Ajuntament de Barcelona

Institut Municipal d'Informàtica
Direcció d'Estratègia i Nous Projectes
C/ Tànger, 98, pl 12
08018 - Barcelona
Telèfon 93 291 81 00
www.bcn.cat

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT DE DISPOSITIUS DE GRAVACIÓ PERSONAL I SOFTWARE DE GESTIÓ PER A LA GUÀRDIA URBANA DE BARCELONA AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE.

CONTINGUT

1 INTRODUCCIÓ

Dins del Pla Director de la Guàrdia Urbana de Barcelona existeix la proposta d'adquisició de Dispositius Personals de Gravació, en endavant DPG. La disponibilitat d'aquest equipament comporta, com en el cas d'altres cossos policials que ja disposen:

- Plenes garanties per a la seguretat pública, tant pel que fa als drets i llibertats de les persones com per a la mateixa actuació policial.
- Reducció de la quantitat de queixes i denuncies per presumpte mala praxis policial.
- Percepció de transparència per part de la ciutadania i del propi cos de la GUB.
- Augment en la qualitat del servei.
- Augment en l'adequació als principis deontològics per tota la plantilla (tant per les persones dotades de càmera com per les que no en portin).
- Augment en la confiança en la valoració del servei per part de la ciutadania.
- Millora en la qualitat de les diligències de la Guàrdia Urbana de Barcelona al permetre que es puguin aportar les imatges com a elements probatoris.

Els DPG ja han estat implantats amb èxit en l'àmbit policial en entorns propers, com els casos de:

- Policia Metropolitana de Londres: va començar la seva prova pilot en l'any 2014 amb 1000 càmeres i, en l'actualitat, en té desplegades 22000 (s'estima que les policies britàniques fan servir un total de 48000 càmeres, desplegades en el 70% dels cossos de seguretat).
- Policia local de Sant Adrià del Besòs: la Direcció General d'Administració de Seguretat va autoritzar l'ús de dues càmeres per al seu ús per part dels agents com a part de la dotació personal el mes d'agost de l'any 2016.
- Policia de la Generalitat – Mossos d'Esquadra: va desplegat 164 dispositius personals de gravació l'any 2018, vinculats parcialment a l'ús dels dispositius conductors d'energia, però amb autorització per ser utilitzats en altres supòsits.

En els cossos amb més experiència en el seu ús, el resultat més positiu ha estat una reducció en la conflictivitat de determinades intervencions amb persones (una estimació efectuada durant la prova pilot a Londres valorava en un 33% la reducció de les queixes presentades contra agents de la policia metropolitana).

Concretament, durant el període 2019-2020, la Guàrdia Urbana de Barcelona juntament amb la Gerència de Prevenció i Seguretat, va dur a terme un projecte d'estudi i anàlisis de necessitats dels DPG, que n'incloïa l'ús i els procediments necessaris per utilitzar-los. Es va realitzar, durant més d'un any, un pilot productiu amb diferents DPG i softwares comercials per conèixer-los i avaluar-ne els resultats. Aquests van resultar satisfactoris i han permès definir principalment:

- Un procediment operatiu de regulació de l'ús dels DPG a la GUB.
- Un sistema de comunicació amb la Direcció General d'Administració de Seguretat per al control de les gravacions efectuades.
- Una valoració dels recursos necessaris per una implantació plenament operativa.
- Una valoració de la utilitat dels DPG per al sistema de seguretat pública de la ciutat.
- Unes característiques de hardware i software necessàries, d'acord amb el funcionament i les necessitats de la GUB.

2 OBJECTE

L'objecte del present contracte és la l'adquisició de 150 Dispositius de Gravació Personal i dels seus accessoris, la implantació de l'aplicació de software de gestió i el desenvolupament de funcionalitats necessàries pel seu ús a la Guàrdia Urbana de Barcelona d'acord amb les previsions del plec de prescripcions tècniques, amb mesures de contractació pública sostenible.

En aquest plec s'estableixen les especificacions tècniques i funcionals sobre la base de les quals ha de realitzar-se el subministrament i configuració dels dispositius pel seu funcionament dins la xarxa corporativa de l'Ajuntament de Barcelona, la implantació i adaptació de l'aplicació de software de gestió que permeti la parametrització, traçabilitat, seguiment, càrrega i descàrrega dels enregistraments així com el desenvolupament de funcionalitats per a l'ús de l'aplicació d'acord amb la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, les especificacions tècniques de l'Institut Municipal d'Informàtica (IMI) i amb les necessitats específiques de Guàrdia Urbana de Barcelona (GUB).

2.1 Procediment de contractació

La contractació es realitzarà pel procediment obert amb publicitat, de regulació harmonitzada i tramitació ordinària, tot entenent que es garanteix la màxima concurrència i competitivitat. Es permetrà la subcontractació.

3 ABAST

L'abast del contracte comprèn tant les tasques directament derivades de l'adquisició del material i la seva instal·lació, com l'adaptació i la implantació del software de gestió i les corresponents tasques de gestió, anàlisi, seguiment, proves, formació i implantació del projecte.

Els dispositius i equipament sol·licitats es lliuraran completament posats en servei operatiu en els diferents departaments i unitats organitzatives de GUB.

3.1 Subministrament

La solució que proveirà l'adjudicatari ha de contenir els següents elements:

3.1.1 Subministrament de hardware

Subministrament de:

Número	Hardware	Referència
150	Dispositius de Gravació Personal	4.1 Dispositius personals de gravació (DPG)
180	Suports d'ancoratge dels dispositius a la uniformitat de GUB	4.3 Suports
15	Carregadors múltiples	4.2 Carregadors i descàrrega dels enregistraments
5	Carregadors individuals	
	Hardware complementari necessari per la descàrrega dels enregistraments	
	Sistema d'identificació i assignació dels dispositius als usuaris	4.4 Mecanismes d'assignació / des-assignació

Amb les següents consideracions:

- En el cas que es requereixi algun tipus de hardware específic per a la descàrrega dels enregistraments, la comunicació, etc. aquest es presentarà en el plec i estarà inclòs en el preu de licitació.
- El producte no podrà ser llicenciat per usuari. L'ús dels dispositius i del software de gestió ha de ser independent del nombre d'usuaris que els puguin utilitzar, ja que tot el cos de policia de la GUB, actualment aproximadament 3.000 operatius, ha de poder fer-ne ús. En el cas que el producte vagi acompanyat d'un llicenciament per l'ús del software d'aplicació, aquest estarà inclòs en el preu del contracte per un període no inferior a 5 anys.
- En el cas de que pel sistema d'identificació i d'assignació dels DPG als usuaris, siguin necessaris elements tipus targetes o adhesius, se subministraran tantes com aproximadament el 70% de la plantilla de GUB (al voltant de 2100 usuaris) amb la possibilitat d'ampliació sense cap cost addicional més que el propi de l'adquisició dels elements identificatius.

  En el cas que el licitador disposi de diferents mecanismes d'identificació i d'assignació dels DPG als usuaris, els presentarà i inclourà en el plec. Durant la implantació del projecte, la Direcció, decidirà el més adient amb la possibilitat de combinar més d'un sistema (per exemple, targetes i adhesius) sense cap cost addicional, sempre que el nombre total no excedeixi el demanat en el plec (70% de la plantilla de GUB).

3.1.2 Subministrament del Software de gestió

Es proporcionarà el software de gestió que compleixi les característiques descrites al plec 5. Descripció del software de gestió i 6. Altres Funcionalitats d'acord a la planificació del projecte 11.3 Planificació del projecte.

Les actualitzacions que el software de gestió pugui tenir el software durant el període de garantia (mínim 6 mesos), estaran incloses en el projecte.

3.1.3 Distribució

A continuació es presenta una possible distribució dels elements de hardware licitats en aquest plec. És important considerar que tots aquells elements no especificats explícitament al plec i propis de cada producte per al necessari funcionament del sistema, també estan inclosos, i que el seu nombre serà determinat pel licitador d'acord amb la distribució física dels DPG per assegurar el correcte funcionament del sistema.

	Total DPG	Total Suports	Total Carregadors múltiples	Total Carregadors individuals
Divisió Territorial	115	120	11	3
Divisió Recursos Operatius i Suport	15	20	1	1
Divisió Trànsit i Seguretat Viària	10	15	2	1
Incidències / Recanvis	10	20	1	
TOTAL	**150**	**180**	**15**	**5**

Amb les següents consideracions:

- La Divisió Territorial consta de diferents Unitats Territorials distribuïdes per tota l'àrea metropolitana de Barcelona en ubicacions físiques diferents:
  - Unitat Territorial del districte de Ciutat Vella (UT1)
  - Unitat Territorial del districte de Eixample (UT2)
  - Unitat Territorial del Districte de Sants-Montjuïc (UT3)
  - Unitat Territorial del Districte de les Corts - Seu Lluch Gervilla (UT4)
  - Unitat Territorial del Districte de Sarrià - Sant Gervasi (UT5)
  - Unitat Territorial del Districte de Gràcia (UT6)
  - Unitat Territorial del Districte d'Horta-Guinardó (UT7)
  - Unitat Territorial del Districte de Nou Barris (UT8)
  - Unitat Territorial del Districte de Sant Andreu (UT9)
  - Unitat Territorial del Districte de Sant Martí (UT10)

  Les Unitats Nocturnes utilitzen els espais físics de les unitats dels territoris que abasten:
  - Unitat Nocturna Tango (Sants-Montjuïc)
  - Unitat Nocturna Victor (Gràcia – Sarrià Sant Gervasi)
  - Unitat Nocturna Oscar (Horta Guinardó – Nou Barris)
  - Unitat Nocturna Eco (Sant Andreu – Sant Martí)

- La Divisió de Recursos Operatius i de Suport:
  - Unitat d'Investigació (*)
  - Unitat de Reforç, Emergències i Proximitat (UREP)
  - Unitat de Suport Diürn
  - Unitat Muntada (*)
  - Unitat de Platges

- La Divisió de Trànsit
  - Unitat Central de Trànsit (UCT)
  - Unitat d'Investigació i Prevenció de l'Accidentalitat (UIPA)
  - Unitat de Denúncies per Imatges Gravades (*)

(*) Unitats que no disposaran de DPG

Totes les unitats es localitzen dins de la ciutat de Barcelona en dependències diferents però totes, tret de les quatre unitats nocturnes, que comparteixen seu amb algunes unitats territorials, de manera que en totes elles caldrà distribuir tots els elements de hardware que permetin l'ús dels DPG.

3.2 Serveis inclosos

- **Llançament, gestió, control i seguiment del projecte:** l'adjudicatari designarà un únic interlocutor per realitzar la gestió, control i seguiment del projecte per aconseguir la correcta implementació. Es duran a terme reunions de Direcció i Seguiment del projecte en les que el licitador participarà activament.

- **Gestió del canvi:** L'adjudicatari estarà obligat a elaborar i a executar un Pla de Gestió del Canvi que inclogui el Pla de Desplegament, el Pla de Formació , el Pla de Suport i el Pla de Riscos.

- **Lliurament de tot el material de hardware**: El material es lliurarà d'acord amb les especificacions tècniques descrites i amb els terminis especificats en el plec. Restarà en dependències de l'adjudicatari fins al moment de la instal·lació en les unitats/dependències de GUB. L'adjudicatari s'haurà d'encarregar de retirar tot el material d'embalatge i peces sobrants, si és el cas.

  Els DPG es lliuraran **etiquetats** per l'adjudicatari amb una etiqueta en un lloc visible en la que apareix el dibuix d'una càmera i el text "VIDEO i AUDIO" com les que estem utilitat a l'interior dels vehicles a l'habitacle de detinguts. GUB passarà el disseny i contingut i l'adjudicatari fa les etiquetes i les enganxarà als DPG abans de lliurar-los. Amb això s'informa a la ciutadania d'aquesta possible gravació.. Les etiquetes han d'estar dissenyades per suportar les situacions meteorològiques comunes (sol, pluja..) sense deteriorar-se.

- **Instal·lació de l'equipament a les dependències físiques de GUB i del software de gestió al servidor proporcionat per l'IMI**. Inclou aspectes com les especificacions de les IPs per poder reconèixer els equipaments dins de la xarxa corporativa, la configuració dels equips amb les dades del servidor, etc.

- **Desenvolupament** de totes les funcionalitats especificades al plec per tal de donar cobertura als requeriments així com les adaptacions necessàries per a la **integració** del software amb els sistemes de l'IMI.

- **Servei de manteniment del software de gestió al servidor**: L'adjudicatari serà responsable de l'administració del software al servidor proporcionat per l'IMI pel projecte. Tindrà la responsabilitat de monitoritzar, supervisar el funcionament, etc. fins a 3 mesos després de la primera instal·lació. L'IMI garantirà les còpies de seguretat del disc del servidor d'acord a les polítiques de seguretat pròpies.

- **Lliurament de documentació** associada als equipaments físics i al software de gestió: manuals d'ús, especificacions funcionals i tècniques, manuals d'arquitectura, disseny tècnic i document de seguretat d'acord amb els estàndards de l'IMI. Tota la documentació que es lliuri i es generi durant el projecte, haurà de facilitar-se en castellà/català. En el cas que algunes funcionalitats s'implementin com aplicacions complementàries del software de gestió, la seva documentació haurà de complir la metodologia ADINET de l'IMI**.**

- **Prestació dels serveis de suport durant el procés d'implantació i un cop posada en marxa la solució**. Inclou suport funcional, operatiu i tècnic (presencial i a distància) gestionant les consultes i resolent les incidències i problemes que puguin sortir durant la implantació i una vegada posada en marxa la solució. Es planteja un desplegament gradual a les unitats de manera que aquest suport es contemplarà durant tota la fase de desplegament i fins a 3 mesos després de la primera instal·lació.

3.3 No inclòs a l'abast:

Estan exclosos de l'abast del projecte:

- L'adquisició del **servidor** on s'ubicarà el software de gestió i/o el seu cost de manteniment.
- Tasques de **backup** del servidor
- **Processos de migració** de dades a excepció de les tasques necessàries per utilitzar les funcionalitats de l'IMI de control d'usuaris i autenticació (CTRLUSER i OAM).
- L'anàlisi, construcció i posada en marxa de possibles canvis sobre aplicacions ja existents amb què el nou sistema i funcionalitats s'integrin directament o indirecta. No obstant, sí caldrà realitzar, sota les directrius de l'IMI, la coordinació de la construcció, proves integrades i implantació d'iteracions amb els interlocutors responsables d'aquestes altres aplicacions, com el CTRLUSER i OAM en el control d'usuaris.

4 DESCRIPCIÓ DEL HARDWARE

L'adjudicatari serà responsable del bon funcionament dels subministres, d'acord amb les normes i els requeriments específics del present plec.

Amb caràcter general, hauran de respectar-se les recomanacions i normatives aplicables i relatives als equips i instal·lacions ofertes.

En aquelles matèries no contemplades expressament en les especificacions tècniques i amb caràcter general, hauran de respectar la normativa internacional i nacional existent relativa als mateixos, i si aquesta no existís, la d'exigència comú per administracions públiques.

El licitador en el moment de presentar l'oferta, haurà de disposar dels permisos o qualificacions necessàries per poder comercialitzar i realitzar el subministrament dels productes oferts.

El licitador serà totalment responsable si s'infringeix qualsevol patent, marca registrada o dret de propietat en els subministres o les seves parts.

A continuació es descriuen els requisits que ha de complir el hardware objecte d'aquest contracte.

4.1 Dispositius personals de gravació (DPG)

4.1.1 Característiques tècniques

Les propostes que ofereixin característiques inferiors no seran tingudes en compte en el present procediment d'adjudicació i resultaran excloses de la licitació per no complir amb els requeriments mínims establerts en aquest plec.

Els requisits mínims detallats en aquest apartat no pretenen ser una relació exhaustiva de les característiques tècniques de l'equip. El plec recull les característiques rellevants per a l'objecte de la licitació. Les ofertes dels licitadors hauran de proporcionar les especificacions tècniques complertes dels equips.

Característiques	Descripció
Dimensions	Altura <=100 mm Amplada <= 90 mm Profunditat <= 30 mm
Pes	< 170 g (sense suport ni mòduls extra)
Grau de protecció	IP65 o superior
Botons configurables	Sí
Mute	NO (en cas de tenir, ha de poder inhabilitar-se)
Infraroigs	NO (en cas de tenir, ha de poder inhabilitar-se)
Format de gravació	H.264 o H.265
Capacitat de gravació	Mínim 64 GB
Resolució	1920 x 1080 p; 1280 x 720 p; 640 x 360 p o 640 x 480 Ha de permetre diferents tipus de resolució, configurable
Frames per segon	Entre 25 i 30
Angle de visió	Visió igual al ull humà Horitzontal >= 120º i 140º <=
Estabilitzador d'imatge	Sí

Encriptació de vídeo	AES 256
Bateria	Duració mínima 12 hores de gravació. S'admet que l'activació de funcionalitats extra com el GPS o la wifi pugui disminuir la duració de la bateria, però amb el seu ús no haurà de baixar de les 8 hores de gravació. Bateria integrada a la càmera. La recàrrega total de la bateria no ha de ser superior a 8 hores.
Captura d'àudio	Micròfon dual
Capacitat d'operació a temperatura d'ambient	-20º a +50º
WIFI	Sí, Integrat. Ha de permetre la transmissió dels enregistraments en àrees amb wifi. Els protocols de seguretat que ha d'admetre ha d'estar entre: WPA2-PSK o WPA-PSK.
Bluethooth	SÍ
GPS	SÍ
Pantalla	NO
Carcassa	Robusta, resistent i rugeritzada
Garantia	Mínim 2 anys

4.1.2 Característiques funcionals

- Els dispositius han de tenir un botó o **mecanisme manual per encendre's**. No han d'estar constantment encesos per evitar la descàrrega de les càmeres o la necessitat d'haver d'estar sempre connectades a la base.

- **L'inici i l'aturada de la gravació** ha de realitzar-se mitjançant un botó o mecanisme **manual**. És a dir, el DPG no haurà de començar a gravar en el moment que s'encengui el dispositiu, sinó que, s'haurà de provocar manualment aquesta acció.

- Els dispositius han de tenir un o diversos **indicadors lluminosos** (per exemple, tipus LED) que permetin identificar
    - Que la càmera està encesa o apagada
    - Que la càmera està en mode gravació o no
    - Que indiqui el nivell de bateria del dispositiu per poder actuar en conseqüència

  Es requereix, però, que la lluminositat pugui ser desactivada per actuacions especials (de forma individual o per a un conjunt de dispositius) des d'administració.

- Enregistraments d'**àudio i vídeo**

- **Encriptació** de les dades durant tot el procés: Les dades hauran d'estar encriptades a la pròpia càmera de manera que cap manipulació no en permeti l'extracció ni la modificació. Tampoc s'han de poder visualitzar les imatges enregistrades si no és amb el software específic de desencriptació, el qual ha de poder permetre demostrar que els enregistraments no han estat alterats ni manipulats.

- El dispositiu ha de permetre **etiquetar** els arxius mentre s'estiguin gravant, és a dir, posar una marca o etiqueta en un punt de la gravació que posteriorment permeti la cerca ràpida del moment amb l'etiqueta

- **Pre-gravació** configurable: Els DPG han de poder configurar-se per enregistrar un temps anterior a la sol·licitud de gravació. Es tracta d'una pre-gravació, d'un temps definit, que s'ha d'afegir a

l'enregistrament constituint una única gravació. Es requereix com a mínim disposar d'una pre-gravació de 30 segons.

- Alta **qualitat** de la imatge.

- **Descàrrega automàtica** dels enregistraments: La descàrrega haurà de realitzar-se amb l'auxili del hardware per aquesta funcionalitat, de manera que l'encriptació dels enregistraments quedi assegurada i mantinguda. En cas de precisar d'un hardware específic, aquest podrà presentar-se com a estacions múltiples o individuals. NO es permetrà la descàrrega directa a un PC, les descàrregues es realitzaran totes a un servidor corporatiu de l'IMI. En el cas de necessitat de descàrrega a través de wifi es realitzarà amb les característiques i d'acord a les polítiques de seguretat de l'IMI (wifi corporatiu).

