versions. L'aplicació mòbil haurà de disposar d'una versió totalment web i d'escriptori a excepció d'aquelles funcionalitats que són exclusivament reproduïbles només en terminals mòbils o tauletes. El backoffice serà totalment web per la policia local que gestiona el sistema. En el cas de l'accés web a l'aplicació, al backoffice o a les crides WS seran sempre segures amb HTTPS. En el

cas de la versió web estarà en un subdomini del propi Ajuntament al igual que el backoffice. El certificat SSL serà proporcionat per l'Ajuntament corresponent si s'escau.

- Haurà de garantir l'accessibilitat de l'aplicació mòbil i de totes les funcionalitats web que interactuen conforme el Real Decret 1112/2018, de 7 de setembre, sobre accessibilitat dels llocs web i aplicacions per dispositius mòbils del sector públic.

- La interfície tant externa al públic com interna al personal municipal tant en l'aplicació mòbil nativa com web i d'escriptori haurà de ser multi-idioma disponible almenys en català, castellà i anglès i serà configurable segons les preferències personals de la persona i en cas que no estigui definit en les preferències, es configurarà per defecte segons el sistema operatiu o si és web del navegador i per la resta de casos per defecte en català. En el cas del backoffice haurà de ser en català. Es valorarà que hi hagin altres idiomes addicionals encara que sigui amb traducció automàtica i aquesta opció és una millora que cal incloure en el sobre C i en cap cas en el sobre B.

- En la part web i d'escriptori, haurà de ser un sistema responsiu multidispositiu suportant mòbils o tauletes (android o iOS en les seves últimes dues versions) o ordinadors escriptori.

- El disseny haurà de seguir les guies i estils de la identitat corporativa de cada Ajuntament seguint els criteris del departament de comunicació corporativa de cada municipi essent HTML5+CSS en cas de web i incorporant les imatges, tipus de lletra, colors, formats i logos municipals seguint la identitat municipal.

- Suporti els navegadors Chrome, Firefox, Edge i Safari en les seves últimes dues versions independentment del sistema operatiu al que accedeixi quan l'accés sigui web.

- Integració i certificació amb entorn ofimàtic quan sigui necessari amb LibreOffice versió 7 o superior i Ms-office 2007 o superior. El llicenciament ofimàtic serà proporcionat per l'Ajuntament.

- Capacitat d'exportació de qualsevol informació en format PDF o mitjançant fulla de càlcul (xls, xlsx, ods i cvs).

- Caldrà configurar i tenir disponibles durant la vigència del contracte dos entorns: un de test per fer les proves abans de la posada en marxa en el projecte

d'implantació o per validar noves actualitzacions o versions en la fase de suport i manteniment i, un entorn de producció que serà el real de funcionament. Només al sistema de producció s'hauran de fer còpies de seguretat.

- El contractista configurarà els processos periòdics d'exportació de dades per fer còpies de seguretat d'acord a les polítiques de seguretat de cada Ajuntament amb coordinació amb els tècnics municipals TIC i generar una còpia de tota la base de dades als sistemes locals municipals de forma periòdica per cada Ajuntament per tal que cada Ajuntament sempre tingui una còpia de la base de dades en local. El model de la base de dades que és còpia en local haurà d'estar documentat per tal que sigui accessible pels tècnics municipals i explotable amb els seus sistemes d'analítica de dades.
- Tots els accessos i usos dels sistemes implantats hauran de ser registrats, auditables i exportables identificant qui entra, a que accedeix, que fa i en quin moment.
- La informació restringida en accés privat haurà de ser accessible segons usuaris i perfils.
- Tots els sistemes implantats i el seu accés i ús haurà de complir les normes de ciberseguretat de cada Ajuntament i seran auditades i en cas de deficiències que es detectin, hauran de ser subsanades abans de la posada en marxa i durant el contracte.

6.2. Requeriments i característiques tècniques de l'aplicació mòbil

De forma general, tota aplicació mòbil vinculada a l'objecte i abast del present contracte cal que:

Requeriments generals

- Es publiqui als markets sota comptes de l'entitat municipal o la que s'acordi entre totes les entitats municipals.
- Serà de descàrrega gratuïta per qualsevol persona.
- Cal que estigui disponible tant per sistemes Android com per IOS
- Els serveis informàtics municipals han de donar el seu vist-i-plau previ a la publicació de l'APP.
- L'App ha de ser lliurada amb la darrera versió compatible del sistema operatiu disponible.

- Cal que s'adeqüi a la imatge i colors corporatius de la identitat visual municipal corporativa.
- Cal que sigui compatible, com a mínim, amb el 90% del parc mòbil.
- Caldrà realitzar joc de proves de camp amb terminals físics.
- Cal que incorpori sistemes de Seguretat i privacitat :
 - * Les contrasenyes no poden mostrar-se en clar i no poden quedar emmagatzemades al dispositiu.
 - * Cal que demani els permisos necessaris per accedir a diferents serveis del dispositiu.
 - * Cal que disposi d'un mecanisme de validació d'usuari propi per accedir a informació confidencial o privada. L'app no pot danyar dades al dispositiu.
- En el cas que no es pugui garantir l'ús de l'app en una versió anterior, s'haurà d'informar a l'usuari si és necessari descarregar una versió més recent de la mateixa.
- Usabilitat i accessibilitat
 - * L'app s'ha de poder visualitzar correctament en els diferents dispositius (mida lletra, elements gràfics, etc).
 - * Cal que mostri el teclat adequat per a cada tipus d'entrada.

Protecció de dades

- * Quan es guardin, utilitzin o es moguin dades personals s'ha de sol·licitar i rebre el consentiment explícit i inequívoc de la persona usuària per poder procedir. A l'inicialitzar-se l'app es mostrarà una pantalla en la qual es sol·licitarà aquest consentiment a la persona usuària mitjançant una sèrie de missatges a on li sol·liciten els permisos i que aquesta ha d'acceptar. Si no s'accepten aquestes condicions de servei l'app s'aturarà, per la qual cosa s'ha de validar que aquests permisos estan informats.
- * Per totes les apps que tinguin condicions d'acceptació d'ús del servei, s'ha de preveure que aquestes condicions poden canviar. Per tant, ha d'haver-hi un mecanisme que permeti forçar a acceptar aquestes condicions quan canviïn, tornant a mostrar la pantalla en la qual es sol·licita el consentiment mostrant les noves condicions.
- * Una vegada la persona usuària ha acceptat les condicions d'ús del servei, la pantalla en la qual es sol·licita el seu consentiment no tornarà a aparèixer, a menys que les condicions d'acceptació canviïn.
- * La informació personal de les persones usuàries s'encriptaran amb algoritmes robustos per minimitzar l'afectació de bretxes en la seguretat. Pel mateix motiu, les comunicacions amb servidors s'hauran de realitzar sota el protocol HTTPS.