- La **descàrrega** dels enregistraments es realitzarà sempre de manera **completa**, és a dir, si durant el procés el DPG s'extreu de la base de descàrrega (o es tallés la comunicació wifi si s'optés per aquest mitjà de descàrrega), l'enregistrament que estigués a mig del procés, no es descarregaria a mitges, continuaria al dispositiu. La descàrrega sempre haurà de ser completa.

- **Identificació de l'estat del dispositiu** quan està a la base de càrrega i descàrrega: quan el DPG es posicioni a la base, ha de permetre identificar mitjançant indicadors lluminosos l'estat del dispositiu (estats mínims: en càrrega, càrrega total, error) així com el de la descàrrega dels seus enregistraments (estats mínims: descarregant, error).

- Quan es realitzi l'assignació d'un DPG a un usuari (manual o automàticament), ha de permetre identificar mitjançant **indicadors lluminosos**, el dispositiu en qüestió.

- **Sense cables**: Els dispositius han de tenir autonomia pròpia, sense necessitat de dispositius externes o cables que els donin aquesta autonomia.

- Tots els dispositius hauran de disposar, a més del **número de sèrie** corresponents i aquells paràmetres necessaris que permetin la seva identificació, d'un número curt i senzill que permeti a l'usuari la seva ràpida identificació. Tots els DPG's hauran de portar una etiqueta amb aquesta identificació que serà la utilitzada per la gestió d'incidències, entre altres. Si els dispositius ja disposen d'un paràmetre únic que compleix aquestes característiques, podrà utilitzar-se també amb aquesta finalitat.

- Els dispositius han de permetre utilitzar la funció de **GPS** que no ha de suposar afegir un mòdul extra a la càmera (+ pes) ni la necessitat d'afegir una sim al dispositiu. La funcionalitat ha de permetre l'ús de la sim d'un dispositiu extern com a punt d'accés WIFI, per exemple, l'smartphone que utilitza la GUB .

- **NO** ha de permetre **visualitzar** els enregistraments des del propi dispositiu.

- **NO** ha de permetre **eliminar ni modificar** cap enregistrament.

- **NO** ha de permetre **l'enregistrament si el dispositiu no està assignat a un usuari**. És a dir, per a que pugui habilitar-se la gravació, tot dispositiu ha d'estar associat a un usuari, d'aquesta manera s'eviten gravacions fetes per usuaris 'desconeguts'.

- En cas que el dispositiu disposi de l'opció **MUTE**, aquesta **NO** ha de poder ser utilitzada per l'usuari. És a dir, no es permetrà silenciar l'enregistrament. Si el dispositiu disposa d'aquesta opció, caldrà que es pugui inhabilitat des d'administració per a tots els usuaris

4.2 Carregadors i descàrrega dels enregistraments

La descàrrega dels enregistraments i la càrrega dels dispositius es realitzarà a través de **carregadors múltiples** o **individuals**. En el cas dels carregadors múltiples, aquests hauran de tindre un mínim de 6 slots i un màxim de 20. Aquesta limitació està especificada per l'espai de què disposa a les dependències on s'instal·laran els

dispositius. En el cas que el fabricant no disposi de carregadors individuals, el licitador haurà d'especificar la solució proposada per la substitució del material citat per un altre d'equivalent. No s'acceptarà la descàrrega dels enregistraments o càrrega del dispositiu, a través de cable a un PC com a solució individual. S'acceptarà el lliurament de carregadors múltiples en substitució dels carregadors individuals si no es disposen.

Quan un DPG es posicioni al carregador, ha de permetre identificar:

- L'estat de bateria del DPG: amb indicadors lluminosos l'usuari ha de ser capaç de saber com a mínim si una càmera està carregant-se, si ja està carregada o si es produeix algun error.
- L'estat de la descàrrega dels enregistraments: amb indicadors lluminosos l'usuari ha de ser capaç de saber si els enregistraments s'estan descarregant, si ja estan tots descarregats o si es produeix algun error.
- Que està llest per utilitzar, és a dir, que no té enregistraments pendents de descarregar i té bateria.
- Que el dispositiu té algun problema: amb indicadors lluminosos l'usuari ha de ser capaç d'identificar l'estat d'error.

Els mateixos carregadors o dispositius addicionals, han de permetre la descàrrega dels enregistraments a un servidor corporatiu (ubicat a l'IMI). No es permetrà la descàrrega directament a un únic PC. La descàrrega podrà realitzar-se a través de la xarxa corporativa o a través de wifi corporatiu.

A més, amb els mateixos carregadors o dispositius addicionals, s'haurà de permetre l'assignació i des-assignació d'usuaris. Concretament, quan el DPG estigui al carregador ha de permetre l'assignació automàtica de l'usuari mitjançant algun mecanisme (veure 4.4 Mecanismes d'assignació) i l'alliberament automàtic de l'usuari que fins al moment del posicionament a la base el tingués assignat.

Per una altra banda, quan el DPG es posicioni al carregador **NO** ha de permetre:

- Assignar a un nou usuari si encara queden enregistraments pendents de descarregar.
- Gravar nous enregistraments si encara queden enregistraments pendents de descarregar o sense estar assignat a un usuari.

4.3 Suports

Per la subjecció dels DPG existeixen al mercat diferents mecanismes, tots ells adequats en funció de la posició on es col·loqui el dispositiu, de la facilitat de posar i treure. D'acord amb l'experiència de la GUB durant l'etapa de proves de diferents dispositius i en relació amb la facilitat d'ús i la ubicació del dispositiu a la uniformitat, es requereix un sistema de suport del tipus Klick Fast (amb una part femella i una altra mascle) com el següent.

Els DPG han de poder carregar-se i descarregar els enregistraments sense necessitat de treure el mecanisme de subjecció evitant així moltes operacions de posar i treure que facilitarien el trencament dels suports.

Es valorarà la disponibilitat d'altres tipus de subjeccions amb imants resistents, subjeccions que permetin cert moviment del dispositiu (cap a baix per poder visualitzar per sota del pit) o subjeccions per ancorar i portar al vehicle. Veure document "Informe Justificatiu".

4.4 Mecanismes d'assignació / des-assignació

L'assignació/des-assignació dels DPG és un funcionalitat molt important per la correcta gestió dels enregistraments. S'ha de disposar de com a mínim dos mecanismes diferents, sent l'automàtica la preferent.

4.4.1 Assignació

- Manual: L'objectiu d'aquest tipus d'assignació és eventual, pensada per aquelles ocasions en les que no funcioni l'assignació automàtica o no es disposi del mecanisme d'assignació.

  Aquesta assignació es realitzarà a través del software de gestió i per perfils que disposin d'aquesta funcionalitat, veure 5.3 Perfils, jerarquia, privilegis. Durant aquest procés, serà necessari que el DPG estigui depositat a la base de càrrega/descàrrega i no tingui cap enregistrament pendent per descarregar. No serà possible assignar un dispositiu que estigui descarregant. L'aplicació ha de permetre identificar l'estat de la descàrrega, veure 5.2.6 Visualització dispositius. Quan el dispositiu estigui lliure, d'usuari i d'enregistraments, manualment es permetrà associar el DPG amb un usuari que ha d'existir a la jerarquia d'usuaris de l'aplicació, veure 5.3 Perfils, jerarquia, privilegis. No es podrà assignar un dispositiu a un usuari no disponible a la bbdd i/o als sistemes d'autorització de l'IMI . L'assignació quedarà registrada a l'aplicació i visualment l'usuari ha de poder reconèixer el DPG assignat.

- Automàtica: Donat el nombre de dispositius, d'usuaris i de les nombroses tasques que es realitzen a les dependències, l'assignació dels DPG ha de ser tan senzilla, ràpida i automàtica com sigui possible i sense intervenció de terceres persones. Es requereix que els propis usuaris puguin assignar-se un DPG amb la utilització d'un mecanisme d'assignació automàtica, com ara targetes, adhesius individuals, o altres sense que calgui disposar d'un recurs humà que manualment hagi de realitzar una a una les assignacions . Amb aquest sistema es descarrega de la tasca d'assignació a terceres persones.

  Es valorarà la disponibilitat de mecanismes d'assignació biomètrica com ara el reconeixement d'empremta dactilar. Veure document "Informe Justificatiu".

  Per a l'assignació automàtica, de la mateixa manera que succeeix amb la manual, el dispositiu ha d'estar dipositat a la base de càrrega/descàrrega i no pot tenir enregistraments pendents per descarregar. Ha de disposar, per tant, d'una intel·ligència d'assignació de manera que, havent-hi diferents DPG a les bases descarregant, quan es realitzi l'acció d'assignació, ha d'assignar automàticament a l'usuari el DPG lliure i, entre els lliures, aquell que tingui la bateria més carregada, per assegurar major autonomia al dispositiu. De la mateixa manera que en el cas manual, l'assignació ha de quedar registrada a l'aplicació i visualment l'usuari ha de poder reconèixer el DPG assignat.

4.4.2 Des-assignació

La des-assignació haurà de realitzar-se sempre automàticament en el moment en que el DPG es dipositi a la base de càrrega/descàrrega o mitjançant qualsevol altre sistema automàtic. La des-assignació manual només es permetrà en casos puntuals en els que no es disposi de la via automàtica.

Quan un usuari retorni el DPG després del seu ús durant la jornada laboral, el procediment de des-assignació ha de ser transparent, automàtic i eficaç. L'usuari ha de tenir la seguretat que el DPG descarregarà els enregistraments realitzats per ell, en cas que n'hi hagin, i que ningú no podrà fer ús del dispositiu amb la seva assignació, sempre que el dipositi i segueixi els passos indicats. Evidentment, un dispositiu que no es posi a la base de càrrega/descàrrega o en el lloc que correspongui, no es des-assignarà sol.

Es requereix un sistema que permeti una des-assignació autònoma i sense intervenció humana més enllà de la del propi usuari que porta el dispositiu.

En cas que es requereixin aparells o mecanismes externs a banda dels carregadors/descarregadors, aquests estaran inclosos dins de l'abast del plec i seran necessaris tants com el licitador estimi en relació amb la distribució orientativa dels dispositius, veure 3.1.3 Distribució. En el cas concret de la necessària identificació

de cada usuari per l'assignació automàtica es considerarà el 70% de la plantilla de GUB com a usuària potencial (aprox 2100 usuaris).

5 DESCRIPCIÓ DEL SOFTWARE DE GESTIÓ

5.1 Conceptes principals

5.1.1 Enregistraments

S'entén per enregistrament cada gravació generada pel DPG, és a dir, el vídeo i àudio generats des del moment que s'inicia manualment la gravació fins que s'atura també manualment. A més de la seva durada pròpia, s'hi ha d'afegir automàticament la **pre-gravació** establerta. És a dir, la pre-gravació formarà part de l'enregistrament. No s'ha de poder eliminar, ni modificar.

En el cas que el software disposi de l'opció de decidir o no incloure la pre-gravació, s'haurà de poder aplicar amb un criteri general a tots els dispositius (no haver de decidir de manera individual) i només ho podran fer els perfils que es defineixin, de manera que aquesta funcionalitat no estigui disponible per a qualsevol usuari.

La pre-gravació ha d'incloure també el so. Si el software disposa de l'opció d'activar o desactivar el so, aquest haurà de poder aplicar-se com en el cas de la pre-gravació: d'una manera general a tots els dispositius i només pels perfils definits amb aquesta funcionalitat.

En cada enregistrament han de quedar identificades i immodificables com a mínim les següents dades:

- Identificador del DPG que ha realitzat la gravació.
- Identificador de l'usuari que ha realitzat la gravació, és a dir, aquell que consta assignat al dispositiu.
- Data i hora del començament de la gravació (incloent el temps de pre-gravació). El format ha de ser dd/mm/aaaa hh:mm:ss i amb el fus horari d'Espanya-Barcelona, UTC +1. Amb canvi d'horari a l'estiu, l'horari serà UTC +2. En el cas que el software treballi amb formats diferents, serà necessària l'adaptació a aquest format o una presentació que permeti ràpidament la identificació.
- Identificador de l'enregistrament. En el cas que el software doni l'opció de parametritzar el nom de l'enregistrament, aquest haurà d'estar format per les seves dades, com ara: identificador dispositiu + data + hora o similar (per decidir durant la realització del projecte). En tot cas, sempre haurà de ser un identificador senzill i fàcilment identificable com a propi de l'enregistrament. No s'admetran com a identificadors cadenes llargues de números o lletres sense una relació fàcilment identificable amb l'enregistrament.
- Incident al que està associat l'enregistrament, en cas de que s'associï a un. Veure 5.1.2 Incidents .
- Usuaris amb els que l'enregistrament s'ha compartit, en cas de que s'utilitzi aquesta funcionalitat. Veure 5.2.2.3 Compartició.

Els enregistraments poden tenir més dades però TOTES han de ser immodificables, s'ha d'assegurar la inviolabilitat de les dades.

5.1.1.1 Partició

Tot i que les situacions i els supòsits de gravació estan identificats i són concrets, de manera que els enregistraments no haurien de ser, en general, de duració molt llarga, des del punt de vista tècnic podrien ser tan llargs com ho permetés la bateria del dispositiu. Però, descarregar enregistraments molt llargs, fa que aquesta sigui més lenta, per la qual cosa la majoria de softwares fan particions de les gravacions en registres de 15, 30 minuts, 1 hora... . Per posar uns exemples:

- Gravació real de 40 minuts amb software que fa particions de 15 minuts: es descarregaria en tres segments: el primer de 15 minuts, el segon de 15 minuts i el tercer de 10 minuts.
- Gravació real de 40 minuts amb software que fa particions cada hora: aquesta gravació descarregaria com a una única gravació.
- Gravació real de 2 hores amb software que fa particions cada 15 minuts: es descarregaria en 8 segments de 15 minuts cadascun.
- Gravació real de 2 hores amb software que fa particions cada hora: es descarregaria en 2 gravacions de 1 hora cadascuna.

No s'admetran particions inferiors a 15 minuts.

Les particions d'un mateix enregistrament han de ser fàcilment identificables com a part d'una única gravació. A més han de tenir tots els paràmetres iguals excepte l'hora d'inici de cada segment i la seva duració i haurien de poder agrupar-se en entitats "superiors" que englobessin les particions, veure 5.1.2 Incidents.

Quan un enregistrament, que ha estat dividit perquè la seva duració ha estat superior a la partició mínima que realitza el software, s'associa a un incident, totes les particions de l'enregistrament s'associaran, automàticament, al mateix incident. És a dir, en el cas de softwares que facin particions cada 15', per a un enregistrament de 40', quan la primera partició de 15 minuts s'associï a un incident, les altres dues particions, de 15 i 10 minuts, han de quedar automàticament associades al mateix incident que la primera.

5.1.2 Incidents

S'entén per incident el conjunt d'un o més enregistraments. En funció de les característiques i circumstàncies de l'actuació, un incident, podrà estar format per:

- Una única gravació produïda per un DPG o diverses gravacions del mateix DPG (per exemple si l'usuari ha aturat la gravació i més tard l'ha tornada a activar).
- Diverses particions d'un mateix enregistrament produïdes per un DPG

El nom d'incident fa referència al "concepte" d'agrupació d'enregistrament o d'enregistraments, però pot adoptar diferents noms depenent del software de gestió.

5.2 Funcionalitats

5.2.1 Entrada a l'aplicació

Totes les aplicacions corporatives de l'Ajuntament de Barcelona disposen d'un mecanisme comú d'autorització i autenticació: el sistema **Control User** i **l'OAM**, veure7.2.2.1 Autenticació i autorització d'usuaris.. Aquests sistemes són els requerits per totes les noves aplicacions que es desenvolupen i implanten a l'IMI.

Per altra banda, els softwares comercials ja existents disposen dels seus propis mecanismes d'accés i gestió d'usuaris i la majoria disposen de mecanismes d'integració que permeten la utilització dels sistemes d'autenticació dels clients.

Concretament, en aquest projecte, s'accepten tots dos mecanismes: una primera utilització del sistema d'autenticació i accés amb el sistema propi del software de gestió i una posterior adaptació als mecanismes d'accés de l'IMI. Es permet aquesta doble vessant per tal de poder donar cobertura a la planificació del projecte. Veure 11.3 Planificació del projecte.

És important però, que el software disposi dels mecanismes d'integració (APIs) necessaris per poder utilitzar els sistemes d'autenticació de l'IMI. Tot i no desenvolupar-se a l'inici del projecte, ha d'assegurar la possibilitat de fer-ho dins del cost del projecte i dels terminis especificats a la fase II. Si per les característiques del software és possible la integració amb l'IMI des de l'inici, es procedirà d'aquesta manera.

En tots dos casos, s'utilitzi el sistema d'autenticació propi del software o el propi de l'IMI, només podran accedir a l'aplicació els usuaris que estiguin prèviament donats d'alta com a tals a la base de dades. Tots els usuaris hauran de disposar de:

- Usuari i contrasenya (psw): La nomenclatura de l'usuari (tot lletres, lletres i números, el DNI, la matrícula, etc.) es decidirà durant el desenvolupament del projecte tot i que l'aplicació ha de permetre que la nomenclatura de l'usuari pugui ser una dada senzilla de recordar i no llargues combinacions de lletres i números escollides a l'atzar, evitant així problemes d'oblit d'usuaris. Quan existeixi la integració amb els sistemes de l'IMI, l'usuari i el psw seran els utilitzats a la resta d'aplicacions departamentals però, fins llavors, no estaran sincronitzats amb els de la resta d'aplicacions, ni es modificaran automàticament quan aquests canviïn.
- Perfil: L'aplicació ha de permetre la definició de perfils amb l'assignació de diferents funcionalitats. L'assignació posterior d'un usuari al perfil implica que l'usuari podrà realitzar totes les funcionalitats especificades al perfil.

- Grup: Opcionalment es permet la utilització de grups que permetin fraccionar la jerarquia i assignar funcionalitats per grups en comptes de directament als perfils.

L'estructura utilitzada ha de ser fàcilment associada amb l'estructura del sistema CtrlUser de l'IMI per tal de facilitat la migració de dades durant la fase II del projecte, veure 11.3 Planificació del projecte.

5.2.2 Enregistraments

5.2.2.1 Visualització

L'aplicació ha de permetre a l'usuari que hi accedeix, visualitzar els vídeos:

- Propis gravats per l'usuari
- Els compartits amb ell, veure 5.2.2.3 Compartició.
- I els cercats amb el 'Cercador' sobre els que l'usuari tingui permisos de visualització, veure 5.3 Perfils, jerarquia, privilegis i 5.2.2.2 Cerca

Els enregistraments han de poder visualitzar-se com a mínim de les següents maneres:

- Visualització en llista: Ha de mostrar una llista de tots els enregistraments amb com a mínim la següent informació:
  - Data i hora de la gravació: format dd/mm/aaaa hh:mm:ss hora de la península, no horari GMT
  - Duració: format hh: mm: ss
  - Usuari: usuari que ha realitzat la gravació
  - Dispositiu: DPG amb el que s'ha realitzat la gravació
  - Incident : opció d'associar l'enregistrament a un incident ja existent o la possibilitat de crear un incident nou al que quedaria associada la gravació, veure 5.2.3.1 Creació.
  - Detall: opció per poder accedir a l'enregistrament bé directament o bé a través d'una visualització prèvia amb miniatura del primer frame i els detalls de la gravació que permeti accedir a la reproducció.

- Visualització en pantalla de reproducció de cada enregistrament: La mateixa informació que a la visualització de la llista però mostrant el primer frame, en una mida que permeti una visualització còmoda, amb el detall de les seves dades, per una identificació ràpida visual de l'enregistrament. Des d'aquesta visualització també s'ha de poder reproduir l'enregistrament.

5.2.2.2 Cerca

La cerca d'enregistraments ha de poder realitzar-se com a mínim pels següents paràmetres:

- Interval de dates: Ha de permetre la cerca en un interval de dates o especificar una data concreta
- Usuari : Usuari que ha realitzat la gravació
- Dispositiu: DPG amb el que s'ha realitzat la gravació

O permetre la cerca sense especificar cap paràmetre, la qual cosa mostraria tot allò que l'usuari que fa la cerca, té permís per visualitzar. Veure apartat 5.3.2 Perfils, jerarquia, privilegis

El resultat de la cerca serà un llistat amb els enregistraments que compleixin els paràmetres indicats i com a mínim la mateixa informació que es mostra a la consulta d'enregistraments en format llista. Veure 5.2.2.1 Visualització.

5.2.2.3 Compartició

La compartició d'enregistraments suposa el poder visualitzar una gravació per a la que l'usuari no té autorització com a tal (per exemple pel fet de pertànyer jeràrquicament a un altre grup). Prèviament, l'enregistrament ha de ser compartir per un usuari que tingui permisos per compartir. Només es podran

compartir enregistraments amb usuaris donats d'alta a l'aplicació, no amb usuaris externs a l'aplicació. Si el software disposa d'aquesta última funcionalitat, ha de poder anul·lar-se o evitar a través de la configuració.

La manera de compartir serà indicant la identificació d'usuari o escollint-lo d'un llistat. La compartició permetrà visualitzar l'enregistrament a l'usuari amb qui s'ha compartit.

5.2.2.4 Eliminació

Cap usuari podrà eliminar els enregistraments excepte l'usuari superadministrador que, en cas de reclamació ciutadana, per exemple, podrà esborrar un enregistrament sempre que no requereixi emmagatzemar-se per temes judicials.

D'acord amb la LOPD, els enregistraments no podran estar al sistema un temps superior a 30 dies. Només s'hi desaran per un període superior les gravacions vinculades a procediments penals, administratius o quan existeixi un requeriment judicial sobre la necessitat de conservar-les. D'aquesta manera, és necessari que el software disposi d'un mecanisme que permeti identificar quins enregistrament s'han de conservar i quins no. Aquesta selecció podrà realitzar-se de diferents formes: marcant amb check que no s'eliminaran, categoritzant els enregistraments amb una classificació que indiqui que no s'eliminaran, etc. El licitador haurà de deixar constància de com es realitza aquesta operativa.

La funcionalitat ha de permetre que automàticament tots els enregistrament s'eliminin en un temps determinat. Ha de ser parametritzable i ha de permetre indicar com a mínim el valor de 30 dies.

5.2.2.5 Exportació

Es requereix poder exportar els incidents en format MP4 o similar, no directament els enregistraments. L'objectiu de l'exportació és extreure aquells incidents amb un procediment associat. Si tenen un procediment associat, caldrà exportar tot l'incident, no els enregistraments per separat. En el cas que el software permeti l'exportació dels enregistraments per separar, haurà de disposar de l'opció parametritzable per bloquejar la funcionalitat.

El licitador haurà de deixar constància de com es realitza aquesta operativa.

5.2.3 Incidents

En el cas que el software de gestió treballi amb entitats superiors, com els incidents (depenent del software la nominació a aquest terme pot ser diferent) , les seves funcionalitats seran com a mínim les mateixes que en el cas dels enregistraments.

5.2.3.1 Creació

La creació de l'incident es realitzarà manualment i podrà dur-se a terme:

- Directament des dels enregistraments: en el cas de gravacions particionades, en associar-hi una de les particions, automàticament, totes han de quedar associades a l'incident.
- Des de la secció d'Incidents: un cop creat permetrà associar-lo als incidents

Per crear un incident caldrà informar com a mínim les següents dades:

- Nom: títol que permeti identificar a l'incident
- Data i hora: en format dd/mm/aaaa hh:mm
- Descripció: Camp de text que permeti explicar o posar notes
- Codi de referència: codi alfanumèric que permeti informar un mínim de 12 caràcters per indicar el codi de servei d'actuació de la GUB corresponent a l'incident. Veure 5.2.4 Associació amb servei Mycellium

Altres dades s'ompliran automàticament com la data de creació així com l'usuari que el crea.

Per cada incident caldrà omplir l'informe, veure 6.1 Informe de la Direcció General d'Administració de Seguretat (CCDVC). Haurà d'informar-se visualment que cal crear l'informe, bé amb un símbol que indiqui que manca la creació/enviament, bé amb algun color, etc. però fàcilment identificable.

5.2.3.2 Visualització

L'aplicació ha de permetre a l'usuari que accedeix a l'aplicació, visualitzar els incidents:

- Creats per l'usuari
- Els compartits amb ell, veure 5.2.2.3 Compartició.
- I els cercats amb el 'Cercador' sobre els que l'usuari té permisos de visualització, veure 5.3.2 Perfils, jerarquia, privilegis i 5.2.3.3 Cerca

La visualització dels incidents ha de ser com a mínim la mateixa que la dels enregistraments:

- Visualització en llista
- Visualització en pantalla de reproducció

Veure apartat 5.2.2.1 Visualització.

5.2.3.3 Cerca

Ídem que en el cas de la cerca d'enregistraments. Veure apartat 5.2.2.2 Cerca

5.2.3.4 Compartició

Ídem que en el cas de la cerca d'enregistraments. Veure apartat 5.2.2.3 Compartició

5.2.3.5 Eliminació

Ídem que en el cas de l'eliminació d'enregistraments. Veure apartat 5.2.2.4 Eliminació

5.2.3.6 Exportació

S'ha de permetre l'exportació dels incidents. Veure apartat 5.2.2.5 Exportació

5.2.4 Associació amb servei Mycellium

Tots els incidents han de poder associar-se a una actuació policial, a un servei realitzat. Per aquest motiu, l'aplicació ha de permetre informar del codi de servei de l'aplicació Mycellium (aplicació de Gestió d'Emergències) per facilitar-ne la posterior explotació. La introducció serà manual sense cap integració amb l'aplicació Mycellium, però es requereix que el software disposi dels mecanismes d'integració necessaris per, en un futur, poder traspassar dades dels incidents a Mycellium.

Pels enregistraments produïts per error (activació involuntària, ..) es decidirà durant el projecte, la necessitat d'associar-los també a un servei de Mycellium o enregistrar-los en un altre sistema.

5.2.5 Associació de documents

Als incidents es podrà afegir informació, documentació o fotografies que complementin l'incident.

5.2.6 Visualització dispositius

Des del software de gestió i per a perfils específics, veure 5.3 Perfils, jerarquia, privilegis, es podrà veure, monitoritzar i fer el seguiment dels dispositius assignats, el seu estat. etc. Concretament ha de permetre:

- La cerca de dispositius per diferents paràmetres, mínim:
  - DPG: especificant la seva identificació
  - Usuari: usuari al que se li ha assignat el dispositiu
  - Estat: escollint l'estat del dispositiu: En ús, descarregant, assignat...
- Visualització dels dispositius mostrant la informació mínima per cadascun de:

- Identificació del DPG
- Usuari assignat
- Estat del dispositiu
- Estat de la bateria

- Assignar manualment un dispositiu sempre que estigui ancorat a la base i des-assignat (lliure). No s'ha de permetre assignar un dispositiu a un usuari quan aquest està en ús o assignat a un altre usuari.
- Veure la informació tècnica del detall del dispositiu.

5.2.7 Auditoria i informes

El software de gestió ha de disposar d'un mòdul d'auditoria/informes on emmagatzemar les traces d'informació útils per a l'usuari i per als administradors. Concretament:

- Auditoria: ha de poder donar resposta a les següents qüestions podent seleccionant l'interval de temps que es vulgui consultar :
  - A quin usuari se li ha assignat un DPG, quin i quan
  - Quines són totes les accions realitzades sobre un DPG: en quin moment se li ha assignat i a qui, en quin moment s'ha tret de la base de descàrrega, en quin moment s'ha tornat a posar a la base de descàrrega, quan de temps ha trigat en descarregar,...
  - Quines i quantes assignacions s'han fet en un dia...
  - ....

  És a dir, per tot enregistrament, dispositiu,.. és necessari guardar la seva informació, totes les accions que es realitzen sobre ell, el seu cicle de vida i poder explotar aquesta informació visualment. També s'ha de permetre l'exportació a través de fitxers.
- Informes: Ha de disposar d'un mòdul per dissenyar informes i programar la seva periodicitat. Els informes han de poder donar respostes a qüestions com les següents:
  - Quants dispositius i a quins usuaris s'han assignat durant un dia/mes...
  - Quantes descàrregues i de quina duració s'han produït en un dia/mes...
  - A quins usuaris s'ha assignat durant un mes el dispositiu X
  - Quins passos ha seguit l'incident X?
  - ....

  És a dir, s'ha de poder crear un informe i programar-lo per la seva execució (diària, setmanal, mensual, etc.) o tornar a executar-lo de nou un cop ja executat; poder cercar informació i obtenir un informe de la informació cercada etc. S'ha de permetre l'exportació de la informació, mínim en format word o txt.

Aquests mòduls només seran accessibles per determinats perfils. Veure 5.3 Perfils, jerarquia, privilegis.

5.2.8 Estadístiques

El software de gestió ha de disposar d'un mòdul d'estadístiques on visualment es proporcioni informació útil de l'ús del software. La informació mínima a mostrar serà:

- La situació del parc de dispositius: en quin estat estan (si s'estan utilitzant, si estan descarregant, etc.)
- El volum d'enregistraments emmagatzemats al servidor
- Nombre d'enregistraments/incidents fets al llarg del dia, setmana, etc.

La informació es mostrarà d'una manera senzilla i clara amb preferència pels diagrames de barres o diagrames de sectors.

5.2.9 Administració

El software de gestió ha de disposar d'un mòdul d'administració que ha de permetre, i d'acord sempre als perfils, veure 5.3 Perfils, jerarquia, privilegis, la introducció de dades, la consulta d'informació, l'administració de paràmetres de l'aplicació, etc. Com a mínim contemplarà els següents aspectes:

- Gestió usuaris i perfils: Durant l'inici i fins la finalització de la fase II del projecte, s'utilitzaran els sistemes d'autenticació/autorització del propi software, posteriorment, s'utilitzaran els sistemes de l'IMI, veure 7.2.2.1 Autenticació i autorització d'usuaris.

  Es permetrà com a mínim:
  - Alta, modificació i baixa d'usuaris: aquestes accions podran realitzar-se manualment però es recomanarà l'ús de la càrrega automàtica per garantir la correcta inclusió/modificació de l'usuari dins la jerarquia , veure 5.3 Perfils, jerarquia, privilegis.
  - Alta, modificació i baixa de perfils i funcionalitats: L'alta o modificació d'un perfil ha de ser una tasca molt senzilla. El funcionament ha de ser similar a la gestió de perfils que actualment es realitza amb l'aplicació Control User de l'IMI, veure 7.2.2.1 Autenticació i autorització d'usuaris i que passarà a utilitzar-se a fase II. L'aplicació ha de mostrar les funcionalitats que permet el software de gestió i, d'una manera fàcil i intuïtiva, ha de permetre activar o desactivar les funcionalitats pel perfil seleccionat. L'afectació serà per tots els usuaris que tinguin el perfil. En cas que algun usuari en concret d'un mateix perfil que un altre, requereixi alguna funcionalitat diferent, caldrà crear un perfil nou. La modificació d'un perfil ha de funcionar de la mateixa manera que l'alta d'un perfil nou, activant i desactivant (o associant i des-associant) funcionalitats. L'eliminació d'un perfil només es podrà realitzar si no hi ha cap usuari associat a ell, en cas contrari, caldrà primer associar a un altre perfil els usuaris amb el perfil que es vol eliminar.

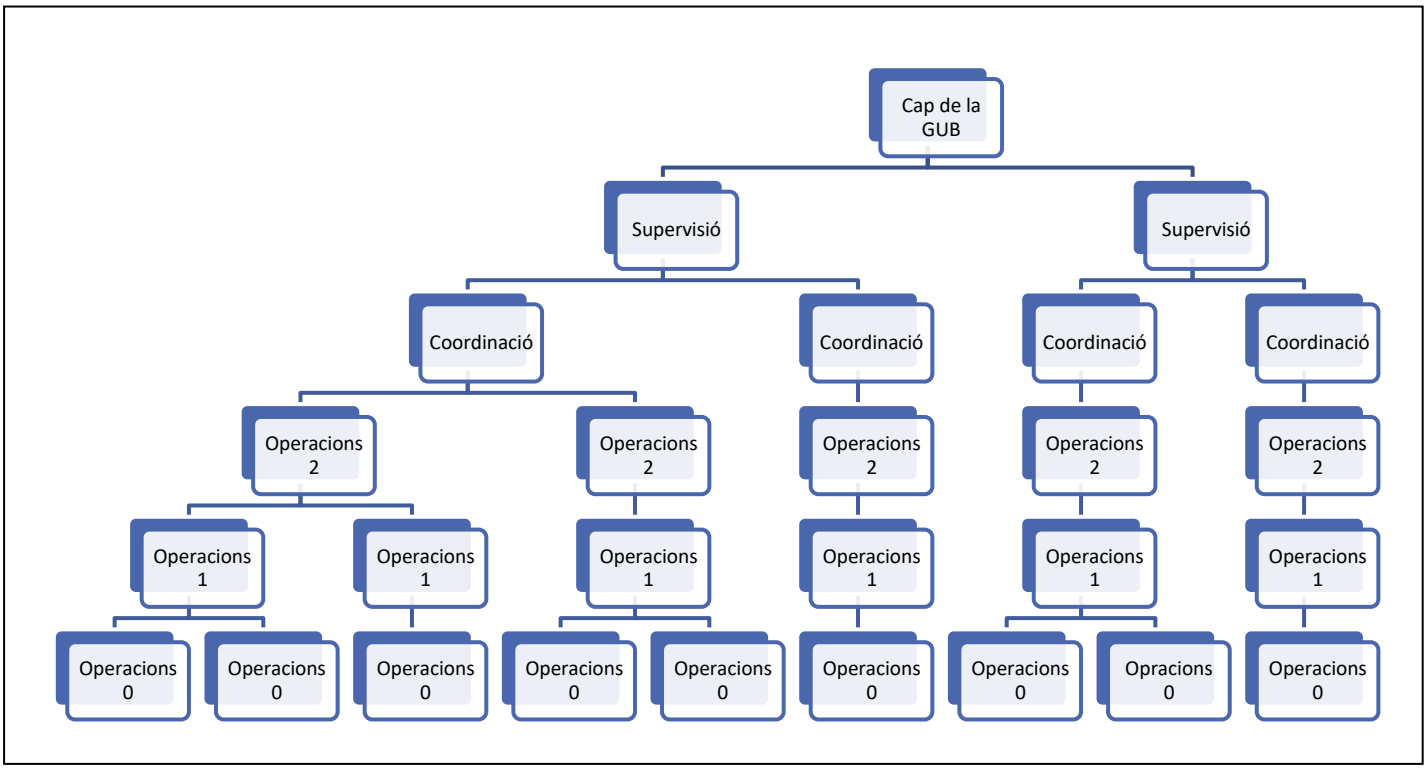
- Gestió de dispositius: Ha de permetre parametritzar les característiques dels dispositius d'una forma general, és a dir per model o tipus, no de manera individual cada dispositiu. Es permetrà modificar diferents aspectes amb la possibilitat de decidir si utilitzar-los o no, sempre que els dispositius els tinguin disponibles. S'aplicaran al conjunt de dispositius.
  - Activació i desactivació de sons
  - Activació i desactivació de parpellejos lluminosos dels indicadors
  - Activar i desactivació de la pregravació i especificació del temps de pregravació: es requereix que hi hagi sempre pregravació però, en el cas que el software disposi de l'opció, ha de poder activar-se pel conjunt de dispositius i des de el software de gestió, no manualment des del dispositiu. La pregravació inicial requerida és de 30" però ha de permetre una finestra de 30" a 2 minuts mínim.
  - Modificar els ajustaments de vídeo: ha de poder especificar-s'hi la qualitat de gravació de l'enregistrament, amb dues opcions com a mínim, una resolució 'Full HD' i una 'Estàndard'. També han de poder especificar-s'hi els fotogrames per segon, amb una finestra mínima de 25 a 30 fotogrames

Totes les accions que es realitzin des d'aquest mòdul, de la mateixa manera que passa amb tots els altres, quedaran registrades a l'auditoria.

5.3 Perfils, jerarquia, privilegis

L'aplicació de software ha de permetre treballar amb una classificació, jerarquia i perfils d'estructura piramidal de manera que els perfils superiors puguin visualitzar els enregistraments dels perfils inferiors.

A continuació mostrem un exemple de jerarquia aplicable d'acord l'estructura i organització de la GUB.



La incorporació de qualsevol usuari a utilitzar un DPG o el software de gestió, ha de situar-se dins de la jerarquia i en funció del perfil podrà enregistrar, visualitzar i/o supervisar els enregistraments, etc.

Es definirà un mínim de 8 perfils, tot i que, durant el projecte és determinarà la jerarquia de perfils i les funcionalitats associades a cadascun d'ells, seguint la filosofia següent:

Perfils	Privilegis / funcionalitats
SUPERVISOR	GENERAL: • ASSIGNAR: un DPG a qualsevol persona usuària de la unitat en la que es trobin adscrits • GRAVAR: amb qualsevol DPG que els sigui assignat • VEURE: les gravacions de qualsevol nivell i de qualsevol unitat • VEURE: L'estat del parc de dispositius • EXPORTAR: les gravacions de qualsevol nivell i de qualsevol unitat a un arxiu informàtic • BLOQUEJAR: les gravacions de qualsevol nivell i de qualsevol unitat per tal que no s'esborrin passats els 30 dies • INFORME CCDVC: Redacció i enviament de l'informe a la CCDVC UNITATS OPERATIVES: el perfil de supervisió GENERAL podria tenir restriccions en funció del territori i de l'organització (Caps d'Unitat, Caps de Divisió, etc.).
COORDINADOR	• ASSIGNAR: un DPG a qualsevol persona usuària de la unitat en la que es trobin adscrits • GRAVAR: amb qualsevol DPG que els sigui assignat • VEURE: les gravacions de qualsevol nivell de la unitat en la que es trobin adscrits • VEURE: L'estat del parc de dispositius • EXPORTAR: les gravacions de qualsevol nivell de la unitat en la que es trobin adscrits • BLOQUEJAR: les gravacions de qualsevol nivell de la unitat en la que es trobin adscrits per tal que no s'esborrin passats els 30 dies.

	• INFORME CCDVC: Creació i enviament de l'informe a la CCDVC
OPERACIONS 2	• ASSIGNAR: un DPG a qualsevol persona usuària de la unitat en la que es trobin adscrits • GRAVAR: amb qualsevol DPG que els sigui assignat • VEURE: les gravacions pròpies i les dels nivells inferiors (OPERACIONS 1 i OPERACIONS 0) de la unitat en la que es trobin adscrits • VEURE: L'estat del parc de dispositius • INFORME CCDVC: Creació i enviament de l'informe a la CCDVC
OPERACIONS 1	• ASSIGNAR: un DPG a qualsevol persona usuària de la unitat en la que es trobin adscrits • GRAVAR: amb qualsevol DPG que els sigui assignat • VEURE: les gravacions pròpies i les del nivell inferior (OPERACIONS 0) de la unitat en la que es trobin adscrits • VEURE: L'estat del parc de dispositius • INFORME CCDVC: Creació i enviament de l'informe a la CCDVC
OPERACIONS 0	• GRAVAR: amb qualsevol DPG que els sigui assignat
MANTENIMENT	• ASSIGNAR: un DPG a qualsevol persona usuària de la unitat en la que es trobin adscrits • VEURE: L'estat del parc de dispositius
USTO	• Accés a TOTES les funcionalitats del software de gestió incloses les de INFORMES, AUDITORIES, INDICADORS, etc. • Accés a algunes funcions d'ADMINISTRACIÓ • Gestió de la bústia de correus dels informes a la CCDVC • Càrrega d'usuaris
ADMINISTRADOR	• Accés a TOTES les funcionalitats del software de gestió incloses les de INFORMES, AUDITORIES, INDICADORS, etc. • Accés a totes les funcions d'ADMINISTRACIÓ Es podran crear diferents nivells d'administrador limitant les funcionalitats

La modificació dels perfils i les seves funcionalitats associades es realitzarà des del mòdul d'administració, veure 5.2.9 Administració

5.4 Comportaments específics

A continuació s'especifiquen algunes qüestions que, tot i estar descrites al llarg del document, és considera necessari tornar a remarcar-les:

Què succeeix quan un DPG que està a la base de càrrega, està descarregant enregistraments i s'assigna a un altre usuari?	No s'ha de permetre. Mentre un DPG tingui enregistraments per descarregar NO es podrà assignar a cap altre usuari.
Es podrà modificar l'usuari que estigui assignat a una càmera mentre estigui fora de la base de càrrega?	No s'ha de permetre. És a dir, si el DPG no està a la base, i per tant, lliure d'usuari, NO es podrà assignar a un altre usuari. Si es permetés, els enregistraments fets per un usuari quedarien en nom del nou usuari que s'assigni, provocant una irregularitat.
Es podrà enregistrar amb un DPG sense usuari assignat?	No s'ha de permetre. Tot DPG que pugui enregistrar ha de tenir un usuari assignat. En cas contrari es generarien enregistraments sense usuari assignat provocant una irregularitat.
Es podrà alliberar un DPG d'usuari sense que el DPG estigui a la base de càrrega?	No s'ha de permetre. Tot DPG s'alliberarà automàticament quan es posicioni a la base de descàrrega. Permetre fer-ho en remot quan el DPG no estigués a la base, podria provocar que un DPG en actiu es des-assignés quan un usuari realment l'estigués utilitzant provocant una irregularitat.
Es podrà assignar un mateix usuari a dos DPG diferents?	No, el sistema ha de ser capaç de detectar que un usuari ja té assignat un DPG i per tant no es podrà tornar a assignar fins que quedi alliberat. És a dir, un mateix usuari només podrà tenir assignat un DPG.