Seguretat

- * Les contrasenyes no han de ser mostrades en clar i no poden ser emmagatzemades en el dispositiu.
- * L'aplicació ha de gestionar correctament l'accés a informació personal (agenda, contactes, imatges...) amb aprovació per part de l'usuari.
- * L'aplicació ha de sol·licitar els permisos necessaris per accedir als diferents serveis del dispositiu i aquests estan publicats i descrits.
- * L'aplicació ha de disposar d'un mecanisme de validació d'usuari propi per accedir a informació confidencial o privada.
- * L'aplicació no pot danyar les dades al dispositiu.

Gestió de permisos

- * S'ha de tenir en compte que les aplicacions, i les seves actualitzacions, han d'implementar la gestió de permisos "on demand", és a dir, es demanaran a mesura que ho necessiti l'app no a l'inici o en un moment que pel context la persona usuària no pugui entendre perquè necessita concedir aquest permís. També es donarà l'explicació de per què és necessari aquest permís justament abans o en el mateix moment de demanar-ho.
- * Per gestionar correctament les notificacions push en dispositius mòbils, un cop oberta l'app, i en el moment que es trobi adequat, s'haurà de mostrar un pop-up o pantalla indicant si vol activar les notificacions push i perquè rebrà notificacions. Si Accepta demanarem el permís de push, perquè l'usuari accepti rebre notificacions. Si Cancel·la, les notificacions quedaran bloquejades i l'app no les rebrà.
- * Si un permís és imprescindible per al funcionalment de l'app s'ha de deixar clar que és així a la persona usuària quan se li demani, i si aquesta no dona el permís s'ha de mostrar un missatge informatiu, explicant que donat que no s'ha concedit el permís no es pot seguir amb el funcionament de l'app, i tancar l'app. No es pot produir un crash ni tornar a demanar el permís fins que es torni a iniciar l'app.
- * Si l'usuari ha denegat la concessió d'un permís, però torna a accedir a una funcionalitat o pantalla en què l'app li demanaria aquest permís, es mostrarà un petit missatge en una zona visible de la pantalla recordant a l'usuari que ha denegat el permís de l'aplicació i amb un botó de "Configuració" que al clicar-ho porti a la configuració de l'app per si vol canviar això i donar el permís.

Analítica

- * L'analítica per aplicacions mòbils recull l'activitat de la ciutadania en la seva interacció i navegació. Més enllà del nombre de descàrregues de les aplicacions i conèixer els usos que se'n fa, ens permet valorar si són els que s'han previst i són d'utilitat per als usuaris.

* La solució ha de disposar d'un sistema d'anàlítica dels accessos i usos. Alternativament ha de permetre integrar el producte Google Analytics que disposi l'entitat municipal.

* A partir d'aquest rastre es generen dades (visites, pàgines vistes, durada de la visita, etc.) que, mitjançant un posterior treball d'anàlisi, han de permetre respondre preguntes com les següents: L'usuari és capaç de trobar la informació que està buscant? Està satisfet amb la seva experiència? Quin és el contingut més popular? Quina àrea podem prioritzar més del que ho fem actualment? Quant de temps necessita el ciutadà per trobar la informació que està buscant? Quins continguts importants poden estar faltant?

Posicionament

Caldrà aplicar contínuament tècniques ASO en les tendes d'aplicacions Play Store i Google Play per augmentar la quantitat de descàrregues orgàniques i millorar la taxa de conversió de visitants a descàrregues.

Notificacions push

* Les notificacions push seran obligatòries.

* La notificació es mostrarà segons l'opció per defecte del sistema operatiu i la configuració de visualització triada, no caldrà fer cap adaptació addicional.

* Amb l'app en foreground es notificarà a la persona usuària mitjançant un pop-up.

* Amb l'app en background es mostrarà en el toolbar.

* La icona de la notificació haurà de ser representativa de l'app, que s'assembli a la icona del launcher.

* L'aplicació ha de disposar d'una opció de menú per consultar les notificacions, aquestes quedaran enregistrades quan es generin (si l'app està instal·lada) i les més recents es podran consultar en aquesta opció de menú. Si encara no han estat consultades es mostrarà un superíndex amb un número a sobre de la icona de l'app a l'escriptori del dispositiu (si està configurat per tal que es mostri el número). El número contindrà el nombre de notificacions pendents de consultar.

* Han de ser visibles amb pantalla emergent, no només amb un avís tipus "campaneta".

Gestió multidioma

* L'APP i al instal·lar, com a mínim, ha d'estar en els idiomes requerits. Els idiomes disponibles han de coincidir amb els especificats en el codi font/binari i per tant, amb els que especificaran els corresponents markets.

* Han d'habilitar una funció dins l'aplicació, que permeti canviar entre els diferents idiomes. Aquest canvi ha de ser automàtic i no pot suposar un reinici de l'aplicació.

* Inicialment, les aplicacions han d'utilitzar l'idioma per defecte del dispositiu. En cas de no coincidir amb cap dels idiomes disponibles, l'aplicació s'executarà per defecte en català amb la possibilitat de canviar-lo manualment.

* Ha de funcionar el canvi d'idioma i aquest s'ha d'ajustar de forma adequada la interfície i els continguts, i la configuració de l'idioma s'ha de mantenir en tancar l'app.

Requeriments funcionals:

A més dels requeriments funcionals requerits per negoci, l'app ha de seguir els següents punts:

- El splash screen cal que es presenti un mínim de 2 segons a l'iniciar l'aplicació.
- La següent informació ha de ser d'accés fàcil i directe (sense necessitat d'estar registrat a l'aplicació o altre pas previ) a totes les aplicacions:

- Un apartat d'ajuda per a les persones usuàries i que com a mínim ha de tenir:

- * Logo i marca

- * Descripció de l'app i objectius

- * Autoria del projecte.

- * Apartat de FAQs on el contractista indicarà aquelles que més consultes i dubtes genera a les persones usuàries o a proposta de l'ajuntament.

- * Contacte amb text descriptiu i mètode de contacte amb l'entitat municipal on consti un telèfon (si es clica obre telèfon) i un correu electrònic (si clica obre el programa de correu per defecte del terminal)

- * Suport tècnic que permeti que l'empresa licitadora pugui donar suport a la persona usuària ja sigui per la pròpia aplicació, correu electrònic o whatsapp

- * Accessibilitat amb l'enllaç a la declaració d'accessibilitat.

- * Condicions d'ús

- * Política de privacitat

- * Intel·ligència artificial informant del registre dels algorismes aplicats

- * Número de versió de l'aplicació i el versionCode / build version, depenent de la plataforma (agafant-lo dinàmicament del binari)

- * Cal indicar si la versió de l'aplicació està funcionant en un entorn de Pre-producció o Producció, on el primer és un entorn de proves.

- Si l'aplicació està oberta, al clicar de nou en la icona cal obrir-la en el punt que es trobava, i no pas arrancar-la de nou.

- Si l'aplicació requereix descarregar un volum de dades superior a 20MB, cal informar prèviament a la persona usuària amb un missatge advertint la situació, donant la possibilitat de no fer-ho (explicant les conseqüències) i recomanant

l'ús de wifi. Si és possible pel bon funcionament de l'aplicació, aquesta descàrrega d'informació caldria fer-se en segon pla.

- En el cas que una url es vulgui mostrar dins l'app amb un webview intern, la pàgina corresponent ha d'estar optimitzada per ser mostrada dins l'app i, per tant, integrada amb el disseny i funcionament de l'app. Qualsevol enllaç que hi hagi dins d'aquesta pàgina ha de complir aquest mateix requeriment. Si es vol enllaçar a una pàgina que no compleixi aquest requeriment, cal obrir-la dins del navegador per defecte del sistema operatiu.

- Si una funcionalitat de l'aplicació implica com arribar a un destí, i aquesta et porta fora de l'app, cal indicar a la persona usuària la possibilitat de seleccionar entre les diferents aplicacions de navegació que té instal·lades en el seu dispositiu, delegant en el sistema operatiu aquesta selecció.

Rendiment

- Tota funcionalitat del sistema i transacció de negoci ha de respondre a la persona usuària en menys de 5 segons en el 90% de les peticions.

S'ha de tenir en compte també la següent informació:

- Segons és el límit perquè la persona usuària senti que el sistema reacciona instantàniament, és a dir, que no es necessita cap retroalimentació especial, excepte per mostrar el resultat.

- En les consultes que el temps sigui superior a 1 segon s'ha de mantenir l'atenció de la persona usuària ocupada amb un spinner, barra de progrés, etc.; un element que mostri que l'app està funcionant i no s'ha quedat bloquejada. La imatge mostrada de progrés serà conforme la escollida pels tècnics municipals

- 10 segons és el límit per mantenir l'atenció de la persona usuària centrada en l'app. En cas de superar-se aquest temps, cal produir un time out, cancel·lar la petició e informar a la persona usuària.

- El procés d'arrancada (startup) no ha de superar els temps indicats en un 95% de les ocasions.

Interoperabilitat

- Els serveis mòbils han d'estar construïts de forma desacoblada a la informació i per tant, cal que incorpori els mecanismes que permeti la integració i interoperabilitat.

Usabilitat

- L'aplicació s'ha de poder visualitzar correctament en els diferents dispositius mòbils establerts en la cobertura (mida de lletra, elements gràfics, etc.).

- El repintat de la pantalla ha de funcionar correctament en canvis d'orientació del dispositiu, menús emergents, finestres emergents, etc.
- La interfície gràfica ha de ser coherent en tota l'aplicació, i es manté la continuïtat en tot l'estil (literals, elements gràfics, errors ortogràfics) en base a la imatge corporativa.
- L'aplicació ha d'estar correctament localitzada (texts per diferents idiomes, monedes, unitats de mesura, etc.).
- S'ha de mostrar el teclat adequat per a cada tipus d'entrada (numèrica o alfanumèrica).
- L'aplicació ha de gestionar adequadament les pulsacions múltiples o multitouch.
- Cada pantalla ha de ser visible durant el temps necessari per llegir còmodament tota la seva informació.

Fiabilitat

- Cal que comprovi la introducció de dades errònies o que compleixi alguns formats (p.e. dni, nif, nie, dates, emails, telèfons, ...)
- Cal que notifiqui a l'usuari en cas d'operacions de llarga durada.
- Cal que avisi a l'usuari quan no es disposa de connectivitat.
- L'app no pot consumir recursos excessius.
- S'ha de poder instal·lar i desinstal·lar adequadament.
- Cal que notifiqui a l'usuari en cas d'interrupció externa

Qualitat

- Cal que que previ al lliurament de l'APP, es disposi del pla de proves corresponent per què el serveis informàtics, durant el procés de testing intern del cicle de vida, pugui validar el correcte funcionament de l'aplicació, i evidències que s'ha fet un joc de proves suficient.

Com a mínim inclourà proves:

- D'instal·lació
- Compatibilitat. Funcionament de l'app en diversos dispositius mòbils, navegadors, mides de pantalla, sistemes operatius, així com l'ús de dispositiu
- Rendiment. Resposta en condicions de poca bateria, memòria, baixa cobertura, transferència de fitxers, etc.
- Interrupció. Comportament en el seu ús quan es reben diferents interrupcions.
- Usabilitat, disseny i localització. Facilitat ús. Experiència satisfactòria. Disseny i continguts correctes en els diversos idiomes.
- Seguretat. Verificació vulnerabilitats en accés a dades, autenticació, autorització, etc.
- Conformitat. Guies acompliment markets.

- El contractista ha d'entregar el resultat d'aquest pla de proves realitzat a cada versió, amb l'objectiu de validar la correctesa de la versió.
- L'aplicació no ha de duplicar funcionalitats ja existents en el dispositiu.
- El conjunt de funcions de l'aplicació ha de ser consistent amb l'ajuda.
- Els enllaços externs han de funcionar correctament.
- L'aplicació ha d'usar capacitats que estan disponibles en tots els dispositius avaluats (GPS, brúixola...).
- L'aplicació ha de gestionar adequadament la configuració de notificacions i esdeveniments push.
- L'aplicació no ha de modificar permanentment cap ajust en el dispositiu per al qual no estigui destinada.

6.3. Requisits i característiques tècniques del servei al núvol

- Es desplegarà el sistema totalment al núvol seguint la definició i característiques del NIST (National Institute of Standards and Technology). El contractista aplicarà les còpies de seguretat conforme a les polítiques de seguretat municipal. L'adjudicatària haurà d'especificar els serveis d'operació, monitorització i administració de la infraestructura de que disposa per tal d'oferir la màxima disponibilitat, rendiment i prestacions.
- Els serveis estaran en un núvol dins la Unió Europea amb un conjunt d'adreces IP fixes conegudes per tal de poder validar els accessos d'aquest servei als WS i sistemes municipals.
- El licitador haurà de descriure les certificacions TIER dels CPDs que suporti el servei al núvol i l'arquitectura amb alta disponibilitat i balanceig de càrrega.
- Caldrà especificar els plans de contingència i de recuperació davant desastres (DR), polítiques de còpies seguretat, polítiques i auditories periòdiques en ciberseguretat d'acord a la normativa i d'acord a les polítiques municipals. Estarà obligat a informar periòdicament en cas de qualsevol canvi, incidència o resultat de les auditories per la seva supervisió i compliment durant la durada del contracte i com a mínim cada any.
- Caldrà indicar segons els requisits de finalització de servei i pla de retorn, com es complirà el retorn de servei finalitzat el contracte i de transició amb un altre adjudicatària i la portabilitat de les dades.

7. INTEL·LIGÈNCIA ARTIFICIAL

El sistema en el cas que usi intel·ligència artificial, els models i algorismes d'IA han d'estar en un núvol privat que no comparteix cap dada amb altres sistemes i només per aquest aplicació municipal objecte del contracte dins la UE.