Es podrà assignar un DPG a qualsevol usuari?	No, només es podran assignar als usuaris donats d'alta al software de gestió/CtrlUser o sistema d'autenticació i autorització corresponent.
Tots els usuaris podran accedir al software de gestió?	No, només aquells d'acord al perfil que tinguin assignats.
Es podrà activar el DPG quan es faci servir un dispositiu de control d'energia?	Es valorarà al document "Informe Justificatiu" que el DPG pugui activar la gravació (prèviament ha d'estar encès) en resposta a un estímul com podria ser desenfundar la pistola o el dispositiu conductor d'energia. El hardware que es requereixi per portar-ho a terme (sensors,..) no estan inclosos dins l'abast del projecte, però sí la capacitat de poder fer-ho.
En el cas de pèrdua d'un DPG, què passarà amb els enregistraments fets però no descarregats?	Els enregistraments gravats pels DPG només podran descarregar-se amb el hardware específic i només podran visualitzar-se amb el software de gestió associat. En el cas de pèrdua d'un DPG els enregistraments no es podran recuperar però cap persona podrà veure'ls. Obrir el dispositiu ha de suposar la destrucció total dels enregistraments.

6 ALTRES FUNCIONALITATS

6.1 Informe a la Comissió de Control dels Dispositius de Videovigilància de Catalunya (CCDVC)

La Comissió de Control dels Dispositius de Videovigilància de Catalunya (CCDVC) és l'òrgan consultiu i de control de la utilització dels DPG, amb la finalitat de vetllar per la garantia del dret a la privacitat, a la intimitat i a la pròpia imatge de la ciutadania. Ha de ser informada de tots els enregistraments que es realitzin amb DPG per assegurar que el seu ús compleix els criteris d'utilització d'aquest tipus de dispositius: es podran utilitzar en situacions relacionades amb la prevenció de la seguretat ciutadana i quan es produeixin o es donin circumstancies d'un risc concret per a la seguretat pública.

La manera d'informar a la CCDVC és a través de l'enviament d'un document complimentat per a cada enregistrament on s'especifiquen dades concretes com les pròpies del dispositiu, de l'usuari que ha fet l'enregistrament, del propi enregistrament, la situació per la que ha estat necessari utilitzar el dispositiu, etc.

Donat l'alt nombre de dispositius que s'adquireixen en aquest plec, es preveu també un alt nombre d'enregistraments i per tant la necessitat de gestionar nombrosos informes. Per aquest motiu es requereix el desenvolupament d'una nova funcionalitat, especifica per la GUB, que permeti la creació automàtica de l'informe, la seva complementació (en tot allò que sigui possible) i el seu enviament per correu electrònic.

Aquesta nova funcionalitat podrà desenvolupar-se com a funcionalitat dins del mateix software de gestió o com nova aplicació que interactua/es relaciona amb el software de gestió. En el cas del desenvolupament d'una nova aplicació, aquesta haurà de dissenyar-se i construir-se d'acord als estàndards i requeriments dels desenvolupaments de l'IMI, veure 7. Requisits tècnics.

El desenvolupament d'aquesta funcionalitat es portarà a terme durant la Fase II del projecte, veure 11.3 Planificació del projecte de manera que durant la Fase I, l'informe s'omplirà i enviarà manualment. La seva gestió serà a càrrec de la GUB. Implementada la funcionalitat automàtica, serà necessari una adaptació/migració de dades per a que tots els informes CCDVC estiguin al mateix repositori, independentment de en quina fase s'han realitzat i enviat.

6.1.1 Creació

La creació de l'informe ha de contemplar els següents aspectes:

- Per cada incident (compost d'un enregistrament o més d'un) serà necessari completar un comunicat d'ús del DPG per informar la CCDVC. Aquest informe s'ha de completar sempre, independentment del motiu origen de la gravació. És a dir, tant si la gravació ha estat produïda per un error, si es tracta d'una gravació que no té conseqüències penals i que s'eliminarà als 30 dies o si és una gravació que caldrà desar, el document s'ha de generar i enviar.

- En el cas de modificació d'alguna dada de l'incident (o dels enregistraments que contingui) una vegada ja creat l'informe i enviat, caldrà tornar a redactar-lo o modificar-lo i enviar-lo novament.

- L'informe es mostrarà per pantalla com un formulari. Les dades que l'aplicació ja conegui i siguin pròpies de l'incident (dispositiu que va gravar l'enregistrament, usuari que portava el dispositiu, data i hora de creació, etc.) es mostraran complementades i sense possibilitat de modificació . Altres com la justificació que va motivar la gravació, caldrà omplir-les manualment.

- Les signatures de l'informe es realitzaran manualment imprimint el formulari. Un cop el formulari estigui correctament signat es pujarà manualment a l'aplicació en format pdf i s'enviarà des de l'aplicació.

- L'informe, un cop finalitzat, es guardarà i enviarà en format pdf. Es guardarà al mateix servidor on s'ubicarà el software de gestió (servidor proporcionat per l'IMI) o a la bbdd de l'aplicació de software

de gestió en el cas que s'opti per implementar la funcionalitat en el mateix software i resulti més adient.

- El nom de l'informe es crearà automàticament. Estarà format com a mínim i a determinar durant el desenvolupament de la funcionalitat, per l'identificador de l'incident i la versió.

- Com a una característica dels incidents, es mostrarà a la pantalla del software de gestió el símbol de l'existència de l'informe de manera que sigui fàcilment identificable que hi ha un informe creat i enviat a la CCDVC (és recomanable l'existència de símbols diferents per identificar quan l'informe està creat però no enviat i quan ja està enviat). En el cas que la nova funcionalitat s'implementi dins del software de gestió, haurà de permetre accedir a l'informe des de les dades de l'incident i visualitzar-lo.

- Es requerirà que si transcorregudes 48 hores no s'ha realitzat el l'informe ni transcorregudes 72 s'ha enviat (temps que s'ha de determinar durant el desenvolupament del projecte), s'informi l'usuari a mode d'alerta. En el cas que la funcionalitat es desenvolupi en el mateix software de gestió, podrà informar-se a la pantalla d'incidents. En el cas de desenvolupar-la en una aplicació independent, pot informar-se a una pantalla inicial en el que mostri els informes pendents de fer i/o enviar.

- El detall dels informes, els símbols o opcions de creació i enviament, només es mostraran per aquells perfils que n'hagin de fer ús i només pels incidents que puguin visualitzar. Veure 5.3 Perfils, jerarquia, privilegis.

6.1.2 Flux d'estats

Caldrà un sistema de flux d'estats per conèixer l'estat de l'informe. Així, com a mínim, encara que pendent d'especificació durant la fase de desenvolupament de la funcionalitat, serà necessari disposar dels següents estats:

- Creat: Estat automàtic que s'assigna en el moment que es crea un incident/enregistrament donat que per tot enregistrament cal informar a la CCDVC.
- Completat: Estat automàtic que s'assigna quan s'omplen manualment les dades pendent de l'informe (aquelles que no es poden completar automàticament) i es desa.
- Imprès: Estat automàtic que s'assigna un cop se selecciona l'opció 'Imprimir'.
- Carregat: Estat automàtic que s'assigna un cop se selecciona l'opció 'Carregat' i es carrega a l'aplicació l'informe. L'aplicació comprovarà que l'informe carregat no té contingut nul, que la mida és superior a la descarregada i que el nom del fitxer és el mateix que el descarregat. Tot i així a la base de dades es guardarà amb un nom diferent per diferenciar la versió sense signar de la signada.
- Enviat: Estat automàtic que s'assigna un cop es selecciona l'opció 'Enviar' i s'envia via correu l'informe. En cas que donés error l'enviament, no es canviaria d'estat
- Revisat: Estat final automàtic que s'assigna un cop es selecciona l'opció 'Revisat'. Aquesta revisió la realitzarà la prefectura de la unitat.

Tots ells han de quedar auditats. Totes les accions que es realitzin sobre un informe han de quedar registrades de manera que es pugui conèixer en quin moment i qui va crear un informe, quan i qui el va imprimir, quan i qui el va carregar, etc. i poder crear alertes.

Ha de contemplar-se que tot i que en la majoria de casos només hi haurà un informe per incident, poden haver-hi més d'un pels casos en els que sigui necessari la modificació de l'informe. De la mateixa manera, es podrà tornar en alguns casos a estats anteriors.

6.1.3 Enviament

La creació de l'informe ha de contemplar els següents aspectes:

- L'enviament es realitzarà per cada enregistrament, incloent tots els segments en els que s'hagi pogut particionar.

- En el cas que enviat l'informe, es realitzi una modificació sobre l'informe, per exemple, s'afegeixi més informació, serà necessari crear-lo novament, imprimir-lo, guardar-lo i tornar a enviar-lo novament, indicant automàticament en l'enviament que es tracta de la modificació d'un informe ja enviat (indicant referències).

- L'informe s'enviarà en format pdf i es guardarà, al servidor o a la bbdd de l'aplicació del software de gestió amb la data de l'enviament i l'usuari que el va enviar. En el cas que l'informe s'implementi a la mateixa aplicació de software, les operacions que es realitzin quedaran registrades a l'auditoria, com qualsevol altre operació del software.

- L'enviament es realitzarà des d'una adreça que l'IMI facilitarà pel projecte (una bústia comuna) a la que tindran accés els usuaris d'acord al seu perfil, veure 5.3 Perfils, jerarquia, privilegis. Com a destinatari de l'enviament es proporcionarà l'adreça de la CCDVC. Durant el desenvolupament del projecte es determinarà si la comunicació serà únicament unidireccional (enviament de l'informe sense possibilitat de rebre a través de la bústia correus de la CCDVC) o bidireccional de manera que la CCDVC pugui respondre amb comentaris, sol·licitud d'aclariments, etc. . En l'últim cas, s'habilitarà el compte de correu per tal que pugui rebre missatges que gestionaran els perfils que tinguin aquesta funcionalitat.

- Missatge:
  - Títol: Durant l'execució del projecte es facilitarà una descripció comuna per als missatges, sent probable que a més d'un text fix, s'hi incorpori una part variable com podria ser el numero d'incident, un codi específic de GUB, etc.
  - Contingut: ídem que el camp anterior amb l'afegit d'incorporar l'informe generat amb pdf

6.1.4 Pantalles de l'aplicació

És important considerar que en el cas que es desenvolupi una aplicació independent (en comptes de com a funcionalitat inclosa dins del software de gestió) caldrà implementar les pantalles bàsiques de qualsevol aplicació:

- Pantalla de login i autenticació d'usuaris. Veure 7.2.2.1 Autenticació i autorització d'usuaris. En el cas que la funcionalitat es desenvolupi en el mateix software de gestió, no serà necessari aquesta pantalla donat que ha estat necessari que l'usuari s'identifiqui per entrar a l'aplicació.

- Pantalla de cerca d'incidents: Ha de permetre la cerca d'incidents amb els paràmetres que s'especifiquen a 5.2.3.3 Cerca. A més, ha de permetre cercar per aquells pendents de crear i /o enviar l'informe i mostrar el llistat amb els incidents que compleixin els criteris. No ha de mostrar els enregistraments, només les dades bàsiques (identificador de l'incident, descripció de l'incident, identificador dels enregistraments que conté, dates i hores, usuari/s que van intervenir-hi...).

- Ha de permetre seleccionar un incident i crear des d'allà l'informe mostrant la pantalla del formulari amb les dades ja omplertes de l'incident seleccionat.

- També ha de ser possible crear un informe directament des de l'opció 'Crear Informe' mostrant el formulari buit. Llavors caldrà especificar un número d'incident i cercar-lo. Al trobar-lo s'omplirien les dades de l'incident. En aquest cas la identificació del número de l'incident ha de ser exacte, si no és així, no trobarà resultats i indicarà que no hi ha dades.

- Un cop omplert el formulari es disposarà de l'opció d' "Imprimir". Aquesta opció converteix el formulari en un pdf que l'usuari es descarregarà i imprimirà. Un cop es cliqui sobre l'opció, s'habilitarà una nova opció 'Carregar' que permetrà la càrrega del document. L'opció "Imprimir" continuarà vigent

per donar la possibilitat de tornar a imprimir. Un cop carregat el document ja no es podrà tornar a imprimir tot i que es podrà consultar el document carregat.

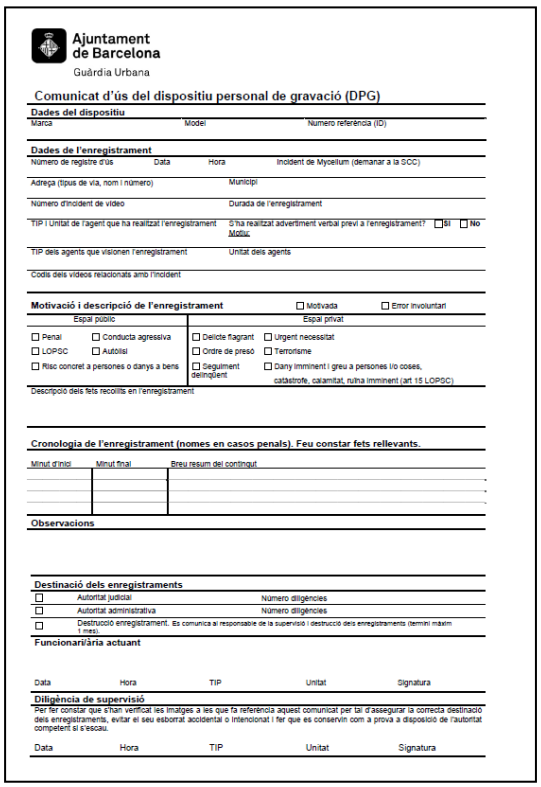
- El document imprès serà signat manualment per les persones encarregades. Completades les signatures, el document tornarà a carregar-se a l'aplicació.

- Carregat el document, que haurà de conservar el mateix nom amb el que es va descarregar, apareixerà l'opció de "enviar". La selecció d'aquesta opció produirà l'enviament a l'adreça establerta. El formulari passarà a estat 'enviat'. En el cas que la funcionalitat s'hagi implementat en una aplicació independent del software de gestió, caldrà informar al software de gestió per tal que ho reflecteixi a la seva pantalla d'incidents. Caldrà establir la comunicació entre el software de gestió i la nova aplicació d'acord amb els mecanismes de què disposi el software de gestió (API..) i amb els mecanismes que especifiqui l'IMI per les noves aplicacions.

- Un cop enviat, l'informe quedarà pendent de la revisió per la prefectura de la unitat. Aquesta revisió consistirà principalment en verificar
  - Que les imatges s'esborraran passats 30 dies si no són prova en cap procediment
  - Que les imatges s'han desat correctament si són prova en un procediment
  - Que s'ha corregit la primera opció escollida per l'agent i el comandament, si és incorrecta

6.1.5 Dades de l'informe

El comunicat que es generarà i s'enviarà ha de tenir el següent aspecte i contingut, tot i que és probable que durant el transcurs del projecte es decideixi incorporar alguna informació o dada extra, sempre disponible dins l'aplicació o que s'hagi d'introduir manualment per l'usuari.



Ajuntament de Barcelona
Guàrdia Urbana

Comunicat d'ús del dispositiu personal de gravació (DPG)

Dades del dispositiu
Marca | Model | Numero referència (ID)

Dades de l'enregistrament
Número de registre d'ús | Data | Hora | Incident de Mycellum (demanar a la SCC)
Adreça (tipus de via, nom i número) | Municipi
Número d'incident de vídeo | Durada de l'enregistrament
TIP i Unitat de l'agent que ha realitzat l'enregistrament | S'ha realitzat advertiment verbal previ a l'enregistrament? ☐ Sí ☐ No
Motiu:
TIP dels agents que visionen l'enregistrament | Unitat dels agents
Codis dels vídeos relacionats amb l'incident

Motivació i descripció de l'enregistrament ☐ Motivada ☐ Error involuntari

Espai públic		Espai privat	
☐ Penal	☐ Conducta agressiva	☐ Delicte flagrant	☐ Urgent necessitat
☐ LOPSC	☐ Autòlisi	☐ Ordre de presó	☐ Terrorisme
☐ Risc concret a persones o danys a bens		☐ Seguiment delinqüent	☐ Dany imminent i greu a persones i/o coses, catàstrofe, calamitat, ruïna imminent (art 15 LOPSC)

Descripció dels fets recollits en l'enregistrament

Cronologia de l'enregistrament (només en casos penals). Feu constar fets rellevants.
Minut d'inici | Minut final | Breu resum del contingut

Observacions

Destinació dels enregistraments
☐ Autoritat judicial — Número diligències
☐ Autoritat administrativa — Número diligències
☐ Destrucció enregistrament. Es comunica al responsable de la supervisió i destrucció dels enregistraments (termini màxim 1 mes).

Funcionari/ària actuant
Data | Hora | TIP | Unitat | Signatura

Diligència de supervisió
Per fer constar que s'han verificat les imatges a les que fa referència aquest comunicat per tal d'assegurar la correcta destinació dels enregistraments, evitar el seu esborrat accidental o intencionat i fer que es conservin com a prova a disposició de l'autoritat competent si s'escau.
Data | Hora | TIP | Unitat | Signatura

L'informe es presentarà per pantalla en format formulari amb camps per omplir o per seleccionar valors de desplegables o check box clicables. Concretament inclourà com a mínim la següent informació:

Dades del dispositiu	
Marca i model	Sempre seran iguals per tots els enregistraments i correspondran a la informació pròpia del DPG. S'ompliran automàticament
Identificador	Identificador unívoc que identifica a cada dispositiu i que com a marca d'aigua forma part de les dades de cada enregistrament. S'omplirà automàticament

Dades de l'enregistrament	
Núm. de registre d'ús	Identificador de l'enregistrament. S'omplirà automàticament
Data i hora	Data i hora de l'inici de l'enregistrament, incloent la pre-gravació. S'omplirà automàticament.
Incident Mycellium	Codi de servei Mycellium associat a l'actuació. Veure 5.2.4 Associació amb servei Mycellium
Adreça i Municipi	Adreça i municipi on s'ha iniciat la gravació. Les dades s'introduiran manualment però es requereix poder utilitzar les funcions de geocodificació de l'IMI durant la fase II del projecte. En el cas que es decideixi utilitzar la funció de GPS dels DPG i es disposi de les coordenades, aquestes seran utilitzades pel càlcul de la informació amb la posterior geocodificació amb les funcions de l'IMI.
Núm. incident de vídeo	Identificador de l'enregistrament principal. S'omplirà automàticament. En el cas d'un enregistrament particionat, els números de la resta de particions s'ompliran al camp 'Codis dels vídeos relacionats amb l'incident'
Durada de l'enregistrament	Durada en format d'hores, minuts i segons de l'enregistrament. En el cas d'enregistraments particionats serà el temps total de la gravació. S'omplirà automàticament.
TIPS i unitat de l'agent que ha realitzat l'enregistrament:	Identificador de l'usuari associat al DPG que ha realitzat la gravació, que coincidirà amb el seu TIP, i unitat a la que pertany. S'omplirà automàticament.
S'ha realitzat advertiment verbal previ a l'enregistrament	Indicador de 'SÍ' ó 'NO' a omplir manualment. Camp obligatori. Per defecte es mostrarà el valor 'SÍ'.
TIPs dels agents que visualitzen l'enregistrament i unitats	Manualment s'informaran els usuaris de les persones que a més de l'autor de l'enregistrament, han visualitzat amb ell, la gravació. Camp predictiu on a mesura que es teclegin els números, mostri els possibles usuaris que compleixen el patró. D'aquesta manera l'aplicació assegura que no s'especifiquin usuaris que no estan donats d'alta a l'aplicació.
Codis dels vídeos relacionats amb l'incident	Automàticament es mostraran tots els enregistraments que formin part de l'incident i no es podran eliminar.