L'algoritme ha d'estar registrat, ser públic i transparent tant en l'app com en les webs municipals que ho publiquin seguint les recomanacions del Digital Forum Lab d'Eurocities (veure <https://www.algorithmregister.org/guidance>) on ha de constar:

- Les dades del registre: nom, breu descripció, organització, departament, contacte, domini, estat, observacions, ...
- Cas d'ús: procés, objectius, impacte, riscos, categoria de risc, proporcionalitat, base legal, ...
- Dades d'entrenament, font, biaix de dades, avaluació de l'impacte de protecció de dades, ...
- Algoritme: tipus, descripció, mètodes, models, rendiment, url codi font, avaluació impacte, ...
- Supervisió i les dades associades

En la integració de components basats en IA l'adjudicatari caldrà que remeti les dades pertinents pel registre d'algoritmes a efectes de transparència i complir el Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial.

En el cas que s'oferta la millora de més idiomes en el sistema, aquests també hauran de ser suportats a l'aplicar la intel·ligència artificial si s'escau.

8. LLICENCIAMENT

El sistema objecte del contracte subministrat, integrat i instal·lat no tindrà cap limitació a nivell de llicència ja sigui per volum de base de dades emmagatzemada, de consum de recursos TIC, de nombre d'usuaris interns, nombre d'usuaris externs, població, qualsevol dispositiu o sistema integrat, ...

Finalitzat el contracte i si s'aplica el pla de retorn, l'adjudicatari haurà de subministrar l'última versió de tot el programari, arquitectura i estructura de

dades que s'ha subministrat i que els Ajuntaments tenen dret de llicenciament que ha adquirit per facilitar el pla de retorn i transició als sistemes municipals.

Si el contractista ha d'utilitzar materials, procediments i/o equipament o programari sotmesos a la propietat industrial i/o intel·lectual haurà d'obtenir prèviament les cessions, els permisos i les autoritzacions necessàries dels seus legítims titulars i hauran d'estar inclosos dins el preu ofert.

9. PLA DE FORMACIÓ, TRANSFERÈNCIA DE CONEIXEMENT I DOCUMENTACIÓ

S'haurà de presentar una proposta de formació que contindrà els diferents cursos que contemplin tant la vessant operativa com la vessant tècnica que inclourà:

- Formació específica a tot el personal usuari intern de la policia local que podran gestionar en el seu backoffice
- Formació específica al personal usuari avançat intern de la policia local en la gestió avançada del seu backoffice
- Formació als tècnics informàtics municipals en l'administració tecnològica i de seguretat del sistema.
- Formació als tècnics informàtics municipals en la integració i desenvolupament del sistema.
- Formació als tècnics de dades en el model de dades, l'extracció i explotació de dades del sistema pel seu anàlisi.

Aquestes formacions hauran de ser les suficients per desenvolupar les funcions d'acord als perfils indicats i hauran de ser realitzades de forma presencial en les instal·lacions municipals que s'indiquin a excepció que s'acordi per ambdues parts que sigui per videoconferència.

El contractista entregarà tota la documentació de caràcter tècnic i funcional configurada tant als tècnics municipals de la policia local i de TIC i els manuals d'ús d'acord al projecte d'implantació en format PDF.

Es valorarà si hi ha també un pla de formació continu durant el contracte de novetats i actualitzacions.

10. IDENTITAT VISUAL CORPORATIVA I MARCA:

El sistema en totes les funcionalitats (app mòbil, web, escriptori i backoffice web) haurà de complir el programa d'identitat visual corporativa d'acord a les indicacions del departament de comunicació corporativa de cada Ajuntament de tal manera que es configuri l'app de la persona usuària segons en quin municipi està o vol tenir configurat per defecte.

L'aplicació mòbil haurà de tenir una marca pròpia específica i exclusiva per aquest projecte acordat per tots els Ajuntaments i visible en els markets d'aplicacions mòbils.

11. PROPOSTA CATÀLEG SERVEIS ADDICIONALS

El contractista haurà de proporcionar consultories, formacions i desenvolupaments addicionals que demani cada Ajuntament quan ho cregui oportú per millores no incloses en el servei de suport i manteniment en el núvol que cada Ajuntament tindrà a la seva disposició per la seva pròpia personalització específica de l'aplicació i que assumirà cadascun segons aquestes hores consumides. Els costos unitaris associats s'hauran d'indicar en la proposta econòmica. Aquests només ho podran fer consultors funcionals i programadors/es apps i web sènior amb almenys 3 anys d'experiència en projectes similars de la mateixa dimensió.

12. MODIFICACIONS DEL CONTRACTE

Durant la durada del contracte, es podran realitzar modificacions en un màxim del 20% del pressupost total (IVA exclòs) per millores del sistema no incloses en el servei de suport i manteniment en el núvol que requereixin tasques de consultoria tècnica, formació o programació.

13. FACTURACIÓ

Per la implantació, es podran fer actes de recepció parcials per funcionalitats entregades en un entorn productiu i percentatges d'execució segons acordin

cada Ajuntament amb el contractista i constarà aquest acord en una acta d'inici de subministrament entre el municipi i l'empresa.

Finalitzada la implantació es realitzarà l'acta de recepció final de la implantació per cada Ajuntament.

La facturació del suport i manteniment del sistema implantat incloent el servei al núvol es realitzarà una vegada s'hagi posat en marxa el sistema en producció i, s'emetrà trimestralment a serveis prestats i trimestre vençut.

De la mateixa manera, s'emetrà facturació trimestral per separat quan es proporcionin consultories, formacions o programacions per millores addicionals una vegada prestades adjuntant els documents justificatius de les hores i millores realitzades.

Totes les factures s'emetran en format electrònic d'acord la normativa d'aplicació.

14. SERVEI DE SUPORT, MANTENIMENT I ACTUALITZACIÓ PRESTAT AL NÚVOL

El licitador haurà de presentar una proposta de suport, actualització i manteniment del sistema, detallant les característiques, horari, cobertura, eines, recursos i metodologia incloent tota la prestació en el núvol i altres serveis addicionals recurrents per garantir el seu funcionament de qualitat fins la finalització del contracte una vegada posat en marxa.

14.1 Horari de cobertura

El servei de suport, actualització i manteniment haurà de cobrir horari laboral de dilluns a dijous de 9:00 a 18:00 i divendres de 9:00 a 14:00 excepte festius nacionals i autonòmics, a excepció del període del 1 de juny al 30 de setembre que haurà de ser de 9:00 a 14:00 de dilluns a divendres per qualsevol incidència, consulta, petició o servei a excepció de les incidències greus o molt greus o actualitzacions que provoquen indisponibilitat del sistema que s'atendran les 24 hores del dia i els 365 dies de l'any.

14.2 Abast de la cobertura

Aquest servei inclourà el següent:

- Suport i manteniment correctiu:

Suport tècnic a les persones usuàries internes o als tècnics informàtics municipals per incidències de qualsevol element del sistema i producte incloent-hi la recuperació de dades errònies generades pel mal funcionament de l'aplicació.

Suport tècnic a la ciutadania usuària de l'aplicació que tinguin incidències en el seu ús.

- Suport i manteniment normatiu:

Servei de vigilància i actualitzacions dels sistemes d'informació objecte del contracte que garantiran en tot moment el compliment normatiu de rang estatal, autonòmic o municipal en matèria de seguretat policial, ciberseguretat, accessibilitat, protecció de dades de caràcter personal i intel·ligència artificial d'acord a l'objecte del contracte.

En especial, s'haurà de garantir la següent normativa:

- Llei 16/1991, de 10 de juliol, de les policies locals
- Llei orgànica 2/1986, de 13 de març, de forces i cossos de seguretat
- Llei 4/2003, de 7 d'abril, d'ordenació del sistema de sistema de seguretat pública de Catalunya.
- Llei orgànica 4/1997, de 4 d'agost, per la qual es regula la utilització de videocàmeres per les forces i cossos de seguretat en llocs públics.
- Esquema Nacional de Seguretat RD 311/2022, de 3 de maig, pel que es regula el Esquema Nacional de Seguretat.
- Real Decret 1112/2018, de 7 de setembre, sobre accessibilitat dels llocs web i aplicacions per dispositius mòbils del sector públic.
- Reglament UE 2016/679 de 27 d'abril del 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 – RGPD
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals – LOPDGDD
- Reglament (UE) 2024/1689 del Parlament Europeu i del Consell, de 13 de juny de 2024, pel qual s'estableixen normes harmonitzades en matèria d'intel·ligència artificial

- Suport i manteniment evolutiu i preventiu:

Actualitzacions de qualsevol element del sistema ja sigui per evitar l'obsolescència tecnològica o per corregir vulnerabilitats així com les incorporacions, modificacions i eliminacions necessàries en el producte per a cobrir l'expansió o canvi en les necessitats municipals.

Es garantirà en tot moment i d'acord als requisits tècnics generals, el seu funcionament en les últimes versions de sistema operatiu de mòbils i navegadors i el compliment dels requisits, publicació i gestió de l'app en les tendes Google Play i Apple Store en els comptes municipals on es donarà accés al contractista per tal que sempre estigui publicada l'aplicació en la seva última versió.

També inclourà tot el manteniment i evolutius de les APIs d'integració del sistema i de les integracions amb els sistemes municipals actuals o futurs si hi han canvis de proveïdors o sistemes municipals que estiguin compresos en els requisits d'integració. D'aquesta manera, en el cas que alguna dels sistemes a integrar indicats anteriorment es modifiquin o canviïn perquè un Ajuntament contracta un altre sistema, el licitador haurà de realitzar les adequacions i integracions necessàries dins del preu fix ofert de servei de suport i manteniment.

S'aplicarà qualsevol parxe o nova versió o subversió ja sigui del propi sistema o de qualsevol dels components que l'utilitzi, per tal de corregir qualsevol vulnerabilitat detectada o per realitzar les actualitzacions del programari necessari per tal de garantir que s'està en tot moment en versions amb suport i no End-Of-Life.

El servei també incorporarà les 'millores' i actualitzacions funcionals segons criteris d'universalitat del sistema implantat que el contractista aplica a tots els seus clients que tenen llicència del mateix tipus de sistema o app. També s'inclou la qualitat interna del sistema subministrat ja sigui per reestructuració del codi, definició més clara del sistema i optimització del rendiment i eficiència.

- Consultes:

El servei atendrà consultes i suport funcional i d'ús del sistema i d'explotació de dades dels interlocutors municipals autoritzats o de consultes de la ciutadania usuària.

També actualitzarà continguts de l'aplicació relacionades amb el compliment

dels requisits establert en el present plec que no es poden gestionar amb el backoffice pels tècnics municipals com poden ser FAQs, condicions d'ús, polítiques de privacitat, declaracions d'accessibilitat, ...

- Millora del posicionament continu en les tendes Google Play i Apple Store:

S'inclourà un suport mensual per millorar contínuament el posicionament amb ASO en les tendes d'aplicacions mòbils Google Play i Apple Store de tal manera que amb cerques segons les paraules clau que interressi surti en la primera posició.

- Servei al núvol:

Dins el servei s'inclourà la prestació de tot el sistema en el núvol que haurà d'estar funcionant les 24 hores i els 365 dies de l'any d'acord a la disponibilitat indicada en l'apartat de SLAs

- Canal d'atenció:

El canal d'atenció serà preferentment per mitjans electrònics amb l'eina de ticketing, correu electrònic o telèfon sense tarificacions especials pel personal municipal intern i per la ciutadania usuària de l'app, a través de la pròpia app, correu electrònic o whatsapp.

- Condicions:

El servei serà realitzat si s'escau de forma remota per part del contractista d'acord a les indicacions dels tècnics municipals de cada Ajuntament mitjançant connexió segura i caldrà que compleixi les instruccions, polítiques i normativa de seguretat TIC municipals.

14.3 Recursos tècnics i de personal i metodologia de gestió

- Eina de ticketing:

Totes les incidències, peticions o consultes ja siguin internes o externes de la ciutadania estaran registrades en un sistema de ticketing i el responsable del contracte o a qui ho delegui de cada Ajuntament, podrà fer un seguiment del seu estat i compliment de SLAs. Caldrà detallar aquesta eina per la seva valoració

- Recursos tècnics:

Caldrà indicar els recursos tècnics, formació, perfils i experiència que donaran aquest servei de suport i manteniment per la seva valoració

- Metodologia de gestió:

Caldrà detallar quina metodologia de gestió i procediments s'utilitza per la gestió del servei d'acord al seu abast i horari amb els recursos tècnics i de personals oferts.

15. ACORDS DE NIVELL DE SERVEI DEL SUPORT I MANTENIMENT TÈCNIC

L'adjudicatari haurà de complir, com a mínim, els acords de nivell de servei mensuals proposats (SLA) i a les penalitzacions previstes en cas d'incompliment següents:

ACORDS DE NIVELL DE SERVEI (SLA)		
CONCEPTE	SLA SOL·LICITAT	PENALITZACIONS SOL·LICITADES
Temps de posta en marxa	L'establert a l'apartat de projecte d'implantació	Infracció greu per cada mes d'endarreriment
Temps màxim resolució d'una consulta o petició del servei de suport i manteniment	< 10 dies laborables	Infracció lleu entre 10 i 20 dies laborals i infracció greu quan es superior a 20 dies laborals
Temps màxim de resolució d'una incidència lleu	< 10 dies laborables	Infracció lleu entre 10 i 20 dies laborals i infracció greu quan es superior a 20 dies laborals
Temps màxim de resolució d'una incidència greu	< 2 dies naturals	Infracció lleu entre 2 i 3 dies naturals i infracció greu quan és superior a 3 dies naturals
Temps màxim de resolució d'una incidència molt greu	< 1 dia natural	Infracció greu entre 1 i 2 dies naturals i molt greu quan és superior a 2 dies naturals
Disponibilitat trimestral del sistema al núvol	>=99,5%	Quan la disponibilitat sigui >=99% i <99,5% es considerarà falta greu i quan sigui <99% es considerarà falta molt

ACORDS DE NIVELL DE SERVEI (SLA)

		greu.
Resposta del sistema a la persona usuària de totes les funcionalitats del sistema i transaccions de negoci	≤ 5 segons en el $\geq 90\%$ peticions	Quan sigui la resposta ≤ 5 segons sigui entre $\geq 80\%$ peticions i $< 90\%$ peticions serà falta greu i si és $< 80\%$ falta molt greu

Criteris d'aplicació dels nivells de servei (SLA)

- Un dia laboral s'entén passat 8 hores en horari laboral del suport i manteniment i un dia natural s'entén passat 24 hores naturals durant els 365 dies l'any.
- Tots aquests paràmetres s'entenen que hauran de ser assumits per l'adjudicatari a excepció dels casos no imputables a aquest

Tipus incidència

- S'entendrà per **incidència lleu** aquelles que entorpeixin el treball de l'usuari sense provocar cap parada.