Motivació i descripció de l'enregistrament	
Motiu	A escollir obligatòriament una de les opcions 'Motivada' o 'Error involuntari'
Espai públic	En el cas que el motiu sigui 'Motivada' llavors caldrà escollir entre els valors: 'Penal', 'LOPSC', 'Conducta agressiva', 'Autòlisi' o 'Risc concret dels fets recollits en l'enregistrament'
Espai privat en certs supòsits recollits en els protocols i procediments interns de la GUB	En el cas que el motiu sigui 'Motivada' llavors caldrà escollir entre els valors: Delicte flagrant', 'Ordre de presó', 'Seguiment delinqüent', 'Urgent necessitat', 'Terrorisme' o 'Dany imminent i greu a persones i/o coses, catàstrofe, calamitat, ruïna imminent (art 15 LOSPC)'. Serà

	necessari seleccionar una opció del camp 'Espai Públic' o 'Espai privat'.
Descripció dels fets	Camp lliure de mínim 300 caràcters per descriure el detall dels fets.

Cronologia de l'enregistrament (només en casos penals)	
Minut d'inici i final	Camp a omplir manualment informant el minut d'inici i fi de l'interès de la gravació. L'aplicació comprovarà que existeixi els minuts indicats. Format mm:ss
Breu resum del contingut	Camp lliure de mínim 150 caràcters per descriure el detall dels fets.

Observacions	
Observacions	Camp lliure de mínim 300 caràcters per afegir informació

Destinació dels enregistraments	
Destinació	Camp per informar la destinació de l'enregistrament. A escollir entre els valors: 'Autoritat judicial', 'Autoritat administrativa' o 'Destrucció enregistrament'. En el cas de les dues primeres opcions caldrà informar manualment del número de diligències.

Funcionari/ària actuant	
Data/hora	Informació a omplir automàticament amb la data i hora del dia en el que s'està omplint el formulari.
TIP	Informació automàtica amb les dades de la persona que ha generat l'enregistrament, no qui ha creat l'incident, que seran en la majoria dels casos persones diferents.
Unitat	Informació a omplir automàticament amb el grup al que pertany l'usuari que ha generat l'enregistrament.
Signatura	S'omplirà **manualment** quan s'imprimeixi el document.

Diligència de supervisió	
Data/hora	Informació a omplir automàticament amb la data i hora del dia en el que s'està omplint el formulari.
TIP	Informació manual amb les dades de la persona que ha supervisar l'enregistrament, no qui ha creat l'incident, que seran en la majoria dels casos persones diferents.
Unitat	Informació a omplir automàticament amb el grup al que pertany l'usuari que ha generat l'enregistrament.
Signatura	S'omplirà **manualment** quan s'imprimeixi el document.

6.1.6 Càrrega dels informes generats manualment

Donat que durant la fase I del projecte, els informes es generaran, completaran i enviaran manualment, es requereix que, un cop implementada la funcionalitat de l'informe automàtic, puguin incorporar-se els documents ja generats i enviats. Donat que es disposen en paper, serà necessari escanejar-los i guardar-los com a pdf. Caldrà doncs crear els registres correctes a la base de dades per a que constin creats i enviats amb les dates que es van realitzar.

Per portar a terme la càrrega caldrà informar per cada incident enviat al a CCDCV les dates de creació, signatura i enviament junt amb el document escanejat (haurà de complir la normativa de nomenclatura). Aquesta informació es traspassarà via excel o el mecanisme que millor compleixi la funcionalitat que proposi l'adjudicatari.

6.2 Alta, modificació i baixa d'usuaris

Per poder utilitzar els dispositius i el software de gestió, es necessari que els usuaris estiguin donats d'alta a l'aplicació, bé a través dels sistemes de l'IMI o bé a través dels propis de l'aplicació per acabar després integrant-se amb els propis de l'IMI.

Es requereix una funcionalitat que permeti una càrrega elevada inicial d'usuaris i un posterior manteniment d'altes, modificacions i baixes que d'una manera senzilla permeti la introducció de qualsevol usuari dins la jerarquia. Aquesta funcionalitat aplicarà durant tot el desenvolupament de la fase I i fins a la implantació de la fase II que utilitzarà els sistemes d'autorització i autenticació de l'IMI, veure 7.2.2.1 Autenticació i autorització d'usuaris.

Aquesta funcionalitat podrà implementar-se dins del software de gestió o com aplicació independent (junt o separada de l'aplicació de l'informe de la CCDVC). En el cas de tractar-se d'una nova aplicació haurà de complir les especificacions tècniques indicades per l'IMI, veure 7. Requisits tècnics.

6.2.1 Pantalles de l'aplicació

És important considerar que en el cas que es desenvolupi una aplicació independent (en comptes de com a funcionalitat inclosa dins del software de gestió) caldrà implementar les pantalles bàsiques de qualsevol aplicació:

- Pantalla de login i autenticació d'usuaris. Veure 7.2.2.1 Autenticació i autorització d'usuaris. En el cas que la funcionalitat es desenvolupi en el mateix software de gestió, no serà necessari aquesta pantalla donat que ha estat necessari que l'usuari es logés per entrar a l'aplicació. Només tindran accés a aquesta funcionalitat els perfils amb la funcionalitat assignada.

- Pantalla de cerca d'usuaris: Ha de permetre la cerca d'usuaris per saber si ja estan al sistema, per modificar-los, eliminar-los, etc. Per tant és necessari que aquesta aplicació tingui integració directa amb el software de gestió que també mostra i gestiona els usuaris. Quan els usuaris es carreguin, modifiquin o eliminin a través d'aquest sistema, els canvis s'hauran de reflectir al software de gestió de la mateixa manera que es veurien si es fessin directament des del software de gestió.

- Ha de permetre seleccionar un usuari i modificar-li el perfil. No es treballarà amb les funcionalitats de cada perfil, aquestes estaran únicament al software de gestió i accessibles només per determinats perfils.

- L'aplicació no ha de tindre una base de dades pròpia sinó que alimentarà i s'alimentarà de la base de dades del software de gestió.
- Les altes, modificacions i baixes a través de l'aplicació només es permetran a través de l'Excel, no es realitzaran a través de la nova aplicació tot i tractar-se de casos individuals. Si es requereix podrà utilitzar-se l'aplicació del software de gestió per realitzar canvis petits però sempre assegurant que es compleix la jerarquia.

6.2.2 Càrrega inicial i manteniment d'usuaris

El nombre d'usuaris aproximadament serà un 70% de la plantilla, aprox, 2100 usuaris, repartits en diferents grups i perfils. Es planteja una càrrega mitjançant l'Excel tot i que s'admet qualsevol altre sistema de càrrega que realitzi la mateixa funció. La càrrega inicial alimentarà la base de dades del software de gestió i posteriorment, el mateix mecanisme s'utilitzarà per les altes, modificacions i baixes puntuals fins a la introducció dels sistemes d'autenticació i autorització de l'IMI.

El fitxer Excel (o similar) inclourà com a mínim la següent informació:

Càrrega d'usuaris	
Identificació usuari	Matrícula complerta de l'usuari tipus AMXXXXX
Grup	Grup o unitat a la que pertany. A escollir entre un llistat predefinit de valors
Perfil	Perfil que li correspon de la jerarquia. El perfil no sempre ha de correspondre amb el seu perfil dins de l'organització de la GUB.
Data de l'operació	Data a partir de la que es efectiu el canvi. D'aquesta manera es poden fer canvis a futur sense haver de realitzar-los el mateix dia en que entrin en vigor.
Operació	Indicador que especificarà si es tracta d'un alta, d'una baixa o d'una modificació (exemple: 0-Alta, 1-Baixa, 2-Modificació)

Construït l'Excel pel perfil corresponent, veure 5.3 Perfils, jerarquia, privilegis es carregarà des de l'aplicació i s'executarà. El procés pot consistir, des d'una execució online a la base de dades de l'aplicació fins a l'execució d'un procés diari que verifiqui si existeix un fitxer Excel al servidor del software i l'executi en el cas que sigui així. En el cas de la realització d'un procés, aquest haurà de complir amb els requisits tècnics de l'IMI i incloure's dins del planificador de processos.

El procés o càrrega ha de tindre control d'errors i logs que permetin analitzar si els canvis s'han realitzat correctament. En el cas que, per algun motiu, algun registre del fitxer doni error durant el procés, aquest continuarà, no s'avortarà, però es deixarà constància del problema per tal que es pugui solucionar i tornar a llançar amb el registre afectat.

6.2.3 Carrega inicial al Ctrluser

Amb la implantació de la fase II del projecte, el sistema d'autenticació i autorització passarà a ser l'OAM i el CtrlUser. Serà necessària una càrrega de dades de la bbdd del software de gestió al Ctrluser. Aquesta càrrega es realitzarà mitjançant un fitxer Excel generat a partir de les dades de la base de dades del software de gestió, que contindrà els usuaris, grups perfils i funcionalitats associades.

7 REQUISITS TÈCNICS

7.1 Aspectes generals

El software de gestió, al tractar-se d'un producte comercial, ja creat i desenvolupat, disposarà per sí mateix d'unes característiques tècniques i d'arquitectura pròpies, moltes vegades sense possibilitat d'adaptar o modificar amb els requeriments d'altres arquitectures. Aquests no seran llavors exigibles.

En el cas de les funcionalitats indicades a 6. Altres funcionalitats, si aquestes es desenvolupen en una aplicació independent del software de gestió, sí hauran de complir els estàndards de desenvolupament i arquitectura especificats per l'IMI.

En tots dos casos però, hi ha un mínim de característiques que els softwares i aplicacions han de tenir:

7.1.1 Accessibilitat

Cal assegurar el compliment de la normativa d'accessibilitat UNE 139803:2004: la interfície de l'aplicació ha de complir amb els punts de control de prioritat 1 i amb els de prioritat 2 que corresponen al nivell d'adequació AA de les directrius WCAG 1.0 (Web Content Accessibility Guideline) de la WAI (Web Accessibility Initiative).

7.1.2 Usabilitat

RU1. [Obligatori] Com a criteri general, s'ha de separar el contingut de la presentació.

RU2. [Obligatori] La presentació s'ha de visualitzar correctament amb els navegadors: Microsoft Internet Explorer 11 o superior, firefox 47+ i Chrome 48+.

RU3. [Obligatori] El temps d'aprenentatge del software per un usuari haurà de ser menor a 4 hores.

RU4. [Obligatori] El software disposarà de manuals d'usuari estructurats adequadament. Preferentment l'idioma serà català tot i que per a productes propietaris o comercials s'admetrà el castellà.

RU5. [Obligatori] El software/sistema ha de proporcionar missatges d'error que siguin informatius i orientats a l'usuari final. Preferentment en idioma català tot i que per a productes propietaris o comercials s'admetrà el castellà.

RU6. [Obligatori] El software haurà de disposar d'un mòdul d'ajuda en línia. Preferentment en idioma català tot i que per a productes propietaris o comercials s'admetrà el castellà.

RU7. [Obligatori] El software ha de posseir un disseny "Responsive" i Multidispositiu, a fi de garantir l'adequada visualització a múltiples dispositius: DeskTop, Tables i Telèfons Intel·ligents. Ha de suportar els sistemes: IOS, ANDROID, WINDOWS i LINUX

7.1.3 Eficiència

RE1. [Obligatori] Tota funcionalitat del software i transacció de negoci ha de respondre a l'usuari en menys de 3 segons en el 90% de les peticions.

RE2. [Obligatori] El software/sistema ha de ser capaç d'operar adequadament amb fins a 150 usuaris amb sessions concurrents (considerant que totes les càmeres estiguessin operant i/o descarregant a la vegada).

RE3. [Obligatori] El software/sistema ha de ser tolerant a errors.

RE4. [Obligatori] El software/sistema ha de garantir la integritat de les transaccions.

7.1.4 Seguretat

RS2. Autenticació: El software/sistema ha de comprovar que l'usuari que vol accedir al sistema és qui diu ser.

Si el software de gestió comercial disposa d'un sistema d'autenticació i autorització, s'utilitzarà aquest sempre que pugui garantir la seguretat (com a mínim amb un sistema d'usuari i psw). A la fase II del projecte haurà d'implementar-se la integració amb els sistemes de l'IMI, veure 7.2.2.1 Autenticació i autorització d'usuaris.

RS3. Autorització: El software/sistema ha d'implementar mecanismes per a restringir a usuaris no identificats i autoritzats l'accés a la informació. Ha de complir les mateixes característiques indicades a RS2.

RS4. Xifrat de dades: La comunicació de l'usuari amb el software/sistema es realitzarà únicament mitjançant canals segurs (https). Els algoritmes criptogràfics emprats seran els acreditats pel Centre Criptològic Nacional per al seu ús en l'Esquema Nacional de Seguretat.

Com a mínim es requerirà xifrat AES 256 i claus específiques per a l'estació base (descàrrega)

RS5. Gestió d'usuaris i sessions: Els mecanismes de control de sessions d'usuaris autenticats contemplaran:

- Tancament de sessió per part de l'usuari.
- Expiració automàtica de sessió.

RS6. Gestió d'errors i excepcions: Es realitzarà un tractament sistematitzat i centralitzat d'errors i excepcions, eliminat la informació interna del sistema o sensible dels missatges mostrats a l'usuari..

RS7. El nou software/sistema s'ha de desenvolupar seguint patrons i recomanacions de programació que incrementin la seguretat de les dades.

RS8. Encriptació: Qualsevol intercanvi de dades entre serveis o aplicacions es realitzarà mitjançant el protocol encriptat HTTPS.

7.2 Requisits d'arquitectura

7.2.1 Aspectes generals

RA1. Utilització de plataformes Open Source: Es requerirà que es prioritzi l'ús de plataformes i eines Open Source. Els llenguatges "base" per programar les aplicacions a mida a l'Ajuntament de Barcelona són Java i Python per a backend i Angular (TypeScript) per al client. Quan el llenguatge escollit sigui Java l'IMI disposa d'un framework propi anomenat OpenFrameIMI i que, actualment, es troba en la versió 4. Aquest framework és d'obligatòria utilització per al desenvolupament d'aplicacions Java. Cal destacar que el framework OpenFrameIMI fixa l'arquitectura i els serveis per les capes de Negoci, integració i persistència. Quan el llenguatge escollit sigui Python, el framework ha de ser Django/Python i seguir les directrius que marca l'IMI.

RA2. Preparada per a ser desplegada en Cloud Públic: El nou desenvolupament caldrà que estigui orientat a serveis. Aïllar els serveis que l'aplicació necessita per a funcionar i implementar-ho com a un component independent, permetrà a aquest tenir la capacitat d'adaptar-se i escalar segons la càrrega o peticions que rebi, sense afectar a la resta de l'aplicació. A la mateixa vegada aquest disseny permet monitoritzar i gestionar amb més precisió els diferents components de software.

RA3. Preparada per a ser desplegada en contenidors dockers: Caldrà orientar el nou desenvolupament al funcionament en contenidors Dockers, replicant d'aquesta manera als contenidors la mateixa infraestructura productiva. Es partirà d'imatges preparades per l'IMI que s'hauran de fer servir de base per a la construcció de les imatges definitives que caldrà desplegar.

Amb això s'aconsegueix :

- Simplificar la Instal·lació: Al fer servir imatges mestres preparades a tal efecte.
- Independitzar-se de la plataforma: Les imatges amb els contenidors es poden canviar d'un sistema a un altre facilitant no només els canvis a nivell productiu sinó les proves a entorns locals o de desenvolupament.
- Aïllar les aplicacions: Cada aplicació pot o no compartir contenidors de forma que es poden aïllar segons les necessitats existents.
- Automatitzar l'administració.

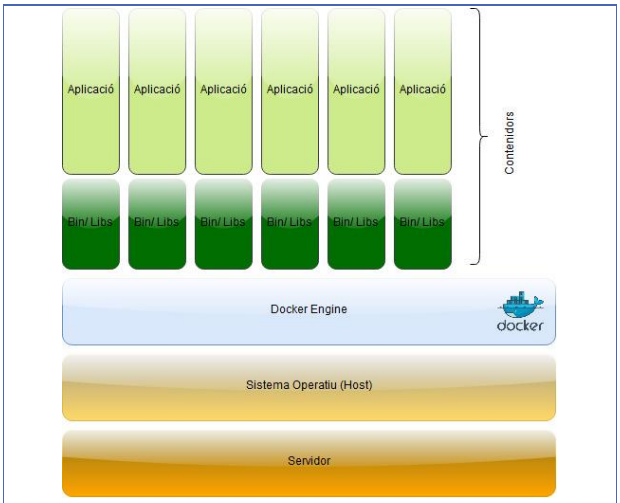


FIG. ARQUITECTURA BASADA EN DOCKERS

RA4. Requisits de modularitat i escalabilitat: Per eficiència i sostenibilitat el software/sistema haurà de ser modular i escalable amb les capa de negoci i de presentació

RA5. Traçabilitat: El software/sistema ha de garantir la traçabilitat de les accions dels usuaris sobre el mateix.

RA6. Multi-idioma: La solució ha de ser multi-idioma. La totalitat dels camps/missatges visibles per l'usuari han de poder traduir-se a taules, de manera que la incorporació d'un o un altre idioma no suposi haver de revisar i traduir codi font.

7.2.2 Serveis transversals

L'IMI disposa d'un conjunt de serveis que es poden accedir des de qualsevol plataforma. Són els que s'anomenen Serveis transversals i que podran utilitzar-se en el desenvolupament de les funcionalitats que el propi software no contempli o es requereixin pel nou desenvolupament.

- Autenticació i autorització.
- Geocodificació.
- Registre d'activitats i tràmits.
- Auditoria de dades afectades per LOPD.
- Generació de reports.
- Registre d'entrada.
- Plataforma d'interoperabilitat.

L'IMI proporcionarà a l'adjudicatari el llistat complet de serveis transversals.

7.2.2.1 Autenticació i autorització d'usuaris

Veure també 7.4.5.11 Gestió d'identitats, autenticació d'usuaris

7.2.2.1.1 Aplicacions de tercers

Pels productes comercials o aplicacions de tercer, per l'autorització i autorització l'IMI ha establert una integració mitjançant l'estàndard SAML (Security Assertion Markup Language). Es tracta d'un estàndard de codi obert basat en XML per l'intercanvi de dades d'autenticació i autorització. L'estàndard SAML està format per diversos components que aporten totes les funcions necessàries per definir i transmetre informació de forma segura. SAML permet, entre altres coses, realitzar declaracions sobre les propietats i autoritzacions d'un usuari respecte a altres usuaris o i especialment respecte d'una aplicació.

7.2.2.1.2 Aplicacions de nou desenvolupament

Per a les aplicacions que s'executen internament des de la pròpia xarxa de l'Ajuntament, es disposa d'un servei per a l'autenticació i autorització dels usuaris. Aplicaria en el cas que el licitador optés per desenvolupar les

funcionalitats descrites a 6. Altres funcionalitats com a una nova aplicació a construir d'acord als requeriments de l'IMI.

L'**OAM** es l'eina transversal per autenticar aplicacions i també serveis en el cas d'una arquitectura basada en serveis. Admet la integració amb aplicacions de tercers o softwares comercials fent ús del protocol SAML. Un cop efectuada l'autenticació a través del portal d'autenticació OAM es procedeix a determinar el perfil i els permisos de que es disposarà a l'aplicació durant la sessió present amb el **Control User** (CtrlUser).

El **CtrlUser** és l'eina web d'autorització on es gestionen els permisos d'usuaris a aplicacions. Qui controla l'accés és OAM mitjançant les dades de CtrlUser de les que es nodreix.

Actualment OAM i CtrlUser són els sistemes utilitzats per l'IMI per l'autenticació i autorització d'usuaris però en el cas que durant el temps de concurs, adjudicació i desenvolupament de fase I, aquests sistemes canviessin, l'adaptació hauria de realitzar-se amb els nous sistemes que tindrien funcions similars.