- S'entendrà per **incidència greu** aquella que sigui lleu i a més degradi el sistema i afecti a l'usuari final, en quant no permeti desenvolupar de forma normal la seva tasca, provocant parades intermitents del sistema. Caigudes intermitents i repetides, caigudes de rendiment que provoquin la parada del desenvolupament de les tasques de l'usuari. Elements que provoquin el reinici reiterat del sistema, etc.

- S'entendrà per **incidència molt greu**, aquelles que son greus i a més afecten molt significativament a l'usuari final de la corporació no podent desenvolupar les seves tasques. Per tant, parada i mal funcionament total del sistema.

En el cas que un Ajuntament contracti un servei d'auditories de ciberseguretat o d'adequació a l'ENS i el sistema es detecti un incompliment, subsanació o problema de seguretat sempre i quan sigui imputable al contractista, l'empresa ho haurà de resoldre segons el seu impacte d'acord als SLAs indicats

anteriorment. El nivell de vulnerabilitat o d'incident de seguretat serà determinat per l'Administrador de Seguretat de l'Ajuntament.

16. ELABORACIÓ D'INFORMES PER LA VALORACIÓ DE LA QUALITAT DEL SERVEI

El contractista lliurarà trimestralment un seguit d'informes de seguiment del servei i compliment de SLAs dins del servei tècnic de suport, actualització i manteniment que entregará als tècnics municipals designats per cada Ajuntament prèviament a la reunió trimestral de seguiment del servei que es realitzarà per ambdues parts on estaran les persones designades de cada Ajuntament i de l'empresa contractista que es podrà fer telemàtica o presencial segons acordin les parts.

La data límit de presentació dels informes serà el dia 25 del mes posterior al compliment del trimestre i si és festiu, l'endemà laborable. No es podran presentar ni s'acceptaran factures de suport mentre no s'hagin presentat els informes de seguiment del trimestre i s'hagi fet la reunió trimestral de seguiment.

Addicionalment i sota demanda per part dels tècnics municipals, es podran demanar nous informes orientats a realitzar un control, seguiment i millora de la gestió dels serveis.

Els aspectes a incloure com a mínim en els informes són:

- Informe d'incidències, consultes, peticions i actuacions correctives, normatives, evolutives i preventives realitzades i compliment dels SLA's que inclou tant internes com externes.
- Propostes de millores orientades a reduir incidències o incorporació de noves funcionalitats o planificació de formacions o actualitzacions.
- Jornades i hores de consultoria i programació realitzades o a planificar

17. DEMOSTRACIÓ PRÀCTICA

Els licitadors hauran de realitzar durant la fase de valoració, una demostració pràctica de la proposta de l'aplicació mòbil, versió web, d'escriptori i backoffice d'acord als requisits establerts al plec als tècnics municipals designats per tal d'aclarir, tots els dubtes funcionals, tècnics i de disseny així com per poder valorar l'agilitat d'ús, proposta innovadora, flexibilitat, capacitat, proactivitat, efectivitat i compliment de requeriments. Aquesta demostració es podrà fer «in situ» en les instal·lacions municipals que es designin o mitjançant videoconferència.

Prèviament a aquesta demostració i dins la documentació tècnica presentada, el licitador haurà de facilitar un accés d'un pilot elaborat per l'empresa licitadora per tal que els tècnics municipals puguin valorar el prototipus dissenyat pel licitador de l'aplicació mòbil, versió web, escriptori i backoffice web proposat en un entorn de proves que simuli el requerit.

18. PROJECTE D'IMPLANTACIÓ

Cada Ajuntament controlarà mitjançant el responsable del contracte, el compliment dels terminis acordats així com la qualitat i l'adequació dels subministraments objecte d'aquest contracte i l'execució del mateix segons els requisits d'aquest plec i cadascun crearà un comitè de direcció de projecte d'implantació format per policia local, TIC, comunicació i altres departaments municipals que es considerin que faran el seguiment de l'execució del projecte d'implantació en cada municipi amb l'adjudicatària.

El responsable del contracte pot delegar la interlocució segons disciplines que es puguin requerir per aspectes tecnològics, funcionals, formatius, comunicatius, etc.

També s'establirà una direcció de projecte a nivell de tots els Ajuntaments participat pels responsables i tècnics designats de la policia local i dels serveis TIC de cada Ajuntament que es reuniran periòdicament amb l'adjudicatària pel seguiment global del projecte d'execució.

El licitador designarà un cap de projecte amb formació universitària amb titulació relacionada amb l'àmbit tecnològic (informàtica, telecomunicacions, electrònica i industrial o equivalent) que actuarà com únic interlocutor per tots els temes relacionats amb la gestió i execució del contracte. Aquest tècnic haurà de tenir una experiència de 3 anys o més com a cap de projecte d'altres contractes amb

el mateix objecte que el present d'implantació d'una aplicació mòbil i un sistema de gestió de seguretat ciutadana.

Proposarà un calendari de reunions de seguiment, començant per la inicial de kick-off amb els principals membres del projecte. El cap del projecte de l'adjudicatari serà l'encarregat de fer les convocatòries i aixecar actes de les reunions.

L'equip de projecte haurà d'incloure també d'un/a consultor/a funcional, d'un/a programador/a d'apps i webs i d'una/a dissenyador/a gràfic/a tots ells amb almenys 3 anys d'experiència en projectes similars de la mateixa dimensió i objecte durant la implantació del projecte. Es valorarà el cap de projecte i l'equip pluridisciplinari proposat i la seva experiència en projectes similars que superin els mínims exigits.

Caldrà aportar documentació acreditativa (certificat i declaracions responsables) que es puguin comprovar aquests requisits de titulació i l'experiència professional i si són de la contractista o subcontractista tenint en compte que el/la Cap de projecte i el consultor/a funcional ha de pertànyer a la plantilla de personal de l'empresa.

Aquests mitjans personals en cas de possibles mancances de coneixement, incompliment de tasques i/o fites, absències o d'altres degudament justificades a petició del responsable del contracte municipal, l'adjudicatari l'haurà de substituir en un termini màxim de 15 dies hàbils garantint els mateixos requisits del personal adscrit.

Tota la documentació acreditativa caldrà aportar-la en el model d'oferta sobre B – judici de valor.