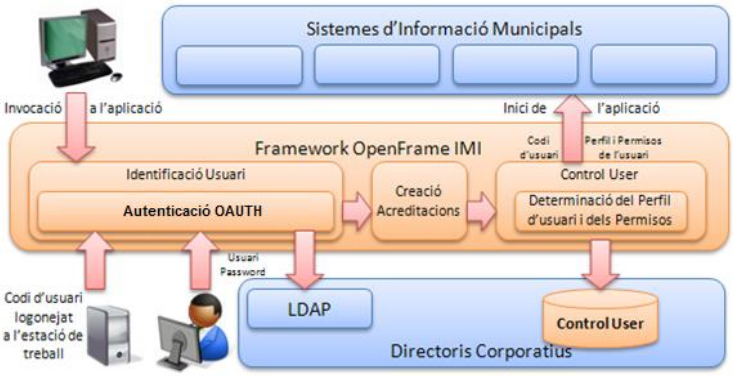


FIG. AUTENTICACIÓ D'USUARIS

7.2.2.2 Gestió d'Usuaris i Permisos

7.2.2.2.1 Aplicacions de tercers

Veure 7.2.2.1.1 Aplicacions de tercers

7.2.2.2.2 Aplicacions de nou desenvolupament

La CtrlUser és el sistema d'informació que permet gestionar els permisos del usuaris a les aplicacions desenvolupades d'acord als estàndards de l'IMI, mitjançant un catàleg d'aplicacions, una llista de funcions agrupades en perfils i aquests perfils assignats a usuaris.

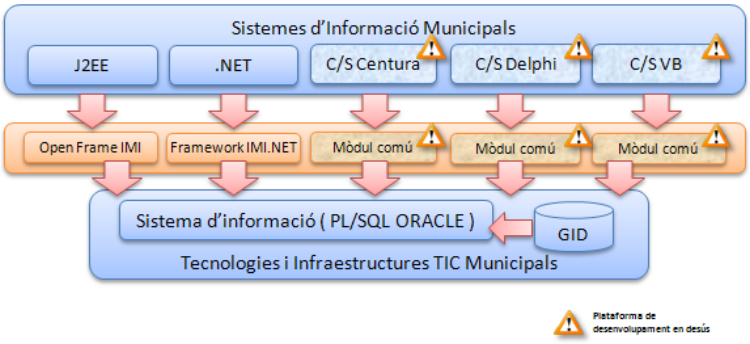
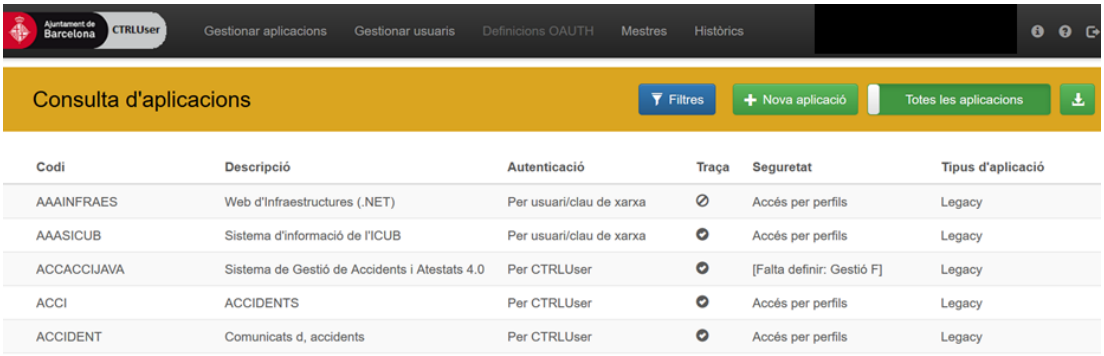


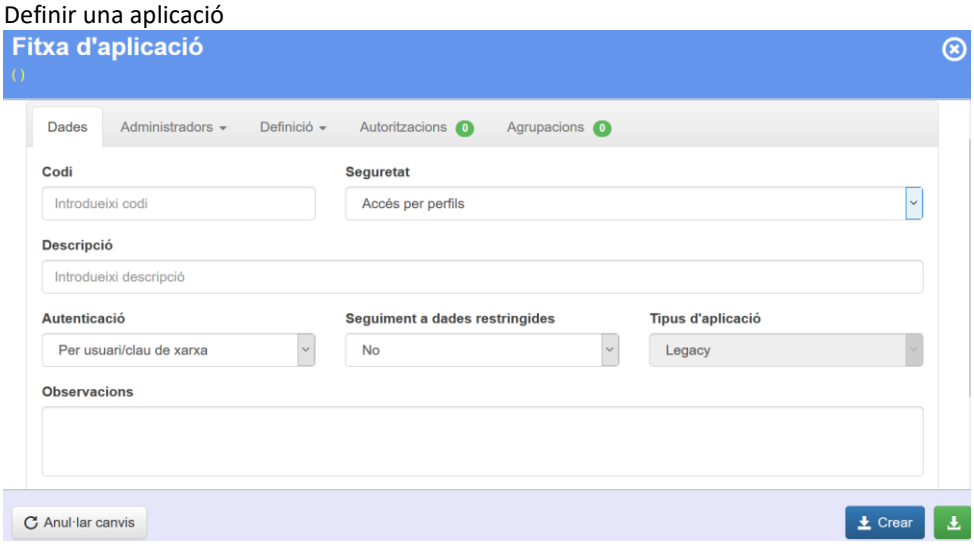
FIG. GESTIÓ D'USUARIS I PERMISOS

Concretament, la CtrlUser permet:

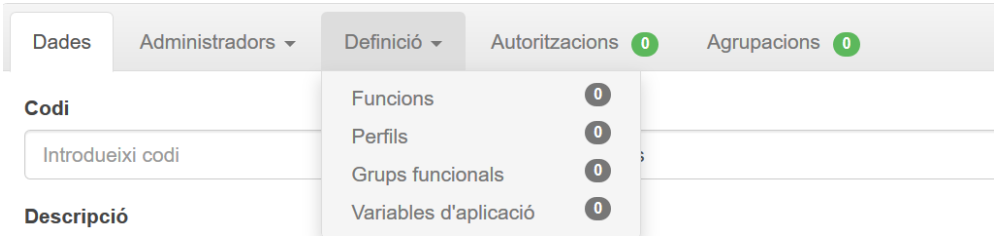
- Veure les aplicacions que utilitzen aquest mètode de control d'usuaris



- Definir una aplicació

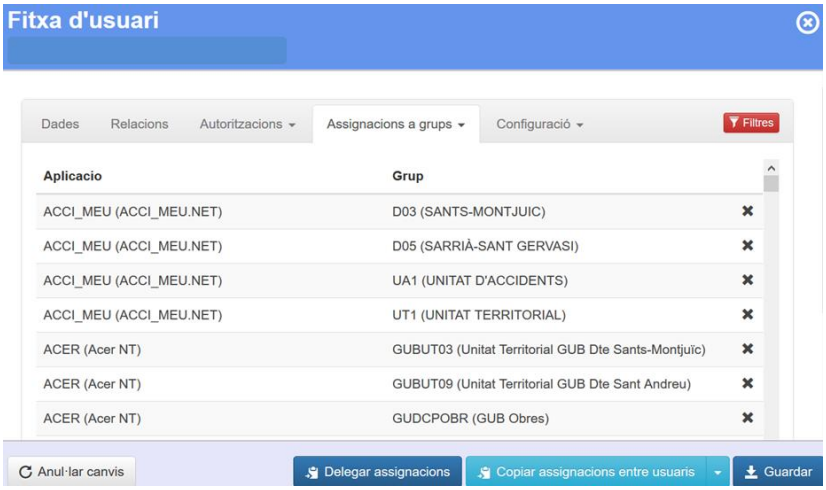


- Definir les funcions, perfils i grups funcionals d'una aplicació



- Crear els usuaris especificant les següents dades:

- Consulta de la fitxa d'un usuari



7.3 Requisits de explotació i sistemes

A nivell d'explotació de sistemes, es requereix que el software estigui preparat per:

Paràmetre	Requisit	Valor
Dimensionament	Nombre d'usuaris	2100 usuaris potencials, 75 concurrents
	Tipologia d'usuaris	Corporatius
	Necessitat de treballa on-line o amb processos batch	Online
	Necessitat de llicències	El producte no podrà ser llicenciat per usuari.
Dades	Tipologia	Dades de negoci. Enregistraments encriptats. Documents.
Proves de càrrega		A estudiar durant el desenvolupament del projecte. Donat a que el nombre d'enregistraments que es produiran no serà elevat, no es preveu que la descàrrega simultània dels DPG amb enregistraments pugui suposar cap problema.
Monitoratge		Sí
Backup		Sí
Nous Serveis d'Atenció a l'Usuari (SAU)		Sí

7.4 Requisits de seguretat

7.4.1 Pla de traces

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

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

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

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

En el cas que el software de gestió ja disposi d'un sistema de traces, tal i com es requereix d'acord 5.3.4 Auditoria i informes, no serà necessari crear un altre, sempre que compleixi amb els requeriments especificats. En el cas que la implementació de les funcionalitats descrites 6. Altres funcionalitats es desenvolupin en aplicacions independents, aquestes hauran de disposar d'un Pla de Traces d'acord amb els models de documents que disposa l'IMI i on es detalli la informació requerida indicada en aquest apartat. En cas que sigui necessari, el proveïdor haurà de proporcionar un repositori central de traces propi amb garanties de veracitat, d'integritat i confidencialitat. Addicionalment la granularitat de les traces serà definida d'acord amb els requeriments de l'IMI tenint en compte les seves necessitats concretes i els requeriments interns de la organització Municipal.

7.4.2 Pla d'autoritzacions

El proveïdor haurà de dissenyar el sistema d'autoritzacions per gestionar l'accés al software/sistema d'acord a l'estructura jeràrquica i de perfils que es defineixi al llarg del projecte, veure 5.3 Perfils, jerarquia, privilegis.

El pla d'autoritzacions haurà de recollir el perfilat d'usuaris, persones que autoritzin, circuit d'autorització i els mecanismes amb els que es gestionen les autoritzacions.

7.4.3 Informe de seguretat

El proveïdor elaborarà a petició de seguretat un informe on es detallaran tots els aspectes rellevants sobre Seguretat del software.

L'estructura d'aquest informe incloent la informació requerida es lliurarà al proveïdor durant les primeres etapes del projecte.

7.4.4 Xifratge de dades

La informació dels enregistraments estarà sempre xifrada. El xifratge es realitzarà en el mateix dispositiu i serà amb el hardware i software on es produirà la desencriptació. Els dispositius han d'assegurar la integritat de les dades. En cas de pèrdua del DPG no podran extreure's les seves gravacions i de la mateixa manera no es podran recuperar tampoc si no han arribat a descarregar-se. Veure més detall 4.1 Dispositius personals de gravació (DPG). Veure també 14.13 Xifratge de dades.

7.4.5 Requeriment de seguretat de tractament tipus 2

A continuació es llisten les clàusules de seguretat pel tractament de tipus 2, on l'adjudicatari prestarà el servei utilitzant els sistemes de l'IMI i/o l'Ajuntament des de les instal·lacions de l'adjudicatari.

7.4.5.1 Auditoria

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

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

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

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

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

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

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

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

7.4.5.2 Gestió d'incidents

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

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

7.4.5.3 Dimensionament/gestió de capacitats

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

7.4.5.4 Accés a la informació

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

7.4.5.5 Control d'accés

7.4.5.5.1 Accés local

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

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

7.4.5.5.2 Accés remot

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

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

7.4.5.6 Gestió del Personal

7.4.5.6.1 Deures i obligacions del personal

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

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

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

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

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

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

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

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

7.4.5.6.2 Formació i conscienciació

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

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

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

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

7.4.5.7 Protecció del lloc de treball

7.4.5.7.1 Lloc de treball buit

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

El material quedarà guardat en un espai tancat quan no s'estigui utilitzant.

7.4.5.7.2 Bloqueig del lloc de treball

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

7.4.5.7.3 Protecció d'equips

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

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

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

Addicionalment, els equips hauran de disposar:

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

7.4.5.7.4 Mitjans alternatius

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

7.4.5.8 Protecció dels Suports Informàtics

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

7.4.5.8.1 Etiquetat

L'adjudicatari es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han

d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

7.4.5.8.2 Criptografia

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

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents a la informació municipal o corporativa, haurà de ser presentat per ser validat per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

7.4.5.8.3 Transport

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

7.4.5.8.4 Esborrat i destrucció

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

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

7.4.5.9 Protecció de la Informació

7.4.5.9.1 Neteja de documents

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

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

7.4.5.9.2 Protecció del correu electrònic

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

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'adjudicatari.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:

- Correu no sol·licitat (*spam*)
- Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
- Codi mòbil de tipus *applet*.

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

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

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

7.4.5.10 Protecció de les Instal·lacions

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

- En cas de emmagatzemar informació de l'Ajuntament de Barcelona, disposar de les mesures de seguretat pertinents per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació.
- Garantir que la informació de l'Ajuntament de Barcelona no pugui ser visible i/o audible des de l'exterior de les instal·lacions.

7.4.5.11 Gestió d'identitats, autenticació d'usuaris

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

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

Autenticació interna

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

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

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

Autenticació externa

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

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació, requerint així una verificació de la identitat de l'usuari que sol·licita accés. Actualment, la solució implantada al IMI fa ús de Google Authenticator.

7.4.5.12 Autorització dels usuaris als sistemes

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

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

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

Perfilat d'usuaris

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

El model proposat haurà de complir amb els següents principis:

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

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

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

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

7.4.5.13 Desenvolupament segur

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

Els següents elements seran part integral del disseny del sistema:

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

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

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

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

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

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

Aquesta clàusula aplica en el cas de que el proveïdor desenvolupi software propi o realitzi alguna modificació sobre el codi del producte, assegurant que en el cas de realitzar evolutius sobre l'eina no s'introdueixen noves vulnerabilitats

7.4.5.14 Configuració de seguretat

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

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

7.4.5.15 Acceptació i posta en servei

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

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

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

- Anàlisis de vulnerabilitats.
- Test de penetració.

7.4.5.16 Dades de proves

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

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

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

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

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

7.5 Requisits de qualitat

L'Oficina de Qualitat de l'IMI estableix un conjunt de processos per tal d'assegurar la qualitat de la documentació i dels processos de gestió i seguiment dels projectes segons marca la metodologia ADINET. En el cas de projectes de desenvolupament d'un nou software, el proveïdor ha de seguir la metodologia ADINET.

En aquest cas, donat que l'adquisició del software de gestió no es tracta d'un nou producte que calgui desenvolupar de zero, sinó principalment de la implantació d'un producte ja existent i en funcionament, no es requerirà el seguiment de la metodologia ADINET. Si se sol·licitarà però, documentació associada, veure 3.2 Serveis inclosos.

Dins de l'àmbit del projecte es defineixen punts de control que permeten assegurar el compliment dels requisits mínims que n'assegurin la viabilitat i l'èxit. Aquests punts de control s'anomenen checkpoints. Al tractar-se de la implantació d'un software comercial, els checkpoints els definirà la Gestió del Projecte a l'inici del projecte.

7.6 Altres requisits

7.6.1 Idioma

En el cas de software propietari o comercial, el software haurà d'estar en castellà o català. En el cas que les funcionalitats descrites a 6. Altres funcionalitats s'implementin en una aplicació independent, aquesta haurà de ser en català.

La documentació tècnica i funcional requerida haurà d'estat en tots els casos en castellà/català. En el cas de manuals molt tècnics del hardware, es permetrà l'idioma anglès sempre que es proporcioni també una versió reduïda en idioma castellà o català.

8 GESTIÓ DEL CANVI I FORMACIÓ

La incorporació dels DPG suposa un canvi important en l'operativitat i manera de procedir de la GUB. Per aquest motiu és necessari que tota l'organització estigui informada de l'evolució del projecte i la seva situació.

Els licitadors hauran de presentar un pla de Gestió del Canvi amb els plans que s'indiquen a continuació. L'adjudicatari haurà de mantenir actualitzada a questa documentació al llarg del projecte.

- Pla de Gestió del Canvi : serà validat per la direcció del Projecte i requerirà de la seva aprovació per a ser admès. En el cas que s'hagi presentat un Pla de Gestió del Canvi durant la fase de licitació, l'adjudicatari podrà presentar-lo per ser aprovat per la Direcció del Projecte. En cas contrari, l'adjudicatari n'haurà d'elaborar un. Ha d'incloure:
    - Pla de Desplegament: és un conjunt d'accions que defineixen el procediment per abordar la posada en marxa del projecte, per tal que sigui efectiva la seva posada en funcionament, que sigui raonablement ràpida, i que no provoqui efectes no desitjats i que, si ho fa, no siguin massa extensos en el temps ni en l'organització. Veure la planificació 11.3 Planificació del projecte per consultar els trets generals de la planificació proposada.
    - Pla de Formació ha d'incloure una descripció detallada de les accions formatives previstes, la definició del públic objectiu i el contingut previst per a cadascuna d'elles. La formació inclourà tant la part de hardware com de software.
    - Pla de Suport i Garantia: ha d'incloure una descripció del suport funcional, tècnic i de hardware que es durà a terme durant el temps de suport establert al projecte, 6 mesos des de la finalització del projecte. La garantia del hardware tindrà una duració mínima de 2 anys.
    - Pla de riscos: ha d'incloure la identificació dels possibles riscos i problemes, proposant quan calgui, accions correctives per cadascun d'ells.

8.1 Pla de Formació

Els licitadors elaboraran un pla de formació sobre els diferents aspectes, sistemes i softwares implementats durant el projecte. La formació serà continua al llarg del projecte. Inclourà la realització dels cursos adients per a tots els usuaris per tal d'assolir els coneixements necessaris per un ús òptim dels dispositius i del software i funcionalitats.

Els cursos s'hauran d'impartir a les dependències de la GUB en horari de matí, tarda i/o nit (a inici o fi de torn) d'acord amb els responsables del cos per tal de no interferir en l'activitat ordinària dels serveis. La modalitat serà preferentment presencial, tret que altres factors externs (com de salut pública per exemple en l'actual situació COVID) que impossibilitin aquesta modalitat.

L'adjudicatari proposarà un pla de formació concret per a cada una de les àrees especificant la duració i contingut de les diferents sessions per coordinar dates i horaris. Aquest pla establirà els continguts, programació i material formatiu per tal d'assolir els nivells de coneixement requerits, que en tot cas s'hauran d'adaptar als convenients per l'Ajuntament de Barcelona.

Les sessions formatives per col·lectius hauran de cobrir com a mínim:

- Usuaris administradors amb l'objectiu de què puguin gestionar el software de gestió, modificar alguns paràmetres, gestionar l'alta, baixa i modificacions d'usuari i revisar les auditories.
- Usuaris encarregats de treballar les estadístiques d'indicadors i els informes necessaris.
- Usuaris de referència del hardware i de software amb l'objectiu de conèixer el seu funcionament de manera que puguin formar a la resta del col·lectiu. Serà necessari diversos cursos a causa de la distribució territorial dels usuaris. Es requerirà un mínim d'un curs per unitat territorial i altres sessions per la resta de divisions, aproximadament 15 sessions d'una duració entre 1-2 hores.
- Usuaris de referència generals amb l'objectiu de proporcionar el coneixement i experiència necessaris per a poder desenvolupar tasques de suport i formació tant de software com de hardware a la resta del col·lectiu.

L'adjudicatari haurà de lliurar la documentació necessari per dur a terme la formació:

- Manuals del funcionament i característiques de cadascun dels elements de hardware i de software en idioma català o castellà, format pdf o word.
- Presentacions, exemples,... o material divers que permeti entendre el funcionament del conjunt de la solució
- Guies ràpides de funcionament bàsic dels dispositius

L'adjudicatari, com a part del subministrament objecte del contracte, haurà de proporcionar el material de formació empleat, per la seva utilització per part de l'Ajuntament de Barcelona, a la seva voluntat, en els processos formatius interns que es desenvolupin posteriorment. El material proporcionat serà utilitzat per l'Ajuntament de Barcelona només per aquesta finalitat.

Els professorat dels cursos haurà de contar amb experiència provada per la configuració i instal·lació de l'equipament i software empleat.