En el projecte, l'adjudicatari caldrà que realitzi les següents tasques:

- Configuració i parametrització del sistema segons els requeriments funcionals, tècnics i d'integració.
- Cursos de formació, manuals d'ús i transferència de coneixement.
- Elaboració de documentació tècnica i entregables.
- Fase de posta en marxa.

- Seguiment per part de les parts del correcte funcionament durant un temps prudencial.

En el document de projecte d'implantació caldrà detallar:

- a) Metodologia de treball i de gestió del projecte
- b) Identificació de les tasques del projecte d'implantació i entregables
- c) Proposta de parametrització funcional, d'integració, tècnica i de seguretat del sistema i de documentació a entregar.
- d) Diagrames de temps de les tasques a realitzar.
- e) Personal tècnic assignat en cada tasca i dels perfils de l'equip de treball del licitador proposat i en especial del cap de projecte.
- f) Punts de coordinació entre els tècnics que realitzen la implantació i el personal tècnic de l'Ajuntament de Reus tant dels responsables funcionals departamentals com de comunicació corporativa i com dels tècnics informàtics municipals.

La fase d'implantació tindrà un termini màxim de 12 mesos. Mentre duri la implantació fins la seva total posada en marxa de totes les funcionalitats, el licitador haurà de proporcionar el servei en el núvol de les funcionalitats que vagi posant en marxa tant en entorn de test com producció i el preu del servei al núvol estarà dins el preu d'implantació fins que duri aquesta fase.

En el cas que les actuacions del projecte afectin el normal funcionament dels sistemes, aquestes hauran de fer-se fora de l'horari laboral normal sense preu addicional i quan hi hagi menys afectació dels serveis municipals prèvia planificació de mutu acord.

El contractista haurà d'entregar la documentació de les actuacions i configuracions realitzades així com manuals de formació a cada perfil indicat en el pla de formació en format PDF. El licitador haurà de concretar quin tipus de documentació detallada entregarà.

Els entregables del sistema implantat inclourà tota la documentació tècnica, documentació funcional, model de dades i de l'API de la plataforma per la seva integració que requereixi els serveis tècnics municipals involucrats en el projecte.

Únicament podran participar en el projecte el personal tècnic del contractista amb experiència demostrada en projectes similars i amb una experiència mínima de 3 anys. En el cas de subcontractació, caldrà que en la proposta s'indiqui quina part se subcontracta i caldrà l'autorització municipal.

19. TITULARITAT I ÚS DE LES DADES

En relació amb la titularitat i ús de les dades l'adjudicatària assumeix que:

- La totalitat de les dades transferides per a la posada en funcionament dels sistemes i de les que es puguin generar en el futur són propietat de cada Ajuntament.
- L'ús d'aquestes dades per part de l'adjudicatària com a banc de proves per a introduir possibles millores en la prestació del servei haurà de ser prèviament autoritzada per cada Ajuntament, que en podrà monitorar l'ús.
- La restricció en l'ús de les dades, més enllà de les limitacions referides a confidencialitat i protecció de dades personals establertes en aquestes prescripcions tècniques, inclou qualsevol ús o explotació, comercial o no, d'aquestes dades de forma anònima i dissociada.

20. PORTABILITAT DE LES DADES I FINALITZACIÓ DEL SERVEI AL NÚVOL

20.1. PORTABILITAT DE LES DADES

L'adjudicatària garantirà en tot moment la portabilitat de les dades derivades de la gestió del servei si es presta al núvol, d'acord amb els següents requisits:

- El lliurament de les dades i documents es realitzarà a la fi del contracte o servei en el format acordat en el contracte.
- Els formats de retorn estaran sempre alineats amb estàndards oberts i que garanteixin la neutralitat tecnològica.
- El termini de lliurament serà el més breu possible i en cap cas impedirà la continuïtat del servei si aquest ha estat adjudicat a un altre proveïdor, d'acord amb el Pla de retorn.

- L'adjudicatària assumeix que facilitarà el traspàs de dades a un altre proveïdor.
- El lliurament de les dades i documents aniran acompanyats dels requisits necessaris per a garantir-ne la seva integritat i autenticitat, ja sigui a la fi del contracte o en qualsevol altre moment que s'estipuli o es consideri necessari per cada Ajuntament.
- Les dades es lliuraran de manera estructurada, basats en model relacional i amb la documentació necessària per a la seva correcta migració i posada en funcionament.
- La portabilitat de les dades i documents no suposarà despeses vinculades a aquestes accions en cap cas.

20.2. FINALITZACIÓ DEL SERVEI AL NÚVOL

La finalització de la prestació del servei en el cas que sigui al «núvol», suposarà l'aplicació del Pla de retorn i l'eliminació de les totes les dades i els documents de manera que aquesta informació no pugui ser recuperada ni reconstituïda, incloses les metadades associades a aquesta informació.

El termini per a portar a terme l'eliminació completa i definitiva de la informació serà com a màxim de 3 mesos a partir del moment que cada Ajuntament i l'empresa prestatària del servei hagin realitzat les corresponents verificacions d'integritat i posada en marxa i signat el corresponent document de recepció.

L'adjudicatària inclourà en el seu Pla de retorn el compromís de certificar l'eliminació de les dades i garantir-ne la traçabilitat i l'auditoria per part de cada Ajuntament.

La portabilitat de dades es podrà exigir de manera anticipada a la fi del contracte si s'acredita l'incompliment de les condicions específiques d'aquest plec o altres causes que ho justifiquin, així com pel tractament inadequat d'una empresa subcontractada o per la falta de seguretat en transferències internacionals de dades. També es podrà exigir quan es produeixin modificacions unilaterals per part del proveïdor de les condicions de la prestació del servei.

Si cada Ajuntament que el servei prestat no és apte per al fi pretès com a conseqüència de penalitzacions aplicades, vicis, defectes o funcionament no satisfactori, i existeixi el fundat temor que les mesures reactives de l'adjudicatària respecte de la solució no siguin suficients per aconseguir aquell fi, podrà rebutjar el servei deixant a compte de l'empresari i quedant exempt de

l'obligació de pagament, o tenint dret, si escau, a la recuperació del preu satisfet.

20.3. PLA DE RETORN DE SERVEIS AL NÚVOL

Quan es requereixi o finalitzi el servei en el «núvol» i sigui retornat a l'Ajuntament corresponent, es podrà exigir l'obtenció de les dades estructurades que ha fet servir, per a posteriorment realitzar la supressió completa i permanent d'aquestes dades en la infraestructura de l'adjudicatària sortint, així com la certificació de que el procés s'ha realitzat correctament.

A l'efecte, els licitadors hauran d'incloure en la seva oferta un Pla de Retorn dels serveis, el qual s'acordarà en cas d'execució, quedant l'adjudicatària obligat al traspàs de aquells elements afectes a la prestació dels Serveis a l'Ajuntament corresponent o a un tercer designat per aquest, sense cap cost addicional per a l'Ajuntament.

El proveïdor sortint estarà obligat a mantenir el compliment del model de mesurament del servei durant el període acordat, així com a col·laborar per facilitar la transferència al proveïdor entrant, traspassant els mitjans i procediments necessaris per al Servei. L'equip del proveïdor sortint encarregat de realitzar el traspàs haurà d'haver format part de la gestió del servei.

Durant aquest període, que serà planificat per l'Ajuntament corresponent i amb una durada màxima de dos mesos, el proveïdor sortint no podrà incrementar els imports del servei, vigents en el moment de la finalització formal del contracte.

21. CONFIDENCIALITAT

L'empresa adjudicatària queda expressament obligada a mantenir absoluta confidencialitat i reserva sobre qualsevol dada o actiu d'informació que pogués conèixer amb ocasió del compliment del contracte, especialment les de caràcter personal o confidencial.

L'empresa adjudicatària quedarà obligada a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes de cada municipi, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeixin al seu personal per a l'execució d'aquest contracte.

L'empresa adjudicatària es farà responsable dels perjudicis que se li puguin ocasionar a algun Ajuntament degut a d'incompliment de qualsevol de les condicions esmentades.

Per tal de garantir la confidencialitat de la informació i documentació facilitada, el licitador haurà de redactar i signar una declaració de confidencialitat.

Aquesta declaració haurà de ser necessària i proporcional a la finalitat o interès que es vol protegir i ha de determinar de forma expressa i justificada els documents i/o les dades facilitades que considerin confidencials. No s'admeten declaracions genèriques, sense referència a documents o apartats concrets, o no justificades del caràcter confidencial.

En cas de manca d'indicació, s'entendrà que la documentació no té caràcter confidencial.

De conformitat amb l'article 133.1 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic, l'òrgan de contractació no podrà divulgar la informació facilitada pels licitadors indicada de forma expressa i justificada, per aquests com a confidencial.

22. PROTECCIÓ DE DADES, ENS I SEGURETAT TIC

En el cas que la prestació dels serveis, suposi la necessitat d'accés a dades de caràcter personal, el contractista, com a encarregat del tractament, queda obligat a garantir el compliment de la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i Garantia dels Drets Digitals i el Reglament (UE) 2016/679 General de Protecció de Dades, així com qualsevol altra normativa vigent nacional i europea en matèria de Protecció de Dades de Caràcter Personal.

El contractista respondrà de totes les infraccions en que podria incórrer en el cas que destini les dades personals a una altra finalitat, les comuniqui a un tercer no autoritzat, o en general, les utilitzi de forma irregular, així mateix quan no adopti les mesures corresponents per l'emmagatzematge i custòdia dels mateixos. A tal efecte, s'obliga a indemnitzar a la corporació municipal, per qualsevol dels perjudicis que sofreixi directament o per tota reclamació, acció o procediment, que porti la seva causa per incompliment o compliment defectuós per part de l'adjudicatari del dispostat tant en el contracte com en la normativa reguladora de la protecció de dades de caràcter personal.

El contractista únicament tractarà les dades de caràcter personal als que pugui tenir accés conforme a les instruccions municipals i no els aplicarà o utilitzarà amb una finalitat diferent a l'objecte del contracte.

El tractament de les dades que pugui originar-se al llarg de l'execució del contracte per part del contractista haurà de realitzar-se a la Unió Europea.

L'empresa caldrà que adopti les mesures tècniques i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, atès que els elements tecnològics objecte del contracte hi seran exposats així com l'acció humana.

Les anteriors obligacions i altres obligacions addicionals en matèria de protecció de dades personals hauran de regular-se mitjançant la signatura d'un contracte de tractament de dades entre cada entitat municipal corresponent i el contractista.

El sistema d'informació prestat al núvol que oferta l'empresa licitadora, cal que disposi de la certificació en vigor del RD 311/2022, de 3 de maig, pel que es regula el Esquema Nacional de Seguretat en la seva categoria alta i se sotmeti a les auditories municipals que siguin oportunes d'acord al compliment de la normativa i en cas de deficiències, a corregir-les dins del preu fix de manteniment. Caldrà que l'empresa licitadora adjunti el certificat en vigor de l'ENS categoria alta en la proposta tècnica del sobre B dins de l'apartat de l'oferta tècnica «ENS i ciberseguretat».

També caldrà acreditar el compliment de la normativa actual en matèria de protecció de dades d'acord al 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 (en endavant, el "RGPD") i de la Llei Orgànica 3/2018, de Protecció de Dades Personals i garantia dels drets digitals (en endavant, la "LOPDGDD")

L'aplicació haurà de contenir clàusules d'acord a les instruccions del/a Delegat/da de Protecció de Dades de caràcter personal de cada Ajuntament en quant a protecció de dades i política de privacitat.

També haurà d'informar de les condicions d'ús de l'aplicació i del registre d'algoritmes utilitzats d'intel·ligència artificial i recollir el consentiment de la persona usuària.

23. DOCUMENTACIÓ DE LA PROPOSTA TÈCNICA

Independentment de la documentació de tipus administratiu sol·licitada, els licitadors presentaran la següent documentació obligatòria de caràcter tècnic en el sobre B - judicis de valor seguint estrictament el següent guió:

1.- Característiques funcionals del sistema

1.1 Funcionalitats generals i arquitectura comuna

1.2 Funcionalitats específiques

2.- Característiques d'integració

2.1.-Integració amb sistemes requerits

2.2.-API integració del sistema ofertat

3.- Característiques tècniques i arquitectura tecnològica

3.1 Característiques i arquitectura tecnològica general

3.2 Característiques tècniques aplicació mòbil

3.3 Característiques tècniques aplicació web, d'escriptori i backoffice

3.4 Característiques tècniques i arquitectura en el núvol, pla de retorn i finalització del servei

3.5 Intel·ligència artificial

4.- Pla de formació, transferència de coneixement i documentació

5.- Característiques del servei de suport, manteniment i actualització prestat al núvol

5.1 Horari de cobertura i abast del servei

5.2 Recursos de personal i tècnics del servei

5.3 Metodologia de gestió del servei i dels informes de seguiment de la qualitat del servei

6.- Projecte d'implantació i documentació acreditativa dels mitjans personals adscrits

7- Confidencialitat, protecció de dades personals, ENS i seguretat TIC

7.1 Confidencialitat

7.2 Protecció de dades personals

7.3 ENS i ciberseguretat

8.- Accés a un entorn pilot del sistema proposat

9.- Altres aspectes addicionals que es considerin oportuns

Serà causa d'exclusió de l'oferta presentada en el cas que la documentació tècnica lliurada no es presenti o no segueixi el guió definit anteriorment i no acrediti en aquesta documentació el compliment de cadascun dels requisits establerts en el plec tècnic, és a dir, cal justificar el compliment de tots i cadascun dels requisits tècnics. També serà motiu exclusió que s'inclogui en el sobre B informació que s'hagi d'incloure al sobre C i, per tant, s'hagi de valorar mitjançant criteris d'adjudicació quantificables de forma automàtica.

Inspector

Cap del Servei de Tecnologies de la

Cap de la Guàrdia Urbana

Informació i Telecomunicacions

Pedro Muñoz de la Paz

Oscar Hellín Escribano