Els licitadors hauran d'incloure a l'oferta una descripció del contingut dels cursos i dels materials de formació. Aquesta informació es valorarà a l'apartat 8.2.2 de l'Informe Justificatiu que acompanya el present plec de prescripcions tècniques.

8.2 Pla de Suport i garantia

Els licitadors elaboraran un pla de suport que contemplarà el suport funcional, operatiu i tècnic (presencial i a distància) gestionant les consultes i resolent les incidències i problemes que puguin sortir una vegada posada en marxa la solució. Aquest pla començarà finalitzat el projecte, donat que ja durant la implantació de les diferents fases es contarà amb el suport de l'adjudicatari. De la mateixa manera servirà també per la gestió de la garantia, veure més detall a 11.6 Garantia. Es valorarà l'ampliació d'aquest termini, veure document "Informe Justificatiu".

Concretament el Pla de suport i garantia ha d'incloure els següents aspectes:

- Horari i mitjà de contacte: els licitadors especificaran en quin horari prestaran el servei i a través de quin mitjà. L'Ajuntament demanarà el contacte directe amb el licitador a través d'un número de telèfon mòbil accessible durant, mínim el següent interval d'hores: 8:00-18:00. També es requerirà disposar d'una adreça de correus per aquelles sol·licituds que requereixin enviament de documentació, imatges, etc. L'idioma de contacte haurà de ser català o castellà.

- Persones de contacte: els licitadors indicaran quines seran les persones que prestaran el servei en cada modalitat (resolució de temes/incidències de software, resolució de temes tècnics, etc..) per tal que la resolució sigui el més àgil possible. De la mateixa manera l'Ajuntament de Barcelona especificarà a l'adjudicatari quines seran les seves persones de contacte per cada cas.

- Lloc i mecanisme de prestació del servei: Els licitadors hauran d'especificar com es resoldran les consultes/incidències i com es realitzarà la gestió del material (espatllat, reparat). Veure més detall a 11.6 Garantia.

- Diagnosi dels problemes: El Pla de Suport inclourà l'anàlisi dels problemes de software, tècnics i de hardware. En el cas del software, el pla inclou assessorament, acompanyament, ... a nous reptes o funcionalitats que l'Ajuntament de Barcelona decideixi portar a terme. Inclourà també valoracions de resolució de problemes o noves funcionalitats. En el cas d'incidències de hardware no contemplades dins de la garantia, per exemple, trencament per mal ús, inclourà l'anàlisi del problema, la causa i el diagnosi de la solució.

- Eines de gestió i seguiment:
  - Hardware: la gestió i seguiment de les incidències de hardware, tant durant el període de garantia com en el de suport, es realitzarà mitjançant l'ús de l'eina corporativa **COOPER**. Aquesta aplicació permet el registre de tot l'inventari de material de la Direcció de Logística i Infraestructura (direcció a la que pertanyeran els dispositius) i les seves incidències. Registra,

gestiona i controla les incidències tècniques dels diferents dispositius, vehicles, equipament, etc. dels cossos de la Guàrdia Urbana de Barcelona i els Serveis de Prevenció i Extinció de Barcelona. L'adjudicatari tindrà la responsabilitat d'accedir diàriament a l'aplicació i realitzar el seguiment, gestió i actualització de l'estat de les incidències. L'adjudicatari disposarà d'accés a l'eina a través de una VPN corporativa, visualitzant únicament les incidències assignades al seu perfil i del seu àmbit de treball. Serà responsabilitat seva:

- Informar de la data d'inici de reparació i la data entrada a taller (automàticament modifica l'estat de l'article a 'Avariat')
- Informar de la data fi reparació i data de sortida de taller (automàticament modifica l'estat de l'article a 'Actiu')

A mode consulta, es permetrà veure les característiques dels dispositius (identificador de la càmera, vehicle al que està associat,..) però no modificar cap paràmetre. En el cas de que algunes d'aquestes dades es vegi modificada (substitució física d'un equip,..) es comunicarà el canvi al gestor assignat al projecte. De la mateixa manera, en el cas de baixa d'elements, aquestes es comunicaran i es duran a terme pel gestor.

Per la resolució de les incidències serà necessari el desplaçament d'un tècnic al lloc d'ubicació del dispositiu (les diferents dependències de GUB) per tal d'avaluar i intentar solucionar la incidència in situ. En el cas de que fos necessari, l'adjudicatari portaria el dispositiu a reparar.

Les incidències incloses a la garantia del material no suposaran cost addicional i aniran a càrrec de l'adjudicatari. Només per les incidències fruit d'un mal ús es sol·licitarà pressupost de reparació o substitució.

- Software: En el cas de les incidències de programari seran escalades a l'adjudicatari des del Servei d'Atenció a l'Usuari, en endavant SAU, que l'IMI disposa per a la gestió i seguiment d'incidències d'aplicacions. L'adjudicatari disposarà d'accés a l'eina corporativa de l'IMI, anomenada HP Service Manager des d'on visualitzarà les incidències assignades i a les que haurà d'actualitzar l'estat i indicar les accions necessàries al finalitzar la seva resolució

8.3 Pla de desplegament

Els licitadors elaboraran un Pla de desplegament. Aquest pla és un conjunt d'accions que defineix el procediment per abordar la posada en marxa del projecte, per tal que sigui efectiva la seva posada en funcionament, que sigui raonablement ràpida, i que no provoqui efectes no desitjats i que, si ho fa, no siguin massa extensos en el temps ni en l'organització.

A 11.3 Planificació del projecte es mostra la planificació prevista que els licitadors hauran d'adaptar i proposar en el seu pla de desplegament. Es valorarà la reducció d'aquesta planificació, veure el document "Informe Justificatiu".

8.4 Pla de Riscos

Els licitadors elaboraran un Pla de Riscos del projecte identificant els possibles riscos i problemes i proposant quan calgui accions correctives per a cadascun d'ells. El Pla de Riscos haurà d'incloure, si més no, els següents punts:

- Identificació del risc.
- Descripció del risc.
- Valoració de la gravetat del risc (Impacte / Probabilitat).
- Accions correctores proposades
- Responsable de les accions correctores.

L'elaboració del Pla de Riscos final serà responsabilitat de l'adjudicatari, però es realitzarà conjuntament entre el Cap de Projecte de l'adjudicatari i el Cap de Projecte de l'Ajuntament de Barcelona.

9 ORGANITZACIÓ I EQUIP DE TREBALL

9.1 Organització

Amb caràcter general, l'Ajuntament de Barcelona controlarà, mitjançant la figura d'un Cap de Projecte, el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte i l'execució del projecte.

Igualment l'IMI proporcionarà interlocutors per a les diferents disciplines del projecte: arquitectura, implantació, desplegament, etc. Aquests interlocutors tindran la responsabilitat de validar les parts del sistema que estiguin sota la seva responsabilitat.

Cal que els licitadors detallin a les seves propostes quina és l'organització que proposen amb l'equip i perfils adients de persones suficientment qualificades, per portar a terme el projecte complint els objectius, els terminis de lliurament i la qualitat exigible. Cal que aquesta organització inclogui la figura del Cap de Projecte del proveïdor, que serà l'interlocutor únic entre l'adjudicatari i l'Ajuntament de Barcelona per a tots els temes relacionats amb la gestió i execució del contracte.

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

- Comitè de direcció

Les seves funcions són les de supervisar la marxa del projecte i la presa de decisions que afecten a l'objectiu i abast del mateix. El Cap de Projecte de l'adjudicatari assistirà a les reunions d'aquest Comitè sempre que sigui requerit per qualsevol dels seus membres. Quan ho faci serà el responsable de l'elaboració de la documentació de seguiment del projecte necessària per a tal fi i també d'aixecar l'acta de les reunions d'aquest Comitè a les que assisteixi.

Es reuneix normalment cada 2 mesos encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari. En formen part:

- Directora d'Estratègia i Nous Projectes de l'IMI o persona en qui delegui
- Director de Desenvolupament de l'IMI o persona en qui delegui
- Cap de Projecte que l'Ajuntament de Barcelona designi
- Director del projecte de la GUB o persona en qui delegui
- Cap de contracte de l'adjudicatari

- Comitè de seguiment

S'encarrega del dia a dia del projecte. Resol les incidències i conflictes menors que apareguin al llarg de la vida del projecte.

Es reuneix normalment un cop a la setmana. Està format pels Caps de Projecte de l'adjudicatari i de l'Ajuntament de Barcelona. Quan calgui, es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip de projecte necessaris per a tractar en profunditat determinats temes. El Cap de Projecte de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

- Reunions de seguiment

Amb caràcter obligatori, es convocarà una reunió de Kick-off o llançament de projecte amb els principals membres del projecte (GUB, Ajuntament de Barcelona).

Es convocaran també amb caràcter obligatori, una reunió per a cada tancament de fase del projecte.

La periodicitat de la resta de reunions es determinarà amb l'adjudicatari a l'inici del projecte.

9.2 Equip

Els licitadors hauran d'incloure en la seva oferta un esquema de l'equip del treball i la seva organització. Cada membre de l'equip ha de poder interactuar i comunicar-se amb l'Ajuntament de Barcelona i amb la resta de membres del projecte, en idioma castellà o català.

S'estima necessari que l'equip de projecte compti amb les següents capacitats per a la prestació dels serveis inclosos al contracte.

Capacitat	Responsabilitat	Experiència / coneixements
Cap de projecte del contracte	Màxim responsable de l'equip de l'empresa adjudicatària, i en conseqüència de la provisió en temps i qualitat dels serveis inclosos en aquest contracte. Màxim interlocutor de l'equip, revisa amb la direcció del contracte per part de l'Ajuntament de Barcelona i GUB, el correcte avenç de les activitats previstes, l'adequació dels recursos humans, i gestiona riscos, desviacions, peticions fora de l'abast inicial, etc. • Seguiment de la planificació i de les fites del contracte. • Control i anàlisi de desviacions (en esforços i econòmiques). • Gestió de riscos del contracte: identificació i proposta d'accions pal·liatives. • Assegurar la correcta interlocució entre els usuaris i l'equip de contracte. • Assegurar la correcta execució i validació dels lliurables • Gestió de les reunions i dels comitès de seguiment i direcció i elaboració d'informes de gestió (informes de seguiment i informes de direcció). • Suport i assessorament a la presa de decisions en els òrgans de direcció del contracte Dissenya, confecciona, realitza les tasques de consultoria, executa i realitza el seguiment de l'estratègia del servei.	Cal que acrediti, durant els darrers 6 anys, una experiència mínima de 4 anys en l'àmbit de la consultoria estratègica i/o projectes de transformació organitzativa. Haurà d'haver participat almenys en dos projectes com a Responsable de Contracte en l'àmbit públic i/o privat i en especial en l'àmbit dels Cossos Policials o Forces de Seguretat. Cal que acrediti una experiència mínima, durant els darrers 5 anys, de 3 anys amb rol de Cap de contracte en els àmbits anteriors.
Cap de projecte	Responsable del seguiment diari del projecte i interlocutor amb el cap de projecte de l'Ajuntament de Barcelona. Encarregat de: • Revisió i tancament de tots els lliurables. • Control i seguiment de la implantació i implementació. • Assegurament del compliment del pla de qualitat i fites definides en el contracte. • Disponibilitat per a reunions presencials periòdiques, coordinació i seguiment del projecte i per organitzar i participar en les iteracions.	Cal que acrediti una experiència mínima de 3 anys d'experiència acreditada en projectes d'implantació de l'àmbit dels Cossos Policials o Forces de Seguretat públics així com un ampli coneixement del hardware licitat i experiència en projectes de desenvolupament de software.
Equip d'implantació tècnica, arquitecte, formació, suport i manteniment	Equip qualificat per realitzar la instal·lació física dels hardware amb experiència demostrable en altres instal·lacions d'aquests equipaments o similars. Equip amb experiència en formació capaç d'elaborar la documentació necessària i transmetre els coneixements del hardware i softwares del projecte. Equip amb coneixement funcional i tècnica de la solució capç de resoldre els problemes tècnics i funcionals que apareguin al llarg del projecte.	Cal que acreditin experiència en implantació, formació i suport en projectes similars i dins l'àmbit dels Cossos Policials o Forces de Seguretat privades o públiques.
Desenvolupador/s especialistes, com a mínim en les següents tecnologies: Java, J2EE, etc. (en el cas de que	Responsable/s de la implementació de les diferents peces de software que formen el producte final: • Utilització de les eines de desenvolupament: Git, Redmine, Jenkins • Empaquetat del producte en la tecnologia de contenidors seleccionada • Participació en totes les iteracions	Com a mínim un membre de l'equip ha d'acreditar: • experiència mínima de 5 anys treballant amb aplicacions Web, Java, Javascript. • experiència mínima de 3

les funcionalitats descrites a 6. Altres funcionalitats s'implementin com a noves aplicacions)	• Dedicació pràcticament completa al projecte i participació en totes les iteracions.	anys treballant amb • experiència mínima de 2 anys treballant amb el llenguatge de programació proposat pel licitador.
Responsable de seguretat	Responsable de fer complir les mesures de seguretat que són d'aplicació al proveïdor a través de l'Esquema Nacionalitat de Seguretat, pel fet de treballar amb una administració pública	Cal que acrediti experiència i coneixements en temes de seguretat de la Informació.

L'incompliment d'aquesta obligació comportarà l'exclusió per raons tècniques de la present licitació.

L'empresa adjudicatària serà responsable de dotar el contracte amb els recursos necessaris, tant humans com materials, que permetin el correcte desenvolupament d'aquestes tasques.

L'Ajuntament de Barcelona podrà demanar en qualsevol moment a l'empresa adjudicatària el llistat de persones que formen part de l'equip de projecte.

Els licitadors concretaran, en la forma que s'indica en el plec de clàusules administratives particulars, la composició de l'equip de treball que posaran a disposició del contracte, acreditant que tenen l'experiència professional exigida en el quadre anterior.

L'Ajuntament de Barcelona es reserva el dret de demanar el canvi de qualsevol persona assignada al contracte, quan consideri que el resultat de la seva feina no és satisfactori. Les despeses que es derivin com a conseqüència de canvis en l'equip del contracte aniran a càrrec de l'empresa adjudicatària.

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

10 PROPOSTA TÈCNICA

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

El licitador haurà de presentar la seva oferta en format electrònic, on tots els arxius han d'estar en qualsevol dels formats admesos per la Plataforma de Contractació Electrònica d'acord amb els requeriments exigits al plec de clàusules administratives particulars.

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

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

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

10.1 Contingut sobre B

S'inclourà la documentació següent indexada de manera que faciliti la seva localització. Per a cada apartat i entre parèntesi s'ha indicat el nombre màxim de pàgines que pot constar, tipus de lletra Arial, grandària 12 i interlineat simple.

La documentació inclourà els següents continguts mínims i ha d'estar obligatòriament estructurada de la forma següent tot i que els licitadors han de tenir en compte de presentar la suficient informació per la valoració del criteris subjectes a judici de valor.

- **Resum executiu** (màxim 3 pàgines)
  Resum per a la Direcció dels continguts més significatius de la proposta del projecte, destacant-ne els recursos i les propostes de valor afegit.
- **Plantejament general del projecte** (màxim 10 pàgines)
  En aquesta secció el licitant ha d'exposar el seu enteniment del projecte i les línies principals de la seva estratègia per afrontar-lo tenint en compte els requeriments exposats en el plec de prescripcions tècniques. El licitador presentarà els diagrames i esquemes que cregui necessaris i que ajudin a visualitzar el grau de comprensió de la solució.
- **Solució tècnica/funcional** (màxim 20 pàgines)
  Descripció detallada de la solució tècnica/funcional plantejada. Inclourà la descripció de les característiques tècniques i funcionals dels elements del hardware així com el compliment de les funcionalitats del software i el plantejament de les funcionalitats requerides.
- **Pla de Riscos** (màxim 3 pàgines)
  La proposta de Pla de Riscos ha d'identificar els riscos que el licitador entengui de la lectura del present plec i proposar-ne una correcta gestió mitjançant la definició d'una matriu de riscos juntament amb les propostes per mitigar-los.
- **Pla de Desplegament (**màxim 8 pàgines**)**
  Aquest document ha de proposar els procediments per abordar la posada en marxa del contracte, i per assegurar l'èxit en la transició del mateix, tenint en compte no només l'estratègia per desplegar la totalitat de l'abast funcional sinó també l'enfocament per abastar els diferents stakeholders del contracte, així com els possibles escenaris alternatius de desplegament, detall i coherència.
- **Pla de Formació (**màxim 6 pàgines**)**
  El Pla de Formació ha de permetre articular en el temps, d'una forma global, coherent, integrada i eficaç, les diverses accions formatives promogudes en el marc del projecte, tenint en compte les necessitats dels diferents col·lectius.

- **Pla de Suport i garantia (**màxim 6 pàgines**)**
  El Pla de Suport posterior a la posada en marxa ha de mostrar una proposta tècnica detallada que, respectant els mínims establerts a l'apartat 8.2 Pla de Suport i garantia del plec de prescripcions tècniques, mostri el detall del servei de suport i la coherència de la relació amb l'IMI durant aquest període. També caldrà descriure el model de garantia proposat.
- **Altra informació** que el licitador consideri rellevant per fer més comprensible la seva proposta **(**màxim 10 pàgines**).**

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

11 CONDICIONS D'EXECUCIÓ

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

11.1 Lloc de prestació del contracte

11.1.1 De manera general

Els serveis es prestaran des de les instal·lacions de l'adjudicatari / proveïdor. En les ocasions que ho requereixin, es podrà demanar el desplaçament a les oficines de l'Ajuntament de Barcelona / IMI per a la prestació d'aquell servei que sigui necessari, essent obligació de l'adjudicatari l'aportació de les eines que siguin necessàries per a la prestació d'aquest.

El proveïdor haurà d'aportar mitjans logístics suficients per a la prestació del servei des de les seves instal·lacions. Concretament, la connexió amb l'IMI es podrà fer amb les següents alternatives:

- En cas de ser factible, mitjançant enllaços propietaris de fibra òptica. L'enllaç serà una connexió Giga bit amb separació i translació d'adreces en el costat de l'adjudicatari. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol actuació necessària per a la posada en marxa de la connexió: esteses de fibra i electrònica addicional, manipulacions de connexions de fibra a la via pública, etc.
- A través d'una connexió al servei Metrolan de Telefònica i amb una connexió d'ample de banda suficient per a garantir un adequat rendiment. L'enllaç serà una connexió Ethernet amb separació i translació d'adreces en el costat de l'adjudicatari. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol adquisició o actuació necessària per a la posada en marxa de la connexió. També serà al seu càrrec la quota mensual de la línia contractada.
- Per últim i de forma preferent, mitjançat solució VPN (lan-to-lan) sobre l'accés a Internet existent a les dependències de l'IMI d'acord amb la normativa establerta per l'IMI per a l'accés remot als seus sistemes d'informació. És responsabilitat de l'adjudicatari la contractació i manteniment del seu accés a Internet així com disposar d'un equip que suporti aquest tipus de connexions i d'un ample de banda suficient en aquesta línia.

És responsabilitat de l'adjudicatari disposar del personal tècnic necessari per a la correcta configuració dels equips que acaben el circuit VPN del seu costat i dels seus sistemes de seguretat i translació d'adreces IP (si cal). L'IMI col·laborarà en la seva implantació facilitant els paràmetres de configuració i el certificat per a l'equip que acaba el circuit. Opcionalment podrà oferir un model de configuració tipus si aquest equip final és un router Cisco de la sèrie 800.

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

Per a realitzar les tasques de desenvolupament requerides caldrà realitzar la instal·lació d'un software a les estacions del client (aquest software està garantit sobre plataformes Windows). Aquest software permetrà accedir a unes màquines de desenvolupament remot que estaran a la seu del IMI. El software que serà necessari instal·lar a les màquines del adjudicatari serà el client de firewall i l'escriptori remot XP a les estacions. És responsabilitat de l'adjudicatari aquesta instal·lació i el seu manteniment així com disposar dels equips que suportin aquest software.

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

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

Les estacions de desenvolupament estan preparades per permetre la impressió a models d'impressores reconeguts per Windows 10. Si es requereix algun model no reconegut, caldrà notificar-ho a l'IMI perquè s'afegeixin els drivers necessaris. Per poder utilitzar la impressió des de sistemes externs (Host Print o Paris) cal que les impressores tinguin assignada una IP del rang subministrat per l'IMI.

S'ofereix la possibilitat de transferir fitxers entre l'estació de desenvolupament i la de l'usuari, però es recomana fer-ho amb moderació a causa de l'alta utilització d'ample de banda que requereix.

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

11.1.2 Instal·lació

La instal·lació de l'equipament ofert es durà a terme físicament a les unitats/dependències especificades en aquest plec i/o indicades per la direcció del projecte.

GUB facilitarà la instal·lació disposant d'un lloc convenient per a la instal·lació dels equips. En cas que fos necessària l'adequació de connexions elèctriques, tomes de xarxa, etc.... serà l'Ajuntament de Barcelona el responsable de la seva gestió.

11.1.3 Formació

La formació es realitzarà en la mesura que sigui possible, a les dependències de l'Ajuntament de Barcelona. Donada la situació especial de pandèmia (COVID), l'Ajuntament de Barcelona serà responsable d'assegurar que les condicions d'impartició dels cursos compleixen totes les mesures de seguretat possibles evitant sempre qualsevol risc.

En cas que per la situació no sigui possible la realització presencial dels cursos, la Direcció del Projecte determinarà conjuntament la solució més adient (reducció de grups, formació online, etc.). Més detall a 8.1 Pla de Formació.

11.2 Durada del contracte

Aquest contracte tindrà vigència a partir del dia següent a la seva formalització i tindrà una durada màxima de 6 mesos a partir d'aquesta data.

11.3 Planificació del projecte

El projecte es durà a terme en dos fases permeten una ràpida implantació i posada en marxa i deixen per una fase posterior les funcionalitats considerades no tan indispensables pel llançament del projecte.

11.3.1 Fase I

Aquesta fase inclourà la implantació i posada en marxa del projecte de manera ràpida (amb el mínim de desenvolupament extra possible) però esglaonada en diferents unitats/dependències, amb els següents ítems i funcionalitats.

- Lliurament de tot el hardware. El material restarà en dependències del licitador i s'anirà instal·lant de forma progressiva a les primeres unitats/dependències incloses en aquesta fase, veure 4. Descripció del hardware
- Lliurament del software de gestió i instal·lació, veure 5. Descripció del software de gestió.
- Lliurament de la documentació del projecte
- Formació a les unitats/dependències on es realitzarà la instal·lació i a la resta de grups generals, veure 8.1 Pla de Formació.
- Instal·lació, parametrització i posada en marxa del hardware a les dependències de GUB: Durant aquesta fase es realitzarà la implantació a dues dependències (torns de matí, tarda i nit) :

- Desenvolupament de la funcionalitat de gestió d'usuaris 6.2 Alta, modificació i baixa d'usuaris . Tant en el cas que la funcionalitat s'implementi en al mateix software de gestió o com a funcionalitat independent però vinculada al software de gestió, no requerirà integració amb el CtrlUser en aquesta fase.

- L'informe a enviar a la CCDCV es realitzarà manualment en paper i serà gestionat i controlat pel USTO fins a la implementació de la funcionalitat en fase II.

11.3.2 Fase II

Aquesta fase, que inclourà el desenvolupament de les noves funcionalitats i la integració amb els sistemes de l'IMI, que es durà a terme també de forma progressiva. Inclourà:

- Tot el hardware ha estat lliurat durant la fase I i per tant es disposar d'ell.

- Formació a les unitats/dependències pendents, veure 8.1 Pla de Formació.

- Implantació del hardware a les unitats/dependències pendents

- Desenvolupament de la funcionalitat de generació i enviament automàtic de l'informe a la CCDVC.

- Integració amb els sistemes d'autenticació/autorització de l'IMI i migració dels usuaris, grups, perfils i funcionalitats als nous sistemes.

11.4 Terminis d'execució i fites de facturació

La duració del contracte serà de 6 mesos distribuïts en les dues fases descrites anteriorment., El contracte es començarà a executar el dia següent a la seva formalització.

S'estableixen fites intermèdies d'obligat compliment per part del contractista, tal com s'assenyala a continuació.

Fase	item	Fita	Fi de la fita	Tasques associades	previsió final
Fase I	1	Disponibilitat i lliurament equipament 95% hardware demanat	4 setmanes des de l'inici de l'execució		nov 2021
	2	Instal·lació equipament/software i posta en marxa	6 setmanes des de l'inici de l'execució	• Instal·lació de l'aplicació del software de gestió al servidor de l'IMI • Instal·lació del hardware i gestió usuaris sense integrar amb Ctrluser a a dos dependències matí i nit	des 2021
	3	Lliurament documentació	Al llarg de la fase i d'acord a cada ítem		des 2021
	4	Formació	6 setmanes des de l'inici de l'execució	La formació es realitzarà en paral·lel a les tasques 2 de manera que hagi finalitzat en acabar aquesta fita	des 2021

	5	Disponibilitat i lliurament equipament del 5% del hardware demanat	12 setmanes des de l'inici de l'execució		gen 2022

Fase	item	Fita	Període màxim lliurament	Fites associades	
Fase II	6	Instal·lació equipament/software i posta en marxa	10 setmanes des de la finalització de la fase I	• Instal·lació del hardware i gestió usuaris sense integrar amb Ctrluser a la resta de dependències	març 2022
	7	Funcionalitat de "Gestió d'usuaris" integrada amb CtrlUser	6 setmanes des de la finalització de la fase I	• Integració amb l'IMI • Migració usuaris introduïts • En paral.lel amb la tasca 5	feb 2022
	8	Desenvolupament i implantació del soft per la creació i enviament automàtic de l'informe de CCDVC	10 setmanes des de la finalització de la fase I	• Migració dades dels informes	abril 2022
	9	Lliurament documentació	Al llarg de la fase i d'acord a cada item		
	10	Formació	12 setmanes des de la finalització de la fase I	La formació es realitzarà en paral·lel a les tasques 5 6 i 7	maig 2022

11.5 Facturació

La facturació es farà d'acord amb l'assoliment de les fites indicades en l'apartat anterior i de la forma següent:

ELEMENTS DE FACTURACIÓ	PERCENTATGE FACTURACIÓ
Realització fita 1	53%
Realització fites 2 a 4	7%
Realització fita 5	2%
Realització Fita 6	15%

Realització Fita 7 Funcionalitat de "Gestió d'usuaris" integrada amb CtrlUser	8%
Realització Fita 8 Desenvolupament i implantació del soft per la creació i enviament automàtic de l'informe de CCDVC	10%
Realització fites 9 i 10	5%

11.6 Garantia

Les condicions de prestació del servei poden consultar-se a 8.2 Pla de Suport i garantia. El contracte inclou obligatòriament una garantia associada al subministraments i instal·lacions realitzades així com del software de gestió.

- Es realitzarà una recepció parcial que inclou totes les fites de la fase 1. Aquest termini parcial obligatori s'ha d'acomplir en un màxim de 12 setmanes des de la formalització del contracte (final fase 1) essent l'incompliment susceptible de penalització. En aquesta recepció parcial també es farà l'acta de comprovació material d'aquesta part del contracte. La data d'aquesta recepció parcial marca l'inici del còmput de la garantia del hard del contracte.
- Es realitzarà una recepció total del contracte al final de les fites de la fase 2. La data d'aquesta recepció total, com a màxim, 12 setmanes des de la finalització de la fase I, marca l'inici del còmput de la garantia del sof del contracte.

La garantia no estarà subjecte a la contractació de cap servei addicional durant el període de duració de la mateixa.

11.6.1 Hardware

El període de garantia tècnica dels aparells i de la seva instal·lació serà com a mínim de 2 anys. Durant aquest període l'adjudicatari es compromet a resoldre satisfactòriament totes aquelles avaries emparades per la garantia, és a dir, produïdes per defectes de fabricació.

El servei de garantia inclourà:

- Gestió de la garantia i reparació dels dispositius: interlocució amb personal autoritzat de l'Ajuntament de Barcelona o Guàrdia Urbana, i la necessària interlocució amb el fabricant.
- Utilització dels sistemes de notificació/gestió d'incidències propis de la Gerència de Seguretat i Mobilitat i l'IMI. Veure 8.2 Pla de Suport i garantia.
- Recollida del material espatllat a la unitat corresponent i lliurament un cop reparat.
- El temps de reparació màxim serà de 10 dies laborables.
- Sistema de suport remot per la gestió d'incidències i consultes. Sistema de reparacions in-situ per la resolució d'averies que no es puguin resoldre per la via anterior.
- Reparació i substitució d'aquells equips en els que es detecti error de hardware per deficiències de l'equip i no atribuïbles a mal ús, sense cost addicional.
- L'Ajuntament de Barcelona junt amb la GUB destinarà un número de DPG per la substitució d'equips e cas d'averia. Es valoraran les propostes dels licitadors que proporcionin dispositius addicionals per aquest servei , veure "Informe Justificatiu".
- Substitució ràpida i posta en marxa dels equips que precisin reparació.
- L'embalatge, recollida, transport i lliurament dels materials tras la seva reparació, i la mà d'obra i despeses necessàries per efectuar la reposició i/o instal·lació, estaran inclosos sense cost addicional.

11.6.2 Software

La garantia del software de gestió inclourà el subministrament de *parches* i/o les versions de manteniment de software que publiqui el fabricant durant el període de garantia.

Tant el software de gestió com les noves funcionalitats desenvolupades disposaran d'un període mínim de sis mesos de garantia comptadors des de la finalització del projecte. Durant aquest període l'adjudicatari estarà obligat a resoldre les anomalies detectades que li siguin imputables.

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

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

La resolució d'incidències relacionades amb la garantia es farà segons els següents nivells de servei.

Resolució d'incidències	Temps de resposta	Temps de diagnòstic	Temps de resolució	Perfil mínim de suport assignat
Incidència crítica	1 hora	4 hores	8 hores	Consultor / Analista Sènior i Analista Programador
Incidència greu	2 hores	8 hores	22 hores	Consultor / Analista Sènior i Analista Programador
Incidència normal	4 hores	16 hores	40 hores	Consultor / Analista Sènior i Analista Programador

Tipus d'incidències:

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

Franges de temps:

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

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

L'adjudicatari facilitarà informes en relació al nombre d'incidències, descripció i temps de resolució requerits per l'equip de gestió de projectes. El detall dels informes i format es determinarà durant el projecte.

11.6.3 Suport després del període de garantia

El licitador haurà de garantir la disponibilitat d'un servei comercial de suport que permeti, com a mínim, la reparació per a tots els sistemes i equips adquirits i l'accés a recanvis compatibles durant un període mínim de 5 anys, a partir de la data de de recepció parcial indicada en el punt 11.6 d'aquest document.

Al finalitzar el període de garantia, hauran d'oferir-se els següents serveis i compromisos:

- Elaboració i transmissió per part de l'adjudicatari a la Gerència de Seguretat i Prevenció i l'IMI, dels procediments generals de manteniment preventiu i correctiu dels equips.
- Compromís de l'adjudicatari a facilitar la informació sobre les revisions i millores futures en components del sistema subministrat.
- Compromís del fabricant a garantir la no obsolescència de la tecnologia seleccionada, emetent un certificat que garanteixi la disponibilitat del producte durant al menys 5 anys des del moment de la seva posta en marxa. Durant aquest període, hauran d'estar disponibles els components, mòduls i equips seleccionats, o en el seu defecte, components compatibles amb iguals o millors característiques, sense modificar els ja instal·lats.

11.7 Qualitat del servei i treballs realitzats

Correspon a l'adjudicatari establir les mesures que consideri adients per lliurar les tasques del contracte amb els nivells mínims de qualitat que li són exigits.

En aquest sentit, l'Ajuntament de Barcelona / IMI exigirà l'acompliment dels següents nivells de servei:

11.7.1 Auditories

L'IMI en funció del desenvolupament del contracte pot exigir la realització, sense càrrec, d'auditories sobre el conjunt del seu treball des del vesant de qualitat.

L'auditoria ha de servir per millorar la qualitat del servei entesa com la millora del procediment del manteniment d'aplicacions.

L'auditoria en cas que s'exigeixi ha de complir els següents requisits:

- Periodicitat: semestral
- Abast: totalitat del software
- Serveis a auditar: nous desenvolupaments, resolució d'incidències i documentació
- Equip: Empresa externa i independent.
- Resultat: informe d'auditoria.

L'objectiu de les Auditories i Revisions de Qualitat dels Serveis Contractats és proporcionar visibilitat i control a la Direcció de l'IMI, sobre el grau de compliment dels adjudicataris amb els aspectes formals del servei.

L'adjudicatari cooperarà en l'auditoria, responent immediatament a les informacions demanades i auxiliant els auditors en el que considerin necessari.

Tota informació addicional o canvis de conducció d'un procés o com a resultat d'auditoria, serà considerada informació confidencial, segons els termes i condicions del Contracte.

La realització de l'auditoria en cap moment no eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis d'acord amb els termes inclosos en aquest Plec.

Els costos dels mitjans emprats per l'adjudicatari associats a les auditories no podran ser repercutits en cap cas a l'Ajuntament de Barcelona.

A la finalització de l'auditoria les parts revisaran les desviacions i / o observacions detectades respecte a l'acord en el contracte. L'adjudicatari haurà d'establir un pla d'acció amb:

- Accions per assegurar que les desviacions i / o observacions detectades es corregeixin.
- Identificació de responsables i dates límit per l'execució de les accions.

L'adjudicatari haurà de presentar a l'IMI el pla d'acció en el termini d'un mes des de la comunicació dels resultats finals de l'auditoria. Serà responsabilitat de l'adjudicatari la realització de les accions en els terminis establertes en el pla d'acció.

12 REVISIÓ PRÈVIA DE LES CARACTERÍSTIQUES OFERTADES DELS PRODUCTES

Amb caràcter previ a l'adjudicació del contracte, l'Ajuntament de Barcelona podrà, si així ho considera el responsable del contracte per part de l'Ajuntament, requerir a l'empresa adjudicatària a lliurar, en un termini no superior a 2 dies hàbils des del requeriment, un "sistema mostra" del model de hardware-software ofertat. Aquesta unitat s'haurà de lliurar a la Plaça de Carles Pi i Sunyer núm 8-10, 4ª planta, 08002 de Barcelona, de 08 a 17 hores.

El "sistema mostra" haurà d'incloure com a mínim un DPG, un carregador i/o base per la càrrega de bateria i descàrrega dels enregistraments, un PC com a servidor amb el software de gestió instal·lat, una estructura jeràrquica d'usuaris creada i els manuals d'ús corresponents. Un cop verificades les característiques del sistema (tant les funcionalitats de hardware com de software, sense incloure les funcionalitats sol·licitades a l'apartat 6. Altres funcionalitats d'aquest plec) i la seva plena adequació a l'oferta presentada, li serà retornat al seu propietari. És possible que es requereixi la presència d'una persona de l'equip de l'adjudicatari per tal de resoldre alguns dubtes que puguin aparèixer durant la comprovació. La superació de les proves tècniques (si es demanen) serà imprescindible per a l'adjudicació del contracte.

En cas que el producte ofert no s'ajusti a les característiques tècniques exigides en el present plec, l'empresa quedarà exclosa d'aquest procediment per no complir els requeriments tècnics del contracte i es procedirà a requerir el sistema mostra al següent licitador segons l'ordre en què hagin quedat classificades les ofertes.

13 CONDICIONS GENERALS D'EXECUCIÓ

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

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

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

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

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

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

13.2 Clàusula de propietat intel·lectual

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

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió de la mateixa.

L'empresa contractada accepta expressament que els drets d'explotació dels productes derivats d'aquest plec, que no corresponguin a un software comercial o propietari de tercers, corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, transformació o modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

13.3 Confidencialitat

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

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

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou als components tecnològics i mesures de seguretat tècniques que s'hi implantin.

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

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

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

13.4 Responsable de seguretat

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

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

13.5 Clàusula programari i metodologia de desenvolupament

L'adjudicatari, disposarà del programari necessari i farà servir la metodologia implantada per l'IMI per al desenvolupament dels serveis contractats.

En el cas del software de gestió o dels desenvolupats realitzats sobre ell, no es requerirà el seguiment d'aquesta metodologia ni la clàusula e programari però si el compliment dels aspectes indicats en aquest plec.

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

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

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

- No reproduir-los.
- No transmetre'ls a un altre sistema.

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

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

13.6 Clàusula de comunicacions externes

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

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

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

13.7 Clàusula de seguretat dels equips, programes i informació

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

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

13.8 Clàusula de personal extern

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

L'empresa contractada està obligada a implantar els mecanismes i controls necessaris per a garantir la confidencialitat, privacitat, integritat i continuïtat de la informació de l'Administració Municipal, i de donar-los a conèixer al seu personal.

El Cap responsable de contracte de l'empresa contractada, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte, formar al seu personal en la política i instruccions de l'Administració Municipal que els sigui d'aplicació, i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal. L'empresa contractada haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

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

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

13.9 Gestió d'incidents

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

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

L'adjudicatari establirà els mecanismes adients per que, en cas d'incident de seguretat i si es considera necessari, el personal de l'IMI-Seguretat pugui accedir a les instal·lacions del proveïdor de forma immediata.

13.10 Anàlisis forenses

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

13.11 Gestió d'excepcions

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

13.12 Xifratge de dades

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

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

13.13 Clàusula Electronic Watch

El Cap responsable de contracte de l'empresa contractada haurà de complir els drets laborals i normes de seguretat en les cadenes de producció de la fàbriques on es produeixen els productes específics o els components produïts.

L'Ajuntament de Barcelona, en data 10 de febrer de 2016, es va adherir al projecte Electronics Watch als efectes de garantir el compliment dels drets laborals i les normes de seguretat dels treballadors de les fàbriques on es produeixen els béns, productes específics o components adquirits de tipus electrònic. Amb aquest objectiu, l'Ajuntament de Barcelona demana al contractista que dugui a terme la diligència deguda perquè, en les fàbriques esmentades, es complexi el Codi de Normes Laborals elaborat per Electronics Watch (Annex I del plec de clàusules administratives particulars).

Dur a terme la diligència deguda per tal que a les fàbriques de producció de béns electrònics es compleixi l'establert al Codi de Normes Laborals elaborat per Electronics Watch, de manera que s'aconsegueixin els béns esmentats per mitjà de condicions de comercialització justa.

Lliurar al responsable del contracte, en el termini de 10 dies després de la formalització del mateix, el Pla del Compliment del Contractista (Annex II del plec de clàusules administratives particulars). Si s'escau, cada 3 mesos el contractista ha d'entregar un informe detallat sobre la seva implementació i ha de lliurar el Pla actualitzat. Aquet Pla ha de prendre en consideració quines pràctiques dels seus proveïdors poden contribuir o provocar l'incompliment del Codi de Normes Laborals en la producció dels béns electrònics i ha d'informar sobre com el contractista exercirà la seva influència per gestionar aquestes pràctiques.

Lliurar al responsable del contracte, en el termini de 10 dies després de la formalització del contracte, el Formulari de divulgació (Annex III del plec de clàusules administratives particulars). Si s'escau, cada 6 mesos el contractista ha de confirmar si s'han dut a terme informes d'auditoria industrial de qualsevol de les fàbriques on es produeixin els béns electrònics.

Exercir tota la influència possible per aconseguir que l'equip de monitoratge independent d'Electronics Watch pugui accedir a les fàbriques de producció dels béns electrònics per mitjà de visites no anunciades als llocs de treball que incloguin: visites a totes les plantes de treball, residències i hostals pertinents; entrevistes amb els/les treballadors/res sense la presència de supervisors/ores o gerents; i anàlisi de registres importants de la fàbrica (convenis de condicions col·lectives, registres de personal, registres d'hores de feina i sous, etc.). En ocasions, aquestes visites es podran dur a terme després d'haver enviat una notificació a la fàbrica de producció dels béns electrònics tot informant que es realitzarà durant un període específic de quatre setmanes.

Aquest plec de prescripcions tècniques ha estat emès, en data 3 de maig de 2021, pel Sr. Josep Clotet Ciruelo, tècnic responsable del contracte i adscrit a la Direcció d'Estratègia i Nous Projectes de l'IMI i amb el vistiplau de

Joana Serra Bosch

Directora d'Estratègia i Nous Projectes